Nathalie DE GROVE-VALDEYRON
Claire BORIES
Directrices scientifiques

Claire BORIES
Coordinatrice

Bulletin de l'EDiHL

European Digital Health Law

ACTUALITÉ DU DROIT EUROPÉEN DU NUMÉRIQUE EN SANTÉ

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

À LA UNE

N° 3

3ème année – Bulletin annuel
Juin 2025 – Juin 2026

Cofinancé par l'Union européenne

Financé par l'Union européenne.

Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables

Funded by the European Union.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

ÉDITORIAL

Nathalie DE GROVE-VALDEYRON
Professeure de droit public
Chaire Jean Monnet (2017-2023) et (2023 - 2026)
Université Toulouse Capitole – IRDEIC

Ce troisième bulletin, qui sera le dernier de la Chaire EDIHL (European Digital Health Law, 2023-2026) se situe dans le prolongement des deux précédents. Il reprend les éléments marquants de l'actualité tant législative que contentieuse, dans le domaine du numérique en santé, tout en se caractérisant par une plus grande place donnée à la mise en œuvre, par les Etats membres, des règlements récemment adoptés, et tout particulièrement, du Règlement sur l'Espace européen des données de santé (ci-après EEDS). Comme cela a déjà été précisé dans les éditions précédentes, si le règlement est bien en vigueur, il implique cependant d'une part, que les États satisfassent à un certain nombre d'obligations préalables pour pouvoir le mettre en œuvre de manière effective, et d'autre part, que les actes d'exécution attendus de la part de la Commission soient aussi adoptés pour disposer d'éléments techniques indispensables.

On peut souligner ici le rôle important joué par l'action conjointe TEHDAS 2 afin de répondre aux questions que les différentes parties prenantes, les acteurs du numérique et, au premier chef, les citoyens se posent sur les conséquences du règlement tant dans le cadre de l'utilisation primaire que de l'utilisation secondaire des données de santé électroniques.

Le lecteur trouvera en outre dans ce bulletin, en français, l'essentiel du contenu des « Guidelines » de TEHDAS soumises encore à consultation publique. Non moins essentielles, les « Guidelines » de l'EMA (Agence européenne des médicaments) adoptées dans le domaine des dispositifs médicaux connectés (DMC) (ou numériques, DMN) apportent des précisions indispensables aux développeurs de tels dispositifs. S'agissant toujours de ces dispositifs médicaux numériques, une incursion dans le droit français (principes applicables par la CNEDIMTS) et dans le droit suédois permet d'avoir une idée des différences de mode de prise en charge de ces DM, en fonction des particularités étatiques, la question du remboursement restant, conformément à l'art. 168 du TFUE, de l'unique compétence des États membres.

On relèvera aussi deux études de première main sur la mise en œuvre de l'EEDS en Italie et en Irlande, des textes ayant été récemment adoptés dans ces deux États. Des textes importants adoptés en Espagne ou en Belgique sont également rapidement évoqués, la dimension du bulletin ne permettant pas de faire état des avancées réalisées au sein de chacun des États membres. Le bulletin comporte enfin, dans le cadre de sa partie contentieuse, les commentaires de quelques arrêts marquants adoptés par le Conseil d'État (France) ou par la Cour de justice.

Ce bulletin n'aurait pu voir le jour sans la participation de fidèles doctorants (Noémie, Lisa, Valentine, Winnie), dont certains sont devenus docteurs depuis le début de la chaire. De plus anciens doctorants encore, devenus avocats (Sarah) ou occupant des fonctions au sein du ministère de la santé (Claire) ont souhaité continuer à s'investir pour le bulletin, malgré leurs obligations professionnelles. Qu'ils soient chaleureusement remerciés.

Mes remerciements vont aussi aux étudiants qui ont découvert cette nouvelle discipline qu'est le droit européen du numérique en santé, grâce au *DU EDIHL* (Thomas, Franck) mais aussi au cours de *droit européen du numérique en santé* que j'ai pu créer grâce à la chaire J Monnet, à l'École de droit de Toulouse (UTC) (Chaimae, Laure, Philippine, Thomas pour cette année 2025-2026). Merci aussi aux étudiants du Master 2 juriste européen et droit européen international et comparé (Salaheddine, Joud, Maddalena) et du Master 2 Santé (Alizée, Lukas, Amina, Marie, Clarance, Mélanie, Maïlys). Enfin mes remerciements les plus chaleureux vont à Claire BORIES, qui s'est chargée, cette année encore, malgré ses obligations professionnelles, de toute la réalisation formelle du bulletin et de la coordination scientifique. Bonne lecture !

Bulletin de l'EDiHL
European Digital Health Law

SOMMAIRE

N°3 /
3ème année – Bulletin annuel
Juin 2025-Juin 2026

VEILLE LÉGISLATIVE

Droit de l'Union européenne

Droit français

Droit belge

Droit espagnol

Droit irlandais

Droit italien

Droit suédois

VEILLE CONTENTIEUSE

Droit de l'Union européenne

Droit français

Droit de l'Union européenne

Étude européenne sur le déploiement de l'IA dans les soins de santé

La Commission européenne (DG SANTE) publie en 2025 une étude consacrée au déploiement de l'intelligence artificielle (IA) dans les systèmes de santé européens. Réalisée à partir d'une revue de littérature, d'enquêtes, d'ateliers et d'études de cas, cette étude analyse à la fois les potentialités offertes par l'IA et les principaux obstacles à son intégration dans la pratique clinique.

Le rapport souligne que les systèmes de santé européens sont confrontés à plusieurs **défis structurels** : vieillissement de la population, augmentation des maladies chroniques, pénurie de professionnels de santé, hausse des dépenses de santé et surcharge administrative. Dans ce contexte, l'IA est présentée comme un levier susceptible d'améliorer l'efficacité opérationnelle des établissements de santé, de réduire les charges administratives et d'améliorer les parcours de diagnostic et de traitement.

Les usages considérés comme les plus prometteurs concernent notamment l'optimisation des flux hospitaliers et de l'allocation des ressources, l'automatisation des tâches administratives et de la documentation clinique, les outils d'aide au diagnostic, la médecine prédictive et personnalisée, ainsi que la télésurveillance et le triage des patients. L'étude cite plusieurs exemples concrets de déploiement dans les établissements de santé, notamment des outils utilisés dans les services d'urgence afin d'améliorer le triage des patients et de réduire les temps d'attente, des solutions déployées en radiologie et en oncologie pour améliorer les performances diagnostiques, ainsi que des outils conversationnels et des modèles de langage destinés à automatiser une partie de la documentation clinique et des tâches administratives.

Toutefois, malgré le potentiel identifié et la disponibilité croissante d'outils d'IA sur le marché, le rapport constate que leur déploiement dans la pratique clinique demeure encore lent. Plusieurs freins sont identifiés : difficultés liées à l'interopérabilité et à la gouvernance des données, insuffisance des infrastructures numériques, complexité du cadre réglementaire, enjeux de cybersécurité et de protection des données, ainsi que manque de confiance et de formation des professionnels et des patients. Le rapport souligne par exemple que certains outils d'IA utilisés dans les services d'urgence ou pour le triage des patients nécessitent une adaptation importante aux organisations locales et aux besoins médicaux

spécifiques. Il insiste également sur les difficultés rencontrées par les établissements de santé pour intégrer ces outils dans des systèmes d'information parfois peu interopérables et insuffisamment adaptés au traitement des données de santé à grande échelle.

Le rapport insiste enfin sur le fait que l'Union européenne dispose d'un cadre particulièrement favorable pour accompagner le développement d'une IA en santé qui soit sûre, efficace, éthique et respectueuse des droits fondamentaux des patients. Il met notamment en avant le rôle du cadre réglementaire européen — AI Act[1], règlement sur l'Espace européen des données de santé (EHDS)[2], RGPD[3] et règlements applicables aux dispositifs médicaux[4] — comme levier structurant pour encadrer et accompagner ce déploiement.

Dans cette perspective, l'étude formule plusieurs **pistes d'action** afin de favoriser une intégration durable de l'IA dans les systèmes de santé européens : développement de standards communs d'interopérabilité, soutien à des centres d'excellence et à des mécanismes de financement adaptés, renforcement des outils d'évaluation et de suivi du déploiement de l'IA en santé. Le rapport propose également un véritable cadre de suivi (« *monitoring framework* ») reposant sur des indicateurs et des mécanismes d'évaluation destinés à mesurer, dans le temps, le niveau de déploiement des outils d'IA, leurs effets sur l'organisation des soins et les difficultés rencontrées lors de leur mise en œuvre.

DG Santé, *Study on the deployment for AI in healthcare. Final report*, January 2024-2025, 241p.

[1] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union et modifiant les règlements n° (CE) 300/2008, n° (UE) 167/2013 n° (UE) 168/2013, n° (UE) 2018/858, n° (UE) 2018/1139 et n° (UE) 2019/2144 et les directives n° (UE) 2014/90, (UE) 2016/797 et n° (UE) 2020/1828 (règlement sur l'intelligence artificielle – « AI Act »), *JOUE* n° L 2024/1689 du 12/07/2024.

[2] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive (UE) 2011/24 et le règlement (UE) 2024/284, *JOUE* n° L 2025/327 du 05/03/2025.

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 (règlement général sur la protection des données – « RGPD »), *JOUE* n° L 119/1 du 04/05/2016.

[4] V. notamment, règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, *JOUE* n° L 117/I du 05/05/2017 et règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive (CE) 98/79 ainsi que la décision (UE) 2010/227 de la Commission, *JOUE* n° L 117/I du 05/05/2017.

Aperçu général sur le plan européen pour vaincre le cancer

Présenté par la Commission européenne en 2021, le Plan européen pour vaincre le cancer constitue l'une des principales stratégies européennes en matière de santé publique. Il vise à renforcer l'action de l'Union européenne tout au long du parcours de soins en cancérologie, depuis la prévention et le dépistage jusqu'au diagnostic, au traitement et à la qualité de vie des patients.
Parmi les initiatives structurantes prévues par ce plan figure notamment l'**initiative européenne en matière d'imagerie du cancer,** présentée comme l'une des actions phares du volet numérique et innovation.

La Cour des comptes européenne a par ailleurs publié en février en 2026 un rapport spécial consacré à la mise en œuvre du Plan européen pour vaincre le cancer, soulignant les avancées engagées mais également plusieurs défis persistants en matière de coordination, de financement et de déploiement opérationnel des actions prévues.

INITIATIVE EUROPÉENNE EN MATIÈRE D'IMAGERIE SUR LE CANCER

Initiative européenne en matière d'imagerie sur le cancer : action phare du plan européen pour vaincre le cancer

par Joud GHARZEDDINE

Étudiante en Master 2 Droit des Libertés et titulaire du Master 2 Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Introduction

« Construire une Union européenne de la santé : renforcer la résilience de l'UE face aux menaces transfrontières pour la santé ». Tel était le titre de la communication de la Commission européenne du 11 novembre 2020 qui faisait état, dans le contexte de la lutte contre la pandémie de la Covid-19, de la nécessité de coordonner les actions nationales afin de garantir leur efficacité[5]. Ce constat ne se limite toutefois pas à ce contexte spécifique. Il pourrait même être légitimement soutenu qu'il n'émerge aucunement du fait de ce contexte. En effet, dès 2019, un combat est placé au centre des préoccupations de la Commission : la lutte contre le cancer[6]. Cette lutte silencieuse[7], portée tant par la Commission[8] que par sa présidente[9], se traduit par un engagement politique fort, baptisé le **plan européen pour vaincre le cancer**[10].

