HAS
HAUTE AUTORITÉ DE SANTÉ

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

RECOMMANDER
LES BONNES PRATIQUES

GUIDE

IA en contexte de soins : accompagner le bon usage

À destination des professionnels et des organisations de santé

Adopté par le Collège le 18 novembre 2026

Descriptif de la publication

Titre	IA en contexte de soins : accompagner le bon usage
Méthode de travail	La méthode de travail inclut : – des auditions ciblées de parties prenantes ; – l'analyse du cadre légal et réglementaire ; – l'analyse de la littérature scientifique ; – un groupe de travail ; – une consultation publique.
Objectif(s)	Ce guide a pour objectif d'accompagner les établissements et les professionnels dans le bon usage des systèmes d'intelligence artificielle utilisés en contexte de soins.
Cibles concernées	Professionnels et organisations de santé
Demandeur	Autosaisine
Promoteurs	Haute Autorité de santé (HAS) Commission nationale de l'informatique et des libertés (CNIL)
Équipes projets	HAS : la mission Numérique en santé et le service Juridique CNIL : le service de la Santé et le service de l'Intelligence artificielle
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 18 novembre 2026

Ce document ainsi que sa référence bibliographique sont téléchargeables sur www.has-sante.fr et sur www.cnil.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
© Haute Autorité de santé – novembre 2026

Commission Nationale de l'Informatique et des Libertés – Service communication
3 place de Fontenoy – 75007 PARIS. Tél. : +33 (0)1 53 73 22 22
© Commission Nationale de l'Informatique et des Libertés – novembre 2026

ISBN : 978-2-11-186355-2

Sommaire

Acronymes 7

Introduction 8

Contexte 8

Définitions et concepts clés 10

Présentation du guide 13

1. Organisation interne et gouvernance 15

Obligations principales 15

Principes prioritaires 15

1.1. Cadre légal et réglementaire 15

1.2. Principes 16

1.2.1. Actions portées par la direction générale 16

1.2.2. Le fonctionnement de la gouvernance dédiée à l'IA 17

1.2.3. Les actions portées par la gouvernance dédiée à l'IA 18

2. Acquisition et contractualisation 21

Obligations principales 22

Principes prioritaires 22

2.1. Cadre légal et réglementaire 22

2.1.1. Le RIA 22

2.1.2. Le RGPD 23

2.1.3. Le CSP 23

2.1.4. Le RDM et le RDIV 23

2.1.5. Actions à réaliser systématiquement 24

2.2. Principes 24

2.2.1. Prérequis à l'acquisition d'un SIA 24

2.2.2. Clauses contractuelles spécifiques 28

3. Sensibilisation, formation et habilitation 31

Obligations principales 31

Principes prioritaires 31

3.1. Cadre légal et réglementaire 31

3.1.1. Pour tous les SIA 32

3.1.2. Pour les SIA avec traitement de données personnelles 32

3.1.3. Pour les SIA à haut risque 32

3.1.4. Actions à réaliser systématiquement 32

3.2. Principes 33

4. Information des usagers 36
Obligations principales 36
Principes prioritaires 37
4.1. Cadre légal et réglementaire 37
4.1.1. Le RIA 37
4.1.2. Le RGPD 37
4.1.3. Le CSP 38
4.2. Principes 38

5. Consentement et droits des usagers 42
Obligations principales 42
Principes prioritaires 43
5.1. Cadre légal et réglementaire 43
5.1.1. Sur le consentement 43
5.1.1.1. Le RIA 43
5.1.1.2. Le RGPD 43
5.1.1.3. Le CSP 44
5.1.1.4. La protection juridique particulière de l'image et de la voix 44
5.1.2. Sur les droits des personnes : usagers et professionnels 44
5.1.2.1. Le RIA 44
5.1.2.2. Le RGPD 45
5.1.2.3. Le CSP 45
5.2. Principes 45

6. Organisation des soins 47
Obligations principales 47
Principes prioritaires 47
6.1. Cadre légal et réglementaire 48
6.2. Principes 49

7. Au cours de l'utilisation 52
Obligations principales 52
Principes prioritaires 52
7.1. Cadre légal et réglementaire 52
7.1.1. Pour tous les SIA 52
7.1.2. Pour les SIA à haut risque 53
7.2. Principes 53

8. Supervision humaine 56
Obligations principales 56
Principes prioritaires 57
8.1. Cadre légal et réglementaire 57
8.1.1. Les exigences de contrôle humain prévues par le RIA 57
8.1.2. La protection contre les décisions automatisées prévue par le RGPD 57
8.1.3. Les dispositions prévues par le CSP 58
8.1.4. Déclinaison du contrôle humain et de la protection contre les décisions automatisées dans le cadre du soin 58
8.1.5. Actions à réaliser systématiquement 58
8.2. Principes 59
8.2.1. Garantir la traçabilité 59
8.2.2. Déterminer et mettre en œuvre la supervision humaine adéquate 60

9. Traçabilité des usages et des résultats 62
Obligations principales 62
Principes prioritaires 62
9.1. Cadre légal et réglementaire 63
9.1.1. Pour tous les SIA 63
9.1.2. Pour les SIA à haut risque 63
9.1.3. Pour les SIA à risque limité 63
9.1.4. Conservation des données d'entrée et des résultats d'un SIA 64
9.2. Principes 64

10. Gestion de la qualité et vigilances 66
Obligations principales 66
Principes prioritaires 66
10.1. Cadre légal et réglementaire 66
10.1.1. Gestion de la qualité 66
10.1.2. Vigilances 67
10.1.2.1. Pour tous les SIA : 67
10.1.2.2. Pour les SIA ayant le statut de DM ou DMDIV : 67
10.1.2.3. Pour les SIA à haut risque : 68
10.1.3. Conformité et mesures correctives 68
10.1.4. Conformité et mesures de sécurité des données à caractère personnel 69
10.2. Principes 69

11. Fin du cycle de vie **73**
Obligations principales 73
Principes prioritaires 73
11.1. Cadre légal et réglementaire 73
11.1.1. Le RIA 73
11.1.2. Le RGPD 73
11.1.3. Le CSP 74
11.2. Principes 74
Table des annexes **76**
Références **95**
Participants **97**
Remerciements **98**

Acronymes

Acronyme	Sens		Acronyme	Sens
AIDF	Analyse d'impact sur les droits fondamentaux		**ANSM**	Agence nationale de sécurité du médicament et des produits de santé
ARS	Agence régionale de santé		**CH**	Centre hospitalier
CHU	Centre hospitalier universitaire		**CNIL**	Commission nationale de l'informatique et des libertés
CNP	Conseils nationaux professionnels		**CPTS**	Communauté professionnelle territoriale de santé
CSP	Code de la santé publique		**CSS**	Code de la sécurité sociale
DM	Dispositif médical		**DMDIV**	Dispositif médical de diagnostic in vitro
DPO	Délégué à la protection des données		**ESPIC**	Établissement de santé privé d'intérêt collectif
FALC	Facile à lire et à comprendre		**GHT**	Groupement hospitalier de territoire
GRADeS	Groupement régional d'appui à la e-santé		**HAS**	Haute Autorité de santé
HDS	Hébergeur de données de santé		**IA**	Intelligence artificielle
MOOC	« *Massive open online course* » ou cours en ligne ouverts à tous		**ONIAM**	Office National d'Indemnisation des Accidents Médicaux, des Affections Iatrogènes et des Infections Nosocomiales
PCA	Plan de continuité d'activité		**PME**	Petites et moyennes entreprises
PRA	Plan de reprise d'activité		**RDIV**	Règlement européen relatif aux dispositifs médicaux de diagnostic in vitro
RDM	Règlement européen relatif aux dispositifs médicaux		**RGPD**	Règlement général sur la protection des données
RIA	Règlement européen sur l'intelligence artificielle		**RSE**	Responsabilité sociétale des entreprises
RSSI	Responsable de la sécurité des systèmes d'information		**SIA**	Système d'intelligence artificielle
SLA	« *Service Level Agreement* » ou contrat de niveau de service		**UE**	Union Européenne
URPS	Union régionale des professionnels de santé			

Introduction

Contexte

L'intelligence artificielle (IA) s'intègre progressivement et concrètement dans les organisations de santé. Une enquête de 2025 met en évidence que 65 % des 110 établissements de santé publics interrogés utilisent déjà des systèmes d'intelligence artificielle (SIA) en production (1).

Cette dynamique de déploiement s'accompagne d'un décalage entre la diffusion des usages et leur encadrement par les organisations de santé. En effet, dans une autre enquête, 32 % des agents hospitaliers interrogés déclarent utiliser des outils personnels d'IA et 45 % d'entre eux estiment que leur établissement ne dispose pas encore d'outil institutionnel dédié (2).

L'introduction de l'IA dans les organisations de santé conduit à réinterroger certaines pratiques et certains fondements organisationnels. Les organisations de santé qui déploient ou utilisent un SIA sont notamment confrontées à deux types d'enjeux :

- déployer les SIA dans des conditions qui permettent de répondre aux besoins du système de santé et des usagers, et garantissent la qualité et de la sécurité des soins ;
- respecter les obligations légales et réglementaires qui leur incombent.

Un enjeu d'amélioration de la qualité et de la sécurité des soins

Les SIA utilisés en santé doivent être mis au service de l'humain, répondre à des besoins réels des patients, des professionnels et des organisations de santé. Ils ne constituent pas une fin en soi : leur utilisation doit être appréciée au regard de leur valeur ajoutée et de leur juste place dans les parcours de soins. Dans cet objectif, la HAS mène depuis 2022 des travaux visant à construire un cadre de confiance pour l'usage des SIA en santé. Cette stratégie repose sur des principes harmonisés et adaptables destinés à accompagner un déploiement sûr, responsable et pertinent.

Cette exigence implique également de prendre en compte les effets de ces technologies sur les relations entre les personnes et les professionnels, sur les risques d'exclusion liés au numérique, ainsi que sur les impacts économiques et environnementaux des solutions déployées (3). Sur le plan environnemental, le développement et l'utilisation des SIA mobilisent des ressources énergétiques, matérielles et hydriques significatives. Les effets associés sur l'environnement doivent être pris en considération dans le déploiement des SIA et tout au long du cycle de vie.

Afin de répondre à l'ensemble de ces enjeux, la Haute Autorité de santé (HAS) et la Commission nationale de l'informatique et des libertés (CNIL) ont signé une convention de partenariat en mars 2026. Elle vise à renforcer les bonnes pratiques, notamment en matière de protection des données personnelles et de promotion des droits fondamentaux liés aux outils numériques dans le secteur sanitaire, social et médico-social. Ce partenariat vise aussi, lorsque cela est pertinent, à fournir aux professionnels et établissements de santé une position commune des deux institutions, afin de faciliter l'appropriation des travaux dans la pratique.

Ce guide est réalisé dans le cadre de la convention de partenariat entre la HAS et la CNIL.

Le détail des stratégies respectives de la HAS et de la CNIL sur l'IA est disponible en Annexe 1.

La HAS et la CNIL ont produit des travaux complémentaires pour accompagner les usages des SIA, détaillés en Annexe 2.

Un corpus réglementaire préexistant

Le cadre légal et réglementaire autour de l'usage de l'IA se met en place tant au niveau français qu'européen, avec notamment le règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'IA (RIA ou « *IA Act* »). Son application n'est pas limitée au secteur de la santé mais concerne l'ensemble des domaines d'activité recourant à des SIA.

Le RIA vient compléter le cadre juridique préexistant et applicable en protection des données de santé et en santé.

Une mise au point sur le RIA est disponible en Annexe 3.

Lorsque l'utilisation d'un SIA implique un traitement des 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 également applicable. Ainsi, le déployeur d'un SIA, en tant que responsable de traitement au sens du RGPD, 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 et a fortiori, lorsqu'il s'agit des données de santé d'un patient. Un focus sur le traitement de données au sens du RGPD est disponible en Annexe 4.

L'utilisation d'un SIA en contexte de soins doit respecter le code de la santé publique (CSP), notamment en matière d'exercice d'une profession de santé et de droits des usagers. À ce jour, l'utilisation d'un SIA par un professionnel de santé n'est pas soumise à un régime de responsabilité spécifique (4).

Un professionnel de santé reste entièrement responsable d'un acte, même lorsque celui-ci est accompli avec l'assistance d'un SIA.

Lorsqu'un SIA répond à la définition d'un dispositif médical (DM) ou d'un dispositif médical de diagnostic in vitro (DMDIV), il est soumis aux obligations du règlement (UE) 2017/745 (RDM) relatifs aux DM ou du règlement (UE) 2017/746 (RDIV) relatifs aux DMDIV, selon le cas, au même titre que les autres DM et DMDIV.

Le cadre légal et réglementaire applicable aux SIA repose donc sur un corpus de textes préexistants, dont l'appropriation peut représenter un défi pour les organisations de santé et les utilisateurs.

D’autres textes peuvent être applicables à l’utilisation de SIA dans un contexte de soins, afin de garantir notamment :

- la sécurité informatique de l’organisation de santé déployant un SIA (directive (UE) 2022/2555 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité) ou du SIA lui-même (règlement (UE) 2025/327 relatif à l’espace européen des données de santé, règlement (UE) 2024/2847 fixant des exigences de cybersécurité pour les produits comportant des éléments électroniques) ;
- un accès et un partage équitable des données générées par les produits connectés et services numériques (règlement (UE) 2023/2854 relatif aux règles harmonisées portant sur l'équité de l’accès aux données et de l’utilisation des données).

Ces textes ne sont pas abordés dans ce guide.

Définitions et concepts clés

Un glossaire du vocabulaire spécifique utilisé dans ce guide est disponible en Annexe 5.

Les SIA et leurs niveaux de risque

Les SIA sont des outils informatiques conçus pour fonctionner avec un niveau d’autonomie variable. Utilisés dans un contexte de soins, les SIA sont capables de déduire et de générer des résultats tels que des prédictions diagnostiques, des recommandations thérapeutiques, des scores de risque ou encore des aides à la décision, à partir de données d’entrée (cliniques, physiologiques, administratives, etc.). Les résultats d’un SIA sont donc susceptibles d’influencer la prise en charge du patient ou l’organisation des soins. Un SIA est défini légalement (article 3.1 du RIA).

Le RIA classe les SIA selon leur niveau de risque. Il distingue les SIA à risque inacceptable, ceux à haut risque, ceux à risque limité et ceux à risque minimal (cf. Annexe 1).

Les **SIA à risque inacceptable** sont interdits (article 5 du RIA). Les autres catégories sont associées à des obligations spécifiques.

Les **SIA à haut risque** présentent un risque significatif pour la santé, la sécurité ou les droits fondamentaux des personnes, y compris en influençant sensiblement le résultat de la prise de décision. En contexte de soins, cette catégorie inclut notamment les dispositifs médicaux (DM ou DMDIV) intégrant de l’IA, ainsi que certains SIA explicitement identifiés par l’annexe III du RIA. Les SIA à haut risque sont soumis à des exigences réglementaires renforcées, visant à garantir leur sécurité, leur fiabilité et un contrôle humain approprié (article 6 du RIA). Ils font l’objet d’obligations spécifiques au titre du RIA synthétisées en Annexe 6.

Les **SIA à risque limité**, soumis au chapitre IV du RIA, pour lesquels le RIA impose des obligations de transparence vis à vis des utilisateurs en plus des dispositions générales du RIA (article 50 du RIA).

Les **SIA à risque minimal** sont soumis aux dispositions générales du RIA.

Les SIA utilisés en contexte de soins

En contexte de soins, les SIA recouvrent une grande diversité de situations et d'usages. Certains sont clairement identifiables, et d'autres s'intègrent de façon plus subtile à des DM, des DMDIV, ou des technologies numériques existantes, ces SIA sont dits « embarqués ».

Cette diversité s'explique notamment par plusieurs caractéristiques :

- leur statut réglementaire, selon qu'ils sont qualifiés de DM, de DMDIV ou non ;
- leur niveau de risque au sens du RIA ;
- leur finalité ou destination d'usage.

Certains SIA interviennent directement dans la prise en charge du patient, qu'il s'agisse d'activités de prévention, de dépistage, de diagnostic ou de soins. Ils peuvent par exemple être utilisés pour la détection de fractures osseuses aux urgences, la délimitation en radiothérapie, l'identification précoce de mélanomes ou de rétinopathies diabétiques. Les SIA ayant une finalité médicale ont le statut réglementaire de DM ou DMDIV et ont donc un marquage CE.

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

L'article 5.5 du RDM relatif aux DM et l'article 5.5 du RDIV relatif aux DMDIV 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 article 5.5 du RDIV). Dans tous les autres cas, un marquage CE est nécessaire avant usage clinique.

D'autres SIA contribuent à l'organisation et à la coordination des activités de soins, notamment à la gestion des flux de patients au bloc opératoire, la rédaction de comptes-rendus ou à la traduction.

Certains SIA sont utilisés en dehors des activités de soin, à l'appui d'activités qui ne relèvent ni de la prise en charge du patient ni de l'organisation des soins. Ils peuvent notamment soutenir les fonctions administratives, logistiques ou de gestion, telles que l'aide à l'élaboration des plannings ou au pré-remplissage de documents administratifs.

Les principaux acteurs du déploiement

Le déploiement d'un SIA implique plusieurs acteurs dont les rôles et les responsabilités sont définis par le RIA. La distinction entre ces acteurs est essentielle pour identifier les obligations applicables à chacun tout au long du cycle de vie du SIA.

Le **fournisseur** du SIA est l'acteur responsable de la conception et de la mise sur le marché du SIA. Le fournisseur est « *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* » (article 3.3 du RIA). Le fournisseur peut confier certaines activités à des prestataires. Cette délégation ne le décharge pas des obligations qui lui incombent en tant que fournisseur au regard du RIA.

Le **déployeur** du SIA est l'acteur responsable du déploiement et des utilisateurs du SIA. Selon le RIA Le déployeur est « *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* » (article 3.4 du RIA). Dans le secteur sanitaire, le déployeur peut notamment être un établissement de santé, un laboratoire de biologie médicale, un centre d'imagerie ou un professionnel de santé exerçant à titre libéral. Le déployeur peut confier certaines activités à des prestataires, notamment l'installation, l'intégration, l'hébergement, la maintenance, le support ou l'exploitation technique du SIA. Cette délégation ne le décharge pas des obligations qui lui incombent en tant que déployeur au regard du RIA.

Dans le présent guide, les termes « déployeur du SIA », issu du RIA, et « responsable de traitement », issu du RGPD, sont utilisés pour désigner le même organisme.

L'**utilisateur** du SIA est la personne physique qui l'utilise. Il l'utilise conformément aux instructions du fournisseur et aux règles définies par le déployeur. Il doit également disposer des connaissances, des compétences et des qualifications nécessaires à une utilisation appropriée.

Dans le cadre d'un exercice libéral, le déployeur et l'utilisateur sont souvent une seule et même personne.

Présentation du guide

Objectifs du guide

Ce guide vise à :

- clarifier les obligations légales et réglementaires des déployeurs et des utilisateurs de SIA. Ces obligations sont applicables quelle que soit la taille de l'organisation de santé (centre hospitalier universitaire (CHU), centre hospitalier (CH), établissement de santé privé d'intérêt collectif (ESPIC), clinique, centre de santé, structure d'exercice libéral, etc.) ;
- soutenir les professionnels de santé et les organisations de santé dans le déploiement des SIA en contexte de soins ;
- accompagner le bon usage des SIA, pour favoriser la qualité et la sécurité des soins ;
- accompagner les établissements de santé dans la certification des établissements de santé pour les critères liés aux SIA (5).

Une synthèse du guide est disponible en Annexe 7.

Méthode d'élaboration du guide

Ce guide s'appuie sur des entretiens ciblés de parties prenantes, l'analyse du cadre légal et réglementaire, l'analyse de la littérature scientifique, un groupe de travail d'experts et une consultation publique. Cette méthode est détaillée en Annexe 8.

Périmètre du guide

Ce guide s'adresse au **secteur sanitaire**, quel que soit le lieu d'exercice. De nombreux principes présentés ici peuvent néanmoins être pertinents pour le secteur médico-social ou le secteur social. Un travail adapté aux spécificités de ces secteurs devra être envisagé afin d'y accompagner le déploiement et le bon usage des SIA.

Ce guide s'adresse en priorité aux **déployeurs** et aux **utilisateurs** d'un SIA, c'est-à-dire aux organisations de santé et aux professionnels souhaitant déployer et utiliser un SIA en contexte de soins.

Ce guide peut être utile aux **usagers** du système de santé, en particulier les fiches concernant leur information (cf. Fiche 4) et leur consentement (cf. Fiche 5). Un document à destination des usagers « Intelligence artificielle en santé. Bien l'utiliser et bien se protéger » a été élaboré par la HAS, en collaboration avec la CNIL et France Assos Santé pour informer les personnes, patients ou non, sur l'IA (6). D'autres travaux à destination des usagers devront être envisagés afin d'accompagner leur compréhension et leur bon usage des SIA.

Ce guide s'applique à **l'ensemble des SIA utilisés en contexte de soins**, quel que soit le type de SIA, son statut réglementaire (DM, DMDIV ou non), son niveau de risque et sa finalité ou sa destination d'usage. Toutefois, en fonction de la classe de risque du SIA, les obligations du déployeur au titre du RIA seront différentes.

Le guide ne concerne pas les SIA utilisés dans le secteur sanitaire sans lien direct avec la prise en charge du patient ou les pratiques de soins (organisation du travail, facturation, etc.). Il ne sera pas traité des obligations des fournisseurs de SIA, qui sont du ressort des autorités compétentes.

Ce guide s'applique une fois que le déployeur a fait le choix d'utiliser un SIA. Il concerne le pré-déploiement (calibrage, contractualisation), l'utilisation et la maintenance ainsi que le post-déploiement (évaluation, fin du cycle de vie et désinstallation). Ce guide ne concerne pas la phase de développement du SIA, les essais en conditions réelles et les bacs à sable réglementaires.

Ce guide ne se substitue pas à l'ensemble des obligations auxquelles une organisation de santé doit se conformer. Il n'impose pas de nouvelles obligations. Il a vocation à accompagner le déploiement de SIA en contexte de soins dans une démarche d'amélioration de la qualité et de la sécurité.

Structuration du guide

Ce guide est structuré en onze fiches qui couvrent l'ensemble du cycle de vie d'un SIA.

Concernant la phase de pré-déploiement et plus spécifiquement l'acquisition du SIA, un guide spécifique sur l'aide aux choix des DM numériques à usage professionnel est disponible sur le site de la HAS. Les principes de ce dernier sont applicables au choix des SIA (7).

Chaque fiche est constituée :

- du cadre légal et réglementaire ;
- des obligations légales devant impérativement être mises en œuvre, et dont le non-respect peut entraîner des conséquences juridiques, administratives ou contentieuses ;
- des actions à réaliser systématiquement pour être en conformité juridique et proscrire les usages inappropriés et illégaux, dangereux, ou non conformes, et garantir le respect des exigences légales applicables ;
- des principes à mettre en œuvre par les déployeurs et aux utilisateurs pour garantir la qualité et la sécurité des soins ;
- certains de ces principes sont considérés comme prioritaires, le déployeur et l'utilisateur du SIA y portent une attention particulière. Ils sont indiqués par le pictogramme : ★★★

Ce guide a vocation à accompagner l'ensemble des déployeurs et des utilisateurs de SIA du secteur sanitaire et offre un cadre adaptable aux différents contextes d'exercice et à leurs différents niveaux de maturité. En effet, certaines organisations de santé disposent déjà d'une organisation structurée pour le déploiement des SIA, alors que d'autres sont encore en phase d'appropriation de ces systèmes. Les principes présentés dans ce guide peuvent être mobilisés par les déployeurs et les utilisateurs de SIA en les adaptant aux caractéristiques de leur organisation, à leurs usages et à leurs contraintes.

1. Organisation interne et gouvernance

La capacité d'une organisation ou d'un individu à comprendre et à gérer le processus de déploiement des SIA est indispensable pour assurer leur bon usage en contexte de soins. Le déploiement d'un SIA n'est possible qu'en mobilisant l'ensemble des parties prenantes, sous l'impulsion du responsable de l'organisation de santé.

Quel que soit le contexte d'exercice, chaque déployeur assume la responsabilité du déploiement du SIA. Il veille à la conformité et à la sécurité de l'utilisation des SIA en contexte de soins.

Synthèse

Obligations principales

Le déployeur :

- met en place une gouvernance adaptée ;
- effectue une AIDF, le cas échéant ;
- tient un registre des traitements ;
- réalise une AIPD, le cas échéant.

Principes prioritaires

- Mettre en place une gouvernance dédiée à l'IA
- Impliquer les représentants des usagers
- Cartographier les SIA

1.1. Cadre légal et réglementaire

Le respect du cadre juridique et réglementaire applicable aux SIA implique la mise en place d'une gouvernance adaptée afin de 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 (cf. Annexe 2).

