l'anap l'expertise en partage | agence nationale de la performance sanitaire et médico-sociale

afnor

DÉCRYPTER L'IA ACT POUR DÉPLOYER EN SÉCURITÉ

SOMMAIRE

Réglementation sur les dispositifs médicaux p. 3
L'IA Act : notions à retenir p. 4
Systèmes d'IA et dispositifs médicaux p. 5
Exigences fournisseurs p. 6
Établissements de santé p. 7
Les bons réflexes « IA Act » p. 8
Calendrier de mise en œuvre de l'IA Act p. 10
Les outils et publications pour vous aider p. 11

L'ESSENTIEL POUR APPRÉHENDER L'IA

- On considère comme « intelligent » tout programme qui exécute des tâches complexes nécessitant du raisonnement, de l'apprentissage ou de la prise de décision.

- Moteur de règles simples, *machine learning*, *deep learning* : certaines notions liées à l'intelligence artificielle (IA) vous échappent ? Consultez notre guide « Déployer l'IA en confiance » pour vous mettre à jour !

NOTE DE L'ANAP
La réutilisation des productions de l'Anap est autorisée, sous réserve que les informations qu'elles contiennent ne soient pas altérées, que leur sens ne soit pas dénaturé et que leurs sources et date de dernière mise à jour soient mentionnées. Toute réutilisation à des fins commerciales doit faire l'objet d'un échange préalable avec l'Anap.

RÉGLEMENTATION SUR LES DISPOSITIFS MÉDICAUX

Un cadre juridique historique qui va jusqu'au numérique

Tout équipement (biomédical, numérique, etc.) utilisé à des fins médicales est considéré comme un dispositif médical (DM). L'établissement de santé doit s'assurer que le fournisseur a bien passé la certification selon sa classe de risque.

LE RÈGLEMENT EUROPÉEN SUR LES DM

Depuis le 5 avril 2017, les DM sont régis par deux règlements européens, l'un relatif aux dispositifs médicaux (2017/745) et l'autre aux dispositifs médicaux de diagnostic in vitro, ou DMDIV (2017/746).

*« On entend par "dispositif médical" tout instrument, **appareil, équipement, logiciel, implant, réactif, matière ou autre article**, destiné [...] à [...] des fins médicales précises suivantes :*

- *diagnostic, prévention, contrôle, prédiction, pronostic, traitement ou atténuation **d'une maladie** ;*
- *diagnostic, contrôle, traitement, atténuation **d'une blessure ou d'un handicap** ou compensation de ceux-ci ;*
- *investigation, remplacement ou modification **d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique** [...]. »*

Règlement (UE) 2017/745 du 5 avril 2017 relatif aux dispositifs médicaux - Article 2

L'OBLIGATION DU MARQUAGE CE

Pour être commercialisés, les DM doivent répondre aux exigences minimales en matière de sécurité, de qualité et d'efficacité définies par les règlements européens relatifs aux DM et DMDIV. Leur conformité à ces exigences est attestée par l'obtention du marquage CE, délivré par un organisme tiers accrédité pour les classes de risque > 1.

UNE CLASSIFICATION SELON LE RISQUE

Le règlement 2017/745 classe les DM en fonction du risque lié à leur utilisation :

- Classe I (faible) - lunettes ;
- Classe IIa (modéré) - lentilles de contact ;
- Classe IIb (élevé) - respirateurs ;
- Classe III (très élevé) - implants.

Attention, pour les DM DIV, les classes sont différentes.

DM NUMÉRIQUE : COMMENT S'Y RETROUVER ?

Pour être qualifié de DM numérique, un logiciel doit :

- Être à usage médical, c'est-à-dire avoir une finalité diagnostique, thérapeutique ou de compensation d'un handicap.
- Donner un résultat propre au bénéfice d'un seul patient.
- Effectuer une action sur les données implémentées « afin de fournir une information médicale nouvelle » (ANSM).

Pour bien comprendre :

EST DM NUMÉRIQUE :

- un logiciel de radiologie ;
- un dossier patient informatisé (DPI) avec un module d'aide à la prescription.