[5] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 11 novembre 2020, *COM(2020)* 724 final (consulté le 22/03/2026).
[6] En atteste le discours prononcé à la séance plénière du Parlement européen par la présidente de la Commission européenne, le 27 novembre 2019 (consulté le 24/03/2026).
[7] Communiqué de presse IP/21/342 de la Commission européenne sur le Plan européen pour vaincre le cancer : une nouvelle approche européenne de la prévention, du traitement et des soins, Bruxelles, le 3 février 2021 (consulté le 24/03/2024).
[8] En 2020, un cancer a été diagnostiqué chez 2,7 millions de citoyens européens et 1,3 ont perdu la vie. En l'absence de mesures concrètes dans ce domaine, les cas de cancer devraient augmenter de 24% d'ici à 2035, ce qui en ferait la cause principale de décès dans l'Union européenne. Ces chiffres, présentés par la Commission et repris dans le communique de presse *précité*, sont corroborés par ceux du Centre international de recherche sur le cancer de l'Organisation mondiale de santé qui prévoient une augmentation de 19,2% d'ici à 2035 en se basant sur le nombre de décès en Europe de cancer en 2022 (consulté le 31/03/2026).
[9] Dans le discours prononcé à la séance plénière du Parlement européen en 2019, *précité*, la présidente s'exprime en ces termes : *« Quand j'étais jeune fille, à Bruxelles, ma petite sœur est décédée d'un cancer à l'âge de 11 ans. Je me souviens du sentiment d'impuissance totale de mes parents – mais aussi du personnel médical qui lui a prodigué tant de soins. Chacun d'entre nous a une histoire semblable à raconter – ou connaît quelqu'un qui a vécu la même expérience. »*.
[10] L'ensemble des documents relatifs à ce plan sont disponibles sur la page web du site de la Commission qui lui est dédiée (consulté le 31/03/2026).

Ce plan se décline en plusieurs actions parmi lesquelles figure l'**initiative européenne en matière d'imagerie sur le cancer**. Cette dernière, lancée officiellement en décembre 2022, se décline elle-aussi en deux axes principaux. Le premier axe vise à mettre fin à l'éparpillement des données d'imagerie du cancer, ce qui limite leur réutilisation à des fins de recherche et d'innovation. La lutte contre cet éparpillement est ainsi placée au cœur du projet **EU**ropean Federation for **CA**ncer **Im**ages, dit aussi « EUCAIM » (I). Le second axe, dans le prolongement du premier, repose sur la centralisation des données au sein d'une infrastructure sécurisée. Cette centralisation faciliterait leur utilisation secondaire, nécessaire à la validation d'algorithmes d'intelligence artificielle (ci-après « IA) qui améliorent la prévention, le diagnostic et le traitement du cancer (II).

I. LA CENTRALISATION DES DONNÉES D'IMAGERIE DU CANCER, AU CŒUR DU PROJET EUCAIM

Le projet « EUCAIM » est la pierre angulaire du plan européen pour vaincre le cancer. Ce projet, lancé en janvier 2023 et financé dans le cadre du programme **DIGITAL**[11], met en œuvre l'initiative européenne en matière d'imagerie sur le cancer en déployant la plateforme **Cancer Image Europe**.

Il s'agit d'une infrastructure numérique, sécurisée et fédérée qui relie les initiatives européennes et nationales dans ce domaine ainsi que les différents réseaux et référentiels de recherche abritant de telles données. L'initiative s'appuie ainsi tout particulièrement sur les réalisations du réseau **AI for Health Imaging** (« AI4HI »), qui regroupe cinq grands projets financés par l'Union européenne sur le big data et l'IA dans le domaine susvisé[12]. Deux projets additionnels, financés dans le cadre du programme **EU4health**[13], étendent cette initiative autour du dépistage et de la détection précoce du cancer : **Unified Network for International Cancer Advancement**[14] et **Breast Image Platform for Advanced AI-Based Breast Cancer Screening**[15].

Face à ces nombreuses initiatives – européennes comme nationales – déjà entreprises dans ce domaine, une question se pose : *au vu de leur importance, quel intérêt présente réellement le déploiement de cette nouvelle infrastructure ?*

La réponse est à la fois claire et complexe, telle que le révèle l'explication même de cette initiative qui se situe au carrefour de plusieurs plans, programmes et stratégies. Le premier avantage résulte du fait qu'elle se bâtit autour d'une infrastructure *« unique »*. Cette caractéristique favorise le partage des données d'imagerie et la collaboration entre prestataires de soins de santé, chercheurs et innovateurs de plusieurs pays. En effet, si les nombreuses initiatives en la matière ont donné naissance à des référentiels d'imagerie, ceux-ci sont souvent spécifiques à un projet, limités dans le temps et *de facto* restreints dans la capacité à être réutilisés[16].

[11] Selon le site dédié à ce programme, DIGITAL – plus connu sous le nom de *programme pour une Europe numérique* – est un programme de financement de l'Union européenne qui vise à apporter la technologie numérique aux entreprises, aux citoyens et aux administrations publiques (consulté le 30/03/2026).

[12] Il s'agissait des projets suivants : Chaimeleon, EuCanImage, ProCancer-I, Incisive et Primage. Une explication détaillée de chacun de ces projets est disponible en ligne (consulté le 30/03/2026).

[13] Pour plus d'informations concernant ce programme, se référer à la page web de la Commission européenne qui lui est dédiée.

[14] https://www.unica-project.eu/.

[15] https://cancerimage.eu/breastscan/.

[16] Carina SOLER PONS,Ana DE MARCO GARCIA, Ricard MARTINEZ et *al.*, « How the First Medical Imaging Cancer Atlas EUCAIM Was Populated : The Experience of a Reference Hospital [Version 3; Peer Review: 2 Approved, 1 Approved with

Le second avantage résulte, quant à lui, du fait que l'infrastructure a été conçue dans le respect des règlementations européennes relatives aux données personnelles, à savoir le règlement général sur la protection des données (RGPD)[17], le règlement européen sur l'intelligence artificielle (AI Act)[18] et plus récemment le règlement relatif à l'espace européen des données de santé (EHDS)[19]. Elle constitue donc un cadre sécurisé dans lequel le traitement licite des données personnelles est assuré. Cela favorise l'utilisation secondaire de ces dernières, élément indispensable à la validation de toute innovation fondée sur l'IA.

II. UN CADRE INSTITUTIONNEL SECURISE, FAVORABLE A L'INNOVATION PAR UN ACCÈS MASSIF AUX DONNÉES

« Si nous souhaitions créer des technologies novatrices dans le domaine du cancer, il faut permettre l'accès à une masse critique de données »[20] affirmait Marco Marsella lors de l'évènement de lancement de l'initiative en matière d'imagerie sur le cancer en 2023. La plateforme **Cancer Image Europe** assure aisément cet accès en ce qu'elle vise à rassembler, d'ici la fin de 2026, *« plus de 100 000 cas et 60 millions d'images »*. Ces données sont de haute qualité et respectent des normes communes concernant leur anonymisation, leur standardisation, leur annotation et leur curation[21]. De plus, l'utilisabilité de l'infrastructure suit les principes FAIR[22], ce qui implique que les données soient *« traçables, accessibles, interopérables et réutilisables »*[23].

Cet accès massif à des données standardisées permet *« la réalisation d'études de validation de l'IA à grande échelle et multicentriques »*. Il aide à produire des preuves quant à *« l'utilité clinique des solutions d'IA »*, de nature à accélérer leur déploiement dans des environnements cliniques réels. En effet, s'il n'est nullement contesté aujourd'hui que les outils numériques intégrant l'IA améliorent significativement l'exactitude des diagnostics et permettent une détection précoce, l'obstacle[24] qui perdure est celui de renforcer la confiance dans l'IA. L'EUCAIM relève cet obstacle, expliquant le rôle central qui lui est octroyé dans la réalisation des objectifs de la stratégie **Appliquer l'IA**[25].

Reservations] », *Open Res Europe 2025*, vol. 5, n° 310 (consulté le 22/03/2026).

[17] Règlement (UE) 2016/679 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.

[18] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements n° (CE) 300/2008, n° (UE) 167/2013, n° (UE) 168/2013, n° (UE) 2018/858, n° (UE) 2018/1139 et n° (UE) 2019/2144 et les directives n° (UE) 2014/90, (UE) 2016/797 et n° (UE) 2020/1828 (règlement sur l'intelligence artificielle).

[19] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° (UE) 2011/24 et le règlement n° (UE) 2024/2847.

[20] Traduction libre de la prise de parole de M. Marco MARSELLA, à l'époque chef de l'unité « eHealth, Well-Being, Ageing », lors de l'évènement de lancement de l'initiative en matière d'imagerie sur le cancer en janvier 2023 (consulté le 22/03/2026).

[21] Carina SOLER PONS et *al.*, *précité*.

[22] Luis MARTI-BONMATI, Ignacio BLANQUER, Manolis TSIKNAKIS et *al.*, « Empowering cancer research in Europe : the EUCAIM cancer imaging infrastructure », *Insights Imaging*, vol. 16, n° 47, 2025 (consulté le 22/03/2026).

[23] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

[24] Pour une liste plus détaillée des Défis liés à l'intégration de l'IA dans les soins de santé, voir : https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_fr.

[25] Il s'agit de la stratégie sectorielle globale de l'Union européenne en matière d'intelligence artificielle. Pour plus d'informations, se référer à la page web du site de la Commission qui y est dédiée.

Conclusion

L'étude de l'initiative européenne en matière d'imagerie sur le cancer nous amène à un constat : l'Union européenne bâtit, initiative par initiative, stratégie par stratégie et plan par plan, un écosystème favorable à l'innovation et à la recherche fondée sur l'IA. Elle vise à se placer en tête du combat contre le cancer, sans pour autant négliger la protection accrue que réserve sa législation aux données de santé. Il en résulte une Union qui, *« Unie dans la diversité »,* devient une Union *« Unie dans l'Unique »*[26]

[26] Il s'agit du thème de la Journée Mondiale contre le Cancer 2025-2027.

INITIATIVE EUROPÉENNE « +1 MILLION GENOMES » (1+MG°)

L'initiative européenne « 1+ Million Genomes » (1+MG) *constitue l'une des principales actions européennes en matière de données génomiques et de médecine personnalisée. Lancée en 2018, elle vise à favoriser le partage sécurisé de données génomiques et cliniques à l'échelle européenne afin de soutenir la recherche et l'innovation. Son objectif est de permettre la mise à disposition de plus d'un million de génomes pour améliorer la prévention, le diagnostic et la prise en charge de nombreuses pathologies, notamment les cancers et les maladies rares.*

Émergence d'une infrastructure européenne fédérée au service de la génomique et de la médecine personnalisée

Le Genomic Data Infrastructure (GDI), dans le cadre de l'initiative européenne « 1+ Million Genomes » (1+MG)

par Salaheddine ZAHID

Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Le développement de la médecine personnalisée constitue aujourd'hui l'un des axes les plus structurants de l'évolution contemporaine des systèmes de santé. Les progrès réalisés dans les technologies de séquençage ont transformé les capacités d'analyse du génome humain, permettant la production massive de données génétiques exploitables à des fins diagnostiques, thérapeutiques et préventives. La génomique occupe désormais une place centrale dans des domaines tels que les maladies rares, l'oncologie de précision, la pharmacogénomique ou encore la médecine prédictive[27].

Cette évolution scientifique s'accompagne d'un défi majeur, à savoir que la valeur clinique et scientifique des données génomiques dépend de leur capacité à être comparées et exploitées à grande échelle.

Or, les données génomiques européennes demeurent fragmentées. Elles sont produites et conservées au sein d'infrastructures nationales, de centres hospitaliers, de biobanques ou de programmes de recherche qui se reposent sur des standards techniques, des terminologies et des cadres juridiques hétérogènes[28].

Face à la dispersion des bases nationales et aux contraintes légales, l'Union européenne a lancé en 2018 l'initiative *1+ Million Genomes* (1+MG)[29]. Vingt-six pays européens[30] ont signé une déclaration visant à permettre un accès sécurisé et transfrontalier aux données génomiques européennes afin de soutenir la recherche médicale, les politiques de

[27] Voir en ce sens, l'initiative européenne « 1+ Million Genomes » ; et la note d'orientation « Genomics in Healthcare. Key issues for implementation ».

[28] Voir en ce sens, la fiche technique « D8.2 Integration of genomics and phénotypic data » publiée le 3 février 2026 ; et la feuille de route B1MG 2023-2027.

[29] Déclaration de coopération, « Towards acess to at least 1 million sequenced genomes in the European Union by 2022 », Bruxelles, 10 avril 2018.

[30] Plus le Royaume-Uni et la Norvège.

santé publique et le développement de la médecine personnalisée. La déclaration identifie trois objectifs principaux : la mise en place d'une infrastructure technique permettant un accès fédéré sécurisé aux données génomiques ; le développement d'un cadre éthique et juridique adapté ; ainsi que l'intégration progressive de la génomique dans les systèmes européens de santé.