La gouvernance d'un SIA ne constitue pas, en tant que telle, une obligation autonome prévue par le RIA. Elle résulte toutefois des différentes obligations mises à la charge des acteurs, en particulier du déployeur, lorsqu'il utilise un SIA à haut risque (article 26 du RIA).

Par ailleurs, certains déployeurs sont soumis à l'obligation d'effectuer une analyse d'impact sur les droits fondamentaux (AIDF) conformément à l'article 27 du RIA. Cette obligation concerne :

- les organismes de droit public ;
- les entités privées fournissant des services publics ;
- les déployeurs de SIA à haut risque.

Le responsable de traitement pour les traitements de données personnelles liées à l'utilisation d'un SIA est le déployeur.

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

- tenir un registre des traitements mis en œuvre (article 30 du RGPD).
- réaliser une analyse d'impact relative à la protection des données (AIPD) (article 35 du RGPD).

1.2. Principes

1.2.1. Actions portées par la direction générale

★★★ Mettre en place une gouvernance dédiée à l'IA

Chaque organisation de santé – publique, privée, libérale ou territoriale – met en place une gouvernance de l'IA claire et structurée afin d'assurer un déploiement maîtrisé et conforme des SIA. 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. Elle alloue les ressources nécessaires pour soutenir sa mise en œuvre et son suivi.

Cette gouvernance dédiée à l'IA doit être adaptée à la structure et à ses ressources.

Les établissements de santé de grande taille (CHU, ESPIC de référence, etc.) constituent un comité pluridisciplinaire dédié à l'IA, rattaché par exemple à la direction générale ou à une cellule innovation. Ce comité inclut par exemple des professionnels de santé, des juristes, des ingénieurs biomédicaux, des experts en système d'information hospitalier, le responsable en sécurité des systèmes d'information (RSSI), des représentants des usagers et, lorsque disponibles, un référent éthique et le délégué à la protection des données (DPO). Entre autres, ce comité définit la stratégie IA, évalue les projets, valide les situations d'utilisation, réalise le suivi de la performance des SIA et organise la transparence vis-à-vis des usagers, par exemple via la mise en place d'informations dans le portail d'accueil ou les comptes-rendus médicaux (cf. Fiche 4).

Les organisations de santé aux ressources limitées nomment un référent local des SIA (clinicien, cadre, qualiticien, etc.). Ce référent peut par exemple être chargé de centraliser les initiatives relatives à l'IA.

Adopter une démarche responsabilité sociétale des entreprises (RSE)

La direction générale de l'établissement de santé adopte une démarche RSE structurée et outillée, afin de maîtriser les risques éthiques, sociaux et environnementaux associés au déploiement des SIA. Dans le cadre de cette démarche, le déployeur sollicite les organisations syndicales et les représentants du personnel.

Sensibiliser les organes de direction aux enjeux spécifiques de l'IA

La direction générale de l'établissement de santé sensibilise les différentes directions aux enjeux posés par les SIA en contexte de soins (cf. Fiche 3). Cette sensibilisation porte sur :

- les obligations réglementaires (RGPD et RIA notamment) ;
- les bénéfices attendus ;
- les risques associés (biais, erreurs, dépendance excessive à l'outil, etc.).

1.2.2. Le fonctionnement de la gouvernance dédiée à l'IA

★★★ Impliquer les représentants des usagers

Les représentants des usagers sont représentés et impliqués au sein de la gouvernance dédiée à l'IA. Les représentants des usagers interviennent dès la définition des besoins et des objectifs, et tout au long du projet de déploiement d'un SIA afin d'intégrer leur expérience, leurs attentes et leur point de vue dans les décisions prises. Par exemple, une présentation annuelle du bilan de déploiement des SIA et des mesures envisagées à la Commission des Usagers est organisée.

Mutualiser les ressources et les réflexions en matière d'IA

Les groupements hospitaliers de territoire (GHT) ou groupes privés développent une réflexion commune en matière d'IA. Ils s'appuient sur des comités et des outils partagés afin d'harmoniser leurs pratiques, de mutualiser leurs ressources et leurs expertises et accompagner les établissements de santé les moins dotés.

Les GHT peuvent par exemple confier la mise en place de cette gouvernance dédiée à l'IA à un établissement support. Ils mobilisent les instances professionnelles ou institutionnelles locales, par exemple l'agence régionale de santé (ARS), le groupement régional d'appui au développement de la e-santé (GRADeS), l'union régionale des professionnels de santé (URPS), la communauté professionnelle territoriale de santé (CPTS), la conférence régionale de la santé et de l'autonomie, pour améliorer le déploiement des SIA à l'échelle territoriale et soutenir la diffusion des bonnes pratiques auprès de l'ensemble des acteurs, quels que soient leur contexte d'exercice ou leurs ressources.

S'appuyer sur les organismes régionaux et nationaux

Les organisations et les professionnels de santé s'appuient sur les organismes régionaux compétents, notamment les ARS, les GRADeS, les URPS et, plus largement au niveau national, sur les conseils nationaux professionnels (CNP), les sociétés savantes, les ordres professionnels et tout autre acteur pertinent, afin de disposer de référentiels, de grilles d'évaluation et de modèles d'information patient communs.

1.2.3. Les actions portées par la gouvernance dédiée à l'IA

★★★ Cartographier les SIA

> La réalisation d'une cartographie des SIA, incluant une analyse des risques, fait partie des éléments d'évaluation de la certification des établissements de santé, dans la version 2027 du référentiel de la HAS. Cette exigence est déclinée dans le critère 3.4-05 pour les DMN faisant appel à de l'IA et dans le critère 3.4-06 pour les SIA sans finalité médicale (5).

La gouvernance dédiée à l'IA cartographie l'ensemble des SIA déployés ou en projet de déploiement, quelle que soit leur classification. Ce recensement porte en priorité sur les SIA ayant un impact direct sur les soins et la prise en charge des patients. Cette cartographie peut être élargie aux autres SIA, comme ceux embarqués dans le matériel biomédical.

Elle peut être mutualisée avec celle du service informatique hospitalier et articulée avec la gouvernance des données et la documentation interne prévue par le RGPD (registre des traitements, AIPD). Cette cartographie est actualisée autant que de besoin et au minimum une fois par an.

Cette cartographie permet :

- d'identifier les SIA déployés au sein d'une organisation de santé, en tant que produit ou que SIA embarqué ;
- de réaliser une analyse des risques associés pour orienter les politiques d'utilisation, d'information des patients, de supervision humaine et de conformité ;
- de déterminer les obligations légales associées ;
- d'anticiper les modalités de continuité d'activité en cas d'indisponibilité du SIA selon son niveau de risque (cf. Fiche 10) ;
- d'informer les usagers du système de santé (cf. Fiche 4).

Pour chaque SIA, la cartographie peut inclure :

- 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 du RIA et plus largement pour l'organisation des soins et la prise en charge des patients ;
- son niveau de déploiement (pilote, usage courant, etc.) ;
- les services qui utilisent le SIA ;
- l'identité du référent local des SIA ;
- les catégories de données nécessaires au fonctionnement du SIA ; les populations de patients susceptibles d'être concernées et, si possible, une approximation de leur effectif (par exemple, sur un an) ;
- les modalités de suivi (indicateurs, incidents, traçabilité, retour d'expérience, etc.).

Mettre en place un guichet unique pour les SIA

La gouvernance dédiée à l'IA met en place un guichet unique à l'échelle de l'organisation de santé. Dans sa forme la plus simple, il peut consister en une adresse électronique unique, dédiée aux sollicitations des entreprises et aux demandes internes.

Il permet :

- de centraliser les propositions de déploiement de SIA à l'échelle d'une structure ;
- d'éclairer la sélection des projets et de les évaluer de façon coordonnée, par exemple via un comité dédié ;
- d'accompagner leur déploiement dans le respect des bonnes pratiques ;
- d'alimenter la cartographie de façon continue.

Garantir une validation par la gouvernance

La gouvernance dédiée à l'IA examine et valide chaque SIA avant son déploiement, via un comité pluridisciplinaire dédié à l'IA, ou le référent local des SIA. Ce comité ou ce référent définit les modalités de suivi du SIA au moyen d'indicateurs, de dispositifs de traçabilité et de revues régulières.

La gouvernance valide :

- un cahier des charges minimales auquel chaque SIA répond (cf. Fiche 2), précisant a minima :
  - la finalité du SIA,
  - la population cible,
  - la classification du SIA (notamment DM ou non),
  - les exigences minimales de sécurité ;
- le déploiement de chaque SIA sur la base d'analyses réalisées par les fonctions compétentes de l'organisation de santé (RSSI, DPO, référent qualité, responsable clinique ou technique concerné, etc.) ;
- la vérification de la couverture assurantielle afin de s'assurer que l'usage de SIA est bien couvert par le contrat avec l'assureur et informe les professionnels concernés.

Formaliser et adopter une charte d'utilisation des SIA

La gouvernance dédiée à l'IA formalise une charte d'utilisation aux SIA adoptée au niveau de l'organisation de santé afin de favoriser la diffusion des bonnes pratiques et de sensibiliser aux risques associés. Cela suppose d'identifier et de recenser les usages, notamment ceux non validés par l'organisation de santé.

Cette charte :

- porte sur l'utilisation des SIA validés par l'organisation de santé, ainsi que sur l'utilisation de ceux non validés par la gouvernance (« *shadow AI* ») ;
- porte sur les risques spécifiques associés aux usages des SIA génératifs ;
- définit les usages approuvés et ceux interdits, ainsi que les recommandations de bonne pratique associées.

Définir une politique unifiée d'information des usagers

L'organisation de santé doit respecter plusieurs obligations d'information issues de différents textes (cf. Fiche 4). Le traitement isolé de ces obligations peut entraîner des redondances, des oublis ou être source de confusion pour les usagers. La gouvernance dédiée à l'IA formalise une politique d'information comprenant :

- une cartographie des différentes obligations applicables à la structure en les associant aux étapes clés du parcours patient ;
- la définition d'un niveau pertinent d'information à diffuser ;
- les modalités d'information des personnes concernant la réutilisation de leurs données, notamment à des fins de développement ou d'amélioration des SIA utilisés.

Définir une politique de formation aux SIA

L'usage responsable des SIA en contexte de soins repose sur la compétence et la sensibilisation des professionnels qui les utilisent. Une formation adaptée est essentielle pour garantir une utilisation qui maximise les bénéfices de ces outils, tout en minimisant les risques pour les patients et les organisations (cf. Fiche 5). Le déployeur définit une politique de formation à destination de l'ensemble des professionnels susceptibles d'utiliser un SIA. La formation concerne les professionnels de santé mais aussi les personnels administratifs, techniques, ou tout autre profil amené à interagir avec ces systèmes dans le cadre de ses missions. La formation porte à la fois sur les principes de fonctionnement du SIA, ses limites et ses risques, ainsi que sur les bonnes pratiques permettant un usage sûr et conforme.

Définir des procédures en cas d'incidents ou de dysfonctionnements

Les incidents ou dysfonctionnements des SIA, qu'ils soient techniques, algorithmiques ou liés à une mauvaise utilisation, peuvent entraîner des conséquences directes sur la qualité des soins, la sécurité des patients ou la conformité réglementaire. Une anticipation de ces situations via des procédures formalisées est donc essentielle pour répondre à ces exigences légales, tout en garantissant la sécurité du patient et des pratiques. Le déployeur définit des procédures permettant de traiter les incidents ou dysfonctionnements liés à l'usage d'un SIA, incluant leur détection, leur signalement, leur analyse et la mise en œuvre des mesures correctives (cf. Fiche 10).

Désigner un référent local dédié aux SIA

Le déployeur désigne un référent local dédié aux SIA. Pour les établissements de grande taille (CHU, ESPIC de référence, etc.), un référent local peut être désigné à l'échelle de chaque service. Dans les organisations de santé aux moyens plus limités, ce référent peut être désigné à l'échelle de l'organisation. Il peut s'agir, par exemple, du référent informatique.

Le référent local dédié aux SIA est chargé :

- de leur suivi fonctionnel ;
- de réaliser l'interface avec les utilisateurs, le fournisseur et la gouvernance (cf. Fiche 1) ;
- de l'accompagnement des équipes à l'utilisation et à la formation (cf. Fiche 3) ;
- de favoriser le respect du cadre légal et réglementaire ;
- de favoriser l'utilisation conforme (cf. Fiche 6) ;
- de tracer les erreurs et événements indésirables (cf. Fiche 9).

2. Acquisition et contractualisation

La contractualisation entre le déployeur et le fournisseur permet de :

- vérifier la conformité légale et réglementaire du SIA ;
- formaliser et clarifier plusieurs éléments essentiels, tels que la répartition des responsabilités, la transparence des performances et le traitement des données personnelles, etc. ;
- répartir clairement les obligations liées à la gestion de la qualité et des risques entre le fournisseur, le déployeur et, le cas échéant, les utilisateurs du SIA.

Les principes développés ici ont vocation à :

- faciliter l'identification des éléments à prendre en compte lors de la contractualisation sans se substituer aux règles de concurrence et de commande publique ainsi qu'aux procédures d'achat applicables ;
- permettre au déployeur de satisfaire à ses obligations, notamment en matière de protection des données personnelles dans le cadre de l'utilisation d'un SIA.

Ces principes s'appliquent aussi bien à l'achat de nouveaux SIA qu'aux SIA embarqués dans des équipements ou logiciels déjà déployés, par exemple aux échographes avec un module d'IA.

La contractualisation permet de clarifier la répartition des responsabilités.

Le contrat :

- précise les obligations et les modalités de coopération du fournisseur en cas d'incident ou de violation de données (accès aux journaux techniques, transparence technique) ;
- encadre les conditions d'utilisation du SIA. Lorsque celui-ci est utilisé en dehors de sa destination ou des conditions générales d'utilisation, la responsabilité du fournisseur ne peut pas être engagée ;
- prévoit les modalités de signalement au fournisseur des usages inadaptés identifiés au sein de l'organisation de santé.

Le contrat ne déroge pas aux règles applicables en matière de délégation d'une activité médicale (cf. Fiche 5), de secret professionnel et d'exercice des professions de santé (cf. Fiche7).

Les étapes de contractualisation doivent être mutualisées autant que possible en s'appuyant sur les procédures et outils existants, afin de limiter les risques et d'optimiser les ressources.

Dans cette logique, les centrales d'achats peuvent jouer un rôle facilitateur, par exemple en mettant à disposition des modèles de contrats (clausiers de sécurité) ou des cahiers des charges spécifiques pour les SIA. Ces réflexions peuvent également être portées à l'échelle territoriale dans le cadre de coopérations entres les structures, notamment au sein des GHT, afin d'harmoniser les pratiques et de faciliter l'accès à des outils contractuels de qualité pour l'ensemble des organisations de santé du territoire.

Synthèse

Obligations principales

Le déployeur :

- dispose des informations pertinentes pour réaliser l'AIPD et l'AIDF lorsqu'elles sont requises ;
- conclue un contrat avec chaque sous-traitant intervenant dans le traitement de données personnelles et en tenant compte des dispositions spécifiquement applicables à la prestation concernée ;
- vérifie que le traitement des données personnelles lié à l'utilisation du SIA est conforme au RGPD ;
- conclue un contrat conforme aux articles du CSP concernant l'hébergement des données de santé lorsque l'utilisation du SIA implique la conservation des données par un tiers ;
- vérifie que le marquage CE est apposé sur le produit conformément aux différentes réglementations européennes en vigueur, notamment celles applicables aux DM et DMDIV.

Principes prioritaires

- Établir un cahier des charges
- Vérifier la conformité réglementaire du SIA

2.1. Cadre légal et réglementaire

2.1.1. Le RIA

Le RIA ne prévoit pas de cadre contractuel spécifique entre le fournisseur et le déployeur permettant de définir clairement leurs obligations respectives. Il définit néanmoins un ensemble d'obligations distinctes à chacun de ces acteurs, en particulier lorsque le SIA est qualifié de système à haut risque (cf. Annexe 3).

À ce titre, il impose notamment :

- au fournisseur d'accompagner les SIA à haut risque d'une notice d'utilisation contenant des informations « *concises, complètes, exactes et claires, qui soient pertinentes, accessibles et compréhensibles pour les déployeurs* » et au minimum celles mentionnées à son article 11 et son article 13 ;
- au déployeur de réaliser, lorsque les conditions sont réunies, une AIDF pour les SIA à haut risque (article 27 du RIA). La réalisation de cette analyse suppose de recueillir auprès du fournisseur certaines informations sur le SIA dont le déploiement est envisagé.

Certains SIA sont soumis à des exigences réglementaires d'interopérabilité. Des obligations spécifiques peuvent notamment résulter de l'article 50 du RIA.

2.1.2. Le RGPD

Lorsque l'utilisation d'un SIA implique le traitement de données personnelles, un encadrement contractuel est requis :

- en cas de sous-traitance, par exemple avec le fournisseur ou le prestataire d'hébergement des données (article 28 du RGPD). Dans cette situation, le déployeur du SIA en tant que responsable de traitement, s'assure avant la conclusion du contrat et pendant toute sa durée que le sous-traitant présente des garanties suffisantes en matière de protection des données. Pour plus d'informations, se référer aux bonnes pratiques édictées par la CNIL ou se reporter aux clauses contractuelles types établies par la Commission européenne, sous réserve de prendre en compte les dispositions nationales applicables (8) ;
- en cas de responsabilité conjointe (article 26 du RGPD).

Le déployeur, en tant que responsable de traitement, est tenu de réaliser une AIPD lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Au regard des lignes directrices définies par le comité européen de la protection des données (CEPD), une AIPD est généralement requise pour l'utilisation de SIA en contexte de soins. Pour mener cette analyse, il doit disposer de certaines informations relatives aux mesures mises en œuvre par ses sous-traitants ou par le fournisseur du SIA utilisé.

Pour plus d'informations, il est possible de se référer aux lignes directrices concernant l'AIDP (9) et aux listes des traitements pour lesquels une AIPD est requise ou non (10), élaborées par la CNIL.

2.1.3. Le CSP

Lorsque l'utilisation du SIA implique l'hébergement par un tiers (par exemple, informatique en nuage ou « *cloud* »), des données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soin ou d'accompagnement, ce tiers doit être certifié hébergeur de données de santé (HDS).

La prestation réalisée et le contrat conclu doivent respecter les obligations imposées par l'article L.1111-8 et les articles R.1111-8-8 et suivants du CSP, notamment :

- les exigences applicables à l'hébergement des données de santé au sein de l'Espace économique européen (EEE) ;
- les obligations d'information du déployeur sur les lieux de stockage des données et sur le recours à des sous-traitants ;
- les conditions applicables aux transferts ou aux accès susceptibles d'intervenir depuis un État situé hors de l'EEE.

2.1.4. Le RDM et le RDIV

Lorsqu'un SIA constitue un DM au sens de l'article 2 du RDM, ou un DMDIV au sens de l'article 2 du RDIV, ou est intégré à un tel dispositif, les dispositions du RDM ou du RDIV sont applicables.

Le marquage CE atteste qu'un DM a fait l'objet des procédures d'évaluation de conformité prévues par la règlementation applicable et qu'il satisfait aux exigences générales de sécurité et de performance qui lui sont applicables.

Le fabricant est seul responsable du marquage CE. Il doit démontrer la conformité du dispositif au RDM ou RDIV, constituer le dossier technique et établir la déclaration de conformité avant toute mise sur le marché.

L'utilisation d'un SIA à finalité médicale au sens du RDM et du RDIV sans marquage CE alors qu'il est requis, peut engager la responsabilité du déployeur ou du professionnel utilisateur.

2.1.5. Actions à réaliser systématiquement

Ne pas conclure de contrat avec un fournisseur lorsque :

- la conformité réglementaire pour l'usage envisagé ne semble pas démontrée ;
- les principes de fonctionnement, d'explicabilité ou d'apprentissage du SIA demeurent insuffisamment compréhensibles et transparents pour le déployeur ou l'utilisateur ;
- aucune preuve de validation n'est disponible dans la population correspondant à l'usage prévu ;
- le circuit des données n'est pas clairement documenté, notamment les acteurs intervenant dans la chaîne de traitement ;
- les conditions de réutilisation des données par le fournisseur ne sont pas définies et formalisées avec le déployeur.

2.2. Principes

2.2.1. Prérequis à l'acquisition d'un SIA

Préalablement à la contractualisation avec un fournisseur de SIA, il est indispensable que le déployeur dispose de certaines informations relatives au fonctionnement du SIA et à son bon usage dans le contexte d'utilisation envisagé.

Ces éléments doivent être :

- intégrés dans des clauses dédiées et/ou annexés au contrat en complément des clauses spécifiques présentées plus loin ;
- mis à jour régulièrement, le cas échéant.

★★★ Établir un cahier des charges

La sélection d'un SIA, quel que soit son statut réglementaire, est réalisée sur la base d'un cahier des charges minimales ou tout document équivalent, établi à l'avance, et dont certaines exigences minimales ont été validées par la gouvernance de la structure (cf. Fiche 1).

Le déployeur précise ce cahier des charges au regard de ses spécificités et de ses besoins propres (fonctionnement, patientèle, etc.).

Ce cahier des charges ou équivalent comporte notamment des exigences relatives aux éléments suivants :

- la finalité du SIA et son statut réglementaire (DM, DMDIV ou non, niveau de risque au titre du RIA) ;
- la phase de développement du SIA, notamment les principes algorithmiques utilisés, la description des données d'entraînement (origine, nature, populations cibles, fiabilité, mise à jour, transparence), les modalités d'évaluation algorithmique, la gestion des biais algorithmiques identifiés et les stratégies d'atténuation prévues, la date de commercialisation ;
- les performances observées du SIA, notamment concernant les seuils validés (sensibilité, spécificité, robustesse, etc.), le contexte de leur validation (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, etc.), la base de données utilisée pour valider les performances (origine, nature, catégories de personnes concernées, fiabilité, mise à jour, transparence, etc.). Les organisations de santé et les utilisateurs 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 ;
- la population cible, c'est-à-dire les patients éligibles à l'utilisation du SIA au regard de la phase de développement, et la population exclue, c'est-à-dire les patients pour lesquels les performances du SIA n'ont été ni testées ni validées ;
- le principe de fonctionnement compréhensible par les utilisateurs afin de limiter l'effet « boîte noire ». À cet égard, des pistes d'audits, c'est-à-dire des enregistrements permettant de retracer les principales étapes, actions ou décisions du système, peuvent être mises à disposition afin d'éclairer les processus décisionnels et de garantir la traçabilité des opérations ;
- les éléments nécessaires au fonctionnement du SIA, tels que l'infrastructure technique et fonctionnelle, les données d'entrée, l'interopérabilité, les conditions de son utilisation, de son évaluation et de son suivi, les modalités de gestion des incidents et de mise en œuvre de mesures correctrices, les modalités de supervision humaine, les modalités de mise à jour et de fonctionnement dégradé ;
- une description des flux de données et les acteurs qui interviennent ;
- des données sur l'impact environnemental du SIA (coût carbone, etc.).

Le fournisseur met à disposition du déployeur les informations pertinentes demandées. Certaines de ces informations peuvent être précisées dans la notice d'utilisation requise par le RIA.

Cette documentation de référence est utile aux professionnels, pour comprendre l'outil, l'utiliser de manière conforme et délivrer une information adaptée au patient, et à la gouvernance de l'organisation, pour définir les spécifications techniques d'installation, définir le cadre de déploiement du système, encadrer les conditions d'utilisation, garantir son bon fonctionnement et assurer son suivi tout au long du cycle de vie.

Cette documentation de référence sur le SIA doit être maintenue à jour pendant toute la durée d'exploitation afin de tenir compte des évolutions du système, des performances observées en pratique réelle, des mises à jour réalisées ainsi que des éventuels incidents ou actions correctrices significatifs.

★★★ Vérifier la conformité réglementaire du SIA

Avant toute acquisition d'un SIA, le déployeur recueille et examine les éléments lui permettant d'apprécier la conformité réglementaire du SIA au regard de l'usage envisagé, notamment au regard du RIA, du RDM, du RDIV et du RGPD.

Le déployeur vérifie, notamment :

- le statut réglementaire du SIA (SIA à haut risque, DM, DMDIV, etc.) ;
- l'existence, lorsqu'elle est requise, d'une procédure d'évaluation de conformité et du marquage CE correspondant ;
- la mise à disposition de la documentation et des informations nécessaires à une utilisation du SIA.

Le déployeur s'assure de la conformité du SIA au RGPD. À cette fin, il peut demander au fournisseur de lui communiquer :

- les éléments permettant d'apprécier les garanties apportées par le fournisseur en matière de protection des données personnelles, notamment les mesures techniques mises en œuvre et, lorsque cela est pertinent, l'AIPD ;
- un certificat « hébergeur de données de santé » (HDS) ou les éléments permettant de démontrer qu'un tel certificat n'est pas requis ;
- une description des flux de données, de leurs finalités, de leur localisation, ainsi que de l'ensemble de la chaîne technique mobilisée pour le fonctionnement du SIA, incluant les acteurs (sous-traitants, sous-traitants ultérieurs) et les outils utilisés, notamment en cas de recours à des modèles commercialisés par des tiers.
- lorsque le SIA s'appuie sur des interfaces de programmation applicative tierces, une description claire de l'ensemble du circuit des flux de données est essentielle ;
- une description claire des conditions dans lesquelles les données peuvent être réutilisées par le fournisseur ou ses sous-traitants, ainsi que les finalités poursuivies.