N'EST PAS DM NUMÉRIQUE :

- un logiciel métier RH ;
- un logiciel de téléexpertise.

Remarque : si un logiciel ou une application pilote ou influence l'utilisation d'un DM, il sera considéré au même titre comme un DM.

L'IA ACT : NOTIONS À RETENIR
Les bases d'une IA sereine

Depuis le 1er août 2024, l'IA est encadrée dans l'Union européenne par un règlement européen : l'IA Act. Il vise à « améliorer le fonctionnement du marché intérieur et promouvoir l'adoption d'une intelligence artificielle axée sur l'humain et digne de confiance, tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux. »

QUELLES DISPOSITIONS POUR LES SYSTÈMES D'IA DANS L'IA ACT ?

L'IA Act a pour objectifs de :

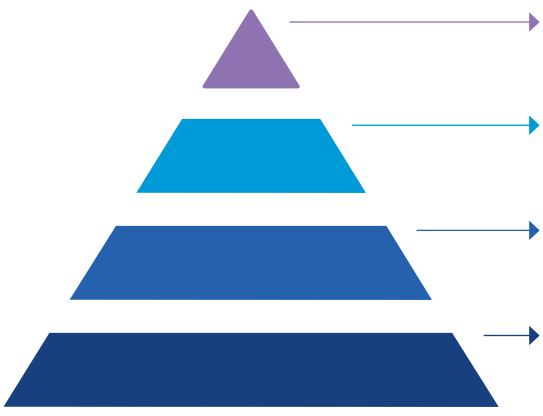
- Permettre des règles harmonisées concernant la mise sur le marché, la mise en service, l'utilisation, la transparence, la surveillance et la gouvernance des systèmes d'IA (SIA).
- Garantir que les SIA mis sur le marché sont sûrs et respectent la législation existante sur les droits fondamentaux, notamment dans leur gouvernance.
- Assurer la sécurité juridique en vue de faciliter l'investissement et l'innovation.
- Faciliter le développement d'un marché unique pour les applications d'IA.
- Définir les pratiques interdites en matière d'IA.

ZOOM SUR LES SIA À HAUT RISQUE

Un système d'IA est considéré comme à haut risque lorsqu'il est utilisé dans l'un des domaines suivants :

- **Produits avec composants de sécurité**
  Systèmes d'IA intégrés dans des produits soumis à une évaluation de conformité par un tiers (ex. : DM, jouets).
- **Biométrie**
  Identification biométrique à distance, catégorisation des personnes selon des attributs sensibles (race, religion, etc.), reconnaissance des émotions (sauf pour vérification d'identité).
- **Infrastructures critiques**
  Systèmes liés à l'eau, au gaz, à l'électricité, au trafic.
- **Éducation et formation**
  Évaluation des acquis, surveillance des examens, accès à l'éducation.
- **Emploi**
  Recrutement, promotion, licenciement, attribution de tâches, suivi des performances.
- **Services essentiels**
  Évaluation de l'admissibilité aux soins de santé, prestations sociales, crédits, assurances, interventions d'urgence.
- **Justice et maintien de l'ordre**
  Évaluation des risques criminels, polygraphes, prévision de récidive, profilage.
- **Migration et contrôle des frontières**
  Évaluation des risques liés à l'asile, aux visas, identification dans des contextes migratoires.
- **Processus démocratique**
  Systèmes influençant les résultats électoraux ou utilisés dans la recherche juridique.

Les niveaux de risque d'un SIA



- **Risque inacceptable**
  Exigence : interdiction
  Exemple : IA de notation sociale
- **Risque haut**
  Exigence : soumis à des obligations strictes
  Exemple : IA d'analyse des fractures
- **Risque modéré (interaction avec du public)**
  Exigence : obligation de transparence
  Exemple : chatbot
- **Risque minimal (ou usage général)**
  Exigence : pas d'exigence
  Exemple : filtre spam

SYSTÈMES D'IA ET DISPOSITIFS MÉDICAUX
Des réglementations complémentaires

COMMENT S'Y RETROUVER ?