Pour concrétiser cette vision, le projet *Genomic Data Infrastructure* (GDI) a été conçu comme l'instrument technique majeur de la phase d'extension du *1+ MG*. Il ne centralise pas les données, au contraire, il définit une architecture fédérée (**I**) où chaque pays conserve ses propres référentiels[31]. Le GDI met en place les interfaces et standards techniques nécessaires[32] pour permettre des requêtes inter-systèmes[33]. Les ensembles de données demeurent donc sous le contrôle des infrastructures numériques nationales (**II**), tandis que le GDI organise les mécanismes d'interrogation, de découverte et de coordination des accès. Cette architecture repose sur des standards ouverts développés notamment par la *Global Alliance for Genomics and Health*, afin de garantir l'interopérabilité entre les systèmes nationaux[34].

I. UNE ARCHITECTURE EUROPÉENNE FEDÉRÉE AU SERVICE DE LA GÉNOMIQUE

Sur le plan opérationnel, le GDI repose sur plusieurs fonctions essentielles : découverte des données, traitement des requêtes, gestion des accès, stockage sécurisé et réception des résultats[35]. Les travaux préparatoires du projet *Beyond One Million Genomes* (B1MG) ont notamment permis de tester plusieurs services interopérables fondés sur les standards de la GA4GH destinés à interroger des bases distribuées notamment afin de « *[o]ffers the possibility to query for the annotations on the variants found, including expert or clinician conclusions — when available — on the pathogenicity of a specific mutation in an individual or its contribution to a particular phenotype* »[36].

[31] Cette approche s'inscrit dans une évolution des pratiques scientifiques en génomique. Les premiers systèmes de partage des données reposaient essentiellement sur des modèles centralisés impliquant le transfert des données vers des dépôts communs. Comme le souligne un article publié le 4 mars 2019 sur le site Nature Biotechnology, *Federated discovery and sharing of genomic data using Beacons*, par plusieurs contributeur.ices, « *many former systems for genomic data sharing have followed a centralized model* […]. *This model requires data generators to transfer whole copies of datasets over the internet, which will become inefficient and expensive as the rate of genomic data acquisition increases. An alternative, federated model for data sharing*[1] *requires organizations to host data independently and to interoperate via an agreed-upon technical language. This model removes the inefficiencies of large data transfers and gives host organizations more control over data privacy, security and representation".*

[32] Pour les aspects techniques, des fiches d'avancements et comptes rendus du projet sont publiées régulièrement sur la page web.

[33] Les documents techniques du projet précisent explicitement que « *data does not need to leave the country of origin* » (GDI « D8.2 Integration of genomics and phénotypic data » précité).

[34] Voir en ce sens « Technical GA4GH Technical Standards Documentation. Policy and processes for developing and communicating maturity of GA4GH Technical Specifications » , 17 September 2025.

[35] Voir en ce sens la documentation B1MG Technical Infrastructure .

[36] Des infrastructures telles que de type *Beacon* dont les bénéfices sont exposés sur le site . Concrètement, un clinicien ou un chercheur peut adresser une requête portant sur un variant donné et recevoir une réponse indiquant si ce variant est présent dans une ou plusieurs bases de données européennes, sans que les données sous-jacentes ne soient transmises. Cette logique est importante dans le domaine des maladies rares, où l'identification de variantes similaires observés dans d'autres pays peut accélérer le

Le GDI repose également sur des mécanismes de gouvernance des accès particulièrement structurés. Les demandes d'accès aux données sont examinées par des *Data Access Committees*, chargés d'évaluer les conditions scientifiques, éthiques et juridiques d'utilisation des données[37]. Les travaux du projet mentionnent également l'utilisation d'outils tels que le *Resource Entitlement Management System (REMS)*, destiné à gérer les autorisations d'accès et les droits des utilisateurs[38].

Le projet doit également composer avec les exigences du Règlement général sur la protection des données de 2016[39], les données génomiques constituant des données sensibles au sens de l'article 9 dudit règlement. L'architecture fédérée permet précisément de limiter les transferts transfrontaliers de données tout en intégrant les principes de « *Data Protection by Design and Default* » prévus à l'article 25 du RGPD[40]. Les mécanismes d'accès distribués permettent ainsi de concilier exploitation scientifique des données et maintien d'un haut niveau de protection des personnes.

Le GDI intègre également une dimension stratégique de confiance et d'acceptabilité sociale. Les documents du projet soulignent l'importance d'une communication destinée à informer les citoyens sur les garanties de sécurité, de gouvernance et d'utilisation responsable des données[41]. Cette question apparaît essentielle dans un contexte où la confiance conditionne directement l'acceptabilité du partage des données génomiques. À cet égard, les professionnels de santé occupent un rôle central dans l'explication des

---

diagnostic et améliorer la caractérisation des pathologies. En oncologie, l'accès à des cohortes européennes permet d'affiner l'interprétation des variants tumoraux et de soutenir le développement de traitements personnalisés (voir en ce sens l'initiative européenne en matière d'imagerie sur le cancer).

[37] Voir en ce sens « Beyond 1 Million Genomes (B1MG) D2.4 Report on data access and governance framework », 5 otobre 2023. Sur les *Data Access Committees*, voir le site internet de la European Genome-Phenome Archive, *What is a DAC ?*.

[38] *Secure cross-border data access roadmap*, version du 23 novembre 2021.

[39] Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive (CE) 95/46 (règlement général sur la protection des données).

[40] L'article 25 du RGPD dispose que : « *1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. 2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.* » ; voir également REGINA Becker et autres « B1MG / 1+MG: IT infrastructure requirements based on a data protection by design and default approach », 4 août 2022.

[41] Deliverable D1.8 Wider Communication Strategy - final evaluation and review, 27 février 2026.

mécanismes de protection et dans l'accompagnement des patients.

Les bénéfices attendus sont alors considérables. L'agrégation fonctionnelle de données issues de plusieurs pays permettrait de constituer des cohortes élargies particulièrement utiles pour les maladies rares et les maladies complexes. Le développement de l'IA appliquée à la santé faciliterait l'accès à des jeux de données plus diversifiés et représentatifs. À long terme, les analyses de ces vastes bases de données pourraient contribuer à renforcer les politiques de santé publique, notamment en matière de prévention, de surveillance épidémiologique ou d'identification précoce des facteurs de risque.

II. LES LIMITES ET DÉFIS DE L'EFFECTIVITE DU *GENOMIC DATA INFRASTRUCTURE*

Toutefois, malgré ces ambitions, le projet demeure confronté à plusieurs limites importantes. Les capacités nationales de séquençage et de structuration des données restent asymétriques. Les données publiées sur les tableaux de bord de l'initiative montrent des écarts entre États membres[42]. Ces disparités reflètent des différences majeures de capacités techniques, financières et institutionnelles en ce qu'elles limitent mécaniquement l'effectivité du GDI et la disponibilité homogène des données génomiques à l'échelle européenne[43].

L'interopérabilité constitue également un défi majeur. Malgré le recours à des standards ouverts, les infrastructures nationales utilisent encore des formats de données, des terminologies cliniques et des référentiels différents[44]. Les documents techniques du projet identifient ainsi des phénomènes de « *geographical, technical, incompatibility, legal and regulatory divergence, semantic barriers* »[45]. Des efforts importants d'harmonisation demeurent donc nécessaires pour assurer une exploitation cohérente des données génomiques à l'échelle européenne.

Enfin, la question de la confiance reste centrale. Toute faille de sécurité ou utilisation abusive des données génomiques pourrait fragiliser la légitimité du projet. Le succès du GDI dépendra donc autant de la robustesse de son architecture technique que de sa capacité à maintenir un haut niveau de protection des données et de transparence vis-à-vis des citoyens.

Dès lors, le GDI apparaît comme l'un des fondements potentiels d'un futur espace européen intégré de médecine personnalisée, dans l'exploitation des données génomiques tout en respectant les enjeux juridiques et éthiques qui structurent la santé numérique européenne.

[42] Renvoi au *1+MG Dashboard Data*. L'Italie se distinguant en ce qu'elle possède 27 datasets contrairement au Danemark qui en a une. Les données génomiques de la France n'étant pas disponibles.

[43] Le projet prévoit qu'au moins quinze pays disposent d'une infrastructure opérationnelle en 2026 (B1MG feuille de route 2023-2027), mais plusieurs États restent loin de cet objectif.

[44] GDI D8.2 précité.

[45] *Ibid.*

INITIATIVE EUROPÉENNE SUR LES JUMEAUX HUMAINS VIRTUELS (VHT)

L'initiative européenne sur les « jumeaux humains virtuels » (« Virtual Human Twins » – VHT) *s'inscrit dans la stratégie européenne de développement de l'IA appliquée à la santé. Elle vise à favoriser l'émergence de représentations numériques du corps humain destinées à mieux comprendre, simuler et anticiper l'évolution des pathologies, dans une logique de médecine personnalisée.*

Commission européenne, European Virtual Humain Twins (VHT) Initiative

par Noémie DUBRUEL

Docteure en Droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier, UMR 1295 Inserm équipe BIOETHICS

Le recours à différents outils numériques, dont l'intelligence artificielle, dans le domaine de la santé permet la création de nombreuses méthodes qui présentent un intérêt considérable pour l'amélioration de la santé, de la recherche et de l'innovation. Parmi celles-ci figure le jumeau humain virtuel (*Virtual Human Twin, VHT*). Ce dernier est défini par la Commission européenne comme une « représentation numérique intégrée à plusieurs niveaux, dans le temps et selon plusieurs disciplines d'un corps, d'un organe ou d'une cellule, permettant la caractérisation complète de l'état physiologique et pathologique dans son hétérogénéité »[46].

S'appuyant sur plusieurs technologies de modélisation et de simulations informatiques, d'intégration de données et de modèles de calcul, cette méthode apparaît particulièrement pertinente pour accélérer l'émergence d'une médecine plus prédictive, préventive et personnalisée. Les VHT présentent alors des opportunités de ciblage des préventions et des parcours cliniques et sont un véritable soutien pour les professionnels de santé et les chercheurs. En effet, ils peuvent particulièrement être sollicités pour la mise en œuvre d'essais cliniques, la formation des professionnels de santé ou bien encore la planification des interventions chirurgicales, par exemple.

Forte des opportunités offertes par ces usages numériques innovants, la Commission européenne a fait le choix d'investir dans leur déploiement, à travers la mise en œuvre d'une initiative spécifique, lancée en décembre 2023 et intitulée « *The European Virtual Human Twins Initiative* »[47]. Le premier objectif poursuivit vise à pallier l'évidente fragmentation de l'écosystème européen dans ce domaine. En effet, si un grand nombre d'innovations émergent en Europe, dans un contexte où le « jumeau numérique » emporte de plus en plus d'intérêt, les méthodes, usages et même terminologies demeurent très disparates, freinant considérablement la

[46] Site officiel de l'initiative : https://www.virtualhumantwins.eu/, (consulté le 30/04/2026).

[47] Commission européenne, "European Virtual Human Twins", Infographics, décembre 2023, p.01.

reconnaissance de cette innovation. Plus encore, la Commission européenne poursuit un objectif fort par le souhait de « renforcer les capacités avancées de supercalcul et l'intelligence artificielle afin de faciliter la recherche collaborative et le développement technologique en matière de VHT ». Afin de répondre à ces attentes, la Commission européenne a d'abord fait le choix de la publication d'un manifeste, officiellement rendu public le 21 décembre 2023, illustrant parfaitement la nécessité de rassembler les différentes forces vives européennes et diverses parties prenantes autour d'une volonté européenne affirmée. Le manifeste, qui a obtenu une centaine de signatures[48], favorise des coopérations et collaborations interdisciplinaires et établit plusieurs pistes d'actions : atteindre un niveau d'excellence européen pour la recherche et l'innovation, identifier des cas d'usage à fort impact clinique et scientifique, valoriser des données et modèles de VHT européens, accompagner et clarifier le paysage réglementaire en la matière, générer des preuves numériques, contribuer à la bonne compréhension des usages des méthodes de VHT et enfin garantir le recours à une technologie au bénéfice du plus grand nombre, permettant un « accès équitable et universel à des traitements sûrs et de qualité »[49].