Ces informations permettent au déployeur de réaliser le test de compatibilité prévu à l'article 6.4 du RGPD et de s'assurer que la réutilisation des données de santé pseudonymisées est conforme aux dispositions du règlement (UE) 2025/327 relatif à l'espace européen des données de santé. La réutilisation de données par un sous-traitant suppose en principe l'accord préalable et écrit du responsable de traitement initial (11).

Associer précocement le DPO ou les référents protection des données

L'utilisation d'un SIA en contexte de soins peut impliquer le traitement de données personnelles, notamment celles des patients ainsi que celles des professionnels participant à leur prise en charge. Le DPO ou les référents « protection des données » sont associés le plus en amont possible du projet de déploiement afin d'accompagner l'organisation de santé dans la contractualisation.

Sensibiliser les services compétents

Il est essentiel d'alerter les services compétents (notamment achats, biomédicaux, informatiques) (cf. Fiche 3) et de préciser dans les appels d'offre que toute composante IA fera 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.

Vérifier la couverture assurantielle du fournisseur et des utilisateurs

Le déployeur s'assure que le fournisseur dispose d'une assurance adaptée aux activités exercées et couvrant les risques susceptibles de résulter du SIA qu'il commercialise. Le déployeur peut demander au fournisseur la communication d'une attestation d'assurance en cours de validité ainsi que des informations sur l'étendue des garanties souscrites.

Le déployeur s'assure que les utilisateurs aient vérifié que les garanties souscrites auprès de leur assureur couvrent l'utilisation des SIA dans le cadre de leur activité (cf. Fiche 7).

Vérifier l'interopérabilité du SIA

L'intérêt d'un SIA dépend de son intégration au système d'information.

Le déployeur vérifie :

- l'interopérabilité du SIA avec le système d'information existant et avec les services numériques utilisés (dossier patient informatisé, système d'information radiologique, etc.), ses conditions de mise en œuvre et son coût d'entrée ;
- l'impact du SIA sur la sécurité informatique des systèmes d'information concernés.

En effet, au-delà de la perte de temps ou d'intérêt qu'elle peut engendrée, la non-interopérabilité d'un SIA peut créer des risques pour la prise en charge des patients, notamment en raison de la double saisie ou d'erreurs de transcription.

Dans certains cas, l'interopérabilité constitue une obligation à la charge du fournisseur ou du fabricant du SIA (article 50 du RIA, article L.1470-5 du CSP, article 27 du règlement (UE) 2025/327 relatif à l'espace européen des données de santé).

Afin de réaliser ces vérifications, le fournisseur met à disposition du déployeur une cartographie des installations techniques et fonctionnelles. Elle précise les modalités d'intégration du SIA au système d'information et dans les processus de travail, ainsi que les flux de données associés.

2.2.2. Clauses contractuelles spécifiques

Certaines clauses contractuelles spécifiques permettent au déployeur de sécuriser les usages.

Prévoir une clause de niveau de service (SLA)

Le déployeur veille à ce que le contrat conclu avec le fournisseur comporte une clause de niveau de service (« *Service Level Agreement* » ou SLA) précisant les garanties de service associées au SIA et les modalités de maintenance prévue (cf. Fiche 10).

Cette clause détaille notamment :

- les délais de résolution en cas d'incident (par exemple, le nombre d'heures maximales pour corriger un incident) ;
- les engagements de disponibilité (par exemple, 99,9 % en cas d'outil critique) ;
- les modalités de maintenance et de mises à jour : fréquence, notification préalable, validation locale, support technique (assistance, horaires, etc.) ;
- les modalités d'installation, de validation et de déploiement des mises à jour. Certaines d'entre elles nécessitent des phases de test, telles qu'une preuve de concept, et de contrôles de compatibilité avec l'environnement d'utilisation.

Prévoir une clause relative à la période de calibrage

Le déployeur veille à ce que le contrat conclu avec le fournisseur prévoit une période de calibrage permettant de valider l'outil dans son environnement d'utilisation, tant sur le plan technique que fonctionnel, par exemple dans un environnement de test.

Cette clause prévoit la possibilité pour le déployeur de se rétracter sans pénalité si l'outil s'avère inadapté à l'environnement dans lequel il est déployé.

Cette clause précise :

- les conditions de réalisation de cette période de calibrage : durée, données concernées, conditions de passage à un déploiement à plus large échelle, sous-populations concernées ;
- les résultats attendus c'est-à-dire, les critères d'acceptation (fonctionnels, opérationnels et de performance) permettant au déployeur de décider de l'acceptation, du refus ou de l'ajournement de la mise en service du système ;
- les contraintes et exigences techniques du déployeur au regard du système d'information existant.

La mise en place d'une phase de test courte, par exemple d'un mois, peut permettre de vérifier l'intégration technique du SIA et de recueillir un premier retour d'expérience des utilisateurs. L'implication des professionnels de santé, de représentants des usagers et, le cas échéant, d'experts en éthique est importante pour évaluer la pertinence et la sécurité des SIA à fort impact clinique.

Même de courte durée, une phase de test peut être encadrée contractuellement (cf. Fiche 6).

Prévoir une clause de performance

Le déployeur veille à ce que le contrat conclu avec le fournisseur prévoit une clause de performance précisant les seuils et les indicateurs applicables. Cette clause s'applique aux performances du SIA au cours de son utilisation. Par exemple, un engagement contractuel de performance peut prévoir que tout ou partie de la rémunération du fournisseur soit conditionnée à l'atteinte de résultats prédéfinis. Ces résultats sont généralement définis en amont dans le cadre d'une démarche d'achat fondée sur la valeur (« *value-based procurement* »), notamment lors de la contractualisation avec des start-ups ou des petites et moyennes entreprises (PME) (cf. Fiche 6 et Fiche 10).

Prévoir une clause sur les conditions de fin de contrat

Le déployeur veille à ce que le contrat conclu avec le fournisseur prévoit les conditions de fin de contrat, notamment de réversibilité des données (cf. Fiche 11).

Cette clause couvre notamment :

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

Prévoir une clause relative à la confidentialité des données

Le déployeur veille à ce que le contrat conclu avec le fournisseur comporte une clause de confidentialité spécifique applicable au fournisseur ainsi qu'aux membres de son personnel habilités à accéder aux données. Cette clause est adaptée à la sensibilité des données traitées et aux exigences de protection associées, notamment lorsqu'elles sont protégées par un secret prévu par la loi.

Prévoir une clause relative à la formation des utilisateurs

Le déployeur veille à ce que le contrat conclu avec le fournisseur comporte une clause encadrant le rôle du fournisseur dans la formation des utilisateurs du SIA. Cette formation peut reposer sur la mise à disposition de supports pédagogiques, un contrôle des connaissances acquises, et peut aller jusqu'à l'habilitation des utilisateurs. L'obligation de formation est maintenue tout au long de l'exploitation du SIA, notamment en cas de mise à jour (cf. Fiche 3).

Prévoir une clause relative à la traçabilité et à l'accès aux journaux d'activité

Le déployeur veille à ce que le contrat conclu avec le fournisseur comporte une clause spécifique définissant les dispositifs de traçabilité mis en œuvre par le fournisseur, ainsi que les modalités d'accès du déployeur aux traces générées (cf. Fiche 9). Cette clause précise également les modalités d'accès aux notices d'utilisation et à leurs versions successives, ainsi que les obligations du fournisseur relatives à leur mise à disposition.

Prévoir une clause relative aux procédures de gestion des incidents

Le déployeur veille à ce que le contrat conclu avec le fournisseur précise qui il doit contacter et les procédures à suivre en cas de dysfonctionnement ou d'incident, notamment lorsqu'ils sont susceptibles d'entraîner une vigilance sanitaire ou une violation de données, quel que soit le statut réglementaire du SIA (cf. Fiche 10).

Prévoir une clause relative au traitement de données personnelles

Le déployeur veille à ce que le contrat conclu avec le fournisseur précise :

- 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, le déployeur c'est-à-dire l'établissement ou le professionnel de santé ayant décidé de recourir à un SIA est qualifié de « responsable de traitement » ;
- les catégories de données à caractère personnel nécessaires au fonctionnement du SIA, ainsi que celles qui ne sont pas nécessaires à son l'utilisation (par exemple, les données d'identité du patient ou l'identité nationale de santé ou INS).

En complément, lorsque le fournisseur est qualifié de sous-traitant de données personnelles, cette clause doit contenir l'ensemble des mentions prévues par l'article 28 du RGPD.

Elle précise notamment :

- les caractéristiques de la prestation fournie et le traitement de données concerné ;
- les mesures techniques et organisationnelles mises en œuvre par le fournisseur afin de garantir la sécurité des données, ainsi que les conditions dans lesquelles ces mesures peuvent être modifiées ;
- les conditions dans lesquelles le fournisseur peut recourir à des sous-traitants ultérieurs, notamment les modalités d'autorisation ou d'information préalable du responsable de traitement dans un délai lui permettant, le cas échéant, de s'y opposer ;
- les mesures prévues pour répondre aux demandes d'exercice des droits des personnes concernées ;
- les réutilisations précises envisagées par le fournisseur ainsi que toute information pertinente à leur compréhension. Sauf disposition légale ou réglementaire contraire, le déployeur peut s'opposer à la réutilisation des données par le fournisseur.

Une vigilance particulière doit être portée en cas de recours à des sous-traitants, y compris à des sous-traitants ultérieurs, soumis à un droit extra-européen, notamment lors de recours à des services d'informatique en nuage (« *cloud* »). Le déployeur demande au fournisseur la liste des sous-traitants auxquels il fait appel ainsi que leur lieu d'établissement. Pour les HDS, la communication de cette information constitue une obligation. Ces HDS sont également tenus d'héberger les données sur le territoire de l'EEE.

Toute réutilisation secondaire des données (apprentissage, annotation, étude, etc.) constitue un traitement de données personnelles distinct, qui doit respecter les exigences des textes applicables, notamment le RGPD, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (loi « informatique et libertés ») et, à terme, le règlement (UE) 2025/327 relatif à l'espace européen des données de santé. Les acteurs peuvent également se référer aux recommandations publiées par la CNIL relatives à l'IA et au secteur de la santé.

3. Sensibilisation, formation et habilitation

La formation favorise l'usage éclairé et sécurisé des SIA, le respect du droit à l'information des personnes (cf. Fiche 4) et la mise en œuvre d'une supervision humaine effective (cf. Fiche 8).

La formation à l'IA des professionnels de santé, des personnels administratifs et des instances de gouvernance permet à chaque acteur de disposer d'un niveau de connaissances et de compétences adapté à son rôle et à ses responsabilités (cf. Fiche 1).

Synthèse

Obligations principales

Le déployeur :

- met en place ou participe à des modules de formation sur l'IA en santé et sur la protection des données personnelles.

Principes prioritaires

- Sensibiliser l'ensemble du personnel à l'IA
- Former les utilisateurs du SIA

3.1. Cadre légal et réglementaire

Quel que soit le niveau de risque du SIA utilisé, les fournisseurs et les déployeurs sont tenus 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 (article 4 du RIA). Le déployeur et l'utilisateur doivent disposer des compétences, des connaissances et du niveau de compréhension nécessaires au déploiement et à l'utilisation du SIA.

Le bureau de l'IA de la Commission européenne, responsable de la mise en œuvre du RIA, n'impose pas, à date, d'exigences formelles en matière de formation ni de mesurer les connaissances des utilisateurs (article 4 du RIA).

Toutefois, pour atteindre les objectifs de conformité, la formation doit permettre :

- d'assurer une compréhension générale de l'IA au sein de l'organisation de santé ;
- de clarifier le rôle de l'organisation de santé, qu'elle soit fournisseur ou déployeur de SIA ;
- d'identifier et d'évaluer les risques liés aux SIA fournis ou déployés et de définir des mesures adaptées pour les prévenir, les réduire et en limiter les conséquences.

Le déployeur et les personnes placées sous son autorité doivent être en mesure de respecter le droit des personnes à obtenir des explications sur les décisions individuelles prises les concernant avec l'assistance d'un SIA (cf. Fiche 8).

3.1.1. Pour tous les SIA

Les articles L.4021-1 à L.4022-11 du CSP prévoient une obligation de formation continue dans le cadre du développement professionnel continu et, pour certains professionnels de santé, de la certification périodique. Les modalités de mise en œuvre de cette obligation sont précisées aux articles R.4021-4 et suivants et aux articles R.4022-6 et suivants du CSP.

3.1.2. Pour les SIA avec traitement de données personnelles

Dès lors que l'utilisation d'un SIA implique le traitement de données personnelles, le déployeur, en tant que responsable de traitement, 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.

3.1.3. Pour les SIA à haut risque

Les déployeurs de SIA à haut risque sont tenus, en vertu de l'article 26 du RIA, de veiller à ce que les personnes chargées de leur utilisation et de leur supervision disposent de la formation et des compétences suffisantes pour en assurer la gestion et la supervision humaine. La Commission européenne souligne que la seule mise à disposition de la notice d'utilisation ne saurait suffire et que le déployeur doit mettre en place des mesures spécifiques de formation (12).

3.1.4. Actions à réaliser systématiquement

La seule consultation de la notice d'utilisation d'un SIA ne constitue pas à elle seule une formation suffisante à son utilisation. Une démarche de formation adaptée est nécessaire pour permettre aux utilisateurs de comprendre le fonctionnement du SIA, ses conditions d'utilisation ainsi que ses limites.

Les pratiques suivantes doivent être systématiquement mises en œuvre :

- accompagner les équipes dans l'appropriation du SIA et son intégration dans les pratiques professionnelles ;
- former les professionnels, y compris les nouveaux arrivants, à l'utilisation du SIA et aux risques associés, notamment avec des sessions obligatoires en matière de protection des données personnelles et de responsabilité professionnelle ;
- sensibiliser à la sécurité des données, par action directe ou par engagement contractuel, les prestataires externes et les intérimaires qui peuvent avoir un impact aussi important que les collaborateurs internes (13).

3.2. Principes

★★★ Sensibiliser l'ensemble du personnel à l'IA

Le déployeur met en place une sensibilisation générale visant à garantir un socle commun minimal de compréhension de l'IA en santé. Cette sensibilisation permet d'atteindre un premier niveau d'acculturation aux risques liés à l'utilisation des données des patients et à aborder les questions de responsabilité individuelle et professionnelle. Cette sensibilisation est proposée à l'ensemble du personnel, incluant les professionnels de santé, les personnels administratifs et techniques, les équipes dirigeantes et encadrantes, et en particulier, les nouveaux arrivants et le personnel temporaire.

Cette sensibilisation peut prendre différentes formes, par exemple via des conférences internes, des ateliers pluriprofessionnels, des retours d'expériences réguliers, des MOOC ou des sessions plénières ouvertes à l'ensemble des personnels.

Cette sensibilisation aborde a minima :

- les avantages et les limites de l'IA en santé, ses risques et les bonnes pratiques à mettre en œuvre ;
- les règles concernant le traitement et la protection des données à caractère personnel ;
- les responsabilités de chacun des utilisateurs ;
- l'exigence de supervision humaine.

★★★ Former les utilisateurs du SIA

> La mise en œuvre de formations à destination des professionnels de santé fait partie des éléments d'évaluation de la certification des établissements de santé, dans la version 2027 du référentiel. Cette exigence est déclinée dans le critère 3.4-05 pour les DMN faisant appel à de l'IA et dans le critère 3.4-06 pour les SIA sans finalité médicale (5).

Le déployeur, du fait de son obligation de moyens, a pour responsabilité juridique d'organiser la formation des utilisateurs d'un SIA avant son utilisation effective. Le fournisseur accompagne le déployeur dans ses actions de formations. Son rôle est particulièrement important lorsque les organisations de santé disposent de ressources limitées pour les réaliser. Cet accompagnement peut être encadré contractuellement (cf. Fiche 2).

Pour chaque SIA, le contenu de la formation intègre :

- une analyse de sa notice d'utilisation et des éventuelles recommandations du fournisseur, pour favoriser un usage sécurisé et éclairé ;
- un rappel sur la responsabilité du professionnel de santé, en insistant sur le fait que celui-ci demeure responsable de ses actes, qu'il soit assisté ou non d'un SIA ;
- la mention des obligations réglementaires associées à l'usage du SIA, notamment en matière d'information des personnes (cf. Fiche 4), de consentement (cf. Fiche 5) et de supervision humaine (cf. Fiche 8) ;
- ses principes généraux de fonctionnement, tels que le type d'algorithme, les données d'apprentissage, les données d'entrée nécessaires à son fonctionnement, ses limites techniques, etc. ;

- sa destination d'usage et sa finalité, afin de préciser le périmètre d'utilisation autorisé et les usages à proscrire ;
- ses performances attendues et leurs implications pratiques (sensibilité, spécificité, valeurs prédictives, etc.) ;
- ses biais potentiels (biais algorithmiques et cognitifs) et les risques associés (cf. Fiche 7) ;
- l'organisation concrète de la prise en charge et l'intégration du SIA dans les processus de travail (cf. Fiche 6) ;
- les modalités de validation humaine des résultats, la primauté du jugement clinique du praticien, la possibilité de s'écarter du résultat du SIA et les procédures à suivre en cas de désaccord (cf. Fiche 8)
- les modalités de communication et d'information à destination des patients concernant le SIA utilisé, notamment sur son intérêt, ses limites et ses conséquences (cf. Fiche 4) ;
- les procédures d'identification et de signalement des incidents, que le SIA soit DM, DMDIV ou non, en les intégrant dans la gestion de la qualité (cf. Fiche 10) ;
- des cas pratiques accompagnés d'une aide à la prise en main, tels que des exercices de détection d'erreurs du SIA, la rédaction de prompts ou l'analyse de problématiques particulières comme le désaccord entre le SIA et la décision d'un clinicien, les décisions de non-recours au SIA, les cas de non-consentement, l'indisponibilité du SIA, etc.

Une évaluation des acquis en fin de formation valide que l'utilisateur est compétent pour utiliser le SIA de façon autonome en contexte de soins.

Renforcer les compétences des acteurs aux fonctions spécifiques

Le déployeur identifie les acteurs dont les fonctions et responsabilités sont directement concernées par les enjeux liés aux SIA et leur propose des formations adaptées selon leur profil. Ces formations approfondies permettent de renforcer la compréhension des enjeux, des principes de fonctionnement, des obligations et des responsabilités dans leurs champs d'activités respectifs.

Ces formations peuvent notamment s'adresser à la gouvernance numérique, à la direction des affaires médicales, à la direction des affaires juridiques, à la direction de l'information médicale, à la commission médicale d'établissement, à la commission des usagers, au délégué à la protection des données, au responsable de la sécurité des systèmes d'information, au qualiticien, au référent biomédical, au référent en charge de la vigilance et aux référents locaux du SIA.

Organiser les formations en cohérence avec les réalités des acteurs

Toute action de formation proposée par le déployeur et le fournisseur se fait en cohérence avec les moyens de l'organisation de santé et avec les besoins, les pratiques, les impératifs et la charge de travail des acteurs concernés. Le déployeur propose des formations :

- sous la forme de modules courts facilement intégrables dans les emplois du temps ;
- à une fréquence adaptée au contexte du déploiement et au niveau de risque des SIA ;
- aux nouveaux arrivants et au personnel temporaire.

Des référents locaux du SIA peuvent être désignés et formés afin d'encadrer la formation au sein de l'organisation de santé et permettre un compagnonnage des utilisateurs (cf. Fiche 6).

Le déployeur et l'utilisateur portent une vigilance particulière au choix des formations, dont l'offre est abondante et de qualité hétérogène. Le déployeur peut élaborer ses propres formations, utiliser les ressources proposées par les fournisseurs et par les institutions publiques, ou mobiliser des prestataires externes, de préférence certifiés Qualiopi. Les engagements relatifs à l'accompagnement des actions de formation par le fournisseur peuvent être encadrés contractuellement (cf. Fiche 2).

La participation systématique des équipes dirigeantes et encadrantes aux actions de formation est essentielle à ces démarches.

Tracer les formations réalisées

Le déployeur organise le suivi systématique des formations du personnel. Il assure une traçabilité des formations réalisées dans un registre nominatif, précisant les dates, les contenus des modules suivis et la fréquence de mise à jour des connaissances.

Habiliter les utilisateurs de SIA à haut risque

Pour les SIA à haut risque au sens du RIA, le déployeur met en place une procédure d'habilitation préalable à l'utilisation. Le déployeur identifie les utilisations pour lesquelles l'habilitation est requise. L'obtention de l'habilitation est subordonnée à l'atteinte d'un niveau minimal de réussite à des tests de validation des acquis et mène à la délivrance d'un certificat interne spécifique à chaque SIA. L'utilisation du SIA est alors strictement conditionnée par l'obtention de ce certificat.

Pour les organisations de santé aux ressources limitées, notamment pour les professionnels libéraux, ce processus d'habilitation peut être conçu et mis en œuvre avec l'appui du fournisseur. Son rôle dans l'habilitation peut être encadré contractuellement (cf. Fiche 2).

4. Information des usagers

L'information des usagers du système de santé (patients, proches, représentants légaux, etc.) est indispensable pour favoriser le bon usage, leur acceptation par les usagers et garantir l'effectivité de leurs droits. Il s'agit d'une obligation légale qui varie selon les caractéristiques du système utilisé, sa finalité et le cadre juridique applicable. À défaut, le professionnel et l'établissement de santé s'exposent à un risque juridique. En effet, un patient insuffisamment informé ne peut ni exercer pleinement ses droits, notamment dans le cadre d'un recours contre le fournisseur ou le fabricant du SIA, ni consentir de manière éclairée aux actes de soins qui lui sont proposés.

Différents types d'information doivent être différenciées, notamment :

- l'information liée à la prise en charge de l'usager (état de santé, traitements proposés, frais correspondants, etc.) ;
- l'information générale sur l'usage de SIA qualifié de DM dans les soins ;
- l'information sur l'utilisation de données personnelles pour le fonctionnement des SIA et leurs droits à cet égard ;
- l'information sur la ou les réutilisation(s) secondaire(s) des données personnelles.

Les principes formulés donnent des orientations pour favoriser une diffusion homogène de l'information. Toutefois, la nature des informations à transmettre, leur niveau de détail et leurs modalités de communication peuvent varier et sont à déterminer au cas par cas.

La mise en œuvre de ces principes repose sur la réalisation préalable de certaines actions, détaillées par ailleurs dans ce guide (cf. Fiche 1, Fiche 2 et Fiche 3).

Synthèse

Obligations principales

Le déployeur :

- informe les personnes concernées lorsqu'un SIA à haut risque relevant de l'annexe III du RIA est utilisé ;
- informe les personnes concernées lorsqu'elles interagissent directement avec un SIA et les sensibilise afin qu'elles communiquent uniquement les informations nécessaires ;
- informe les personnes concernées conformément au RGPD lorsque l'utilisation d'un SIA implique le traitement de données personnelles ;
- informe les personnes concernées conformément au RGPD lorsque les données personnelles collectées et utilisées dans le cadre du soin sont réutilisées, notamment à des fins de développement, de recherche clinique ou d'évaluation du déploiement du SIA.

Le professionnel :

- informe les personnes concernées lorsqu'il décide de recourir à un DM intégrant un SIA. En effet, il convient d'anticiper les textes d'application de l'article L. 4001-3 du CSP encore en cours d'élaboration.

Principes prioritaires

- Informer les usagers sur les réutilisations de leurs données envisagées
- Diffuser la politique d'utilisation des SIA auprès des usagers
- Informer les usagers directement concernés par l'utilisation d'un SIA

4.1. Cadre légal et réglementaire

Plusieurs normes juridiques imposent des obligations d'information à l'égard des usagers du système de santé, et notamment des patients. Si ces normes ne répondent pas nécessairement aux mêmes impératifs, elles poursuivent des objectifs communs : créer un climat de confiance et permettre aux usagers de participer activement aux décisions les concernant.

4.1.1. Le RIA

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

- lorsqu'un SIA à haut risque (hors DM/DMDIV) est utilisé pour prendre ou faciliter la prise de décision concernant des personnes physiques (article 26.11 du RIA) ;
- lorsqu'un SIA à risque limité (soumis au chapitre IV du RIA) est utilisé, notamment lorsqu'il interagit directement avec l'usager ou génère des contenus, tels que des documents (article 50 du RIA).

4.1.2. Le RGPD

Le RGPD impose au déployeur d'un SIA, en tant que responsable de traitement, d'informer les personnes de l'utilisation de leurs données personnelles. Cette obligation s'applique dès lors que des données personnelles sont utilisées, quelle que soit la classification du SIA.