Dans le domaine de la santé, les SIA peuvent avoir des usages multiples à la fois dans le soin (diagnostique, prévention, etc.) et dans le secteur administratif (chatbot, etc.).

Une application numérique peut ainsi être à la fois :

- dispositif médical et système d'IA ;
- dispositif médical sans être système d'IA ;
- système d'IA sans être dispositif médical.

Ce qui est important, c'est le **niveau de risque** dans lequel l'IA Act classe le SIA.

À noter que les DM et DMDIV qui intègrent de l'IA sont considérés automatiquement comme des SIA à haut risque car régis par la législation d'harmonisation de l'Union européenne (annexe I de l'IA Act).

CERTIFICATION OU AUTODÉCLARATION ?

Les modalités de mise en conformité diffèrent selon le niveau de risque :

- **Risque minimal :** aucune obligation de conformité spécifique.
- **Risque modéré :** obligation de transparence uniquement (information des utilisateurs).

Pour **les SIA à haut risque**, plusieurs modalités existent :

- Pour les SIA déjà couverts par une législation européenne (annexe I) comme les DM : l'organisme certificateur réalise la double évaluation requise (règlement 2017/745, ou RDM, et IA Act). Le marquage CE est obligatoire.
- Pour les SIA non couverts par une législation européenne (annexe III) : certification ou autodéclaration de conformité par le fournisseur.

Selon la nature du SIA, la durée de certification varie de 4 à 5 ans.

La législation sur l'IA ne s'applique à aucune activité de recherche, d'essai ou de développement concernant des SIA ou des modèles d'IA avant leur mise sur le marché ou leur mise en service.

DM ET NIVEAUX DE RISQUE : QUELQUES EXEMPLES

- IA de gestion des plannings (IA administrative) : risque minimal, aucune exigence.
- IA avec un robot d'accueil (IA administrative) : risque modéré, obligation de transparence et d'information des utilisateurs.
- IA d'analyse des fractures (IA de diagnostic, annexe I - DM) : risque haut, double certification RDM et IA Act.
- IA de sécurisation des prescriptions médicamenteuses (IA thérapeutique, annexe I - DM) : risque haut, double certification RDM et IA Act.
- IA de recrutement de personnel de santé (IA administrative, annexe III) : risque haut, autodéclaration du fournisseur.

EXIGENCES FOURNISSEURS :
Que doivent respecter les logiciels que vous achetez ?

Le règlement IA Act distingue cinq catégories d'acteurs essentiels dans le cycle de vie des SIA : les fournisseurs, les mandataires, les importateurs, les distributeurs et les déployeurs. Les fournisseurs sont les entités qui développent ou font développer un SIA. Ils portent la responsabilité principale de la conformité du système avec les exigences du règlement.

POUR TOUS LES FOURNISSEURS DE SIA À USAGE GÉNÉRAL

L'IA Act a établi des exigences spécifiques applicables aux SIA à usage général (large spectre de fonctionnalités comme les assistants virtuels ou les grands modèles type OpenAI) :

- élaboration et mise à jour de la documentation technique du modèle d'IA ;
- élaboration et mise à disposition du public d'un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général ;
- enregistrement dans **la base de données de l'UE**.

POUR LES FOURNISSEURS D' IA GÉNÉRATIVES

Des exigences complémentaires sont prévues pour les IA à risque systémique (modèles d'IA très puissants et polyvalents dont l'usage pourrait avoir des impacts majeurs et généralisés, par exemple, les IA génératives) :

- évaluation des modèles et atténuation des risques systémiques éventuels ;
- suivi, documentation et communication au Bureau de l'IA (créé par l'IA Act) des incidents graves et des mesures correctrices ;
- garantie d'un niveau approprié de protection en matière de cybersécurité et d'infrastructure physique.

POUR LES FOURNISSEURS DE SIA À HAUT RISQUE

L'IA Act a établi des exigences supplémentaires applicables aux SIA à haut risque :

- mise en place d'un système de gestion des risques et de la possibilité d'un contrôle humain effectif ;
- respect des règles de gouvernance et de qualité des jeux de données utilisées pour entraîner l'IA ;
- enregistrement et traçabilité des événements (journalisation automatique) ;
- transparence et fourniture d'informations aux déployeurs sur la conception et le développement de l'IA ;
- exactitude, robustesse et cybersécurité tout au long du cycle de vie du SIA ;
- soumission du SIA à la procédure d'évaluation de la conformité (notamment **apposition du marquage CE**).