En complément, diverses actions de recherche et de déploiement alimentent cette initiative. En premier lieu, le projet européen « VHT » (EDITH) permet l'élaboration d'une action de coordination et de soutien financée au titre du programme DIGITAL[50]. Ce projet se veut mettre en évidence les leviers et points bloquants pour le déploiement des VHT en Europe, dans les domaines de la santé et de la recherche, au bénéfice des patients, des professionnels de santé, des régulateurs et de l'industrie. En ce sens, un chantier essentiel réside dans la cartographie et la structuration d'un écosystème collaboratif et inclusif à l'échelle européenne, fondé sur un consensus entre les parties prenantes. De même, le projet insiste sur l'importance de produire une feuille de route permettant de passer des modèles existants (souvent limités à un organe ou à un système) à un VHT multi-échelle, multi-organes, intégré et fondé sur les données et les connaissances.

Par ailleurs, l'initiative repose sur des financements complémentaires générés au titre du programme « Horizon Europe » ainsi que de l'initiative en matière de santé innovante[51] pour de meilleurs suivis et visualisations des accidents vasculaires cérébraux via l'usage de modèles de calcul prédictifs et de données intégrées.

Enfin, le programme pour une Europe numérique (DIGITAL) est source de soutien pour l'initiative VHT en ce qu'il permet le financement d'une plateforme numérique de pointe pour l'intégration et la validation de modèles de jumeaux humains virtuels. Initié le 26 juin 2025, le processus de développement d'une plateforme met en évidence la forte volonté de la Commission européenne de déployer les générations et les usages des VHT en se positionnant comme moteur en la matière. Annoncée dans le « programme de travail pour une Europe numérique 2023-2024 », la création de cette plateforme s'inscrit largement dans la volonté européenne de mettre en œuvre une stratégie d'intelligence artificielle[52]. Cette récente avancée met également en exergue le souhait primordial de la Commission européenne de placer sur le

[48] Commission européenne, "European Virtual Human Twins (VHT) Initiative" (consulté le 30/04/2026).

[49] Commission européenne, "Virtual Human Twins Manifesto", Manifesto, décembre 2023, p.03.

[50] Commission européenne, "EDHITH. Building the European Virtual Human Twin", livrable 3.2 "VHT roadmap", décembre 2024, 362p.

[51] Site officiel de l'initiative en matière de santé innovante : https://www.ihi.europa.eu/, (consulté le 30/04/2026).

[52] European Commission, "ANNEX to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2025- 2027", Digital Europe Programme, *C(2025)* 1839 final, Brussels, 28 march 2025, p.16 et p.79.

devant de la scène les différents acteurs des modèles VHT (chercheurs, innovateurs et cliniciens) afin, non seulement, de les solliciter dès les prémices de la mise en œuvre de cette plateforme, mais également de leur offrir un maximum d'outils et de ressources pour déployer, connecter, articuler et valider les modèles et méthodes VHT. Le choix d'intégrer les utilisateurs de la plateforme dès sa conception participe à l'acceptation de cette dernière. Ainsi, les utilisateurs futurs peuvent exprimer leurs besoins, souhaits ou inquiétudes concernant la création de cet espace de partage. Les objectifs poursuivis par cette plateforme sont multiples : fournir aux divers acteurs des secteurs publics et privés un espace commun d'intégration voire de génération des modèles ; assurer un espace d'accès à des technologies de pointe, à des modèles de calcul, à des données synthétiques, voire directement à des modèles VHT[53]. Assurément, l'initiative insiste sur l'importance que de fortes garanties de protection des droits de propriété intellectuelle et de cybersécurité soit assurées lors de l'usage de la plateforme.

Enfin, la Commission européenne annonce souhaiter passer une étape importante afin de combler le fossé entre la génération, la mise sur le marché et l'adoption des VHT dans les établissements de santé et organismes de recherche[54]. Pour cela, l'initiative soutient la création d'un incubateur[55], dit « VHT Uptake » correspondant à « un centre de partage des connaissances, de mise en réseau, de coopération et de collaboration »[56].

À travers cette initiative, la Commission européenne affirme sa volonté de positionner l'Europe comme un réel acteur moteur dans la création et l'usage d'innovations numériques qui semblent révolutionner les manières de considérer la santé et de faire de la recherche. Pour autant, ce tournant numérique ne peut se faire sans garantir une réelle acceptabilité de ces nouveaux usages et, de fait, une prise en compte concrète et précoce de l'ensemble des acteurs, concernés par les préoccupations tant technologiques et scientifiques qu'éthiques et réglementaires. Si cette initiative présente un réel intérêt pour le déploiement des méthodes VHT en Europe, il s'agit de vérifier si la création d'un tel écosystème participatif peut perdurer et rester à la pointe d'une technologie qui évolue si rapidement.

[53] En ce sens, la Commission européenne prévoit que la plateforme puisse offrir certaines spécificités d'accès en *open source*, sans que ces dernières ne soient définies à ce jour.

[54] European Commission, "ANNEX to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2025- 2027", *Op. Cit.,* p.79.

[55] *Ibid*., pp.79-80.

[56] Commission européenne, « Plate-forme pour les modèles VHT (Advanced Virtual Human Twin) », (consulté le 30/04/2026).

Les jumeaux humains virtuels

par Alizée FERNANDEZ

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Si la médecine s'est longtemps attachée à soigner un corps tangible, fait de chair et d'os, elle est aujourd'hui confrontée à une nouvelle réalité : celle de gouverner son double de données. La simulation numérique tend ainsi à devenir un outil central de la décision clinique, ouvrant, par ricochet, un champ inédit pour le droit.

Après vingt ans de transition numérique centrée sur la gestion administrative et la dématérialisation des dossiers médicaux, l'innovation en santé prend désormais un tournant majeur avec la modélisation du vivant. Initialement conçue pour l'ingénierie aéronautique et automobile afin de simuler le comportement de systèmes complexes et prévenir leurs défaillances, la technologie du jumeau numérique a récemment été adaptée au domaine médical. Ce passage de la machine à l'organisme humain transforme profondément la nature et la portée de cette technologie.

En santé, le Virtual Human Twin (VHT), ou jumeau humain virtuel, est une représentation mathématique et dynamique d'un patient ou d'un organe. Ce n'est pas une image figée, mais un modèle évolutif, constamment alimenté par des données médicales, biologiques, comportementales et environnementales. L'objectif n'est pas de reproduire intégralement un individu, ce qui est à la fois irréaliste d'un point de vue technique aujourd'hui et éthiquement délicat, mais de créer une représentation suffisamment fidèle pour tester des hypothèses de soins sans exposer directement le patient à un risque.

L'enjeu est considérable. Le jumeau numérique porte la promesse d'une médecine plus personnalisée, plus prédictive et plus précise, capable d'anticiper l'évolution d'une pathologie ou la réponse d'un patient à un traitement donné. Toutefois, cette promesse s'accompagne de tensions profondes. Le corps humain ne se réduit pas à un système mécanique : il est traversé par une histoire, une subjectivité et des choix. L'essor des VHT soulève ainsi des interrogations majeures relatives à la protection des données de santé, à la responsabilité en cas d'erreur algorithmique et au risque de réduire la personne à une simple agrégation de variables numériques.

Conscients de ces enjeux, les pouvoirs publics européens ont structuré le développement des jumeaux humains virtuels autour d'une architecture hybride, au confluent de la stratégie industrielle et de la régulation des données. Dès lors, comment l'Union européenne (UE) parvient-elle à pallier ses limites de compétence par des mécanismes de coordination stratégique, tout en instaurant via l'Espace européen des données de santé (EHDS), un cadre normatif indispensable à l'interopérabilité des données nécessaires au déploiement des jumeaux virtuels ?

L'architecture de ce dispositif repose sur le fondement de l'initiative entre soft law et stratégie de coordination (I), laquelle se déploie à travers l'Espace européen des données de santé comme levier d'interopérabilité et d'exploitation systémique des données de santé (II).

I. LE FONDEMENT DE L'INITIATIVE : ENTRE SOFT LAW ET STRATÉGIE DE COORDINATION

L'initiative VHT privilégie une approche pragmatique au sein de l'UE, où la contrainte législative s'efface au profit d'une convergence stratégique des acteurs. Lancé le 21 décembre 2023, le Manifeste pour les jumeaux humains virtuels constitue

la pierre angulaire de cette approche[57]. En tant qu'instrument de droit souple, cette déclaration d'intention sur le développement collaboratif des VHT et leur adoption accrue dans l'ensemble de l'UE, ne crée pas d'obligations juridiques contraignantes au sens de l'article 288 du Traité sur le fonctionnement de l'UE (TFUE). Toutefois, sa portée ne doit pas être sous-estimée car il remplit une fonction de pré-normalisation. En recueillant l'adhésion volontaire des chercheurs, des professionnels de santé, des innovateurs de l'industrie, des décideurs politiques et des autorités des États membres, il installe un consensus sur des standards éthiques et techniques communs. Cette coopération permet à la Commission européenne de structurer un secteur technologique émergent avant même que le législateur ne vienne codifier ces pratiques garantissant ainsi une unité d'action sans passer par le temps long de la navette législative.

Cette stratégie de coordination apparaît d'autant plus pertinente que l'action de l'Union en matière de santé est encadrée par un cadre constitutionnel strict. En vertu de l'article 168 du TFUE, la santé publique relève principalement d'une compétence d'appui (dite aussi « de coordination » ou de complément). Conformément à l'article 168§7, l'Union doit respecter la responsabilité des États membres dans la définition de leurs politiques de santé ainsi que dans l'organisation et la fourniture des soins et de plus, toute harmonisation législative directe est exclue dans le cadre de cet article. L'Union dispose par ailleurs d'une compétence partagée avec les États membres pour les enjeux communs de sécurité en matière de santé, conformément à l'article 168§4 du TFUE, qui autorise le Parlement européen et le Conseil à adopter des mesures fixant des normes élevées de qualité et de sécurité des organes et substances d'origine humaine, du sang et des dérivés du sang (art. 168 §4 a)), des mesures dans les domaines vétérinaire et phytosanitaire ayant directement pour objectif la protection de la santé publique (art. 168 §4 b)), ainsi que des mesures fixant des normes élevées de qualité et de sécurité des médicaments et des dispositifs à usage médical (art. 168 §4 c)).

Les jumeaux humains virtuels n'entrant pas dans ces catégories, la Commission européenne a choisi de les appréhender comme un objet de haute technologie, assimilable à un logiciel ou à une infrastructure de données, plutôt que comme un acte médical stricto sensu.

Ainsi on pourrait considérer qu'au sens de l'article 3§1 de l'IA Act[58], un VHT constituerait un système d'IA dès lors qu'il déduit, à partir des données médicales qu'il reçoit, la manière de générer des sorties telles que des prédictions ou des recommandations susceptibles d'influencer une décision clinique. Cette qualification acquise, le règlement appelle une classification par niveau de risque. Or, l'annexe III du règlement, qui liste limitativement les systèmes d'IA à haut risque, ne prévoit aucune catégorie dédiée aux outils de simulation médicale. Le rattachement le plus plausible serait celui du point 5 d), qui vise les systèmes d'IA utilisés pour le tri des patients dans les services d'urgence, ce qui pourrait couvrir un VHT à visée pronostique en soins intensifs, mais reste insuffisant pour couvrir l'ensemble des usages cliniques des jumeaux numériques. Par ailleurs, lorsque le VHT est intégré comme composant de sécurité d'un dispositif médical au sens du règlement (UE) 2017/745, qui figure à l'annexe I, point 11 de l'IA Act, et que ce dispositif est soumis à une évaluation de conformité par un tiers, l'article 6§1 entraîne sa

[57] « Lancement de l'initiative européenne sur les jumeaux humains virtuels », *Digital Strategy*, 21 déc. 2023.

[58] Règlement (UE) 2024/1689/UE du 13 juin 2024 sur l'intelligence artificielle du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, *JOUE* n° L 2024/1689 du 12/07/2024.

qualification automatique de système à haut risque, indépendamment de tout rattachement à l'annexe III[59]. Si l'IA Act peut donc offrir des pistes de qualification en fonction de la finalité d'usage du VHT, force est de constater qu'à ce jour aucune qualification juridique n'a été officiellement retenue, ce qui n'empêche pas des initiatives telles que celle mentionnée.