Cette information doit être compréhensible, aisément accessible et comporter les mentions prévues à l'article 13 du RGPD et à l'article 14 du RGPD (par exemple : la finalité du traitement, les catégories de données traitées, les destinataires des données, leur durée de conservation, ainsi que les droits des personnes concernées).

Cette obligation s'applique à l'utilisation primaire des données dans le cadre du soin et à leur réutilisation, par exemple pour le développement ou l'amélioration du modèle d'IA (ou modèle d'apprentissage), ou pour l'évaluation du SIA.

4.1.3. Le CSP

Le CSP prévoit plusieurs obligations d'information à la charge des établissements et des professionnels de santé à l'égard de leurs patients, notamment :

- l'obligation d'informer le patient sur son état de santé et sur les investigations, traitements ou actions de prévention proposés (article L.1111-2 du CSP) ;
- l'obligation d'informer le patient du recours à certains SIA qualifiés de DM dans le cadre d'un acte de prévention, de diagnostic ou de soin, ainsi que des conséquences qui en découlent (article L.4001-3 du CSP) ;
- une obligation d'information quant aux frais auxquels le patient pourrait être exposé à l'occasion d'activités de prévention, de diagnostic et de soins et, le cas échéant, sur les conditions de leur prise en charge (article L.1111-3 du CSP).

4.2. Principes

Au-delà des obligations légales et réglementaires, la transparence vis-à-vis des usagers est une condition essentielle pour leur permettre de comprendre ces technologies, leurs utilisations et leurs limites. Cette transparence contribue à garantir une pratique professionnelle cohérente avec la relation de confiance établie entre le patient et le professionnel.

★★★ Informer les usagers sur les réutilisations de leurs données envisagées

La réutilisation des données personnelles collectées dans le cadre du fonctionnement d'un SIA constitue une pratique courante. Ces réutilisations peuvent avoir des finalités variées (amélioration des performances, vigilances sanitaires, évaluation de l'impact du SIA sur le parcours patient et sur les pratiques professionnelles, etc.) et être réalisées par différents acteurs (le déployeur, le fournisseur ou un organisme tiers). Elles doivent être conformes au RGPD qui impose notamment aux organismes responsables de traitement d'informer les personnes concernées et de leur communiquer certains éléments.

Ainsi, même lorsque cette obligation d'information n'incombe pas directement au déployeur du SIA, il est essentiel d'anticiper la réutilisation des données de ses prestataires pour informer les personnes. Cette information leur permet de comprendre les réutilisations envisagées et d'exercer effectivement leurs droits, notamment le droit d'opposition à la réutilisation de leurs données, lorsqu'il est applicable.

Dans cette perspective, une information dès la collecte initiale des données, c'est à dire lors de l'utilisation du SIA dans le cadre du soin, est privilégiée. La mise à disposition de la cartographie des SIA utilisés, précisant notamment ceux pour lesquels une réutilisation est prévue et renvoyant vers les notices d'information correspondantes, constitue une bonne pratique à cet égard.

Quelles modalités d'information ?

L'information relative à l'IA transmise au patient peut susciter des interrogations, voire des inquiétudes, tant au sujet des résultats d'un SIA que de son utilisation. La formation des professionnels à la compréhension du fonctionnement et des limites des SIA constitue une condition essentielle pour leur permettre d'en parler de manière adaptée aux patients et favoriser une compréhension éclairée de ces technologies (cf. Fiche 3).

Le déployeur :

- privilégie une approche pédagogique pour délivrer une information claire et compréhensible, centrée sur les bénéfices attendus pour le patient (par exemple, en termes de sécurité ou de rapidité), tout en évitant une surcharge d'information ou un recours excessif à des termes techniques ;
- assure une traçabilité formalisée de l'information délivrée au patient, tant pour des raisons juridiques que pour garantir la continuité de son information ;
- distingue cette information de celle requise par la réglementation, telle que l'information relative aux frais ;
- prend en compte les éventuelles situations de vulnérabilité des personnes concernées lors de leur prise en charge ;
- associe les représentants des usagers, notamment la commission des usagers et les associations de patients ainsi que les professionnels, dans l'élaboration des messages d'information afin d'adapter le vocabulaire aux perceptions et aux besoins des patients, par exemple en évitant les termes anxiogènes. L'objectif est de garantir une information compréhensible et accessible à l'ensemble des personnes concernées.

Dans tous les cas, diversifier les modalités d'information des patients favorise une information plus large et plus inclusive, en tenant compte des différents niveaux de littératie en santé et en numérique. Cette information peut s'appuyer sur différents supports (vidéos, brochures, documents, etc.), sur la méthode Facile à lire et à comprendre (FALC) et être diffusée via plusieurs canaux (site internet, affichage dans les espaces d'accueil, etc.).

Afin d'adapter l'information aux enjeux associés aux SIA, une gradation en trois niveaux est proposée en fonction des risques pour les patients et des droits qu'ils sont susceptibles d'exercer :

- niveau 1 : une information générale à l'échelle de l'organisation de santé ;
- niveau 2 : pour les patients concernés par une utilisation spécifique du SIA, l'ajout d'une phrase type dans les documents qui leurs sont remis, notamment les comptes rendus ;
- niveau 3 : pour les SIA présentant des risques importants pour le patient, une information individuelle détaillée est délivrée en amont de l'utilisation ou de la prise de décision médicale.

Le niveau d'information délivré est déterminé selon le patient, son parcours et le niveau de risque du SIA. Ainsi, un SIA d'aide à la décision justifie généralement d'un niveau de transparence plus élevé (niveau 3) qu'un SIA ayant une incidence plus limitée sur la prise en charge (niveau 1 ou niveau 2). Cette gradation de l'information peut être formalisée dans la politique d'information adoptée par les instances de gouvernance de l'organisation de santé (cf. Fiche1).

★★★ Diffuser la politique d'utilisation des SIA auprès des usagers (niveau 1)

Un premier niveau d'information générale est diffusé à l'ensemble des patients sur l'utilisation potentielle de SIA dans leur prise en charge.

Cette information générale peut être diffusée au moyen de différents supports, par exemple :

- une mention dans le livret d'accueil, une affiche dans la salle d'attente, une page dédiée sur le site internet de l'organisation de santé ou une brochure présentant des exemples d'utilisation et leurs finalités.

  > Par exemple : « Dans le cadre de votre prise en charge, des systèmes d'intelligence artificielle peuvent être utilisés. Pour plus d'informations, consultez le site internet de l'établissement ou adressez-vous à l'accueil. »

- une charte relative à l'utilisation des SIA, présentant les principes retenus pour la sélection, le déploiement et l'utilisation des SIA (cf. Fiche 1). Cette charte peut préciser les engagements pris par l'organisation de santé en matière de qualité, de supervision humaine, de sécurité, de transparence et les situations dans lesquelles une information renforcée, voire un consentement formalisé, sont nécessaires.

★★★ Informer les usagers directement concernés par l'utilisation d'un SIA (niveau 2)

Une information spécifique et contextualisée est délivrée lorsqu'un patient est directement concerné par l'utilisation d'un SIA dans le cadre de sa prise en charge, notamment pour les SIA d'aide au dépistage, au diagnostic ou à la décision médicale, ainsi que pour les SIA reposant sur l'IA générative comme les SIA d'aide à la rédaction de comptes rendus. Cette information est portée à la connaissance des patients, a minima via le dossier médical, notamment via les traces fonctionnelles et les traces applicatives et par une mention spécifique dans les documents qui leur sont remis, notamment dans les comptes rendus.

> Par exemple l'ajout systématique d'une mention personnalisable dans les documents remis au patient constitue une bonne pratique :
>
> « 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(e) par le Dr [Nom, fonction]. »
>
> « Le système d'intelligence artificielle [Nom, Version] a été 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]. »

Ces mentions peuvent également contribuer à l'information d'autres professionnels participants à la prise en charge, notamment dans le cadre de demandes d'avis de confrères ou d'expertises complémentaires.

Lorsque cela est pertinent, des supports pédagogiques dédiés à certains SIA, peuvent être mis à disposition en salle d'attente ou remis aux patients concernés (brochure d'information, fiche explicative, notice, etc.), en complément de l'information délivrée par le professionnel.

Mettre à disposition la cartographie des SIA de la structure (niveau 1)

La diffusion de ce premier niveau d'information générale peut également être assurée par la mise à disposition de la cartographie des SIA utilisés au sein de l'organisation de santé (cf. Fiche 1).

L'organisation de santé peut choisir de rendre publique cette cartographie dans son intégralité ou, a minima, de communiquer les informations suivantes :

- les principales utilisations des SIA (par exemple, l'aide à l'interprétation en radiologie ou l'aide à la génération de comptes rendus de consultation) ;
- les bénéfices attendus ;
- les populations cibles ;
- le stade de déploiement des SIA (utilisation généralisée ou limitée à certains services) ;
- les éventuelles réutilisations de données envisagées.

La diffusion de ces informations peut renforcer l'attractivité de la structure et permettre de développer la confiance des usagers. Elle peut également susciter des interrogations et des réticences chez certains patients, y compris lorsque les SIA concernés sont déjà couramment utilisés dans le cadre de certains actes de soin. La formation des professionnels à l'information des patients est donc essentielle pour favoriser la communication d'une information loyale, claire et adaptée sur les finalités du SIA, ses bénéfices, ses limites, ses risques et ses incidences potentielles sur la prise en charge (cf. Fiche 3).

Informer l'usager de manière individuelle et détaillée, avant l'utilisation d'un SIA (niveau 3)

Dans certaines situations, une information individuelle et exhaustive, préalable à l'utilisation d'un SIA, peut être apportée au patient, notamment lorsque cette information est nécessaire à l'exercice de ses droits ou lorsque l'utilisation du SIA est susceptible d'avoir un impact important sur la prise en charge. Cela peut notamment être le cas lorsque la prise en charge repose largement sur les résultats ou les prédictions du SIA, en l'absence d'autres données cliniques objectivables par un professionnel.

5. Consentement et droits des usagers

Le consentement libre et éclairé du patient est un droit fondamental, selon lequel aucun acte ne peut être réalisé sans l'accord préalable du patient ou de ses représentants légaux. Cet accord n'est pas une simple formalité administrative : il incarne l'autonomie du patient, son droit à l'information et lui permet de participer activement aux décisions concernant sa santé. À défaut de consentement valablement recueilli, la responsabilité civile et pénale des professionnels et des établissements de santé est susceptible d'être engagée. Indissociable des obligations d'information présentées précédemment, ce droit occupe une place centrale dans les débats relatifs à l'utilisation des SIA en contexte de soins.

La notion de consentement recouvre plusieurs réalités juridiques qui doivent être distinguées, notamment :

- le consentement requis pour la réalisation d'un acte médical ou de soins ;
- le consentement requis pour participer à certaines recherches en santé ;
- le consentement susceptible de fonder un traitement des données personnelles ;
- le consentement requis pour la réalisation des essais en conditions réelles de SIA à haut risque.

Les principes formulés ci-dessous visent ainsi à éclairer les professionnels et les structures de soins sur les exigences légales, les bonnes pratiques lors de l'utilisation d'un SIA en contexte de soins. Il appartient à chaque professionnel de déterminer, au regard de la situation particulière de son patient, si des mesures complémentaires doivent être mises en œuvre afin de garantir une prise de décision consensuelle, conforme aux règles d'exercice professionnel.

Au-delà du droit de consentir, les usagers du système de santé disposent également de droits en leur qualité de patient et de personne concernée par un traitement de leurs données personnelles.

Synthèse

Obligations principales

Le déployeur :

- en tant que responsable de traitement, donne suite aux demandes d'exercice des droits au sens du RGPD qui lui sont adressées ;
- permet aux personnes concernées par l'utilisation d'un SIA d'exercer les droits issus du RIA et du CSP, en particulier leur droit à l'information, au consentement et à la participation aux décisions concernant leur santé ;
- garantit la maitrise des personnes sur leurs attributs de personnalité, en particulier sur leur voix et leur image.

Principes prioritaires

- Informer l'usager et recueillir son accord pour les enregistrements vocaux et vidéo ainsi que pour les photographies

5.1. Cadre légal et réglementaire

En complément des obligations d'information (cf. Fiche 4), différentes dispositions applicables dans le cadre des soins prévoient le recueil d'un consentement libre et éclairé de la personne.

5.1.1. Sur le consentement

5.1.1.1. Le RIA

L'article 60 du RIA et l'article 61 du RIA imposent de recueillir un consentement spécifique pour les essais en conditions réelles de SIA à haut risque, qui ne sont pas abordés dans ce guide.

5.1.1.2. Le RGPD

Le consentement au sens du RGPD constitue l'un des fondements juridiques prévus pour le traitement des données personnelles, y compris des données de santé. Ce consentement 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. Pour plus d'information, se référer au guide sur le recueil du consentement élaboré par la CNIL (14).

Toutefois, le traitement des données mis en œuvre dans le cadre du fonctionnement d'un SIA utilisé en contexte de soins repose sur d'autres fondements juridiques. Cette affirmation concerne la base légale prévue à l'article 6 du RGPD ou les exceptions applicables aux données de santé au titre de l'article 9 du RGPD.

Dans le contexte de soins, ces utilisations reposent sur :

- l'intérêt légitime du responsable de traitement (article 6.1.f du RGPD) ou la poursuite d'une mission d'intérêt public qui lui incombe (article 6.1.e du RGPD). Le choix de la base légale appropriée dépend de la qualification du responsable de traitement et du SIA concerné ;
- l'exception relative à la médecine et aux soins en santé (article 9.2.h du RGPD), lorsque le responsable de traitement est un établissement ou un professionnel de santé tenu au secret professionnel.

5.1.1.3. Le CSP

Aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne, lequel peut être retiré à tout moment (article L.1111-4 du CSP).

Par ailleurs, le CSP prévoit d'autres exigences en matière de recueil de consentement, et des obligations spécifiques applicables à certaines situations et à certaines catégories d'actes ou de prises en charge. À titre d'exemple, un consentement spécifique est requis pour la réalisation d'examen des caractéristiques génétiques (articles L.1130-1 et suivants du CSP), le prélèvement d'éléments et produits du corps humain (articles L.1241-1 et suivants du CSP), ou encore l'assistance médicale à la procréation (articles L.2141-1 et suivants du CSP).

5.1.1.4. La protection juridique particulière de l'image et de la voix

Le code pénal sanctionne la captation, l'enregistrement ou la transmission de la voix ou de l'image d'une personne lorsque ces actes sont réalisés sans son consentement (article 226-1 du code pénal).

En complément, le juge considère, sur le fondement du droit à la vie privée, dont le droit à la protection des données est une composante, que la captation ou l'utilisation d'image d'une personne nécessite au préalable de recueillir son consentement lorsqu'elle permet son identification (15). Il considère également que la voix d'une personne est l'un des attributs principaux de la personnalité et bénéficie, à ce titre, d'une protection comparable à celle reconnue à l'image.

Il juge ainsi que le droit au respect à la vie privée, garanti par l'article 9 du code civil et l'article 8 de la Convention européenne des droits de l'homme, inclut, outre le droit au respect de l'image, le droit au respect de la voix de la personne (16).

La protection de l'image et de la voix a été reconnue par la Cour européenne des droits de l'Homme (17, 18) et par le juge national (19).

Le droit à l'image et à la voix du code civil s'applique à toute personne, qu'il soit patient ou professionnel de santé.

5.1.2. Sur les droits des personnes : usagers et professionnels

5.1.2.1. Le RIA

Le RIA reconnaît, à toute personne concernée par l'utilisation d'un SIA, des droits, dont :

- le droit d'introduire une réclamation auprès de l'autorité de surveillance du marché compétente (article 85 du RIA) ;
- le droit d'obtenir des explications sur une décision individuelle prise avec l'assistance de certains SIA (article 86 du RIA).

5.1.2.2. Le RGPD

Le RGPD reconnaît aux personnes concernées (usagers ou professionnels) des droits sur leurs données personnelles, dont :

- le droit d'accès (article 15 du RGPD) ;
- le droit de rectification (article 16 du RGPD) ;
- le droit à l'effacement des données dans certaines situations (article 17 du RGPD) ;
- le droit à la limitation du traitement (article 18 du RGPD) ;
- le droit d'opposition au traitement de leurs données personnelles (article 21 du RGPD) ;
- le droit d'introduire une réclamation auprès de la CNIL (article 77 du RGPD).

Le déployeur du SIA, en tant que responsable de traitement, est tenu de donner suite aux demandes d'exercice des droits qui lui sont adressées. Pour ce faire, il peut s'appuyer sur ses sous-traitants, notamment le fournisseur du SIA, qui sont tenus de mettre en œuvre les mesures appropriées afin de lui permettre de respecter ses obligations en la matière.

5.1.2.3. Le CSP

Le CSP reconnaît aux usagers du système de santé différents droits, notamment en matière de respect de leur dignité tout au long de leur prise en charge (article L.1110-2 du CSP), de respect de leur vie privée et de confidentialité des informations les concernant (article L.1110-4 du CSP), d'information, de consentement et de participation aux décisions concernant leur santé (article L.1111-4 du CSP) et d'accès aux informations relatives à leur santé (article L.1111-7 du CSP).

5.2. Principes

★★★ Informer l'usager et recueillir son accord pour les enregistrements vocaux et vidéo ainsi que pour les photographies

Les SIA dédiés à la retranscription d'échanges ou à l'analyse de photos et vidéos dans le cadre des soins doivent respecter les règles applicables à la protection de l'image et de la voix des personnes, dès lors que les enregistrements ou les photos permettent de les identifier.

Dans cette perspective, le professionnel utilisateur d'un tel SIA en informe l'usager, recueille son accord et veille à en assurer la traçabilité. Une formalisation écrite systématique n'est pas nécessairement requise. Par exemple, le professionnel peut mentionner dans les documents remis à l'usager que celui-ci a été informé et a donné son accord. Cette fonctionnalité peut également être directement intégrée dans les SIA utilisés. S'agissant des outils de retranscription d'échanges, les enregistrements bruts sont conservés uniquement pour la durée nécessaire à la retranscription des échanges et à la validation du résultat par le professionnel ayant pris en charge l'usager.

L'information de l'usager et le recueil de son accord concernent uniquement l'utilisation des enregistrements ou des photographies dans le cadre de la prise en charge. Toute réutilisation à d'autres fins (par exemple, pour l'entraînement ou l'amélioration d'un SIA, la recherche, la formation ou d'autres usages) doit respecter les règles applicables en matière de protection des données personnelles et de protection de l'image et de la voix des personnes.

Absence de consentement spécifique pour l'utilisation d'un SIA

Le recours à un consentement spécifique pour l'utilisation d'un SIA dans le cadre du soin courant n'apparaît généralement pas nécessaire. En effet, le recueil d'un consentement constitue un processus exigeant qui ne paraît pas adapté à la majorité des situations d'utilisation d'un SIA. Dans la majorité des cas, une information loyale, claire et accessible, associée à la possibilité pour la personne d'exercer ses droits apparaît suffisante.

L'absence de consentement spécifique à l'utilisation d'un SIA dans le cadre du soin courant ne dispense pas du recueil du consentement lorsqu'il est exigé par les textes.

Ainsi :

- la réalisation d'un acte de prévention, de diagnostic ou de soin demeure soumise au consentement de la personne au titre du CSP ;
- la captation ou l'utilisation de photographies, d'images, d'enregistrements vidéo ou vocaux permettant d'identifier une personne nécessite le recueil du consentement de la personne au titre du droit à l'image et à la voix du code civil.

Possibilité de recueillir un accord à visée éthique dans certaines situations

Dans certaines situations, l'utilisation d'un SIA ou la mise en œuvre d'une procédure particulière peuvent être susceptibles d'engendrer des risques spécifiques pour les patients. Cela peut être le cas, par exemple, en raison d'une situation de vulnérabilité de la personne, du contexte, des risques et des conséquences potentiels induits par le recours au SIA ou, à l'inverse, par son absence d'utilisation. Le professionnel ou la structure de soin peut alors envisager de recueillir un accord à visée éthique.

Cette démarche répond à des objectifs de loyauté, de transparence et de pédagogie vis-à-vis du patient. D'une part, elle contribue à garantir que la personne a été informée de cette utilisation et en a compris les implications. D'autre part, elle renforce la participation active du patient dans les prises de décisions concernant sa santé.

Cet accord peut être recueilli à l'écrit, par exemple par une case à cocher par le professionnel, ou à l'oral et ne nécessite pas de formalisme particulier. Lorsqu'il est mis en œuvre, une attention particulière doit être portée à la qualité de l'information délivrée, ainsi qu'à sa bonne compréhension par le patient.

Cet accord à visée éthique ne se substitue pas aux obligations légales applicables, ni aux règles de responsabilité, notamment médicale et ne permet pas d'y déroger.

En cas de préjudice, la responsabilité du professionnel ou de la structure de soins est susceptible d'être engagée, y compris lorsqu'un tel accord est recueilli.

6. Organisation des soins

Le déploiement d'un SIA est susceptible de modifier l'organisation locale des soins, notamment les flux, les processus et l'organisation du travail, la répartition des activités médicales et non médicales, les rôles et les compétences des différentes parties prenantes.

Le déploiement d'un SIA nécessite de vérifier son adéquation avec le contexte de soins avant et au cours de son utilisation en routine. Cette vérification est particulièrement importante lorsque le SIA n'a pas fait l'objet d'une validation externe sur un jeu de données indépendant. Le fournisseur doit être en mesure de fournir au déployeur la documentation décrivant notamment les données d'entraînement du SIA et la méthodologie employée. Cela peut être encadré contractuellement (cf. Fiche 2).

La vérification de l'adéquation au contexte de soins permet notamment de vérifier la pertinence du SIA par rapport au besoin et à la population locale, son adéquation technique, son intégration dans le flux de travail, son positionnement dans l'organisation des soins et ses performances dans le contexte réel.

Dans une démarche d'amélioration continue, le déployeur :

- analyse l'impact que le SIA peut avoir sur l'organisation des soins, et encadre les rôles et les responsabilités de chacun des utilisateurs, en particulier toute délégation de tâche ou d'activité en lien avec l'utilisation d'un SIA ;
- réalise le bilan du déploiement et de l'utilisation, par exemple via une évaluation scientifique.

Synthèse

Obligations principales

Le déployeur :

- respecte les règles d'exercice des professions réglementées par le CSP afin d'éviter toute requalification en exercice illégal ;
- réalise les formalités CNIL en cas d'utilisation de données pour une autre finalité que la prise en charge, notamment dans les phases de test ou les bilans.

Principes prioritaires

- Vérifier l'adéquation du SIA au contexte et au besoin
- Analyser l'impact organisationnel du SIA

6.1. Cadre légal et réglementaire

L'utilisation d'un SIA doit respecter les règles d'exercice des professions régies par le CSP, afin d'éviter toute requalification en exercice illégal. Cette utilisation doit également se conformer aux conditions prévues par le fournisseur, afin d'éviter une requalification du déployeur en fournisseur (cf. Fiche 7).

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, définies aux articles L.4011-1 à L.4011-5 du CSP. Ces règles précisent en particulier que :

- la délégation d'activité médicale est possible uniquement à un professionnel de santé dans le cadre d'un protocole de coopération local ou national ;
- le 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'organisation spécifiques ;
- le patient doit être informé des conditions de sa prise en charge.

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 (articles L.4161-1 à L.4161-6 du CSP).

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 CSS.

Le RIA n'impose pas au déployeur de mettre en place un contrôle des performances du SIA en amont de son déploiement. Toutefois, des phases de test sont fortement recommandées afin de vérifier l'adéquation du SIA au contexte. 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 (20). Ces tests doivent par ailleurs être distingués des essais en conditions réelles, qu'ils soient réalisés dans le cadre d'un bac à sable réglementaire ou non (article 58 du RIA et article 60 du RIA). Ces essais ne sont pas abordés dans ce guide.

Lorsque le déployeur traite des données personnelles de santé pour une autre finalité que la prise en charge des patients, ces traitements peuvent être soumis au régime de formalités préalables auprès de la CNIL, prévu aux articles 65 et suivants de la loi « informatique et libertés » (21).

6.2. Principes

★★★ Vérifier l'adéquation du SIA au contexte et au besoin

Le déployeur vérifie l'adéquation au contexte local du SIA avant son déploiement en routine clinique et son utilisation effective, aussi bien pour les SIA ayant le statut de DM ou DMDIV, que pour les SIA non-DM. Il s'agit de réaliser une vérification des performances du SIA et de son intérêt, selon les ressources du déployeur.

Ce contrôle permet d'évaluer l'intérêt et la performance du SIA dans le contexte local, notamment d'identifier des biais spécifiques à la population et de vérifier l'interopérabilité avec l'environnement technique. Cette vérification permet de repérer d'éventuelles difficultés d'utilisation ou d'intégration du SIA dans l'organisation des soins.