DE DÉPLOYEUR À FOURNISSEUR

Un établissement de santé peut être considéré comme un « fournisseur » s'il :

- développe ou fait développer en propre un SIA pour une commercialisation ou un usage en interne ;
- commercialise sous son nom propre un SIA déjà mis sur le marché ;
- modifie un SIA au point d'en altérer l'objet, le comportement ou les performances ;
- modifie un modèle d'IA générative pour un usage spécifique.

ÉTABLISSEMENTS DE SANTÉ : Quelles évolutions pour vous ?

Selon l'IA Act, les établissements de santé sont considérés comme des « déployeurs » dès qu'ils utilisent un SIA.

UNE RESPONSABILITÉ RENFORCÉE

Bien que le fournisseur demeure le garant principal de la conformité de son SIA, les établissements seront tenus de respecter certaines obligations. Les SIA à haut risque impliqueront une responsabilité accrue pour les établissements utilisateurs.

Ils devront s'assurer que le SIA est :

- conforme à l'IA Act et aux règlements DM/DMDIV (marquage CE) ;
- fonctionnel et que les défaillances ou effets indésirables survenus sont documentés et signalés aux fournisseurs et aux autorités du marché ;
- soumis à un contrôle humain.

Le cas échéant ils assurent la tenue des journaux générés automatiquement.

DES PRATIQUES INTERNES À ADAPTER

Pour les usages de SIA à haut risque, les établissements devront également adapter leur organisation interne et s'assurer que les utilisateurs ont reçu une formation adaptée pour leur permettre d'expliquer les décisions prises avec ou à l'aide de l'IA. Par exemple, ils devront procéder à la mise en place d'une procédure de remontée des incidents, d'un plan de formation spécifique à l'usage des SIA, etc.

Ces évolutions doivent permettre de répondre :

- à la mise en place de mesures techniques et organisationnelles conformes aux notices d'utilisation du SIA ;
- au besoin de contrôle du SIA par des personnes qui disposent des compétences, de la formation, de l'autorité et du soutien nécessaire pour en faire usage.

UNE PLUS GRANDE TRANSPARENCE DES USAGES ATTENDUE

L'IA Act impose une grande transparence dans l'usage des SIA en interaction avec le public. Les établissements ont l'obligation d'informer toutes les personnes en contact avec l'IA, les professionnels comme les patients. Par exemple, le patient doit être prévenu dans le cas d'une interaction avec un callbot.

Pour les SIA à haut risque, le règlement souligne l'obligation de fournir aux utilisateurs une notice d'utilisation qui reprend les caractéristiques, les capacités et les limites de l'IA.

UNE VIGILANCE ACCRUE SUR LA DONNÉE

Le déployeur exerce un contrôle sur les données d'entrée vers les SIA à haut risque. Il a pour responsabilité que ces données soient « pertinentes et suffisamment représentatives au regard de la destination du système ». Cette obligation est particulièrement importante pour les SIA en apprentissage continu.

IA ACT OU RGPD : QUI PRIME ?

L'IA Act et le règlement général sur la protection des données (RGPD) s'appliquent de façon complémentaire et doivent être respectés simultanément dès lors qu'un SIA traite des données personnelles, aussi bien pour son développement et son déploiement.

Le SIA devra ainsi garantir la protection des données de santé (RGPD) et la conformité technique et organisationnelle exigée par l'IA Act.

LES BONS RÉFLEXES « IA ACT »
Par où commencer ?

CONFORMITÉ IA : VOTRE CHECK-LIST EN 4 TEMPS

1 Réaliser un état des lieux de tous les SIA présents et de leurs usages au sein de l'établissement.

2 Définir par SIA son domaine d'application, ses utilisateurs et donc sa nature de risque selon l'IA Act.

3 Vérifier pour chaque SIA sa conformité et le respect par le fournisseur des exigences prévues par l'IA Act.

4 S'assurer que, pour chaque SIA, l'établissement a mis en place les actions permettant de répondre aux exigences de l'IA Act et du RGPD.