En effet, en intervenant sur les infrastructures technologiques qui conditionnent l'exercice des soins, l'UE respecte les limites de l'article 168 du TFUE, tout en exerçant une influence indirecte sur les pratiques médicales nationales. Cette approche est renforcée par le recours aux instruments de la politique industrielle, qui permettent à l'UE, conformément à l'art 173 du TFUE, de soutenir la compétitivité de son industrie. Ainsi, dans le cadre du programme politique de la « Décennie numérique 2030 », la Commission mobilise l'European Digital Infrastructure Consortia (EDIC), mis à la disposition des Etats membres afin de faciliter la mise en oeuvre de projets multinationaux de grande ampleur[3]. En rattachant l'initiative VHT à ce dispositif, le développement des jumeaux humains virtuels s'inscrit dans une dynamique de souveraineté technologique et de concurrence mondiale[60].

Toutefois, la coordination institutionnelle et la politique industrielle ne suffisent pas à garantir le déploiement effectif des jumeaux humains virtuels. Leur viabilité dépend avant tout de la circulation et de l'interopérabilité des données de santé, ce qui rend indispensable leur articulation avec le cadre normatif de l'EHDS (**II**).

II. L'ESPACE EUROPÉEN DES DONNÉES DE SANTE COMME LEVIER D'INTEROPERABILITE : VERS UNE EXPLOITATION SYSTEMIQUE DES DONNÉES DE SANTE

Bien que des prototypes de jumeaux numériques d'organes isolés existent déjà, à l'instar du projet « Living Heart » pour la cardiologie ou du projet « NeuroTwin » pour les pathologies cérébrales, créer un jumeau du corps humain entier est encore impossible aujourd'hui. Les freins au déploiement des jumeaux numériques résultent de la complexité du fonctionnement du corps humain dans son entièreté mais aussi du manque d'accès à des données de santé massives et hétérogènes. Actuellement cantonnés à des projets de recherches spécifiques, ces modèles pourront profiter des opportunités offertes par la création de l'Espace européen des données de santé.

Entré en vigueur le 26 mars 2025, le Règlement (UE) 2025/327 établissant l'EHDS instaure un cadre juridique et infrastructurel propre au secteur sanitaire. S'il garantit d'abord aux patients un accès transfrontalier à leurs dossiers médicaux électroniques via l'utilisation primaire des données de santé, il opère surtout un changement de paradigme pour le développement des jumeaux numériques grâce à son régime d'utilisation secondaire. Ce mécanisme autorise la réutilisation sécurisée des informations à des fins de recherche et d'innovation, dépassant la seule finalité de soins. En effet, un modèle de simulation cardiaque ou neurologique n'a de valeur prédictive que s'il est alimenté par des milliers de trajectoires de patients réels, ce que le cadre contractuel préexistant rendait impossible à l'échelle européenne. Sur le plan juridique, cette articulation

[59] Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030, *JOUE* n° L 323 du 19/12/2022.

[60] « Virtual Human Twins », Digital Strategy.

garantit que le traitement des données pour l'entraînement des modèles de simulation ne soit plus perçu comme une violation du principe de limitation des finalités posé par le règlement général sur la protection des données (RGPD), mais comme un prolongement légitime et sécurisé de leur exploitation initiale, à condition de respecter strictement les conditions prévues par le règlement, comme nous le verrons ci-après.

L'apport majeur de l'EHDS réside dans le passage d'une gestion contractuelle et individuelle des données à une gouvernance publique régulée. Si le consentement individuel demeure un principe directeur tant pour l'utilisation primaire que secondaire des données, le règlement laisse pour cette dernière une marge de manœuvre aux États membres qui peuvent, à certaines conditions permettre la réutilisation des données nonobstant le refus du patient. En s'appuyant sur une base légale harmonisée fondée sur l'intérêt public et la recherche scientifique, l'EHDS facilite l'accès aux données de santé électroniques, par la mise en place d'organismes responsables de l'accès aux données de santé, les ORAD, désignés par les États membres et chargés d'instruire les demandes de réutilisation dans le respect des garanties prévues par le règlement. Ce système centralisé autour des ORAD permettra de remplacer la fragmentation des accords locaux par une procédure qui offre aux innovateurs un cadre prévisible et unifié, condition indispensable au développement des projets technologiques à dimension européenne.

L'article 53 du règlement EHDS énumère les finalités légitimes de ce type d'accès aux données de santé. Celles-ci incluent notamment l'amélioration des soins, la surveillance de la sécurité des médicaments, l'élaboration de politiques sanitaires, les statistiques officielles ou encore l'intelligence artificielle de santé[5]. Un chercheur ou un industriel souhaitant réutiliser ces données ne pourra pas s'adresser directement à un hôpital ou à un fournisseur de données. Il devra présenter une demande complète aux ORAD, justifiant la finalité, la proportionnalité et les garanties mises en œuvre. À cet égard, l'article 68 du règlement prévoit des critères stricts : l'anonymisation des données est privilégiée, la pseudonymisation n'étant admise qu'à titre subsidiaire et dûment justifiée, auxquelles s'ajoutent des exigences de documentation transparente, de limitation d'accès et de sécurité renforcée. Cette « harmonisation » des procédures d'accès, toujours en cours de d'élaboration dans le cadre des travaux de l'action conjointe TehdAs, devrait garantir aux projets des jumeaux humains virtuels une alimentation en données continue et sécurisée.

Au-delà de l'accès aux données, le succès du VHT repose sur la capacité à croiser des données massives et hétérogènes. Dans cette optique, l'EEDS et le projet *European Digital Innovation Hub* (EDITH), dédié au développement de l'innovation numérique[61], forment un binôme indissociable. Tandis que l'EEDS impose une interopérabilité juridique indispensable à l'usage secondaire des données de santé, le projet EDITH en assure la traduction technique par une feuille de route stratégique visant à intégrer des informations hétérogènes. Ce projet structure un écosystème collaboratif via un répertoire fédéré sur le cloud, mutualisant modèles et algorithmes pour lever les barrières technologiques à l'échelle européenne. L'aboutissement de cette démarche est une plateforme de simulation conçue comme un guichet unique ou *one-stopshop*, permettant aux utilisateurs non seulement de valider des modèles d'organes spécifiques, mais aussi de les combiner pour aboutir à une vision holistique et intégrée du corps humain. En somme, si l'EEDS apparaît être un excellent levier

[61] Règlement (UE) 2025/327 du Parlement européen et du Conseil relatif à l'Espace européen des données de santé, *JOUE* n° L 2025/327 du 5/03/2025.

pour ouvrir l'accès aux données, il participe également à instaurer un cadre de confiance nécessaire pour que les VHT passent du stade de prototypes de recherche à celui d'outils cliniques quotidiennement exploitables.

Ainsi, en imposant que les données soient traitées au sein de l'UE, l'EHDS assure un cadre protecteur de l'intégrité des informations de santé face aux géants numériques de la *Big Tech.* En outre, à travers des prototypes appliqués à des domaines critiques tels que l'oncologie cérébrale, les maladies cardiovasculaires ou les soins intensifs, le projet EDITH se prépare à un déploiement clinique à grande échelle où l'interopérabilité imposée par l'EHDS devient la condition sine qua non de la libre circulation et de la reconnaissance mutuelle des jumeaux numériques au sein de l'Union européenne.

Toutefois, ce déploiement ne saurait occulter les défis de régulation que suscite l'intégration des VHT dans le parcours de soin. En ce qu'il constitue le prolongement numérique d'un patient réel, le jumeau humain virtuel fait émerger une notion d'intégrité numérique, qui exige de concilier la complétude des données, la condition de sa fiabilité avec les principes de minimisation et de finalité du RGPD, tout en préservant l'autonomie décisionnelle du patient face à la force prédictive de l'algorithme. Cela se traduit concrètement dans la relation de soin, désormais structurée autour d'un quatuor inédit entre patient, médecin, jumeau numérique et concepteur, appelant un passage du consentement figé vers un consentement dynamique et modulaire. Par ailleurs, la nature hybride de ces systèmes, qui sont à la fois logiciel dispositif médical au sens du Règlement (UE) 2017/745 et système à haut risque au sens de l'AI Act, impose un régime de responsabilité adapté, associant obligation de sécurité de résultat, traçabilité infalsifiable par *smart contracts* et socialisation des risques via des fonds d'indemnisation sectoriels et des polices d'assurance dédiées, afin que le jumeau humain virtuel demeure un outil d'aide à la décision et non un substitut à la responsabilité humaine[62].

Si l'encadrement juridique et éthique s'efforce aujourd'hui de protéger les droits des patients et de sécuriser cette innovation, un défi ultime demeure pourtant en dehors du champ strictement normatif : celui de son impact environnemental. En effet, l'initiative des VHT repose sur des infrastructures matérielles énergivores dont l'empreinte carbone interroge la finalité même du soin. Dès lors, quel sens aurait l'amélioration de la santé d'un patient si elle participe, par son coût écologique, à la dégradation de la santé mondiale

[62] https://www.village-justice.com/articles/les-jumeaux-numeriques-digital-twins-defis-juridiques-implications,49211.html.

Décrypter la stratégie européenne pour les données

L'essor de l'intelligence artificielle repose largement sur la disponibilité de jeux de données de qualité, tout en renouvelant les interrogations relatives à la protection des droits fondamentaux et à la maîtrise des flux informationnels. Présentée par la Commission européenne en novembre 2025, la stratégie pour l'Union des données vise à favoriser l'accès et le partage des données au sein de l'Union tout en renforçant la souveraineté numérique européenne.
Les contributions réunies dans cette rubrique éclairent plusieurs enjeux au cœur de cette ambition. Elles abordent tant la stratégie institutionnelle portée par l'Union européenne que les débats juridiques relatifs à l'anonymisation, aux données synthétiques et au risque de réidentification, qui conditionnent la confiance dans les mécanismes de partage et de réutilisation des données.

La stratégie pour une union des données : vers une mobilisation stratégique des données au service de l'intelligence artificielle dans l'Union européenne

par Salaheddine ZADINE

Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Introduction

A l'heure où l'intelligence artificielle « *métamorphose* » les équilibres économiques, industriels et géopolitiques mondiaux, l'accès à « *de volumes massifs de données de grande qualité* » apparaît comme une condition essentielle pour la stimulation de l'innovation[63] au sein de l'Union européenne.

Par la communication de la Commission du 19 novembre 2025[64], cette dernière entend faire évoluer la Stratégie européenne pour les données de 2020[65], qui n'a posé que « *de simples bases* », aux fins de « *libérer le potentiel des données* » au sein « *d'un marché unique des données sûr et interopérable* »[66], permettant ainsi à l'Union de « *jouer un rôle de premier plan dans le développement et l'adoption de l'IA* »[67]. La Commission constate que, malgré l'existence d'un cadre juridique « *visant à instaurer la confiance, à promouvoir le partage des données et à clarifier les règles tout au long de la chaîne*

[63] Mise à point de modèles d'IA solides, optimisation des soins de santé ou du système énergétique et soutenir la primauté industrielle.
[64] *COM(2025)* 835 final précitée
[65] La Commission européenne a publié le 19 février 2020 une communication intitulée « Une stratégie européenne pour les données » (*COM(2020)* 66 final), qui fait partie d'un paquet plus vaste de documents stratégiques comprenant également une communication intitulée « Façonner l'avenir numérique de l'Europe » (COM (2020) 67 final) et un livre blanc intitulé « Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance » (*COM(2020)* 65 final).
[66] Voir en ce sens, Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (dit « *Data Act* »). Pour ce qui concerne l'investissement de l'UE dans des espaces européens communs de données, v. notamment Commission européenne, document de travail des services de la Commission sur les espaces européens communs des données, *SWD(2024)* 21 final, 24 janvier 2024. La Commission aurait investi, entre 2021 et 2024, un montant de 336 millions d'euros dans 14 espaces européens communs de données stratégiques.
[67] Voir en ce sens, Communication de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée « Plan d'action pour un continent de l'IA », *COM(2025)* 165 final ; et, Communication de la Commission européenne au Parlement européen et au Conseil portant sur la « Stratégie pour l'application de l'IA », *COM (2025)* 723 final, 8 octobre 2025.

de valeur de données »[68], l'Union demeure confrontée à une pénurie de données[69] mobilisables pour le développement de l'IA[70].

