HAUTE AUTORITÉ DE SANTÉ

COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

IA en contexte de soins : accompagner le bon usage – Synthèse

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