Nature de l'IA selon l'IA Act	À vérifier auprès du fournisseur	Information de l'utilisation d'un SIA auprès des professionnels	Information de l'utilisation d'un SIA auprès des patients	Plan de formation à destination des utilisateurs	Soumis à un contrôle humain	Suivi qualité et gestion spécifiques des risques et incidents IA
SIA à risque minimal						
SIA à risque modéré (interaction avec le public)			Requis	Recommandé	Recommandé	Recommandé
SIA à haut risque couvert par la législation européenne, comme les DM (annexe I)	Certification par un organisme tiers à partir du 02/08/2027	Requis	Seulement en cas d'interaction avec le patient	Requis	Requis	Requis
SIA à haut risque non couvert par la législation européenne (annexe III)	Autodéclaration ou certification à partir du 02/08/2026	Requis	Seulement en cas d'interaction avec le patient	Requis	Requis	Requis

Récapitulatif des exigences de l'IA Act demandées aux déployeurs de SIA par niveau de risque.

CALENDRIER DE MISE EN ŒUVRE
De l'IA Act

2024

22 avril 2024
Adoption de l'**IA Act.**

2025

2 février 2025
Entrée en application des interdictions relatives à certains SIA (IA inacceptables).

2 août 2025
Entrée en application des règles relatives aux organismes notifiés, **aux nouveaux modèles d'IA à usage général**, à la gouvernance, à la confidentialité et aux sanctions.

2026

2 août 2026
Entrée en application des autres dispositions de la loi sur l'IA à l'exception de celle relative à la classification des SIA à haut risque présents en annexe I.

Entrée en application des exigences et obligations pour **les nouveaux SIA à haut risque (annexe III)** et pour **les SIA à haut risque déjà mis sur le marché qui font l'objet d'une modification importante** dans leur conception à partir de cette date.

2027

2 août 2027
Les modèles d'IA à usage général mis sur le marché avant le 2 août 2025 doivent être conformes aux exigences de l'IA Act.

Entrée en application des exigences de l'IA Act aux **SIA à haut risque déjà soumis à une législation européenne (annexe I).**

LES OUTILS ET PUBLICATIONS
Pour vous aider

IA Act
➔ www.europarl.europa.eu

Code de bonnes pratiques sur l'IA à usage général
➔ www.digital-strategy.ec.europa.eu/fr/news/general-purpose-ai-code-practice-now-available

Règlements DM et DMDIV
➔ www.eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017R0746

➔ https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017R0745

Cartographie des usages du numérique dans l'offre de soins DGOS
➔ www.sante.gouv.fr/systeme-de-sante/e-sante/usages-du-numerique-dans-l-offre-de-soins/article/numerique-et-offre-de-soins

Déployer l'IA en toute confiance
➔ https://www.anap.fr/s/article/Déployer-l-Intelligence-Artificielle-en-toute-confiance

Observatoire des usages de l'IA en santé
➔ https://www.anap.fr/s/article/numerique-publication-2855

l'anap
l'expertise en partage
agence nationale de
la performance sanitaire
et médico-sociale

L'Agence nationale de la performance sanitaire et médico-sociale est une agence publique de conseil et d'expertise qui agit avec et pour les professionnels des établissements sanitaires et médico-sociaux. Depuis 2009, elle a pour mission de soutenir, d'outiller et d'accompagner les établissements dans l'amélioration de leur performance sous toutes ses dimensions. Pour la mener à bien, l'Anap propose une offre d'accompagnement globale : diffusion de contenus opérationnels, organisation et animation de la mise en réseau et intervention sur le terrain.

Pour plus d'information :
www.anap.fr

Anap
23, Avenue d'Italie
75013 Paris
Tél. : 01 57 27 12 00

Retrouvez-nous sur

anap.fr

DATA_IA_02
IMPRIM'VERT®