A cet égard, la Commission structure sa stratégie autour de trois piliers complémentaires : élargir l'accès à des données de qualité pour l'IA et l'innovation (**I**), rationaliser les règles applicables aux données (**II**) et renforcer la position de l'Union européenne dans les flux internationaux de données (**III**).

I. UN ACCÈS PLUS LARGE A DES DONNÉES DE QUALITÉ POUR L'IA ET L'INNOVATION

Le premier pilier de la stratégie repose sur l'idée que la compétitivité de l'Union européenne en matière d'IA dépend directement de l'accès à des données de grande qualité ainsi qu'à des infrastructures permettant leur partage sécurisé à grande échelle. A cette fin, la Commission européenne entend notamment renforcer les espaces européens communs de données (**i**), développer des « *laboratoires de données* » destinés à faciliter l'utilisation sécurisée des données pour l'IA (**ii**), soutenir les infrastructures européennes d'informatique en nuage et d'IA (**iii**), mobiliser des ressources stratégiques publiques, scientifiques et culturelles (**iv**), ainsi que des mesures horizontales relative aux données synthétiques, à la mise en commun des données et aux normes (**v**).

i. Le développement des espaces européens communs de données

Les espaces européens communs de données constituent l'un des principaux instruments de la stratégie pour une Union des données. Ils doivent permettre de passer d' « *initiatives fragmentées* » à un « *écosystème de donnée continu, interopérable*[71] *et durable* », qui reposerait sur des infrastructures en nuage et sur des règles communes de gouvernance définissant les conditions d'accès, d'utilisation et de partage des données[72].

Les espaces européens de données sont directement intégrés à la stratégie européenne pour l'application de l'IA[73], puisqu'ils doivent fournir les ressources

[68] Voir en ce sens, Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (dit « *Data Governance Act* ») ; Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public ; et le Règlement sur les données 2023/2854 précité.

[69] Les données en question sont qualifiées par la Commission comme un « *atout stratégique* » précieux. Pourtant, beaucoup de données restent encore peu exploitées ou enfermées dans des silos, notamment à cause de règles complexes et fragmentées. Afin de simplifier ce cadre, la Commission propose, dans le cadre du « *train de mesures omnibus sur le numérique* », de fusionner plusieurs instruments juridiques afin de créer un cadre européen des données cohérent et prévisible. La stratégie prévoit également plusieurs mesures d'accompagnement – telles que des clauses contractuelles types, des standards applicables aux services clous et des services d'assistance – destinées notamment à aider les PME à respecter plus facilement leurs obligations et à favoriser le partage des données dans les relations B2B et B2G.

[70] L'ambition de cette stratégie apparaît notamment à travers certains projets européens déjà en cours, tels que l'espace européen des données d'imagerie sur le cancer, qui devrait regrouper plus de 60 millions d'images anonymisées et annotées d'ici à 2027, afin de soutenir le développement de systèmes d'IA dans le domaine médical.

[71] Afin de garantir l'interopérabilité entre les différents espaces européens de données, la stratégie prévoir le développement de la plateforme *Simpl*, présentée comme un intergiciel sécurisé et à code source ouvert destiné à faciliter la circulation des données. Simpl devrait fournir « *plusieurs composants compatibles, d'utilisation gratuite, conformes à une norme commune en matière de qualité et de partage des données* ».

[72] Ces espaces doivent être progressivement reliés aux infrastructures européennes d'IA grâce aux « *laboratoires de données* » et aux « *fabriques d'IA* » (voir *infra*). Ces derniers fourniront notamment des outils de mise en commun, de curation, de pseudonymisation et d'anonymisation afin de rendre les données directement utilisables pour l'entraînement des systèmes d'IA.

[73] *COM(2025)* 723 final, *op. cit.*

sectorielles[74] nécessaires au développement de modèles d'IA spécialisés et d'« *avant-garde* »[75].

Les futurs financements européens donneront ainsi la priorité aux secteurs d'intérêt public (notamment la santé, la mobilité, l'énergie, les administrations publiques et l'environnement). A titre d'exemple concret de cette approche, la communication évoque le développement de « *centres de dépistage fondés sur l'IA dans le domaine des soins de santé* », destinés à valider des outils de diagnostic grâce à l'exploitation des données issues de l'Espace européen des données de santé[76]. Cette initiative s'inscrit plus largement dans les actions menées au titre du plan européen pour vaincre le cancer[77] ainsi que du plan de l'Union européenne pour la santé cardiovasculaire[78].

A partir de 2026, le déploiement des espaces de données dans les secteurs prioritaires sera soutenu par des investissements européens d'environ 100 millions d'euros afin de permettre une utilisation « *fiable et à grande échelle* » des données pour les applications d'IA.

En ce qui concerne le domaine de la santé, l'EEDS occupe alors une place centrale dans ce dispositif puisqu'il doit constituer une « *passerelle essentielle* » entre les écosystèmes de données de santé et le développement de l'IA. A ce titre, la stratégie prévoit notamment le développement d'applications de diagnostic fondées sur l'IA et de médecine grâce à l'utilisation d'ensembles de données « *anonymisées et synthétiques dans des environnements de traitement fiables* ».

ii. « Les laboratoires de données »

Les laboratoires de données sont définis en tant qu'« *installations spécialisées* » permettant, de manière similaire à des conteneurs de données - tout en favorisant l'interopérabilité et la cohérence dans l'ensemble de l'écosystème d'IA de l'Union - de faciliter leur utilisation pour l'entraînement des systèmes d'IA. Pour arriver à ces fins, ces laboratoires doivent fournir des services pratiques, notamment, de mise en commun, de curation, d'étiquetage et de pseudonymisation des données[79].

Les laboratoires de données sont ainsi conçus comme des « *catalyseurs* » de l'expérimentation et du déploiement de l'IA à partir de données de grande qualité. Ces catalyseurs constituent ainsi une réponse à

[74] Pour un exemple concret de l'application concrète de cette approche : des centres de dépistage fondés sur l'IA dans le domaine des soins de santé, qui valident les outils de diagnostic en utilisant l'espace européen des données de santé, dans le cadre d'actions menées dans le cadre du plan européen pour vaincre le cancer, de la stratégie pour les sciences du vivant et du plan de l'UE pour la santé cardiovasculaire.

[75] La communication mentionne ainsi plusieurs initiatives fondées sur l'exploitation de données sectorielles mises à disposition par ces espaces européens communs, telles que « Foundational Models for Industry », « AI-powered Pharma Discovery » ou « Autonomous Drive Ambition Cities ».

[76] Voir en ce sens le Règlement (UE) 2025/32 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive (UE) 2011/24 et le règlement (UE) 2024/2847(dit « Règlement EEDS »).

[77] Voir « Commission staff working document. Review of Europe's Beating Cancer Plan », SWD (2025) 39 final, Bruxelles, 4 février 2025.

[78] Voir Communication de la Commission européenne sur un plan de l'Union européenne pour la santé cardiovasculaire : plan pour un cœur en bonne santé, *COM(2025)* 1024 final, du 16 décembre 2025.

[79] D'autres services sont prévus tels que, bien évidemment, la facilitation de l'accès aux données ; des conseils d'orientations réglementaires et des formations ; la production de données synthétiques sans divulgation d'informations sensibles ou confidentielles ; ainsi que des outils techniques et infrastructures simples et fiables permettant le traitement su site des données sensibles. La stratégie vise ainsi à permettre, en particulier, aux start-ups et aux entreprises en expansion de partager et d'utiliser des données « *en toute sécurité* », de favoriser l'entraînement coopératif de modèles d'IA et de soutenir le développement de modèles sectoriels fondés sur différents mécanismes de gouvernance et de licences.

une « *défaillance majeure du marché* », tenant à la « *disponibilité limitée* » de données diverses ainsi qu'à la réticence des acteurs privés à partager leurs données pour l'entraînement des systèmes d'IA.

En ce sens, les laboratoires fonctionneront à partir de « *canaux d'accès* » et des « *cadres de gouvernance* » déjà existants, sans nécessiter d'une centralisation massive des données impliquant leur transfert[80].

La participation aux laboratoires doit demeurer volontaire et les détenteurs de données conserveront le contrôle des conditions (consentement explicite) d'utilisation de leurs données. La stratégie insiste également sur le recours à des techniques « *préservant la confidentialité* »[81] afin de garantir le respect du RGPD[82] et renforcer la confiance « *tout en augmentant l'utilisation des données pour l'IA* ».

Plus largement, les laboratoires de données s'inscrivent dans l'évolution des infrastructures européennes de calcul développées autour d'EuroHPC[83]. La stratégie prévoit désormais le déploiement de « *fabriques d'IA* », puis à terme de « *gigafabriques d'IA* », destinées à relier capacités de calcul, accès aux données et expérimentation en matière d'IA. Les premiers laboratoires de données doivent être opérationnels dans ce cadre afin de mettre les développeurs d'IA en relation avec les espaces européens communs de données[84].

iii. Acte législatif sur le développement de l'informatique en nuage et de l'IA

Le développement d'une véritable Union européenne des données suppose l'existence d'infrastructures souveraines de calcul, de centres de données et de services d'informatiques en nuage capables de soutenir le développement de l'IA à grande échelle.

Face à l'augmentation continue des volumes de données et à la dépendance de l'Union à l'égard structures situées hors de son territoire, la Commission européenne annonce la présentation, au premier trimestre 2026, d'un acte législatif sur le développement de l'informatique aux nuages et de l'IA destiné à soutenir l'ensemble de la chaîne de valeur européenne du cloud et de l'IA. Ce dernier devra favoriser le développement de capacités durables de centre de données afin de garantir « *la sécurité et la souveraineté des futurs services européens d'informatique en nuage et d'IA* ». La stratégie précise également que cette initiative couvrira l'ensemble des infrastructures nécessaires de développement de l'IA, « *des processeurs de pointe jusqu'au matériel, logiciel et technologie de refroidissement durable* ».

---

[80] Ainsi, les espaces européens communs de données demeurent les infrastructures de confiance au sein desquelles les données sont gouvernées et mises à disposition, tandis que les laboratoires de données en assurent l'exploitation opérationnelle pour le développement de l'IA « *en toute sécurité et en apportant une valeur ajoutée* ».

[81] Telles que l'apprentissage fédéré, le chiffrement homomorphe et le calcul multipartite sécurisé. De plus, les données pourront être traitées localement ou à travers différents nœuds sans être fusionnées dans un répertoire unique, ce qui permet aux détenteurs initiaux de conserver le contrôle sur leurs données.

[82] Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive n° 95/46/CE (règlement général sur la protection des données).

[83] Entreprise commune pour le calcul à haute performance européen (EuroHPC), créée en 2020 à Luxembourg (Luxembourg). Son rôle est celui de développer un écosystème de supercalcul de classe mondiale en mettant en commun les ressources de l'Union européenne, des pays européens et de partenaires privés destiné à la recherche scientifique.

[84] Les laboratoires doivent également travailler en coordination avec les pôles européens d'innovation numérique (EDIH) qui font office de points de contact orientés vers les utilisateurs et aident à mettre les besoins en données en correspondance avec des applications concrètes.

iv. Ressources en données stratégiques : secteur public et données scientifiques

La stratégie fait de l'accès à des données « *de qualité, structurées et fiables* » une condition essentielle du développement de l'IA et de la souveraineté numériques européenne. A cette fin, la Commission entend renforcer l'exploitation des ensembles de données du secteur public, notamment les « *ensembles de données de forte valeur* » prévus par la Directive sur les données ouvertes[85], qui doivent être accessibles gratuitement, dans des formats lisibles par machine et via des d'interfaces de programmation d'applications (API)[86].

La Commission insiste également sur le potentiel stratégique des données scientifiques, illustré par l'exemple d'AlphaFold, dont les capacités de prédiction des structures protéiques ont profondément accéléré « *l'innovation* ». Des bases de données scientifiques bien structurées sont ainsi présentées comme des leviers permettant de réduire les « *coûts de recherche et développement et d'accélerer l'innovation dans des domaines tels que les produits pharmaceutiques, l'énergie, les matériaux ou les biotechnologies* ».

La stratégie prévoit dès lors le développement de nouvelles infrastructures numériques de recherche ainsi que le renforcement du « *nuage européen pour la science ouverte* » (EOSC), présenté comme un espace européen de partage et de réutilisation de données de recherche « FAIR »[87].