La vérification de l'adéquation peut inclure :

- l'examen des documents de contractualisation (cf. Fiche 2) pour vérifier l'adéquation avec la finalité d'usage, les données d'entraînement et de performance, la description des patients éligibles, les principes de fonctionnement, le dossier technique, etc. ;
- une phase de test d'utilisation avant la finalisation du contrat, période au cours de laquelle le fournisseur peut mettre à disposition un environnement de test interopérable avec les systèmes d'information du déployeur. Cette phase de test est encadrée contractuellement (cf. Fiche 2) ;
- une observation clinique structurée ;
- une analyse d'impact organisationnel ;
- un retour d'expérience des utilisateurs.

★★★ Analyser l'impact organisationnel du SIA

Le déployeur anticipe et analyse l'impact du SIA sur l'organisation des soins, notamment sur les processus de soins, les rôles et les compétences des acteurs, et sur la population générale. Le déployeur peut s'appuyer sur la cartographie des impacts organisationnels publiée par la HAS (22).

Cette analyse peut cibler :

- l'impact sur les processus de soins, sur les parcours de soins et de vie du patient ;
- l'impact sur les rôles professionnels et les compétences nécessaires aux acteurs ;
- l'impact sociétale en termes de sécurité sanitaire, d'inégalités sociales et d'accès aux soins, de relations sociales, d'enjeu médico-économique et d'empreinte écologique.

Encadrer et formaliser les rôles et les responsabilités des utilisateurs

Lors de l'intégration d'un SIA, le déployeur encadre et formalise les rôles et les responsabilités de chaque utilisateur. Les délégations de tâches ou d'activités induites par le SIA sont encadrées dans le respect des compétences professionnelles, des textes réglementaires et des protocoles de coopération autorisés.

Le déployeur formalise :

- les différents profils d'utilisateur concernés ;
- les actions et rôles attendus pour chaque profil d'utilisateur : usage technique du SIA (exécution, saisie), interprétation des résultats, décision clinique, supervision humaine, etc. ;
- les actes autorisés ou non selon leur statut : décision clinique, validation médicale, etc. ;
- les conditions de supervision ou de délégation lorsque plusieurs organisations de santé partagent un même SIA ;
- les modalités de formation attendues selon le profil d'utilisateur (cf. Fiche 3) ;
- l'organisation des soins à mettre en place et à respecter.

Cette formalisation peut donner lieu à une fiche d'information dédiée par profil d'utilisateur du SIA.

Réaliser un test d'utilisation sur un jeu de données locales

Pendant la phase de calibrage du SIA et avant son utilisation effective en routine clinique, le déployeur réalise un test d'utilisation sur un jeu de données local. Cette phase est encadrée contractuellement (cf. Fiche 2) et des formalités préalables auprès de la CNIL peuvent s'appliquer (21).

Ce jeu de données est représentatif de la population de patients prise en charge (genre, tranche d'âge, pathologie, etc.) et intègre des cas cliniques atypiques, par exemple les maladies rares. Une attention particulière est portée à la constitution de ce jeu de données locales, en particulier à la méthodologie mise en œuvre (biais, échantillonnage, représentativité, etc.) et au respect des règles de confidentialité.

Chaque fois que cela est possible, ces tests sont standardisés afin de pouvoir les répliquer si nécessaire, par exemple après une mise à jour importante du modèle d'apprentissage. Ces tests d'utilisation peuvent être réalisés par des sites pilotes ou des organismes territoriaux, tels que les CNP ou les tiers lieux d'expérimentation.

Réaliser des bilans du déploiement et de l'utilisation

Afin de vérifier l'adéquation du SIA au contexte local, le déployeur réalise régulièrement un bilan de son déploiement et de son utilisation par les professionnels.

Ces bilans s'inscrivent dans une démarche de suivi des performances et des usages réels dans une perspective d'amélioration continue (cf. Fiche 10).

Ces bilans peuvent prendre différentes formes, telles qu'une évaluation de la satisfaction des utilisateurs, l'identification d'éventuels décalages populationnels, la quantification de faux positifs et de faux négatifs, une évaluation avant/après sur des indicateurs de performance prédéfinis, une évaluation médico économique, une évaluation du temps passé sur une tâche, le suivi de la volumétrie et des régressions, l'identification des mésusages et des usages non prévus des utilisateurs, etc. Ces bilans sont, dans la mesure du possible, mutualisés ou partagés avec les organisations de santé et les professionnels qui ne disposent pas des ressources nécessaires pour les réaliser.

Le référent local dédié aux SIA peut être mobilisé pour réaliser ces bilans (cf. Fiche 1). Il évalue les indicateurs de performance à intervalles réguliers. Il trace et analyse a posteriori les incidents, les journaux techniques et les discordances entre le résultat du SIA et la décision de l'utilisateur (cf. Fiche 9 et Fiche 10). Ce travail de traçabilité et de vigilance permet de repérer les biais et d'évaluer les risques.

Encourager la production d'évaluations scientifiques

Le déployeur encourage la production de connaissances scientifiques sur les SIA.

Les évaluations scientifiques permettent d'objectiver l'intérêt d'un SIA (clinique, organisationnel, économique, humain, etc.), de mieux comprendre et mesurer leur impact sur l'organisation des soins ou encore d'améliorer la conception, le développement et le déploiement de ces outils.

Les organisations de santé ne disposant pas des ressources nécessaires pour conduire ces évaluations peuvent s'appuyer sur les publications scientifiques, les retours d'expérience existants ou le développement de partenariats avec des établissements de santé, des universités, des équipes de recherche ou des structures d'appui à la recherche et à l'innovation.

7. Au cours de l'utilisation

L'utilisation d'un SIA en contexte de soins nécessite de :

- respecter sa notice d'utilisation, son usage prévu par le fournisseur et les bonnes pratiques professionnelles ;
- contrôler les biais et limiter les risques ;
- maintenir une supervision humaine (cf. Fiche 8).

Synthèse

Obligations principales

Le déployeur :

- prend les mesures techniques et organisationnelles appropriées afin de garantir l'utilisation du SIA conformément à sa notice d'utilisation ;
- garantit le respect du principe de minimisation des données en sensibilisant le personnel.

Principes prioritaires

- Exercer son jugement en toute responsabilité pour prévenir les biais liés aux SIA
- Utiliser le SIA conformément à la notice

7.1. Cadre légal et réglementaire

7.1.1. Pour tous les SIA

Si le SIA n'est pas utilisé par le déployeur et son personnel conformément aux conditions fixées par le fournisseur, le déployeur risque d'être requalifié en fournisseur (article 25 du RIA).

Dès lors que l'utilisation d'un SIA implique le traitement de données personnelles, le déployeur du SIA, en tant que responsable de traitement et de son personnel, porte une attention particulière 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 dans la prise en charge n'a aucune incidence sur les droits reconnus aux usagers par le CSP, ni sur les obligations applicables à l'exercice des professions de santé prévues par le CSP.

7.1.2. Pour les SIA à haut risque

L'article 26 du RIA 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 ;
- veiller à ce que les données d'entrée utilisées pour le fonctionnement d'un SIA soient pertinentes et suffisamment représentatives ;
- confier le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires ;
- surveiller le fonctionnement du système au cours de son utilisation ;
- assurer la tenue des journaux techniques générés automatiquement, dans la mesure où ces journaux se trouvent sous leur contrôle.

7.2. Principes

★★★ Exercer son jugement en toute responsabilité pour prévenir les biais liés aux SIA

L'utilisateur est responsable de ses actes et décisions, même lorsque ceux-ci sont assistés par un SIA. Il exerce une supervision humaine et confronte l'avis du SIA à son propre raisonnement et à son expertise (cf. Fiche 8). L'utilisateur conserve un regard critique et une autonomie décisionnelle pour prévenir certains biais liés aux SIA. Il contextualise le résultat du SIA en regard de la situation personnelle du patient (contexte clinique, bio-psycho-social, environnemental et à ses choix), ainsi qu'à toute autre information pertinente pour la prise en charge. Le gain de temps ne justifie aucune réduction du niveau de supervision humaine.

Les biais et les risques liés à l'utilisation des SIA :

Dans le cadre de l'utilisation des SIA, deux types de biais principaux peuvent être distingués : les biais cognitifs et les biais algorithmiques.

Les **biais cognitifs** influencent le processus de décision humaine et peuvent conduire l'utilisateur à accorder une confiance excessive au SIA au détriment du jugement humain.

Par exemple :

- Le **biais de surconfiance** est la tendance des utilisateurs à accorder une confiance aveugle au SIA, ce qui peut entraîner des erreurs de jugement et l'empêcher de repérer les erreurs algorithmiques. Pour limiter ce biais, les utilisateurs exercent leur jugement critique.
- Le **biais d'ancrage** est la tendance des utilisateurs à s'appuyer excessivement, dans leur prise de décision, sur la première information reçue, qui peut être le résultat du SIA, plutôt que sur leur propre jugement clinique. Pour limiter ce biais, les utilisateurs exercent leur jugement avant d'utiliser le SIA.

- Le **biais d'automatisation** est la tendance des utilisateurs à privilégier systématiquement les résultats du SIA dans la prise de décision, au détriment de leur propre jugement. Ce biais est en lien avec la tendance naturelle des individus à privilégier les approches qui demandent le moins d'effort. Pour limiter ce biais, les utilisateurs prennent le temps d'exercer systématiquement leur jugement.
- Le **biais de tunnelisation attentionnelle** est la tendance des utilisateurs à avoir leur attention tellement focalisée sur un objectif, qu'ils n'entendent ni ne voient les signaux d'alerte qui devraient les amener à modifier leur approche, voire à l'arrêter avant que ne survienne un évènement indésirable associé aux soins (EIAS). Dans le cadre de l'utilisation d'un SIA, la fixation de l'attention sur le résultat du SIA peut entraîner une fermeture mentale aux autres possibilités, avec disparition de tout esprit critique. Pour limiter ce biais, les utilisateurs explorent les hypothèses diagnostiques alternatives (23).

Les **biais algorithmiques** influencent le résultat du SIA lorsque les données sur lesquelles son modèle est entraîné ne sont pas représentatives de la population cible (genre, âge, ethnie, type de pathologie, etc.) ou de qualité insuffisante. Ce manque de représentativité ou de qualité peut provoquer une dérive algorithmique et donner lieu à des erreurs de diagnostic ou de traitement. Pour limiter ce biais, une algorithmovigilance est mise en place (cf. Fiche 10). Les utilisateurs signalent les discordances entre le résultat du SIA et leur décision finale, et le déployeur vérifie régulièrement l'adéquation du SIA avec l'organisation des soins et le contexte local (cf. Fiche 6).

Par ailleurs, les SIA induisent d'autres risques spécifiques.

Par exemple :

- La **perte d'expertise humaine** peut survenir lorsque le SIA est utilisé pour compenser un manque de compétence humaine à défaut de former les individus à développer des compétences propres. Il peut s'agir, par exemple, de l'utilisation d'électrocardiogrammes (ECG) intégrant un SIA qui propose aux professionnels un premier diagnostic d'arythmie, sans les former à l'analyse autonome des tracés en première instance. Pour limiter ce risque, et afin de garantir la supervision humaine, les utilisateurs doivent être suffisamment compétents pour pouvoir exercer un regard critique sur le résultat du SIA et pour pouvoir exercer de façon autonome en cas d'indisponibilité du SIA (cf. Fiche 8).
- L'**intelligence artificielle fantôme**, ou en anglais « *shadow AI* », survient lorsque l'utilisation des SIA dans le cadre professionnel se fait sans autorisation institutionnelle préalable. L'intelligence artificielle fantôme expose le déployeur à des risques importants en termes de sécurité, de conformité réglementaire et de gestion des données. Pour limiter ce risque, la gouvernance met en place une cartographie des SIA déployés (cf. Fiche 1) et les utilisateurs sont formés (cf. Fiche 3).

★★★ Utiliser le SIA conformément à la notice

L'utilisateur utilise le SIA conformément à la notice d'utilisation et à la finalité d'usage prévue.

Il s'assure que :

- le patient relève du périmètre général d'utilisation prévu, notamment pour les systèmes conçus pour un type de population précis (âge, pathologie, contexte clinique, etc.) ;
- le patient ne présente pas de critères d'exclusion connus (antécédent, comorbidité, iatrogénie, etc.) ;
- 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 responsabilités correspondantes.

Vérifier la couverture de l'assurance responsabilité civile professionnelle

L'utilisateur vérifie auprès de son assurance responsabilité civile professionnelle (RCP) que l'usage des SIA est bien couvert dans le cadre de son activité.

Maîtriser les bonnes pratiques d'utilisation

L'utilisateur du SIA :

- est formé ou habilité à son utilisation (cf. Fiche 3) ;
- vérifie que sa pratique permet au SIA de fonctionner correctement, notamment lorsque des ajustements de pratique sont nécessaires. C'est par exemple le cas des SIA d'aide à la rédaction de comptes rendus médicaux sur la base d'enregistrements de la voix dont l'utilisation peut nécessiter d'oraliser une partie de l'examen clinique afin que le système enregistre les informations pertinentes pour générer le compte rendu ;
- vérifie la pertinence et minimise les données du patient transmises au SIA afin de préserver la confidentialité et d'assurer la sécurité des données. Par exemple, la transmission de données d'identification n'est, dans la majorité des cas, pas nécessaire pour le fonctionnement d'un SIA d'aide à la décision médicale ;
- met en perspective les caractéristiques du patient (données démographiques – genre, ethnie, âge – et plus largement les facteurs bio-psycho-sociaux) avec les biais algorithmiques identifiés et avec le contexte local (cf. Fiche 6) ;
- informe le patient sur le fonctionnement du SIA, ses risques et l'utilisation de ses données (cf. Fiche 4) ;
- identifie, trace et signale toute anomalie ou effet indésirable lié au SIA, ainsi que toute discordance entre le résultat du SIA et la décision clinique (cf. Fiche 9 et Fiche 10) ;
- connaît les scénarios et les procédures de fonctionnement en mode dégradé en cas d'indisponibilité du SIA (cf. Fiche 10).

8. Supervision humaine

La supervision humaine constitue un socle éthique, juridique et organisationnel fondamental pour le bon usage des SIA en santé. Il permet de s'assurer que toute décision médicale est prise sous la responsabilité du professionnel de santé. La mise en œuvre concrète de cette supervision humaine soulève toutefois plusieurs questions :

- quel acteur doit assurer cette supervision ?
- quelles compétences ou qualifications sont nécessaires ?
- dans quelles situations, à quel moment et selon quelles modalités, la supervision doit-elle être exercée ?

Mise au point sur les notions de décision automatisée (RGPD) et de contrôle humain (RIA)

Les notions de décision automatisée (RGPD) et de contrôle humain (RIA) sont étroitement liées mais ne se confondent pas. Le RGPD vise à garantir que les droits des personnes sont respectés là où le RIA entend garantir la qualité et la sécurité de l'usage du SIA. De plus, ces textes s'adressent à des acteurs différents. Le RGPD fixe des obligations à la charge des responsables de traitement de données personnelles, tandis que le RIA vise principalement le fournisseur de SIA et, à la marge, les déployeurs.

Ces deux réglementations prévoient des obligations distinctes qui poursuivent un objectif commun : assurer un encadrement adapté des SIA et des traitements de données personnelles associés à leur utilisation.

Le guide emploie la notion de « *supervision humaine* » qui comprend à la fois la notion d'intervention humaine du RGPD et celle de contrôle humain du RIA. Il s'agit d'un concept de travail qui n'engage pas les autorités rédactrices du guide, mais a pour objet de faciliter sa lecture.

Synthèse

Obligations principales

Toutes les décisions liées à l'utilisation d'un SIA doivent faire l'objet d'une supervision humaine et impliquent :

- une validation par le professionnel prenant en charge la personne (intervention humaine au titre du RGPD) ;
- la mise en œuvre d'un contrôle humain, par le fournisseur, proportionné à l'impact sur les soins (contrôle humain par le fournisseur au titre du RIA). À ce jour, il n'y a pas de standard sur les modalités de mise en place de ce contrôle humain qui doit être adapté, au cas par cas, au contexte dans lequel le SIA est déployé ;
- la formation du professionnel par le déployeur (contrôle humain au titre du RIA) (cf. Fiche 3).

Principes prioritaires

- Tracer et analyser régulièrement les incidents liés à l'utilisation du SIA
- Préserver explicitement l'indépendance et la liberté de décision du praticien
- Adapter le niveau de supervision humaine

8.1. Cadre légal et réglementaire

8.1.1. Les exigences de contrôle humain prévues par le RIA

Les fournisseurs de SIA à haut risque doivent intégrer, dès la conception des systèmes, 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 du RIA).

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

Les déployeurs sont responsables :

- d'assigner la supervision des SIA lors de leur utilisation à des personnes ayant la compétence, la formation, l'autorité et le soutien nécessaires (article 26 du RIA) ;
- de documenter les modalités de supervision humaine dans l'AIDF, le cas échéant (article 27 du RIA) ;
- de garantir que toute personne faisant l'objet d'une décision fondée sur les résultats d'un SIA à haut risque doit obtenir des explications claires et pertinentes sur le rôle joué par le SIA dans le processus décisionnel ainsi que les principaux éléments ayant conduit à cette décision (article 86 du RIA).

8.1.2. La protection contre les décisions automatisées prévue par le RGPD

Les décisions fondées entièrement sur un traitement automatisé des données, produisant des effets juridiques ou affectant significativement la personne concernée, sont par principe interdites, sauf si elles reposent sur le consentement explicite de la personne ou si un texte européen ou national les autorise (article 22 du RGPD). En dehors des dérogations mentionnées ci-dessus, toute décision nécessite une intervention humaine.

Les articles 13 à 15 du RGPD imposent au déployeur du SIA, en tant que responsable de traitement, de garantir aux personnes concernées :

- un droit à l'information sur l'existence d'une décision automatisée ;
- un droit à l'explicabilité, pour comprendre la logique et les critères utilisés par le SIA ;
- un droit à l'information sur les conséquences potentielles de la décision du SIA.

La Cour de justice de l'Union européenne a précisé que ces informations doivent être pertinentes, transparentes, compréhensibles et accessibles (24). Dans le cas des décisions partiellement automatisées, les modalités de l'intervention humaine et les garanties mises en place pour maîtriser les risques doivent, le cas échéant, être décrites dans l'AIPD.

Pour rappel, lorsqu'un SIA a recours à des données personnelles pour fonctionner, le déployeur est, dans la grande majorité des cas, qualifié de responsable du traitement mis en œuvre dans le cadre de cette utilisation.

8.1.3. Les dispositions prévues par le CSP

Le CSP dispose 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* » (article L.1111-4 du CSP) ;
- « *le médecin ne peut aliéner son indépendance professionnelle sous quelque forme que ce soit* » (article R.4127-5 du CSP) ;
- « *le médecin est libre de ses prescriptions qui seront celles qu'il estime les plus appropriées en la circonstance* » (article R.4127-8 du CSP).

8.1.4. Déclinaison du contrôle humain et de la protection contre les décisions automatisées dans le cadre du soin

À date et en l'état du droit, toute décision entièrement automatisée est interdite en matière de prise en charge sanitaire, les conditions prévues par l'article 22 du RGPD ne pouvant être remplies. Le RGPD précise qu'une décision entièrement automatisée est une décision « *fondée exclusivement sur un traitement automatisé [...] produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ».

En effet, aucun texte national ou européen ne reconnaît à l'utilisation d'un SIA la poursuite d'un motif d'intérêt public important ni n'autorise expressément la prise de décision automatisée dans un contexte de soins. Dans ce contexte, les conditions de validité du consentement de la personne (liberté, information préalable, etc.) ne sont généralement pas réunies.

8.1.5. Actions à réaliser systématiquement

Les résultats du SIA sont systématiquement revus par le professionnel de santé prenant en charge la personne avant d'être versés dans le dossier patient (cf. Fiche 9).

Dans le cas particulier d'un SIA d'aide à la rédaction de comptes rendus, la validation du document relève de la responsabilité du professionnel ayant participé à la consultation ou à la réalisation de l'acte, par exemple de la secrétaire médicale ou du professionnel de santé. En effet, une personne absente lors de la prise en charge ne dispose pas des éléments nécessaires pour vérifier l'exactitude du résultat d'un SIA et identifier d'éventuelles hallucinations ou omissions.

8.2. Principes

8.2.1. Garantir la traçabilité

★★★ Tracer et analyser régulièrement les incidents liés à l'utilisation du SIA

Afin de garantir la meilleure qualité et sécurité des soins, le déployeur trace et analyse régulièrement les incidents liés à l'utilisation des SIA afin d'ajuster finement les modalités de supervision humaine en fonction des résultats observés, par exemple en renforçant la supervision pour certains types d'erreurs récurrentes. Ces analyses peuvent être partagées à l'échelle du territoire (ARS, GRADeS, etc.).

Pour les SIA à haut risque, si l'utilisation d'un SIA conformément à sa notice est susceptible de présenter un risque, il convient d'en informer, sans retard injustifié, le fournisseur ainsi que l'autorité de surveillance du marché compétente. En cas d'incident grave, cette information doit être transmise immédiatement (cf. Fiche 10).

Tracer l'utilisation d'un SIA dans le cadre des soins

Le déployeur assure la traçabilité de l'utilisation d'un SIA. Cette traçabilité peut se matérialiser de différentes manières :

- au sein des traces fonctionnelles du dossier patient, qui permettront de documenter l'accès du SIA aux données personnelles du patient dans ce dossier (cf. Fiche 9) ;
- par une mention dédiée au sein des résultats d'un SIA qui sont remis au patient, notamment dans les comptes rendus (cf. Fiche 4).

Assurer et documenter la formation des professionnels réalisant la supervision humaine

La supervision humaine suppose que l'ensemble des professionnels utilisant un SIA sont formés et disposent de l'ensemble des informations, des compétences et des moyens nécessaires pour effectuer correctement leur tâche, quelle que soit la validation scientifique du SIA. Dans cette perspective, des formations à l'utilisation des SIA sont régulièrement proposées pour sensibiliser et familiariser le personnel en charge (cf. Fiche 3).

Le déployeur veille à documenter la participation aux formations des professionnels utilisant un SIA (cf. Fiche 3). Cette documentation précise, pour chaque professionnel réalisant la supervision humaine, l'intitulé et le contenu de la formation suivie, sa date de réalisation, l'organisme l'ayant dispensée et s'appuie, le cas échéant, sur une attestation ou un justificatif de suivi. Elle permet de démontrer que les professionnels concernés disposent effectivement des compétences requises pour exercer la supervision humaine, et non uniquement que la formation leur a été proposée. Elle est actualisée à chaque évolution significative du SIA.

8.2.2. Déterminer et mettre en œuvre la supervision humaine adéquate

★★★ Préserver explicitement l'indépendance et la liberté de décision du praticien

Afin de préserver l'indépendance et l'expertise professionnelle des praticiens, tout en excluant la prise de décision automatisée, le déployeur garantit explicitement la liberté de décision du professionnel de santé face aux propositions du SIA, conformément au Code de déontologie médicale.

Le déployeur veille à :

- prévenir tout phénomène de « dilution de responsabilité » lié à l'utilisation du SIA, en rappelant clairement que la responsabilité finale de la décision demeure humaine ;
- encourager les professionnels à exercer systématiquement leur propre jugement clinique, tout en justifiant et traçant les décisions prises, y compris lorsque celles-ci s'écartent des résultats du SIA ;
- définir, lorsque cela est pertinent, une procédure de gestion des situations de désaccord du professionnel avec le SIA afin de promouvoir la réflexivité clinique. En complément du signalement auprès du fournisseur, et des autorités nationales compétentes le cas échéant, un recensement interne de ces situations ou des retours d'expérience (RETEX) peut être effectué, notamment pour identifier d'éventuels biais ou dysfonctionnements du SIA.

★★★ Adapter le niveau de supervision humaine

La supervision humaine est systématique Le déployeur met en œuvre une supervision humaine pour l'ensemble des SIA utilisés en contexte de soins, y compris les SIA à risque limité (soumis au chapitre IV du RIA).

Le déployeur adapte les modalités de supervision humaine au niveau de risque associé, à l'utilisation prévue du SIA et à sa place dans l'organisation des soins, notamment au moyen :

- d'une supervision intégrale consistant en une revue humaine systématique de 100 % des résultats d'un SIA, lorsque ceux-ci peuvent conduire à des décisions ayant un impact important sur la prise en charge du patient, comme la réalisation d'un acte invasif. Pour ces situations, le déployeur met en place une organisation adaptée afin d'appliquer aux SIA n'ayant pas le statut de DM ou de DMDIV les mêmes exigences de validation et de vigilance qu'aux SIA ayant le statut de DM ou de DMDIV. Cette organisation permet de limiter tout risque de dégradation de la qualité et de la sécurité des soins ;
- d'une supervision allégée pour les utilisations non-cliniques du SIA ou n'impliquant pas de décision directe pour le patient. Cette supervision prend la forme d'une validation et d'une relecture des résultats d'un SIA afin de vérifier leur pertinence et de repérer d'éventuelles erreurs (ex : relecture d'un document reformaté).