Ces ressources doivent soutenir les activités scientifiques fondées sur l'IA dans le cadre de RAISE[88]. En parallèle, le futur acte législatif sur l'Espace européen de la recherche « EER »[89] doit renforcer les conditions juridiques de partage, d'accès et de réutilisation des résultats, publications et données issues de la recherche financée par des fonds publics.

v. Mesures horizontales : données synthétiques, mise en commun des données et normes

La stratégie prévoit également plusieurs mesures transversales destinées à soutenir l'économie européenne des données. Premièrement, la Commission identifie notamment les données synthétiques comme un levier essentiel pour entraîner des systèmes d'IA dans des domaines où les « *données sont rares ou sensibles* », notamment en santé. Il s'agira alors de créer une « *usine de données synthétiques* » et d'élaborer des orientations et de normes relatives à leur utilisation fiable[90].

Deuxièmement, la stratégie entend sécuriser juridiquement la mise en commun des données, notamment dans des secteurs tels que la santé, où les entreprises ne disposent pas individuellement de volumes suffisants pour entraîner des modèles d'IA[91].

Enfin, la stratégie insiste sur la nécessité de renforcer la qualité et la standardisation des données afin d'éviter une fragmentation des pratiques de partage et de réutilisation

[85] Directive n° 2019/1024 précitée.
[86] La liste de ces données devrait être étendue dès 2026 aux données juridiques, judiciaires et administratives.
[87] De haute qualité, faciles à trouver, accessibles, interopérables et réutilisables.
[88] Communication de la Commission européenne au Parlement européen et au Conseil portant sur Une stratégie européenne pour l'intelligence artificielle dans le domaine de la science: poser les jalons du centre de ressources de la science pour et par l'IA en Europe (RAISE) *COM(2025)*724 final, du 8 octobre 2025.
[89] Proposition de Recommandation du Conseil sur le programme stratégique 2025-2027 de l'Espace européen de la recherche, Bruxelles, 28 février 2025, COM (2025) 62 final.
[90] Horizon Europe doit également financer des travaux de recherche sur les techniques de production de données synthétiques.
[91] Des lignes directrices sur les futures orientations sur les bonnes pratiques d'échange et de mutualisation des données par la Commission sont attendues afin de réduire l'insécurité juridique liée notamment au droit de la concurrence de l'Union.

efficace. La Commission prévoit, à ce titre, une future « *norme européenne relative à la qualité des données* »[92].

II. RATIONALISER LES REGLES EN MATIERE DE DONNEES

Le deuxième pilier de la stratégie vise à simplifier le cadre européen des données afin de « *moderniser et consolider l'acquis horizontal de l'UE en matière de données* ». La Commission européenne annonce notamment « *un train de mesures omnibus sur le numérique* »[93] destiné à *supprimer les règles obsolètes*, à *rationaliser les règles en matière de partage de données*[94], à *consolider le partage des données du secteur public* ainsi qu'à *moderniser les règles applicables aux cookies* et à la *protection des données*.

La stratégie prévoit également des adaptations ciblées du RGPD afin de clarifier certaines notions essentielles pour le développement de l'IA[95], ainsi que plusieurs ajustements du Règlement sur les données permettant « *d'éviter les « fuites » de données vers des pays tiers, d'introduire des régimes adaptés pour les services en nuage sur mesure et de supprimer les dispositions relatives aux contrats intelligents* », afin de *réduire les contraintes pesant sur les entreprises en expansion*[96].

FOCUS — LE « DIGITAL OMNIBUS »

Présentée par la Commission européenne le 19 novembre 2025, la proposition de règlement « Digital Omnibus » s'inscrit dans la stratégie pour l'Union des données. Elle vise à simplifier et rationaliser plusieurs textes européens relatifs au numérique, notamment en matière de partage des données, de protection des données personnelles et d'intelligence artificielle. Son objectif est de réduire les charges administratives tout en favorisant l'innovation et la compétitivité européennes.

III. PRESERVER LA SOUVERAINETE DE L'EUROPE EN MATIERE DE DONNEES GRACE A UNE APPROCHE STRATEGIQUE DE LA POLITIQUE INTERNATIONALE EN MATIERE DE DONNEES

Le troisième pilier de la stratégie repose sur l'idée que la souveraineté européenne en matière de données suppose non plus seulement la protection des données sensibles de l'Union, mais également la capacité de l'Union européenne à contrôler les conditions dans lesquelles les données circulent au niveau international.

La communication critique explicitement la situation actuelle dans laquelle des acteurs étrangers bénéficient d'un accès abusif au marché européen des

[92] Couvrant notamment les aspects d'exhaustivité, de cohérence, de clarté sémantique et de gouvernance, ainsi que des travaux de normalisation relatifs à l'annotation, à l'étiquetage et à la capture des données utilisées pour le développement des systèmes d'IA.

[93] Proposition de Règlement du Parlement et du Conseil modifiant les règlements n°s 2016/679/UE, 2018/1724/UE, 2018/1725/UE et 2023/2854/UE ainsi que les directives n°s 2002/58/CE, 2022/2555/UE et 2022/2557/UE en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements 2018/1807/UE, 2019/1150/UE et 2022/868/UE ainsi que la directive 2019/1024/UE (règlement omnibus numérique), *COM(2025)* 837 final, du19 novembre 2025.

[94] La Commission annonce vouloir identifier les chevauchements et interactions peu claires entre les différents régimes relatifs aux données pour *aider les entreprises à se conformer au Règlement sur les données*.

[95] Il s'agira, pour l'essentiel, de la notion de données à caractère personnel, les conditions d'anonymisation et de pseudonymisation, l'intérêt légitime comme base juridique de l'entraînement des systèmes d'IA ou encore les règles relatives à la prise de décision automatisée. La Commission entend réduire l'insécurité juridique encadrant la réutilisation des données tout en maintenant les garanties de respect de la vie privée.

[96] Le concept de « conformité en un clic » permettra ainsi d'automatiser certaines obligations réglementaires grâce à des certificats numériques de conformité et au futur « portefeuille européen d'identité numérique pour les entreprises ».

données tandis que les entreprises européennes demeurent confrontées à des exigences de localisation, à des restrictions d'accès ou à des règles discriminatoires dans certains Etats tiers. A cet égard, « *[l]a Commission agira donc de manière plus ferme pour défendre les intérêts et l'autonomie réglementaire de l'UE, en adoptant des mesures proportionnées lorsque la politique d'ouverture donne lieu à des abus ou lorsque les vulnérabilités sont instrumentalisées* ».

La stratégie identifie également plusieurs risques liés aux cyberattaques, aux fuites de technologie[97], à la surveillance et les dépendances coercitives pour la souveraineté européenne des données critiques[98].

Dans cette logique, la Commission annonce vouloir faire des « *conditions équitables pour l'accès aux données et les transferts transfrontières* » un « *pilier du commerce numérique* ». Elle prévoit également l'adoption de mesures destinées à renforcer la protection des « *données sensibles à caractère non personnel* » de l'Union, en complément des garanties offertes par le RGPD[99].

En parallèle, la Commission relève la nécessité de renforcer les liens entre les écosystèmes européens de données et ceux des « *partenaires partageant les mêmes valeurs* »[100]. Elle prévoit notamment de développer « *des services et des infrastructures de soutien tels que les espaces européens communs des données* », afin d'assurer un partage transfrontière ininterrompu [des données] ; de fournir « *des clauses contractuelles* standard », pour sécuriser les échanges internationaux de données ; et « *d'intégrer les engagements en matière de partage transfrontière des données dans des accords commerciaux internationaux* »[101].

Enfin, la communication affirme la volonté de l'Union de renforcer son influence dans la gouvernance mondiale des données en promouvant ses standards au sein du G7, du G20, de l'OCDE et des Nations Unies, tout en développant des coopérations spécifiques avec les pays candidats et partenaires proches de l'Union autour de plateformes partagée de données publiques et d'accords de confiance relatifs aux flux de données sensibles.

Conclusion

Pour conclure, la stratégie du 19 novembre 2025 pour une *Union des données* marque une nouvelle étape de la politique numérique européenne. Au-delà

[97] Au premier trimestre 2026, sera prévue la publication de lignes directrices destinées à évaluer le traitement réservé aux données européennes dans les Etats tiers ainsi qu'une « boîte outils de lutte contre la fuite de données ». Cette dernière fait l'objet d'une action phare de la stratégie (Création d'une boîte à outils pour lutter contre la localisation injustifiée, l'exclusion, la faiblesse des garanties et les fuites de données (T2 2026).

[98] A cet égard, la Commission envisage de mobiliser plusieurs instruments européens déjà existants, notamment le Règlement (UE) 654/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant l'exercice des droits de l'Union pour l'application et le respect des règles du commerce international, le Règlement (UE) 2023/2675 du Parlement européen et du Conseil du 22 novembre 2023 relatif à la protection de l'Union et de ses États membres contre la coercition économique exercée par des pays tiers (Instrument anticoercition).

[99] Ce qui fait de l'adoption de mesures visant à protéger les données sensibles à caractère non personnel (T3 2026), une action phare de la stratégie.

[100] D'ici 2026, conformément à la stratégie numérique internationale (Communication conjointe de la Commission européenne et du Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité au Parlement européen et au Conseil sur « Une stratégie numérique internationale pour l'Union européenne », *JOIN(2025)* 140 final, du 5 juin 2025), la Commission et le Service européen pour l'action extérieure entendent renforcer les partenariats numériques de l'Union avec des Etats partageant les mêmes objectifs, notamment à travers le développement des accords sur le commerce numérique et l'intégration de chapitres numériques dans les accords commerciaux internationaux.

[101] L'objectif étant celui de promouvoir le cadre européen de données fiables dans les « *dialogues internationaux et dans le réseau de partenariat numérique* ».

de la seule régulation des données, la Commission cherche désormais à construire une véritable infrastructure européenne de l'IA fondée sur la circulation, l'(la) (ré)utilisation et la sécurisation des données de grande qualité et à grande échelle.

Un constat peut être fait, les données ne sont plus seulement envisagées comme des objets de protection juridique, mais comme des ressources stratégiques conditionnant la souveraineté numérique, la compétitivité industrielle et la capacité d'innovation de l'Union.

Communication de la Commission européenne du 19 novembre 2025 sur la « Stratégie pour une union des données – Faciliter l'accès aux données pour l'intelligence artificielle », *COM(2025) 835 final*.

La crise identitaire des données synthétiques en Europe face au diagnostic jurisprudentiel de la CJUE sur la définition de l'anonymisation

Compte rendu de la présentation à l'occasion de la rencontre Québec/Toulouse sur l'Espace Européen des Données de Santé

par Winnie DONGBOU WAMBA

Doctorant en Droit public, EDT-R-IRDEIC, Université Toulouse Capitole
Juriste en droit de la protection des données de santé MyData-TRUST

La journée – ou soirée selon le fuseau horaire concerné – du 29 avril fut marquée par une rencontre entre l'Université Toulouse Capitole et l'Université de Laval autour des enjeux de l'Espace Européen des Données de Santé[102]. A cette occasion, nous avions le plaisir de discuter de la qualification juridique des données synthétiques en matière de protection des données personnelles en Europe. Une question qui, à première vue technique, revêt des implications légales fondamentales pour les acteurs de la recherche en santé, notamment dans le cadre du déploiement de l'Espace Européen des Données de Santé (EEDS)[103].

I. DÉFINITION ET UTILITÉ SCIENTIFIQUES DES DONNÉES SYNTHÉTIQUES

Les données synthétiques peuvent être définies comme des données de patients générées soit par calcul, algorithmes et processus automatisés, soit par agrégation de données de patients collectées antérieurement, soit par une combinaison des deux approches[104]. Elles sont ainsi le produit d'un traitement algorithmique qui vise à reproduire les caractéristiques statistiques de données réelles sans en être une copie directe.

L'état de l'art en recherche clinique identifie plusieurs cas d'usage majeurs pour les données synthétiques dont la facilitation du partage de données entre acteurs internationaux, notamment pour les transferts de données de l'Europe vers les États-Unis ; l'augmentation des données pour la recherche sur les maladies rares, où les données de vie réelle sont insuffisantes ; l'entraînement de modèles d'apprentissage automatique en santé et la simulation de cohortes de patients afin d'explorer différentes hypothèses avant toute mise en application sur des patients réels. Tous ces usages convergent vers une interaction importante entre les patients, ou plutôt leurs données de santé et des modèles d'IA. Une interaction que les données synthétiques elles-mêmes promettent de limiter si elles peuvent être qualifiées de données anonymes.