Définir des modalités de supervision humaine dans les protocoles

Le déployeur définit clairement les modalités de supervision humaine à mettre en œuvre dans des protocoles internes, notamment lorsque les résultats d'un SIA sont susceptibles de conduire à des décisions à fort impact pour le patient et sa prise en charge, par exemple en mentionnant clairement qu'aucune décision relative à un traitement ou de diagnostic n'est laissée à la seule appréciation d'un SIA.

Ces protocoles cliniques s'appuient sur les conditions d'utilisation définies par le fournisseur du SIA et précisent notamment les seuils d'alerte ainsi que les responsabilités des différents intervenants. Les sociétés savantes et les CNP peuvent jouer un rôle majeur dans l'élaboration de ces protocoles.

L'exemple prospectif des SIA de tri ou de dépistage :

Les performances atteintes par certains SIA permettent d'envisager de nouvelles organisations de soins dans lesquelles seuls certains résultats feraient l'objet d'une supervision humaine, notamment à des fins de dépistage ou de priorisation. À titre d'exemple, les cas identifiés par le SIA comme "ne présentant pas la pathologie recherchée" pourraient ne pas être revus de façon systématique par un professionnel de santé. À ce jour, le cadre réglementaire applicable interdit toutefois le recours aux prises de décision entièrement automatisées, sans supervision humaine, produisant des effets juridiques ou un impact significatif sur les personnes. Dans ce contexte, une organisation des soins reposant sur l'absence de supervision humaine, y compris dans certains cas particuliers, est contraire à la réglementation et expose le professionnel ou l'établissement de santé à un risque juridique, en particulier si le l'utilisation du SIA se substitue à une intervention humaine jusqu'alors bien établie.

Pour autant, les SIA offrent par exemple l'opportunité de développer de nouvelles stratégies de dépistage à large échelle. Ces évolutions soulèvent des enjeux juridiques, éthiques et sociétaux qui appellent un débat collectif afin de déterminer les usages pouvant être admis et les garanties qui devraient les accompagner.

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

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

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

- la définition et à la mise en œuvre d'une stratégie nationale organisée, notamment pour le dépistage, impliquant l'utilisation d'un SIA ne creusant pas les inégalités de soins ;
- une implication forte des conseils nationaux professionnels (CNP), des représentants des spécialités médicales concernées et des représentants de patients qui devront être sollicitées pour avis ;
- une réflexion sur la pertinence d'étendre les dispositifs d'indemnisation des accidents médicaux non fautifs aux dommages résultant de résultats erronés liés à l'utilisation d'un SIA, lorsque ces dommages répondent aux conditions ouvrant droit à une indemnisation par l'Office National d'Indemnisation des Accidents Médicaux des Affections Iatrogènes et des Infections Nosocomiales (ONIAM).

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

9. Traçabilité des usages et des résultats

La traçabilité rigoureuse des usages et des résultats des SIA permet de documenter les conditions de leur utilisation et de soutenir les démarches d'évaluation et de vigilance, tout en contribuant à la sécurité des données et des systèmes d'information.

La notion de « traçabilité » des SIA, telle qu'utilisée dans ce guide, repose notamment sur :

- la conservation des résultats d'un SIA, qu'ils soient pris en compte par le professionnel ou non. Les résultats d'un SIA sont les sorties produites par un SIA telles que des prédictions, des contenus ou des recommandations en lien avec une décision clinique ou une prise en charge (25) ;
- la conservation des données d'un SIA utilisées pour son fonctionnement ;
- l'identification de l'utilisation d'un SIA dans le parcours de soins de la personne, ainsi que les décisions associées ;
- la mise en œuvre de mesures de journalisation pour assurer la traçabilité des accès aux systèmes d'informations du traitement des données personnelles (26). La journalisation constitue une mesure de sécurité importante encouragée systématiquement par la CNIL. Les données de journalisation doivent faire l'objet d'analyses automatiques permettant la détection rapide d'utilisations inappropriées des données ou de comportements anormaux.

Ce guide a vocation à attirer l'attention sur des points spécifiques et ne remplace pas les exigences ou recommandations existantes propres aux systèmes d'informations.

Synthèse

Obligations principales

Le déployeur :

- conserve les journaux placés sous son contrôle ;
- détermine une durée de conservation adaptée à la finalité poursuivie et à celles prévues par le CSP ;
- recourt au service d'un prestataire certifié HDS, le cas échéant.

Principes prioritaires

- Intégrer la traçabilité comme outil de prévention des risques
- Conserver systématiquement les résultats du SIA

9.1. Cadre légal et réglementaire

9.1.1. Pour tous les SIA

Le RIA impose au fournisseur plusieurs obligations en matière de traçabilité, visant notamment à :

- garantir la transparence du SIA vis-à-vis des déployeurs et des personnes ;
- faciliter le suivi de la qualité, des performances et de la sécurité du SIA ;
- permettre au déployeur d'assurer le suivi de l'utilisation du SIA dans des conditions réelles de fonctionnement.

Le RGPD prévoit une obligation générale de sécurité des traitements de données personnelles (article 5.1.f du RGPD et article 32 du RGPD). Cette exigence s'applique tant aux déployeurs du SIA, en tant que responsables de traitement, qu'à leurs sous-traitants, notamment les fournisseurs de SIA.

Pour plus de précisions sur les mesures de sécurité applicables aux données personnelles, il convient de se reporter notamment au Guide de la sécurité des données personnelles de la CNIL dans sa version la plus récente, ainsi qu'aux éventuelles recommandations sectorielles adoptées par celle-ci (27).

9.1.2. Pour les SIA à haut risque

Pour les SIA à haut risque, le RIA prévoit à la charge du fournisseur les obligations suivantes :

- la mise en place d'un enregistrement automatique des événements, sous forme de journaux, tout au long du cycle de vie du SIA (article 12 du RIA) ;
- l'élaboration d'une notice d'utilisation contenant notamment une description des mécanismes du SIA permettant aux déployeurs de collecter, de stocker et d'interpréter correctement les journaux (article 13.3.f du RIA) ;
- la conservation des journaux pendant une durée adaptée à la finalité du SIA à haut risque et, dans tous les cas, pendant au moins 6 mois (article 19 du RIA). Les déployeurs de SIA à haut risque sont soumis à une obligation similaire à celle prévue à l'article 19 du RIA, dès lors que les journaux sont « sous leur contrôle ».

9.1.3. Pour les SIA à risque limité

Pour les SIA à risque limité (soumis au chapitre IV du RIA), les fournisseurs 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* » (article 50 du RIA). Si cette obligation ne relève pas directement du déployeur, celui-ci doit néanmoins veiller au respect de ces exigences de transparence lors de l'utilisation du SIA.

La Commission européenne a par ailleurs élaboré un code de bonnes pratiques relatif à la transparence des résultats d'un SIA, qui précise les modalités d'application des obligations de transparence prévues à l'article 50 du RIA (25).

9.1.4. Conservation des données d'entrée et des résultats d'un SIA

Lorsque les données d'entrée, telles que définies à l'article 3 du RIA, et les résultats du SIA sont intégrés ou conservés dans le dossier patient, ils sont soumis aux règles de conservation applicables au dossier patient prévues par le CSP.

Conformément à l'article R.1112-7 du CSP, le dossier patient est conservé pendant une durée de 20 ans à compter de la date du dernier séjour ou de la dernière consultation externe du patient au sein de l'établissement. 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 moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant 10 ans à compter de la date du décès.

L'article R.4127-45 du CSP prévoit une durée de conservation similaire s'agissant des dossiers mis en œuvre par des médecins, quelle que soit leur modalité d'exercice professionnel.

Lorsque les données liées à l'utilisation d'un SIA (données d'entrée, telles que définies à l'article 3 du RIA) ou les résultats du SIA ne sont ni intégrés au dossier patient ni conservés dans celui-ci, aucun texte n'impose de durées minimales ou maximales de conservation. Le principe selon lequel les données ne doivent pas être conservées pendant une durée excédante celle nécessaire aux finalités pour lesquelles elles sont traitées (article 5.1.e du RGPD), doit être respecté et apprécié au cas par cas.

Lorsque les données d'entrée ou les résultats d'un SIA contiennent des données de santé à caractère personnel qui sont conservées ou stockées par un organisme autre que le déployeur, par exemple par le fournisseur du SIA ou un autre prestataire, cette conservation doit être assurée par un HDS certifié au sens de l'article L.1111-8 du CSP.

9.2. Principes

★★★ Intégrer la traçabilité comme outil de prévention des risques

La traçabilité constitue un outil de prévention des risques et un support à la redevabilité des professionnels en cas de litige ou de contrôle réglementaire. Elle repose notamment sur une journalisation, conformément aux recommandations de la CNIL, ainsi que sur une revue régulière des données de traçabilité produites.

Le déployeur :

- clarifie et formalise les responsabilités de chaque acteur en matière de traçabilité (éditeur, professionnels de santé, services qualité et informatique) ;
- intègre systématiquement la traçabilité (« IA utilisée : oui/non ») dans les procédures internes (check-lists qualité, validation des dossiers) ;
- trace la décision du professionnel, le désaccord ou non avec les résultats d'un SIA, ainsi que la justification associée ;
- veille à la génération automatique par le SIA de journaux techniques (logs) détaillant chaque analyse (date, heure, identifiant du cas, résultats, utilisateur) en précisant, le cas échéant, le professionnel à l'origine de la sollicitation du SIA ;

- garantit contractuellement l'accès de l'organisation de santé aux journaux techniques, y compris lorsque le SIA est hébergé chez le fournisseur par une solution « *cloud* » ou "en nuage" (cf. Fiche 2) ;
- anticipe les éventuelles évolutions des exigences nationales relatives à la remontée d'informations sur les incidents impliquant les SIA, notamment si une base nationale de signalement est créée.

★★★ Conserver systématiquement les résultats du SIA

Les résultats d'un SIA (rapports, annotations, images, etc.) sont systématiquement conservés par le déployeur dans une rubrique dédiée à l'utilisation du SIA au sein du dossier patient. Ces résultats sont conservés selon les mêmes modalités et pour la même durée que les autres données du dossier patient.

Conserver la notice d'utilisation du SIA

Le déployeur conserve une copie de la notice d'utilisation du SIA ainsi que ses versions successives. Elles constituent un support essentiel à une utilisation conforme et sécurisée. Le fournisseur transmet au déployeur une notice d'utilisation complète lui permettant d'interpréter les résultats du SIA et de les utiliser de manière appropriée (article 13 du RIA).

Lorsque cette notice est mise à disposition par le fournisseur via un site internet, chaque modification apportée doit être facilement identifiable par le déployeur et être conservée dans un format pérenne et facilement accessible.

Lorsque la notice d'utilisation du SIA fait l'objet de mises à jour successives, la date de chaque version doit être est précisée, en particulier lorsque les évolutions du SIA sont significatives.

Dès l'acquisition du SIA, le déployeur prévoit contractuellement les modalités de traçabilité et d'accès à la notice d'utilisation et à ses différentes versions, ainsi que les modalités selon lesquelles le fournisseur l'informera en cas de mise à jour (cf. Fiche 2).

Identifier les résultats d'un SIA grâce à un marquage spécifique

Le déployeur veille à ce que le fournisseur du SIA ait mis en place un marquage spécifique, par exemple un marquage informatique ou un filigrane. Cette vérification permet de garantir la mise en œuvre effective des obligations de marquage des résultats d'un SIA à risque limité, soumis au chapitre IV du RIA (article 50.2 du RIA). Le marquage doit être visible, compréhensible et appliqué systématiquement à l'ensemble des résultats du SIA. Le marquage permet d'en identifier l'origine et de les distinguer clairement des autres informations figurant dans le dossier patient.

10. Gestion de la qualité et vigilances

Le déploiement d'un SIA en contexte de soins nécessite sa maintenance, un suivi de sa performance, une gestion des vigilances et les mesures correctives associées, le respect de sa conformité et l'anticipation de son indisponibilité.

La mise en œuvre de procédures adaptées vise à maintenir, dans la durée, un niveau de sécurité et de performance compatible avec les enjeux de la prise en charge des patients, à prévenir les incidents et à garantir la continuité des activités. La coopération entre l'utilisateur, le déployeur et le fournisseur est nécessaire pour cette mise en œuvre.

Synthèse

Obligations principales

Le déployeur ou l'utilisateur :

- veille à la conformité du traitement de données lié à un SIA dès sa première utilisation et de manière régulière ;
- veille à la mise en place de mesures de sécurité adaptées à la sensibilité des données et aux risques ;
- les cas échéant, notifie les violations de données et en informe les personnes concernées ;
- déclare les événements indésirables graves associés aux soins (EIGS) ;
- déclare les incidents graves, et réalise la matériovigilance ou la réactovigilance des SIA ayant le statut de DM ou DMDIV ;
- déclare les incidents graves liés aux SIA à haut risque.

Principes prioritaires

- Réaliser le suivi des performances
- Organiser un circuit de vigilance et de signalement des incidents pour les SIA, qu'ils soient DM, DMDIV ou non
- Organiser la gestion des mises à jour

10.1. Cadre légal et réglementaire

10.1.1. Gestion de la qualité

Parmi les obligations à la charge du déployeur en tant que responsable de traitement, celui-ci est tenu de veiller à la confidentialité, à l'intégrité et à la disponibilité des données personnelles qu'il traite (article 5 du RGPD et article 32 du RGPD).

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 (article 33 du RGPD) ;
- à l'information des personnes concernées (article 34 du RGPD).

Les déployeurs sont invités à consulter le site web de la CNIL en ce qui concerne :

- les mesures de sécurité à mettre en œuvre pour la protection des données personnelles (27) ;
- la conduite à tenir en cas de violations de données personnelles (28).

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 (article 20 du RIA). Cette démarche peut être menée en collaboration avec le déployeur à l'origine du signalement, afin d'assurer une réponse rapide et coordonnée face aux risques.

Le déployeur est tenu de surveiller le fonctionnement des SIA à haut risque utilisés sur la base de la notice d'utilisation transmise par le fournisseur. S'il constate que le fonctionnement présente un risque pour la santé, la sécurité ou les droits fondamentaux des personnes, ou a des raisons de le croire, il informe sans retard le fournisseur, le distributeur et l'autorité de surveillance du marché (article 26 du RIA).

10.1.2. Vigilances

10.1.2.1. Pour tous les SIA :

Les professionnels de santé et les responsables de structures sanitaires et médico-sociales ont une obligation réglementaire (article L.1413-14 du CSP) de déclarer les événements indésirables graves associés aux soins (29).

Événements indésirables graves associés aux soins (EIGS)

Un EIGS est un évènement inattendu au regard de l'état de santé et de la pathologie de la personne et dont les conséquences sont le décès, la mise en jeu du pronostic vital, la survenue probable d'un déficit fonctionnel permanent, y compris une anomalie ou une malformation congénitale (article R.1413-67 du CSP).

10.1.2.2. Pour les SIA ayant le statut de DM ou DMDIV :

Le RDM et le RDIV, 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 vigilances. À ce titre, les SIA ayant le statut de DM ou de DMDIV doivent faire l'objet de déclaration de matériovigilance ou de réactovigilance, au même titre que les autres DM et DMDIV.

La surveillance des DM et des DMDIV relève de la compétence de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM). 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.

En ce qui concerne les autres incidents, il n'y a pas d'obligation de signalement mais l'utilisateur *« 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* » (article L.5212-2 du CSP). Ainsi, les utilisateurs sont incités à les transmettre au fournisseur afin qu'il puisse exercer ses activités de surveillance après commercialisation.

Le circuit de vigilance des SIA utilisés en contexte de soins n'ayant pas le statut de DM ou de DMDIV, ou n'étant pas classés à haut risque, n'est pas encore formalisé et reste à clarifier.

10.1.2.3. Pour les SIA à haut risque :

L'article 73 du RIA impose 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.

Incident grave :

Selon l'article 3.49 du RIA, un « *incident grave* » est un incident ou dysfonctionnement d'un SIA entraînant directement ou indirectement :

a) le décès d'une personne ou une atteinte grave à la santé d'une personne ;

b) une perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques ;

c) la violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux ;

d) un dommage grave à des biens ou à l'environnement.

10.1.3. Conformité et mesures correctives

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 de prendre immédiatement les mesures correctives nécessaires (article 20 du RIA). Ces mesures peuvent inclure la mise en conformité du SIA, son retrait, sa désactivation ou son rappel. Le fournisseur doit également informer, le cas échéant, les déployeurs concernés.

10.1.4. Conformité et mesures de sécurité des données à caractère personnel

Lorsque le fonctionnement d'un SIA implique le traitement de données personnelles, le déployeur, en tant que 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 (article 25 du RGPD).

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 déployeur, en tant que responsable de traitement, celui-ci est tenu de veiller à la confidentialité, à l'intégrité et à la disponibilité des données personnelles qu'il traite (article 5 du RGPD et article 32 du RGPD).

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 (article 33 du RGPD) ;
- à l'information des personnes concernées (article 34 du RGPD).

Les déployeurs sont invités à consulter le site web de la CNIL en ce qui concerne :

- les mesures de sécurité à mettre en œuvre pour la protection des données personnelles (27) ;
- la conduite à tenir en cas de violations de données personnelles (28).

10.2. Principes

★★★ Réaliser le suivi des performances

Le déployeur réalise un suivi des performances du SIA adapté à sa finalité, à son niveau de risque et à son contexte d'utilisation. Cette démarche s'inscrit dans une logique de surveillance continue du SIA tout au long de son cycle de vie en conditions réelles. Elle vise à détecter une dégradation des performances, l'émergence de biais, des difficultés d'utilisation et des effets inattendus et de favoriser le maintien de la pertinence du SIA. Cette démarche inclut une algorithmovigilance du SIA. Des contrôles sont réalisés dès que nécessaire, en particulier en cas de mise à jour majeure du SIA ou de changements de l'environnement clinique, de l'organisation des soins, de la population de patients concernés, etc.

Algorithmovigilance :

C'est la vigilance consacrée au modèle algorithmique du SIA. Cette démarche s'inscrit dans une logique de surveillance continue du SIA tout au long de son cycle de vie et en particulier après son déploiement en routine clinique.

Les contrôles de performance peuvent s'appuyer sur différentes méthodes : des analyses d'échantillons de dossiers, des audits ciblés, des analyses d'incidents ou des suivis d'indicateurs, etc.

Ces indicateurs portent, par exemple, sur :

- les résultats en pratique (taux de faux positifs, taux de faux négatifs) ;
- la fréquence des écarts entre le résultat du SIA et les avis des professionnels utilisateurs ;
- les disparités au sein de la population cible, et entre la population cible et les données sur lesquelles le modèle du SIA est entraîné (dérives algorithmiques) ;
- les incidents ou dysfonctionnements signalés ;
- les alertes non suivies ;
- le taux d'utilisation effective ;
- les retours et difficultés d'utilisation signalés par les utilisateurs.

Lorsque qu'une baisse significative des performances du SIA est observée, le déployeur en analyse les causes, met en œuvre des mesures correctrices et en informe, sans retard injustifié, le fournisseur.

Des audits ciblés et réguliers sont réalisés, si possible, en particulier pour les SIA à haut risques, afin d'éviter toute omission critique due au biais de surconfiance en le SIA. Ces audits visent aussi à évaluer comment est utilisé le SIA en pratique et l'impact du SIA sur l'organisation des soins et sur les pratiques professionnelles (cf. Fiche 6). Dans le cadre d'un établissement de santé, le résultat de ces audits est partagé avec la gouvernance de l'établissement, les professionnels utilisateurs et la commission des usagers. Ces analyses peuvent être partagées à l'échelle du territoire (ARS, GRADeS, etc.).

★★★ Organiser un circuit de signalement des incidents pour les SIA, qu'ils soient DM, DMDIV ou non

Pour les SIA ayant le statut de DM ou de DMDIV, le déployeur désigne un responsable des déclarations de vigilance afin de respecter les principes et les obligations du CSP existants en matière de vigilance pour les SIA ayant un statut de DM ou de DMDIV. Pour les professionnels exerçant en libéral, ces déclarations leur incombent directement. Les déclarations à l'ANSM sont obligatoires pour les incidents graves des DM ou DMDIV.

Pour les SIA n'ayant pas le statut de DM ni de DMDIV, un circuit de signalement des incidents est mis en place afin de faciliter les identifications, corrections et remontées nationales éventuelles. Ce circuit peut intégrer le circuit général de signalement des incidents au sein de l'organisation de santé.

Pour les SIA ne relevant pas du statut de DM ou DMDIV, le déployeur :

- crée ou adapte les procédures internes de gestion des incidents (cf. Fiche10) ;
- crée ou adapte les formulaires de signalement d'événements indésirables ;
- sensibilise les professionnels de santé à l'identification, la gestion et le signalement systématique des erreurs ou dysfonctionnements (cf. Fiche 3) ;
- prévoit la désactivation rapide ou l'arrêt immédiat en cas de détection d'incident grave, en respectant les procédures établies de mode dégradé ;
- prévoit des modes dégradés en cas d'indisponibilité.

L'analyse des événements indésirables en lien avec les SIA est abordée au sein de la Commission médicale d'établissement, de la Commission des usagers, la direction de la qualité et le comité de gestion des risques. Les outils existants comme les revues de morbi-mortalité ou les grilles ALARM peuvent être mobilisés pour cette analyse (30).

★★★ Organiser la gestion des mises à jour

Le déployeur réalise les mises à jour d'un SIA dans le cadre défini contractuellement avec le fournisseur (cf. Fiche 2). Les mises à jour peuvent notamment concerner le modèle algorithmique, l'interface utilisateur, l'infrastructure technique, l'intégration au système d'information, l'interopérabilité et la correction de dysfonctionnements.

Le déployeur :

- contractualise la planification des mises à jour en dehors des horaires de travail afin de minimiser l'impact sur l'activité clinique en privilégiant, par exemple, les créneaux de nuit ou de week-end (cf. Fiche 2) ;
- exige dans le contrat avec le fournisseur la réception d'une information préalable à toute mise à jour importante du SIA qui précise la nature des modifications (cf. Fiche 2) ;
- désigne un responsable du suivi des mises à jour du SIA, par exemple le référent local du SIA le responsable des systèmes d'information ou un ingénieur biomédical (cf. Fiche 1) ;
- dispose, si possible, d'un environnement de test permettant de vérifier, avant la mise à jour du SIA, l'adéquation de cette nouvelle version au contexte de soins (cf. Fiche 6) ;
- met à jour les supports de formation destinés aux utilisateurs lorsque nécessaire (cf. Fiche 3) ;
- réalise un contrôle des performances du SIA, en particulier après une mise à jour importante ;
- actualise la documentation décrivant les performances observées et les limites du SIA ;
- trace l'ensemble des mises à jour techniques et algorithmiques du SIA incluant notamment, la date, la version, la nature des modifications, les objectifs poursuivis et les résultats attendus (cf. Fiche 9).

En cas de défaut de mise à jour relevant des obligations du fournisseur, sa responsabilité pourrait être engagée, notamment en cas de dommage ou d'incident. Si le déployeur n'effectue pas la mise à jour prévue par le fournisseur, il pourrait être tenu responsable en cas de dommage ou d'incident.

Formaliser une procédure de gestion de la maintenance partagée

La maintenance est une obligation partagée entre le fournisseur et le déployeur du SIA. Elle peut être encadrée contractuellement (cf. Fiche 2). Les responsabilités et les actions qui reviennent à chaque acteur mobilisé sont alors clairement identifiées et explicitées.

Une procédure interne formalise :

- le plan de suivi des performances (indicateurs, fréquences d'évaluation, suivi des résultats) ;
- le processus de déclaration des vigilances (formulaires, canaux dédiés, responsables) ;
- le plan de gestion des mises à jour (qui, quand, comment) ;
- le plan de continuité d'activité (PCA) et le plan de reprise d'activité (PRA) en cas d'indisponibilité du SIA.

Anticiper l'indisponibilité du SIA

Le niveau de service type SLA, encadré contractuellement, fixe les délais d'intervention et de résolution d'incidents. Dès la contractualisation, le déployeur anticipe l'indisponibilité du SIA et prévoit des modes dégradés selon leur niveau de criticité clinique afin d'assurer la continuité de l'activité (cf. Fiche 2).

Le déployeur :

- prend en compte les SIA dans le plan de continuité d'activité (PCA) et le plan de reprise d'activité (PRA) ;
- prévoit un mode dégradé de fonctionnement en cas d'indisponibilité du SIA avec des scénarios et procédures établies en lien avec les utilisateurs, en particulier pour les SIA ayant le statut de DM ou DMDIV et pour les SIA ayant un impact important sur la prise en charge des patients ;
- forme les utilisateurs à ces scénarios et à ces procédures, par exemple avec des simulations de mode dégradé (cf. Fiche 3) ;
- prévoit des sauvegardes régulières dont la fréquence est à adapter en fonction de la criticité du SIA. Le déployeur conserve ces sauvegardes selon des mesures de sécurité appropriées et conformes au cadre juridique applicable.

11. Fin du cycle de vie

La fin du cycle de vie d'un SIA correspond à l'arrêt définitif de son utilisation au sein d'une organisation de santé. Elle peut résulter d'une décision du déployeur, du fournisseur ou d'une autorité compétente. La fin du cycle de vie du SIA doit être anticipée dès la contractualisation avec le fournisseur (cf. Fiche 2).

Cette anticipation permet d'assurer la continuité des soins, la protection des données, ainsi que la maîtrise des risques liés à son arrêt ou à son remplacement. Elle implique notamment de prévoir les conditions de décommissionnement, de réversibilité et de transition, conformément aux exigences réglementaires applicables.

Synthèse

Obligations principales

Le déployeur :

- détermine le devenir des données personnelles dont le traitement a été confié au sous-traitant au terme de la prestation ;
- conclut avec le prestataire HDS un contrat contenant les engagements requis pas le CSP, le cas échéant.

Principes prioritaires

- Anticiper et organiser la fin du cycle de vie du SIA
- Prévoir des clauses de réversibilité

11.1. Cadre légal et réglementaire

11.1.1. Le RIA

Le RIA ne prévoit pas d'obligation pour le déployeur applicable à la fin de la période de déploiement du SIA. Il impose toutefois au fournisseur d'informer les déployeurs du SIA de toute décision de retrait, de désactivation ou de rappel (article 20 du RIA).

11.1.2. Le RGPD

Lorsque le traitement de données personnelles lié à l'utilisation d'un SIA implique un sous-traitant, le contrat associé est tenu de déterminer, dès sa conclusion et selon le choix du responsable de traitement, le devenir des données traitées (article 28.3.g du RGPD).

La fin du cycle de vie d'un SIA dont le fonctionnement implique un traitement de données personnelles ne doit pas être confondue avec le principe de limitation des durées de conservation prévu par le RGPD. En effet, ces durées doivent être fixées au regard des finalités pour lesquelles les données sont traitées et des exigences réglementaires applicables.

À cet égard, l'utilisation d'un SIA en contexte de soins vise à générer, à partir de données d'entrée, des résultats ayant comme vocation principale d'intégrer le dossier patient.

11.1.3. Le CSP

Lorsque l'utilisation d'un SIA implique l'intervention d'un prestataire HDS certifié, le contrat conclu avec cet acteur doit notamment contenir les engagements prévus à l'article R.1111-11 du CSP.

11.2. Principes

★★★ Anticiper et organiser la fin du cycle de vie du SIA

La fin du cycle de vie du SIA est anticipée dès la contractualisation avec le fournisseur afin de préciser les conditions de la désinstallation ou du décommissionnement (cf. Fiche 2). Cette anticipation permet de sécuriser le processus de désinstallation, d'éviter toute situation de dépendance disproportionnée à un prestataire, de faciliter un éventuel changement de fournisseur, et de préserver la continuité des activités.

Le déployeur anticipe :

- les enjeux de conservation légale et de sécurité des données ;
- les conditions de restitution, de suppression ou de migration des données ;
- les conditions d'archivage des données conservées ;
- les conséquences pour les utilisateurs en termes d'adaptation des pratiques et de continuité des soins ;
- les modes dégradés ou alternatifs en cas d'indisponibilité du SIA (cf. Fiche 10) ;
- les conséquences pour les patients pour éviter toute perte de chance ;
- les coûts et les gains estimés liés au changement (évolution de l'organisation du travail, impact sur les données, évolution des formations, etc.).

★★★ Prévoir des clauses de réversibilité

Lors de la contractualisation avec le fournisseur, le déployeur prévoit des clauses de réversibilité des données en cas de rupture contractuelle (cf. Fiche 2).

Ces clauses définissent le périmètre des SIA concernés ainsi que leur environnement d'exploitation (données, documents, processus, applications, licences, infrastructures, logiciels, etc.).

Elles organisent les conditions de restitution des données concernées et, le cas échéant, de transfert vers une solution alternative.

À ce titre, ces clauses précisent notamment les éléments concernés par la réversibilité, les modalités et les formats de restitution, le transfert de la documentation nécessaire à la reprise ou à la poursuite de l'exploitation du SIA, les procédures et les modalités techniques à mettre en œuvre, le calendrier et les délais d'exécution, les conditions d'assistance du fournisseur pendant la phase de transition, les modalités de suppression des données résiduelles, les coûts associés, ainsi que les responsabilités respectives du fournisseur et du déployeur.

Fixer un délai de transition minimum

Le déployeur fixe, dès la contractualisation avec le fournisseur, un délai minimum de transition permettant d'assurer la continuité du service lors du décommissionnement d'un SIA (cf. Fiche 2).

Le délai de transition est fixé selon le niveau de risque du SIA et la sensibilité des données concernées.

Organiser et mettre en œuvre le décommissionnement

Le déployeur organise et met en œuvre le décommissionnement en impliquant l'ensemble des parties prenantes. Dans le cadre d'un établissement de santé, cela concerne par exemple le service juridique, le service financier, la Direction des systèmes d'informations, le RSSI, le DPO et l'archiviste.

Le déployeur :

- s'assure de la conformité réglementaire et de la protection des données ;
- organise la continuité des activités sans dégradation de service ni perte d'information ;
- vérifie la restitution des données de la part du fournisseur du SIA ;
- conserve les jeux de données d'entraînement des modèles algorithmiques utilisés lors des périodes de calibrage et de mise à jour ;
- obtient la preuve de la suppression des données de la part du fournisseur du SIA, par exemple une preuve de destruction de la clé de chiffrement détenue par le fournisseur ;
- organise et vérifie la révocation des accès et des connecteurs de l'ensemble des parties prenantes (utilisateur, gouvernance, fournisseur) ;
- vérifie auprès du service juridique et du service financier que le contrat avec le fournisseur du SIA est résilié et l'arrêt des coûts associés.

Table des annexes

Annexe 1.	Stratégie de la HAS et de la CNIL concernant l'IA	77
Annexe 2.	Travaux complémentaires de la HAS et de la CNIL	78
Annexe 3.	Classification des SIA au sens du RIA	79
Annexe 4.	Le traitement des données au sens du RGPD	80
Annexe 5.	Glossaire du vocabulaire spécifique utilisé dans ce guide	82
Annexe 6.	Synthèse des obligations applicables pour les SIA à haut risque au titre du RIA	85
Annexe 7.	Synthèse du guide	86
Annexe 8.	Méthode de travail	94

Annexe 1. Stratégie de la HAS et de la CNIL concernant l'IA

Stratégie de la HAS

La majorité des SIA utilisés en contexte de soins, 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 ;
- 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 2025-2030 de la HAS (3) et ont été intégrés depuis 2024 au cycle de certification des établissements de santé (5) pour renforcer la stratégie de maîtrise des risques numériques et liés aux SIA.

Stratégie de la CNIL

Le développement de l'IA s'accompagne d'enjeux en matière de protection des données et de libertés individuelles. En effet, de très nombreux SIA se reposent 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 veille 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 innovants 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 et CNIL. La CNIL a publié 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 2. Travaux complémentaires de la HAS et de la CNIL

HAS

Intelligence artificielle en santé. Bien l'utiliser et se protéger, 2025

Premières clefs d'usage de l'IA générative en santé, 2025

Guide d'aide au choix des dispositifs médicaux numérique à usage professionnel, 2023

L'effet tunnel en santé. Comment faire pour en voir le bout ?, 2023

Déclarer les événements indésirables graves associés aux soins (EIGS), 2022

Cartographie des impacts organisationnels pour l'évaluation des technologies de santé, 2020

CNIL

Projet de recommandation sur le dossier patient informatisé, 2025

Le règlement sur les données (Data Act) : un nouveau cadre européen pour le partage et l'utilisation des données, 2025

Utilisation d'un SIA générative, 2024

Guide de la sécurité des données personnelles, 2024

Sécurité : Encadrer les développements informatiques, 2024

Sécurité : Impliquer et former les utilisateurs, 2024

Formalités préalables, 2024

Mesures de journalisation, 2021

Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles, 2020

Violation de données personnelles : les règles à suivre, 2018

Conformité RGPD : comment recueillir le consentement des personnes ?, 2018

Listes des traitements pour lesquels une AIPD est requise ou non, 2018

L'analyse d'impact relative à la protection des données (AIPD), 2017

Transfert de données : les clauses contractuelles types (CCT) de la Commission européenne, 2016

Annexe 3. Classification des SIA au sens du RIA

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, par exemple la notation sociale, l'exploitation de la vulnérabilité des personnes, le recours à des techniques subliminales, 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 au 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 du RIA et article 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, soumis au chapitre IV du RIA 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, considérés à l'heure actuelle comme des 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.

SIA à usage général : 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 conçus intentionnellement et spécifiquement, par exemple les SIA pour la génération de texte ou d'image. Des obligations spécifiques s'appliquent également à ces SIA à usage général.

Publié au Journal officiel le 12 juillet 2024, la majorité des obligations du RIA seront applicables à partir du 2 août 2026.

Les règles relatives aux SIA à haut risque de l'annexe III du RIA seront applicables à partir du 2 décembre 2027.

Les règles relatives aux SIA à haut risque de l'annexe I du RIA (dont les DM et DMDIV) seront applicables à partir du 2 août 2028.

Annexe 4. Le traitement des données au sens du RGPD

L'utilisation de SIA en contexte de soins conduit, dans la majorité des cas, au traitement de données personnelles concernant les patients, de leurs proches et des professionnels qui ont assuré leur prise en charge. Ces traitements nécessaires au fonctionnement du SIA doivent être conformes aux cadres juridiques applicables à :

- la protection des données personnelles (RGPD, loi « informatique et libertés ») ;
- la protection des données, notamment de santé, collectées dans le cadre d'une prise en charge sanitaire (CSP, notamment aux exigences en matière d'hébergement des données de santé et de secret professionnel).

Qui est responsable ?

La structure de soin, quelle que soit sa taille, décidant d'utiliser un SIA pour la prise en charge de ses patients sera qualifiée de responsable de traitement. Elle devra veiller au respect des cadres juridiques applicables à la protection des données, ce qui implique notamment de :

- documenter sa conformité par la mise à jour de son registre de traitement et la réalisation d'une analyse d'impact sur la protection des données (AIPD) (cf. Fiche 1) ;
- sélectionner des SIA intégrant dès la conception et par défaut la protection des données (cf. Fiche 2) ;
- conclure des contrats avec ses sous-traitants en apportant une attention particulière aux prestataires, directs et indirects, soumis à un droit extra-européen (cf. Fiche 2) ;
- veiller à la formation régulière de son personnel concernant la protection des données (cf. Fiche 3) ;
- veiller au respect du principe de minimisation (cf. Fiche 7) ;
- informer les personnes concernées (cf. Fiche 4) ;
- garantir une intervention humaine (cf. Fiche 8) ;
- mettre en œuvre les mesures de sécurité appropriées, notamment des mesures de journalisation et les revoir régulièrement (cf. Fiche 9) ;
- notifier les violations de données personnelles (cf. Fiche 10).

Dans le présent guide, les termes « déployeur du SIA » issu du RIA, et « responsable de traitement » issu du RGPD, sont utilisés pour désigner le même organisme.

Quel est le fondement juridique pour le traitement de données personnelles ?

Le RGPD impose que tout traitement de données personnelles soit fondé sur une base légale (article 6 du RGPD) ainsi que sur une exception pour l'utilisation de données sensibles, notamment de santé (article 9 du RGPD). Ces deux exigences se cumulent. Au regard du contexte dans lequel l'utilisation de données personnelles intervient, la CNIL estime que celle-ci peut être fondée sur :

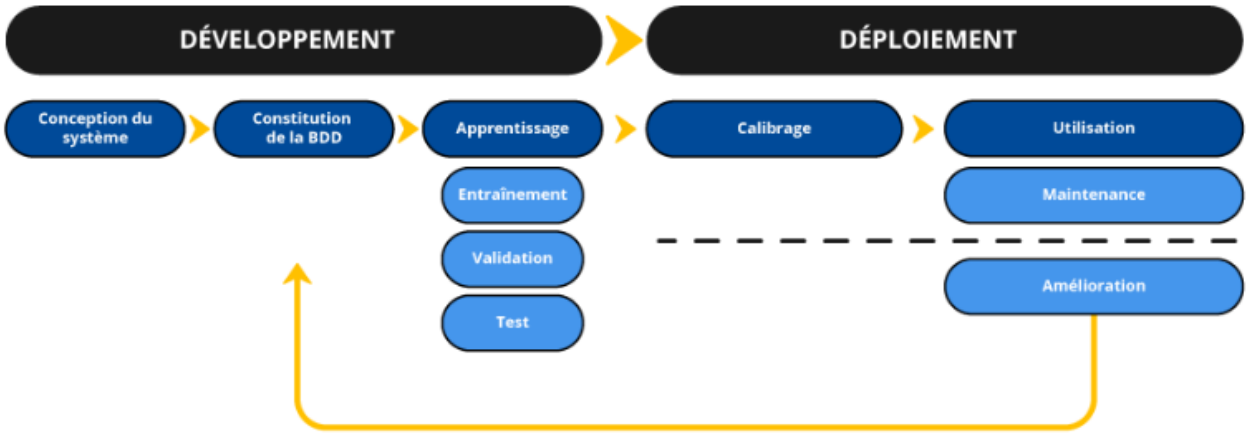
- les intérêts légitimes du responsable de traitement (article 6.1.f du RGPD) ou la poursuite d'une mission d'intérêt public qui lui incombe (article 6.1.e du RGPD). Le choix de la base légale appropriée tiendra compte de la qualification du responsable de traitement et du SIA concerné ;
- l'exception « 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.

Bien qu'il constitue l'une des bases légales et exceptions prévues par le RGPD, le consentement des personnes n'est pas approprié dans ce contexte. Par exemple, son caractère libre est remis en cause par le déséquilibre des relations entre les patients et les professionnels ou les établissements de santé.

Quels sont les traitements de données personnelles couverts par ce guide ?

Le guide concerne exclusivement la phase de déploiement des SIA et les traitements de données personnelles associés.

Les fiches concernent l'étape d'utilisation du SIA, à l'exception de la Fiche 3 qui contient certaines recommandations applicables à l'étape de calibrage.



Source : Quel est le périmètre des fiches pratiques sur l'IA ? | CNIL

Le guide traite-t-il des réutilisations de données à des fins d'amélioration du système ?

Non, bien que certaines fiches formulent des recommandations étroitement liées à ces réutilisations (cf. Fiche 4, Fiche 6 et Fiche 10).

Les réutilisations de données personnelles (utilisation secondaire) constituent des traitements distincts de ceux intervenant lors de l'utilisation de SIA en contexte de soins (utilisation primaire). Ces réutilisations (réentrainement, évaluation de l'impact sur le parcours patient, etc.) devront être conformes aux cadres juridiques applicables à la protection des données (RGPD, la loi « informatique et libertés », et à terme le règlement (UE) 2025/327 relatif à l'espace européen des données de santé). Les acteurs peuvent se reporter aux contenus publiés par la CNIL concernant l'IA et le secteur de la santé.

Que deviennent les enregistrements bruts des outils de retranscription d'échanges ?

Les enregistrements bruts doivent **être conservés** uniquement pour la durée nécessaire à la retranscription des échanges et à la validation du résultat par le professionnel ayant pris en charge l'usager. Ils doivent donc être **supprimés** dès que la retranscription est validée.

Annexe 5. Glossaire du vocabulaire spécifique utilisé dans ce guide

Algorithmovigilance : l'algorithmovigilance désigne la vigilance consacrée au modèle algorithmique du SIA. Cette démarche s'inscrit dans une logique de surveillance continue du SIA, tout au long de son cycle de vie et en particulier après son déploiement en routine clinique.

Bac à sable réglementaire : cadre d'expérimentation contrôlé mis en place sous la supervision d'une autorité compétente afin de permettre le développement, l'entraînement, l'essai ou la validation d'un système d'intelligence artificielle innovant dans des conditions réelles ou proches du réel, avant sa mise sur le marché ou sa mise en service. Ce dispositif permet d'évaluer le système, d'identifier les risques et de vérifier sa conformité aux exigences réglementaires dans un environnement encadré et pour une durée limitée.

Déployeur du SIA : acteur responsable du déploiement et des utilisateurs du SIA sous sa responsabilité. Selon l'article 3.4 du RIA, le déployeur est « *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* ». Dans le secteur sanitaire, le déployeur peut notamment être un établissement de santé, un laboratoire de biologie médicale, un centre d'imagerie ou un professionnel de santé exerçant à titre libéral. Le déployeur peut confier certaines activités à des prestataires, notamment l'installation, l'intégration, l'hébergement, la maintenance, le support ou l'exploitation technique du SIA. Cette délégation ne le décharge pas des obligations qui lui incombent en tant que déployeur au regard du RIA.

Dérive algorithmique : apparition d'un décalage entre la population cible 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. Ce décalage est à l'origine d'une éventuelle dégradation de la performance du SIA (cf. Fiche 2).

Données d'entrée : ensemble des données transmises à un SIA afin qu'il puisse traiter une situation donnée et générer un résultat, tel qu'une prédiction, une recommandation, une classification, un score ou une aide à la décision. Les données d'entrée peuvent notamment être des données cliniques, biologiques, d'imagerie ou administratives.

Événements indésirables graves associés aux soins (EIGS)

Un EIGS est un évènement inattendu au regard de l'état de santé et de la pathologie de la personne et dont les conséquences sont le décès, la mise en jeu du pronostic vital, la survenue probable d'un déficit fonctionnel permanent, y compris une anomalie ou une malformation congénitale (article R.1413-67 du CSP).

Fournisseur du SIA : acteur responsable de la conception et de la mise sur le marché du SIA. Selon l'article 3.3 du RIA, le fournisseur est « *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* ». Le fournisseur peut confier certaines activités à des prestataires. Cette délégation ne le décharge pas des obligations qui lui incombent en tant que fournisseur au regard du RIA.

Incident grave : Selon l'article 3.49 du RIA, un incident grave est un incident ou dysfonctionnement d'un SIA entraînant directement ou indirectement :

a) le décès d'une personne ou une atteinte grave à la santé d'une personne ;

b) une perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques ;

c) la violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux ;

d) un dommage grave à des biens ou à l'environnement.

Informatique en nuage ou « cloud » : mode de fourniture de services informatiques permettant d'accéder, via un réseau, à des ressources informatiques hébergées et administrées par un prestataire, telles que des capacités de stockage, de calcul, des logiciels ou des bases de données. Les données et traitements sont alors réalisés sur des infrastructures distantes plutôt que sur les équipements de l'utilisateur ou de l'organisation de santé.

Intelligence artificielle fantôme ou « shadow IA » : situation dans laquelle des professionnels utilisent, dans le cadre de leur activité, des systèmes d'intelligence artificielle sans autorisation, validation ou supervision préalables de l'organisation de santé. L'intelligence artificielle fantôme peut exposer le déployeur à des risques en matière de sécurité, de protection des données, de conformité réglementaire, d'interopérabilité et de gouvernance des systèmes d'information.

Journaux techniques : ensemble des informations enregistrées automatiquement par les composants techniques d'une application, d'un système d'information, d'un système d'intelligence artificielle ou d'une infrastructure informatique dans le cadre de la journalisation. Ces journaux consignent notamment les événements liés à l'authentification, aux connexions afin de retracer leur fonctionnement et leur utilisation, aux accès aux ressources, aux opérations d'administration, aux anomalies, aux erreurs et aux incidents de sécurité, ainsi que, selon les besoins de traçabilité, aux opérations réalisées, aux interventions humaines et aux informations pertinentes relatives aux données d'entrée et de sorite. Ils contribuent à assurer la sécurité des systèmes, à détecter les dysfonctionnements ou usages inappropriés, à permettre la supervision humaine, l'audit et l'analyse des incidents et à démontrer la conformité des traitements.

Modèle algorithmique (modèle d'IA ou modèle d'apprentissage) : composante d'un système d'intelligence artificielle qui a été entraîné ou configuré pour réaliser une ou plusieurs tâches à partir de données. Le modèle analyse les données d'entrée et produit un résultat, par exemple une prédiction, une classification, une recommandation ou un contenu généré. Il constitue le « moteur » du SIA sur lequel reposent les résultats produits.

Résultat du SIA : toute sortie produite par un SIA à partir des données qu'il traite (données de sortie). Selon le système concerné, ce résultat peut prendre la forme d'une prédiction, d'une recommandation, d'une classification, d'un score, d'une alerte, d'une proposition de décision ou d'un contenu généré.

Système d'intelligence artificielle (SIA) : outils informatiques conçus pour fonctionner avec un niveau d'autonomie variable. Utilisés dans un contexte de soins, les SIA sont capables de déduire et de générer des résultats tels que des prédictions diagnostiques, des recommandations thérapeutiques, des scores de risques ou encore des aides à la décision, à partir de données d'entrée (cliniques, physiologiques, administratives, et.). Les résultats d'un SIA sont donc susceptibles d'influencer la prise en charge du patient ou l'organisation des soins. Un SIA est défini légalement (article 3.1 du RIA).

Traces fonctionnelles ou applicatives : l'ensemble des informations enregistrées dans les outils métier qui reflètent les actions effectuées par un système ou un utilisateur. Dans le contexte de l'utilisation de l'IA dans les soins, ces traces permettent de documenter et de retracer l'utilisation d'un système d'intelligence artificielle, les conditions dans lesquelles il a été utilisé, les résultats générés et les décisions ou actions réalisées par les professionnels à la suite de cette utilisation. Elles se distinguent des journaux techniques, qui retracent principalement les événements informatiques liés au fonctionnement et à la sécurité du système.

Utilisateur du SIA : est la personne physique qui l'utilise. Il l'utilise conformément aux instructions du fournisseur et aux règles définies par le déployeur. Il doit également disposer des connaissances, des compétences et des qualifications nécessaires à une utilisation appropriée.

Annexe 6. Synthèse des obligations applicables pour les SIA à haut risque au titre du RIA

Le déployeur d'un SIA à haut risque doit respecter certaines obligations au titre du RIA (articles 26, 27 et 86 du RIA).

Le déployeur d'un SIA à haut risque doit :

- réaliser une analyse d'impact sur les droits fondamentaux (AIDF) lorsque requise (cf. Fiche 1) ;
- former les utilisateurs et les superviseurs du SIA (cf. Fiche 3) ;
- informer les personnes concernées de l'utilisation du SIA (cf. Fiche 4) ;
- utiliser le SIA conformément à la notice (cf. Fiche 7) ;
- veiller à la qualité et à la représentativité des données d'entrée (cf. Fiche 7) ;
- organiser une supervision humaine par des personnes compétentes (cf. Fiche 8) ;
- garantir aux personnes concernées le droit à une explication sur l'utilisation du SIA (cf. Fiche 8) ;
- assurer la tenue et la conservation des journaux lorsqu'ils sont sous son contrôle (cf. Fiche 9) ;
- surveiller le fonctionnement du SIA (cf. Fiche 10) ;
- signaler les risques graves et incidents aux autorités compétentes (cf. Fiche 10).

Annexe 7. Synthèse du guide

L'intelligence artificielle (IA) s'intègre rapidement dans les pratiques et les organisations de santé, faisant émerger de nouveaux enjeux en matière de qualité, de sécurité, de gouvernance et de conformité réglementaire. Afin d'accompagner ces évolutions, la HAS et la CNIL proposent un guide destiné aux déployeurs et aux utilisateurs de systèmes d'IA (SIA). Il a pour objectif de clarifier les obligations applicables, d'accompagner le bon usage de ces systèmes et de fournir un cadre pratique pour leur déploiement, leur utilisation et leur suivi dans les organisations de santé.

1. Organisation interne et gouvernance

La capacité d'une organisation ou d'un individu à comprendre et à gérer le processus de déploiement des SIA est indispensable pour assurer leur bon usage en contexte de soins. Le déploiement d'un SIA n'est possible qu'en mobilisant l'ensemble des parties prenantes, sous l'impulsion du responsable de l'organisation de santé. Quel que soit le contexte d'exercice, chaque déployeur assume cette responsabilité et veille à la conformité et à la sécurité de l'utilisation des SIA en contexte de soins.

Obligations principales

Le déployeur :

- met en place une gouvernance adaptée ;
- effectue une AIDF, le cas échéant ;
- tient un registre des traitements ;
- réalise une AIPD, le cas échéant.

Principes prioritaires ★★★

- Mettre en place une gouvernance dédiée à l'IA
- Cartographier les SIA
- Impliquer les représentants des usagers

Principes

- Adopter une démarche responsabilité sociétale des entreprises (RSE)
- Sensibiliser les organes de direction aux enjeux spécifiques de l'IA
- Mutualiser les ressources et les réflexions en matière d'IA
- S'appuyer sur les organismes régionaux et nationaux
- Mettre en place un guichet unique pour les SIA
- Garantir une validation par la gouvernance
- Formaliser et adopter une charte d'utilisation des SIA
- Définir une politique unifiée d'information des usagers
- Définir une politique de formation aux SIA
- Définir des procédures en cas d'incidents ou de dysfonctionnements
- Désigner un référent local dédié aux SIA

2. Acquisition et contractualisation

La contractualisation entre le déployeur et le fournisseur permet de vérifier la conformité du SIA aux exigences applicables et de répartir clairement les responsabilités entre les parties. Le contrat encadre les conditions d'utilisation du SIA, la gestion des incidents et la coopération avec le fournisseur. Il précise les obligations et les modalités de coopération du fournisseur et encadre les conditions d'utilisation du SIA. Le contrat ne déroge pas aux règles applicables en matière de délégation d'activité médicale, de secret professionnel et d'exercice des professions de santé. Lorsque cela est possible, les démarches de contractualisation gagnent à être mutualisées afin de favoriser une meilleure maîtrise des risques et des ressources.

Obligations principales

Le déployeur :

- dispose des informations pertinentes pour réaliser l'AIPD et l'AIDF lorsqu'elles sont requises ;
- conclue un contrat avec chaque sous-traitant intervenant dans le traitement de données personnelles et en tenant compte des dispositions spécifiquement applicables à la prestation concernée ;
- vérifie que le traitement des données personnelles lié à l'utilisation du SIA est conforme au RGPD ;
- conclue un contrat conforme aux articles du CSP concernant l'hébergement des données de santé lorsque l'utilisation du SIA implique la conservation des données par un tiers ;
- vérifie que le marquage CE est apposé sur le produit conformément aux différentes réglementations européennes en vigueur, notamment celles applicables aux DM et DMDIV.

Principes prioritaires ★★★

- Établir un cahier des charges
- Vérifier la conformité réglementaire du SIA

Principes

- Associer précocement le DPO ou les référents protection des données
- Sensibiliser les services compétents
- Vérifier la couverture assurantielle du fournisseur et des utilisateurs
- Vérifier l'interopérabilité du SIA
- Prévoir une clause de niveau de service (SLA)
- Prévoir une clause relative à la période de calibrage
- Prévoir une clause de performance
- Prévoir une clause sur les conditions de fin de contrat
- Prévoir une clause relative à la confidentialité des données
- Prévoir une clause relative à la formation des utilisateurs
- Prévoir une clause relative à la traçabilité et à l'accès aux journaux d'activité
- Prévoir une clause relative aux procédures de gestion des incidents
- Prévoir une clause relative au traitement de données personnelles

3. Sensibilisation, formation et habilitation

La formation favorise l'usage éclairé et sécurisé des SIA, le respect du droit à l'information des personnes (cf. Fiche 4) et la mise en œuvre d'une supervision humaine effective. La formation à l'IA des professionnels de santé, des personnels administratifs et des instances de gouvernance permet à chaque acteur de disposer d'un niveau de connaissances et de compétences adapté à son rôle et à ses responsabilités.

Obligations principales

Le déployeur :

- met en place ou participe à des modules de formation sur l'IA en santé et sur la protection des données personnelles.

Principes prioritaires ★★★

- Sensibiliser l'ensemble du personnel à l'IA
- Former les utilisateurs du SIA

Principes

- Renforcer les compétences des acteurs aux fonctions spécifiques
- Organiser les formations en cohérence avec les réalités des acteurs
- Tracer les formations réalisées
- Habiliter les utilisateurs de SIA à haut risque

4. Information des usagers

L'information des usagers sur l'utilisation des SIA est essentielle pour favoriser leur compréhension, leur confiance et l'exercice effectif de leurs droits. Elle constitue une obligation légale dont le contenu dépend des caractéristiques du SIA, de sa finalité et du cadre juridique applicable. Une information insuffisante peut exposer les professionnels et les établissements à un risque juridique et compromettre le consentement éclairé du patient. Cette information porte notamment sur l'usage des SIA dans les soins, l'utilisation des données personnelles et, le cas échéant, leur réutilisation à des fins secondaires. Les modalités de communication doivent être adaptées à chaque situation afin de garantir une information claire, pertinente et accessible.

Obligations principales

Le déployeur :

- informe les personnes concernées lorsqu'un SIA à haut risque relevant de l'annexe III du RIA est utilisé ;
- informe les personnes concernées lorsqu'elles interagissent directement avec un SIA et les sensibilise afin qu'elles communiquent uniquement les informations nécessaires ;
- informe les personnes concernées conformément au RGPD lorsque l'utilisation d'un SIA implique le traitement de données personnelles ;
- informe les personnes concernées conformément au RGPD lorsque les données personnelles collectées et utilisées dans le cadre du soin sont réutilisées, notamment à des fins de développement, de recherche clinique ou d'évaluation du déploiement du SIA.

Le professionnel :

- informe les personnes concernées lorsqu'il décide de recourir à un DM intégrant un SIA. En effet, il convient d'anticiper les textes d'application de l'article L. 4001-3 du CSP encore en cours d'élaboration.

Principes prioritaires ★★★

- Informer les usagers sur les réutilisations de leurs données envisagées
- Diffuser la politique d'utilisation des SIA auprès des usagers
- Informer les usagers directement concernés par l'utilisation d'un SIA

Principes

- Mettre à disposition la cartographie des SIA de la structure
- Informer l'usager de manière individuelle et détaillée, avant l'utilisation d'un SIA

5. Consentement et droits des usagers

Le consentement libre et éclairé du patient constitue un droit fondamental et une condition préalable à la réalisation des actes de soins. Fondé sur une information adaptée, il permet au patient de participer aux décisions concernant sa santé et participe à la sécurisation juridique des pratiques des professionnels et des établissements. Plusieurs formes de consentement doivent être distinguées selon le contexte, notamment pour les soins, certaines recherches en santé, les traitements de données personnelles ou les essais de SIA à haut risque. Lors de l'utilisation d'un SIA, il appartient aux professionnels d'apprécier, au regard de chaque situation, les mesures nécessaires pour garantir une décision éclairée et conforme aux règles professionnelles. Au-delà du consentement, les usagers disposent également de droits en tant que patients et personnes concernées par le traitement de leurs données personnelles.

Obligations principales

Le déployeur :

- en tant que responsable de traitement, donne suite aux demandes d'exercice des droits au sens du RGPD qui lui sont adressées ;
- permet aux personnes concernées par l'utilisation d'un SIA d'exercer les droits issus du RIA et du CSP, en particulier leur droit à l'information, au consentement et à la participation aux décisions concernant leur santé ;
- garantit la maitrise des personnes sur leurs attributs de personnalité, en particulier sur leur voix et leur image.

Principes prioritaires ★★★

- Informer l'usager et recueillir son accord pour les enregistrements vocaux et vidéo ainsi que pour les photographies

Principes

- Absence de consentement spécifique pour l'utilisation d'un SIA
- Possibilité de recueillir un accord à visée éthique dans certaines situations

6. Organisation des soins

Le déploiement d'un SIA peut modifier l'organisation des soins, les processus de travail ainsi que les rôles et responsabilités des professionnels. Avant sa mise en œuvre et tout au long de son utilisation, le déployeur doit vérifier son adéquation au contexte de soins, notamment sa pertinence pour les besoins locaux, son intégration dans les pratiques et ses performances en conditions réelles. Cette démarche s'appuie sur une documentation fournie par le fournisseur et peut être encadrée contractuellement. Dans une logique d'amélioration continue, le déployeur évalue les impacts du SIA sur l'organisation des soins et définit clairement les responsabilités des utilisateurs. Il réalise également un bilan du déploiement et de l'utilisation du système, par exemple au moyen d'une évaluation scientifique.

Obligations principales

Le déployeur :

- respecte les règles d'exercice des professions réglementées par le CSP afin d'éviter toute requalification en exercice illégal ;
- réalise les formalités CNIL en cas d'utilisation de données pour une autre finalité que la prise en charge, notamment dans les phases de test ou les bilans.

Principes prioritaires ★★★

- Vérifier l'adéquation du SIA au contexte et au besoin
- Analyser l'impact organisationnel du SIA

Principes

- Encadrer et formaliser les rôles et les responsabilités des utilisateurs
- Réaliser un test d'utilisation sur un jeu de données locales
- Réaliser des bilans du déploiement et de l'utilisation
- Encourager la production d'évaluations scientifiques

7. Au cours de l'utilisation

L'utilisation d'un SIA en contexte de soins nécessite de :

- respecter sa notice d'utilisation, son usage prévu par le fournisseur et les bonnes pratiques professionnelles ;
- contrôler les biais et limiter les risques ;
- maintenir une supervision humaine.

Obligations principales

Le déployeur :

- prend les mesures techniques et organisationnelles appropriées afin de garantir l'utilisation du SIA conformément à sa notice d'utilisation ;
- garantit le respect du principe de minimisation des données en sensibilisant le personnel.

Principes prioritaires ★★★

- Exercer son jugement en toute responsabilité pour prévenir les biais liés aux SIA
- Utiliser le SIA conformément à la notice

Principes

- Vérifier la couverture de l'assurance responsabilité civile professionnelle
- Maîtriser les bonnes pratiques d'utilisation

8. Supervision humaine

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. La mise en œuvre concrète de cette supervision humaine soulève toutefois plusieurs questions :

- quel acteur doit assurer cette supervision ?
- quelles compétences ou qualifications sont nécessaires ?
- dans quelles situations, à quel moment et selon quelles modalités, la supervision doit-elle être exercée ?

Obligations principales

Toutes les décisions liées à l'utilisation d'un SIA doivent faire l'objet d'une supervision humaine et impliquent :

- une validation par le professionnel prenant en charge la personne (intervention humaine au titre du RGPD) ;
- la mise en œuvre d'un contrôle humain, par le fournisseur, proportionné à l'impact sur les soins (contrôle humain par le fournisseur au titre du RIA). À ce jour, il n'y a pas de standard sur les modalités de mise en place de ce contrôle humain qui doit être adapté, au cas par cas, au contexte dans lequel le SIA est déployé ;
- la formation du professionnel par le déployeur (contrôle humain au titre du RIA) (cf. Fiche 3).

Principes prioritaires ★★★

- Tracer et analyser régulièrement les incidents liés à l'utilisation du SIA
- Préserver explicitement l'indépendance et la liberté de décision du praticien
- Adapter le niveau de supervision humaine

Principes

- Tracer l'utilisation d'un SIA dans le cadre des soins
- Assurer et documenter la formation des professionnels réalisant la supervision humaine
- Définir des modalités de supervision humaine dans les protocoles

9. Traçabilité des usages et des résultats

La traçabilité des SIA permet de documenter leurs conditions d'utilisation, de soutenir les démarches d'évaluation et de vigilance, et de contribuer à la sécurité des données et des systèmes d'information. Elle repose notamment sur la conservation des résultats du SIA, des données nécessaires à son fonctionnement et des informations relatives à son utilisation dans le parcours de soins. Elle comprend également l'identification des décisions associées à l'usage du SIA ainsi que la mise en œuvre de mesures de journalisation des accès et des traitements réalisés. Les données de journalisation doivent pouvoir être analysées afin de détecter rapidement les utilisations inappropriées ou les comportements anormaux. Ces principes complètent les exigences et recommandations déjà applicables aux systèmes d'information.

Obligations principales

Le déployeur :

- conserve les journaux placés sous son contrôle ;
- détermine une durée de conservation adaptée à la finalité poursuivie et à celles prévues par le CSP ;
- recourt au service d'un prestataire certifié HDS, le cas échéant.

Principes prioritaires ★★★

- Intégrer la traçabilité comme outil de prévention des risques
- Conserver systématiquement les résultats du SIA

Principes

- Conserver la notice d'utilisation du SIA
- Identifier les résultats d'un SIA grâce à un marquage spécifique

10. Gestion de la qualité et des vigilances

Le déploiement d'un SIA en contexte de soins nécessite sa maintenance, un suivi de sa performance, une gestion des vigilances et les mesures correctives associées, le respect de sa conformité et l'anticipation de son indisponibilité. La mise en œuvre de procédures adaptées vise à maintenir, dans la durée, un niveau de sécurité et de performance compatible avec les enjeux de la prise en charge des patients, à prévenir les incidents et à garantir la continuité des activités. La coopération entre l'utilisateur, le déployeur et le fournisseur est nécessaire pour cette mise en œuvre.

Obligations principales

Le déployeur ou l'utilisateur :

- veille à la conformité du traitement de données lié à un SIA dès sa première utilisation et de manière régulière ;
- veille à la mise en place de mesures de sécurité adaptées à la sensibilité des données et aux risques ;
- les cas échéant, notifie les violations de données et en informe les personnes concernées ;
- déclare les événements indésirables graves associés aux soins (EIGS) ;

- déclare les incidents graves, et réalise la matériovigilance ou la réactovigilance des SIA ayant le statut de DM ou DMDIV ;
- déclare les incidents graves liés aux SIA à haut risque.

Principes prioritaires ★★★

- Réaliser le suivi des performances
- Organiser un circuit de vigilance et de signalement des incidents pour les SIA, qu'ils soient DM, DMDIV ou non
- Organiser la gestion des mises à jour

Principes

- Formaliser une procédure de gestion de la maintenance partagée
- Anticiper l'indisponibilité du SIA

11. Fin du cycle de vie

La fin du cycle de vie d'un SIA correspond à l'arrêt définitif de son utilisation au sein d'une organisation de santé. Elle peut résulter d'une décision du déployeur, du fournisseur ou d'une autorité compétente. La fin du cycle de vie du SIA doit être anticipée dès la contractualisation avec le fournisseur (cf. Fiche 2). Cette anticipation permet d'assurer la continuité des soins, la protection des données, ainsi que la maîtrise des risques liés à son arrêt ou à son remplacement. Elle implique notamment de prévoir les conditions de décommissionnement, de réversibilité et de transition, conformément aux exigences réglementaires applicables.

Synthèse des obligations légales

Le déployeur :

- détermine le devenir des données personnelles dont le traitement a été confié au sous-traitant au terme de la prestation ;
- conclut avec le prestataire HDS un contrat contenant les engagements requis pas le CSP, le cas échéant.

Principes prioritaires ★★★

- Anticiper et organiser la fin du cycle de vie du SIA
- Prévoir des clauses de réversibilité

Principes

- Fixer un délai de transition minimum
- Organiser et mettre en œuvre le décommissionnement

Annexe 8. Méthode de travail

La démarche suivie pour l'élaboration du guide a été structurée autour de plusieurs étapes complémentaires :

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

Des entretiens semi-dirigés avec 31 parties prenantes ont été réalisés et analysés lors du cadrage des travaux. Afin d'enrichir les travaux du groupe de travail, un questionnaire structuré a été transmis à des CNP, établissements de santé, professionnels libéraux, industriels et 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.

2. **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 et leurs obligations spécifiques ;
- les modalités de mises en œuvre des obligations pour les déployeurs et fournisseurs.

En conséquence, certaines des principes proposés ici, bien qu'ancrés dans le droit en vigueur, pourront nécessiter des ajustements ultérieurs.

3. **Revue ciblée de la littérature.**

Une revue systématique ciblée a été menée, 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.

4. **Mobilisation d'un groupe de travail d'experts pluridisciplinaire.**

Un groupe de travail a été mis en place. Il est composé de 11 experts aux profils variés : professionnels de santé de diverses disciplines, experts du numérique en santé, ingénieurs biomédicaux, juristes spécialisés et représentant d'usagers. La composition du groupe de travail est détaillée dans les participants de la production.

5. **Consultation publique.**

Une version intermédiaire du guide a été soumise à consultation publique afin de permettre à l'ensemble des acteurs - établissements, professionnels, industriels, usagers, etc. – de contribuer aux travaux. Les 79 retours de cette consultation ont été systématiquement analysés. Les évolutions issues de ces analyses ont été soumises à la validation du groupe de travail et intégrées dans la version finale du guide.

Références

1. Fédération hospitalière de France. L'IA en santé : qui est le maître ? Ambitions et perspectives. Paris: FHF; 2025.
https://www.calameo.com/fhf/read/0037957021bc5deb3eade?page=11

2. Institut français d'opinion publique. Baromètre à l'hôpital : adoption et impact de l'intelligence artificielle dans le secteur hospitalier. Etude Ifop pour Acteurs publics et UniHA. Paris: Ifop; 2025.
https://www.uniha.org/actualites/tendances/lhopital-lheure-de-lia-resultats-du-premier-barometre-national

3. Haute Autorité de santé. Projet stratégique 2025-2030. Saint-Denis La Plaine: HAS; 2025.
https://www.has-sante.fr/jcms/p_3588048/fr/projet-strategique-2025-2030-de-la-has

4. Williate L. L'intelligence artificielle et la responsabilité du médecin : quel impact ? Le magazine de l'Ordre des avocats au barreau de Lille 2025:1-3.

5. Haute Autorité de santé. Certification des établissements de santé pour la qualité des soins. Version 2027. Référentiel. Saint-Denis La Plaine: HAS; 2026.
https://www.has-sante.fr/upload/docs/application/pdf/2026-07/dir2/referentiel_certification_es_qualite_des_soins_version_2027.pdf

6. Haute Autorité de santé, Commission nationale informatique et libertés, France assos santé. Intelligence artificielle en santé. Bien l'utiliser et bien se protéger. Saint-Denis La Plaine: HAS; 2026.
https://www.has-sante.fr/upload/docs/application/pdf/2026-06/dir1/ia_sante_synthese.pdf

7. Haute Autorité de santé. Guide d'aide au choix des dispositifs médicaux numériques à usage professionnel. A destination des professionnels et des établissements de santé. Guide. Saint-Denis La Plaine: HAS; 2023.
https://www.has-sante.fr/upload/docs/application/pdf/2023-06/dispositif_medicaux_numerique_a_usage_professionnel_guide_daide_au_choix.pdf

8. Commission nationale informatique et libertés. Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles [En ligne]. Paris: CNIL; 2020.
https://www.cnil.fr/fr/responsable-de-traitement-et-sous-traitant-6-bonnes-pratiques-pour-respecter-les-donnees

9. Commission nationale informatique et libertés. L'analyse d'impact relative à la protection des données (AIPD) [En ligne]. Paris: CNIL; 2017.
https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

10. Commission nationale informatique et libertés. Liste des traitements pour lesquels une AIPD est requise ou non [En ligne]. Paris: CNIL; 2018.
https://www.cnil.fr/fr/listes-des-traitements-pour-lesquels-une-aipd-est-requise-ou-non

11. Commission nationale informatique et libertés. Sous-traitants : la réutilisation de données confiées par un responsable de traitement [En ligne]. Paris: CNIL; 2022.
https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement

12. European Commission. AI literacy- Questions and answers [En ligne]. Bruxelles: European Commission; 2026.
https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers

13. Commission nationale informatique et libertés. Sécurité : impliquer et former les utilisateurs [En ligne]. Paris: CNIL; 2024.
https://www.cnil.fr/fr/securite-impliquer-et-former-les-utilisateurs

14. Commission nationale informatique et libertés. Conformité RGPD : comment recueillir le consentement des personnes ? [En ligne]. Paris: CNIL; 2018.
https://cnil.fr/fr/les-bases-legales/consentement

15. Cour de Cassation. Cour de Cassation, Assemblée plénière, du 7 mai 2004, 02-10.450 [En ligne]. Rouen: Legifrance; 2004.
https://www.legifrance.gouv.fr/juri/id/JURITEXT000007048576/

16. Cour de Cassation. Cour de cassation, civile, Chambre civile 1, 24 juin 2026, 25-20.483 [En ligne]. Paris: Legifrance; 2026.
https://www.legifrance.gouv.fr/juri/id/JURITEXT000054339869

17. Cour européenne des droits de l'Homme. Affaire Reklos et Davourlis c. Grèce (requête n°1234/05) [En ligne]. Strasbourg 2009.

18. Cour européenne des droits de l'Homme. Affaire de la Flor Cabrera c. Espagne (Requête n° 10764/09 [En ligne]. Strasbourg 2014.

19. Cour de Cassation. Cour de Cassation, Chambre civile 1 du 21 mars 2006, 05-16.817 [En ligne]. Versailles: Legifrance; 2006.

20. Commission nationale informatique et libertés. Sécurité : encadrer les développements informatiques [En ligne]. Paris: CNIL; 2024.
https://www.cnil.fr/fr/securite-encadrer-les-developpements-informatiques

21. Commission nationale informatique et libertés. Formalités préalables [En ligne]. Paris: CNIL; 2024.
https://www.cnil.fr/fr/sante-formalites-prealables

22. Haute Autorité de santé. Cartographie des impacts organisationnels pour l'évaluation des technologies de santé. Guide méthodologique. Saint-Denis La Plaine: HAS; 2020.
https://www.has-sante.fr/jcms/p_3227435/fr/cartographie-des-impacts-organisationnels-pour-l-evaluation-des-technologies-de-sante-guide-methodologique

23. Haute Autorité de santé. L'effet tunnel en santé. Comment faire pour en voir le bout ? Saint-Denis La Plaine: HAS; 2023.
https://www.has-sante.fr/upload/docs/application/pdf/2023-06/l-effet-tunnel-en-sante-comment-en-venir-a-bout.pdf

24. Cour de justice de l'Union européenne. Arrêt de la cour (première chambre) C-203/22 [En ligne]. Luxembourg: Curia; 2025.
https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=295841

25. European Commission. The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rles application. Bruxelles: European Commission; 2025.
https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

26. Commission nationale informatique et libertés. La CNIL publie une recommandation relative aux mesures de journalisation [En ligne]. Paris: CNIL; 2021.
https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-relative-aux-mesures-de-journalisation

27. Commission nationale informatique et libertés. Guide de la sécurité des données personnelles [En ligne]. Paris: CNIL; 2024.
https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles-nouvelle-edition-2024

28. Commission nationale informatique et libertés. Violation de données personnelles : les règles à suivre [En ligne]. Paris: CNIL; 2018.
https://www.cnil.fr/fr/violations-de-donnees-personnelles-les-regles-suivre

29. Haute Autorité de santé. EIGS : de la déclaration par les professionnels au retour d'expérience. Saint-Denis La Plaine: HAS; 2026.
https://www.has-sante.fr/jcms/p_3887965/fr/eigs-de-la-declaration-par-les-professionnels-au-retour-d-experience-infographie

30. Haute Autorité de santé. Grille ALARM. Facteurs contributrifs par catégorie. Saint-Denis La Plaine: HAS; 2026.
https://www.has-sante.fr/jcms/p_4414980/fr/grille-alarm

Participants

Groupe de travail

BENDJEBBAR Étienne, Responsable innovation, CHU de Nantes

BOULOGNE Philippe, Directeur des systèmes d'information, Hôpital Foch et Expert visiteur numérique de la HAS

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

DAUPHIN Arthur, Représentant des usagers, France Assos Santé

DUFOURT Caroline, Directrice juridique et Déléguée à la protection des données, Hôpital Américain de Paris

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

FÉVRIER Yann, Chargé de mission SI, GHT Est-Hérault Sud-Aveyron et Expert visiteur numérique de la HAS

Dr. GÉRARDIN Christel, Interniste, AP-HP

Pr. ISNARD BAGNIS Corinne, Néphrologue, AP-HP

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

SUMBAL Davina, Responsable qualité, Hôpital Saint Joseph

Pr. VUIBLET Vincent, Pathologiste, CHU de Reims

WILLIATTE Lina, Professeur des Universités Catholiques et Avocat, Lille

HAS

Mission Numérique en Santé

RENNER Simon, chef de projet

VALOIS PAUL, chef de projet

PIFARRÉ COUTROT Isabel, cheffe de projet

SAINT-CAST Aubry, chef de projet stagiaire

MAMOURI Annissa, assistante

TOUNKARA Yakaré, assistante

MARC Julie, cheffe de service

Service Juridique

LOUYER Adriane, juriste et DPO

BURKIC Emmanuelle, juriste

GASTO Floriane, adjointe au chef de service

LYONNET Maxence, chef de service

Gouvernance

COLLIGNON Corinne, ex-cheffe de la MNS, conseillère numérique et IA

Service Documentation Veille

RENNESSON Marina, documentaliste

DIVOL-FABRE Estelle, assistante-documentaliste

CNIL

Service de la Santé

GAIGNON Aurore, juriste

TAYAR Laura, juriste

GUIMIOT Hélène, cheffe de service

Service de l'IA

BAROT Charlotte, analyste

VALLET Félicien, chef de service

Remerciements

La HAS et la CNIL tiennent à remercier l'ensemble des participants cités ci-dessus, l'ensemble des parties prenantes interrogées et l'ensemble des contributeurs à la consultation publique.

La HAS et la CNIL tiennent à remercier le collège de la HAS et le collège de la CNIL, en particulier Pr COLLET Lionel et Dr GRALL Jean-Yves, référents de ce guide au collège de la HAS, ainsi que Pr ZINS Marie et Pr NGUYEN Benjamin, référents de ce guide au collège de la CNIL.

Retrouvez tous les travaux de la HAS sur

www.has-sante.fr

Retrouvez tous les travaux de la CNIL sur

www.cnil.fr

HAS
HAUTE AUTORITÉ DE SANTÉ

Développer la qualité dans le champ sanitaire, social et médico-social

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

© Haute Autorité de santé & Commission nationale de l'informatique et des libertés – novembre 2026 – ISBN : 978-2-11-186355-2