II. LA CRISE IDENTITAIRE DES DONNÉES SYNTHÉTIQUES : DEUX THÈSES EN TENSION

Le cœur de la problématique réside dans la qualification juridique des données synthétiques au regard du droit européen de la protection des données (RGPD). Deux thèses structurent le débat. Il s'agit de la

[102] Un enregistrement de la rencontre sera d'ailleurs disponible sur la chaîne Youtube de la chaire DOSA https://www.youtube.com/@ChaireDOSA

[103] DDONGBOU WAMBA W., « Tentative d'une qualification juridique de la donnée synthétique au regard du règlement sur l'espace européen des données de santé », Le droit en mouvement : les évolutions du droit d'hier à aujourd'hui, Colloque jeunes chercheuses et chercheurs de la Faculté de droit de l'Université de Sherbrooke, 2025.

[104] Voy. le glossaire SILICA disponible ici : https://silica-asso.fr/glossaire-silica/ et FRAYSSE J.-L. et ALLASSONNIERE S., *Données de santé artificielles: analyse et pistes de réflexion* [en ligne], [s. n.], 2024, [consulté le 27 février 2025].

thèse de la dépersonnalisation complète[105] réfutée par la doctrine au profit de la thèse de la personnalité résiduelle[106].

Selon la thèse de la dépersonnalisation complète, les données synthétiques, étant par nature artificielles et non directement issues d'individus identifiables, seraient par définition des données à caractère non personnel. Elles échapperaient ainsi au champ d'application du RGPD et pourraient circuler librement, sans les contraintes réglementaires applicables aux données de santé. La thèse de la personnalité résiduelle, aujourd'hui dominante, reconnaît que les données synthétiques peuvent conserver un risque résiduel de réidentification. Deux arguments viennent étayer cette position :

- l'impossibilité d'atteindre un risque zéro de réidentification en raison de certains attributs présents dans les données synthétiques (notamment lorsqu'elles sont générées à partir de données réelles) ;
- la vulnérabilité des modèles génératifs face à des attaques spécifiques permettant de reconstituer des informations sur les individus ayant servi à l'entraînement du modèle.

Si un risque résiduel de réidentification subsiste, se pose alors la question de l'articulation entre anonymisation relative et anonymisation absolue : l'anonymisation parfaite est-elle un standard atteignable, ou le droit doit-il s'accommoder d'une approche probabiliste et contextuelle ? Comme nous le verrons ci-dessous, une conclusion déjà implicite dans le Règlement sur l'EEDS a été confirmée par la Cour de justice de l'UE (CJUE)[107].

III. DONNÉES SYNTHÉTIQUES ET EEDS : UNE QUALIFICATION INDIRECTE ET PRUDENTE

Le Règlement relatif à l'Espace Européen des Données de Santé ne mentionne pas explicitement les données synthétiques. On y trouve en revanche une première reconnaissance fonctionnelle dans les projets de lignes directrices de l'action TEHDAS2 :

- comme alternative pour la description des jeux de données sensibles disponibles (draft guidance M5.1)[108] ;
- comme alternative pour l'extraction autorisée des résultats de recherche depuis les environnements sécurisés

[105] NIŠEVIĆ M., MILOJEVIC D. et SPAJIĆ D., « Synthetic data in medicine: Legal and ethical considerations for patient profiling », *Computational and Structural Biotechnology Journal*, 28, 2025 ; VALLEVIK V., BEFRING A., ELVATUN S. *et al.*, « Processing of synthetic data in AI development for healthcare and the definition of personal data in EU law » [en ligne], *ArXiv*, abs/2508.08353, 2025.

[106] BEDUSCHI A., « Synthetic data protection: Towards a paradigm change in data regulation? » [en ligne], *Big Data & Society*, 11, 2024 ; NIŠEVIĆ M., MILOJEVIC D. et SPAJIĆ D., *op. cit.* ; PALACIOS M., BOUDEWIJN A., SACCANI S. *et al.*, « Empirical Evaluation of Structured Synthetic Data Privacy Metrics: Novel experimental framework » [en ligne], *ArXiv*, abs/2512.16284, 2025 ; GANEV G. et DE CRISTOFARO E., « Rethinking Anonymity Claims in Synthetic Data Generation: A Model-Centric Privacy Attack Perspective », *ArXiv*, abs/2601.22434, 2026.

[107] Analyses des décisions Patrick Breyer contre Bundesrepublik Deutschland, C-582/14, 2016, ECLI:EU:C:2016:779. ; IAB Europe v. Gegevensbeschermingsautoriteit, C-604/22, 2022, ECLI:EU:C:2024:214. Et Contrôleur Européen de la Protection des Données (CEPD) contre Conseil de Résolution Unique (CRU), C-413/23 P, 2025, ECLI:EU:C:2025:645. Bien que cette dernière décision concerne principalement la question de savoir si des données pseudonymisées seraient anonymes dans le chef du destinataire desdites données, la Cour cite les décisions précédentes en rappelant que « la perspective pertinente pour apprécier le caractère identifiable de la personne concernée dépend essentiellement des circonstances caractérisant le traitement des données dans chaque cas particulier » : Voir le résumé de l'affaire.

[108] Draft guideline for data holders on data description.

de traitement des données (draft guidance M7.2)[109].

Au sujet de l'anonymisation, L'EEDS semble se ranger du côté de l'approche relative et contextuelle. A juste titre, le considérant 92 du Règlement reconnaît explicitement que certaines catégories de données de santé restent particulièrement sensibles même après anonymisation, et qu'un risque résiduel de réidentification ne peut pas toujours être raisonnablement atténué. La question non résolue sur l'atténuation raisonnable du risque résiduel de réidentification est renvoyée au RGPD qui a fait l'objet d'une interprétation intéressante sur la question par la CJUE.

IV. LE DIAGNOSTIC DE LA CJUE : UNE JURISPRUDENCE CONSTANTE SUR L'ANONYMISATION CONTEXTUELLE

La jurisprudence de la Cour de justice de l'Union européenne offre un cadre interprétatif essentiel pour trancher la question de la qualification de l'anonymité des données et partant, celle des données synthétiques. À travers plusieurs décisions de référence[110] la Cour décide que l'anonymisation ne peut être considérée comme une qualité intrinsèque d'une information, mais comme le résultat d'une évaluation contextuelle de l'identifiabilité, variable selon les acteurs, les moyens de réidentification et le moment du traitement.

La transposition de cette position jurisprudentielle aux données synthétiques conduit à quatre implications concrètes :

- L'analyse doit tenir compte des catégories de données utilisées pour la génération des données synthétiques – certaines données sources étant plus sensibles et plus propices à la réidentification.
- L'évaluation de l'anonymité s'apprécie dans le chef du destinataire des données : c'est sa capacité concrète à réidentifier qui est déterminante, et non une propriété abstraite des données.
- La question des moyens raisonnables et légaux à disposition du destinataire pour procéder à une réidentification est centrale dans l'évaluation.
- L'évaluation doit être périodique : l'évolution de l'état de l'art technologique (modèles d'attaque, puissance de calcul, bases de données tierces disponibles) peut augmenter le risque de réidentification dans le temps.

CONCLUSION : AU-DELÀ DE LA CATÉGORISATION, LA DÉMONSTRATION DU RISQUE

Le rattachement des données synthétiques à une catégorie préexistante de données – personnelles ou non personnelles – importe finalement moins que la capacité à démontrer que le risque de réidentification est suffisamment réduit pour justifier l'application d'un régime allégé de protection des données.

Cette approche fonctionnelle, cohérente avec la jurisprudence de la CJUE, invite les Organismes Responsables de l'Accès aux Données, les détenteurs et les utilisateurs des données dans le cadre de l'EEDS à ne pas chercher à trancher définitivement la question de la nature des données synthétiques, mais plutôt à mettre en place des mécanismes robustes d'évaluation et de documentation du risque résiduel de réidentification, au regard du contexte précis de chaque traitement et de chaque destinataire.

[109] Draft guideline on data minimisation, pseudonymisation, anonymisation and synthetic data, consulté le 17/05/2026.

[110] Voy. *supra*, note de bas de page 6.

En somme, la « crise identitaire » des données synthétiques ne se résoudra pas par une définition législative figée, mais par une méthodologie juridique et technique de l'évaluation continue du risque, dans l'esprit même de l'approche contextuelle consacrée par la Cour de justice.

Second Joint Action Towards the European Health Data Space – TEHDaS 2

23.06.2025

Workshop on the ethical dimensions of the European Health Data Space

par Lisa FÉRIOL

Doctorante CIFRE, Ekitia et Équipe BIOETHICS,
CERPOP UMR1295 Inserm et Université Toulouse Capitole

Introduction

L'action conjointe TEHDaS 2 (*Toward European Health Data Space*) [111] a organisé en ligne le 23 juin 2025 un atelier pour réfléchir collectivement à ce que devrait, de manière concrète, recouvrir les obligations en matière d'éthique introduites lors des discussions sur le texte du Règlement sur l'Espace européen des données de santé (Reg. EEDS)[112]. L'atelier a réuni 174 participants. Quatre experts[113] ont été invités afin de discuter ces enjeux autour d'une table ronde. Trois sessions en petits groupes se sont également tenues. Ce commentaire visera à résumer les principaux apports de cet atelier dont le contenu a été colligé au sein d'un document par TEHDaS2[114].

Rappelons pour commencer que l'article 67 du Reg. EEDS sur les *Demandes d'accès aux données de santé* en son paragraphe 2 point j) impose que les demandes d'accès aux données comportent des éléments éthiques précis concernant l'utilisation secondaire des données de santé lorsque ces derniers sont requis « au titre du droit national ». Ces dispositions permettent de valoriser le processus d'évaluation éthique de manière structurée et transparente dans ce nouveau système visant à faciliter l'utilisation secondaire des données de santé. Elles permettent également de réfléchir aux coopérations à mettre en œuvre au niveau européen sur ces procédures qui restent de la compétence nationale.

Les questions soulevées au cours de l'atelier portaient principalement sur l'interprétation et l'application des exigences prévues par le règlement par les parties prenantes concernées (comme les futurs organismes d'accès aux données de santé, les comités d'éthique existants, les chercheurs, les patients, les citoyens et professionnels). L'adéquation des

[111] L'action commune TEHDaS2 (deuxième phase de l'action conjointe TEHDaS qui a débutée en mai 2024) vise à soutenir la mise en œuvre de l'EEDS en promouvant des pratiques harmonisées pour l'utilisation secondaire des données de santé grâce à l'élaboration de lignes directrices et des spécifications techniques destinées aux détenteurs de données de santé, aux utilisateurs et aux organismes chargés de l'accès aux données de santé. V. Site internet de TEHDaS : https://tehdas.eu/ [consulté le 10-04-26].

[112] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive (UE) 2011/24 et le règlement (UE) 2024/2847, *JOUE* n° L 2025/327.

[113] Rosa JUUTI DE FINDATA, Magdalena EITENBERGER de l'Université de Vienne, Mikkel LINDSKOV Sachs du National Center for Ethics au Danemark, et Ole JOHAN BAKKE, Président du Standing Committee of European Doctors ont chacun donné une présentation.

[114] Site internet de TEHDaS, Workshop report "Workshop on the ethical dimensions of the European Health Data Space", 19.09.2025 [consulté le 10-04-26].

procédures nationales existantes avec les requis du règlement par ailleurs été questionnée, soulevant la potentielle nécessité de réfléchir à de nouveaux outils, rôles et collaborations afin d'assurer la bonne mise en œuvre du règlement. Les participants ont discuté comment de larges principes comme l'intérêt public, le bénéfice pour la société et l'intérêt légitime pouvaient être traduits de manière opérationnelle et cohérente pour les Etats membres impliquant des contextes culturels différents.

L'objectif principal était de s'accorder sur une conception commune de la gouvernance éthique dans le cadre de l'EEDS. Pour ce faire, différentes thématiques se sont dégagées lors de ces discussions. Parmi elles nous pouvons mentionner la reconnaissance mutuelle des avis éthiques émis par les différents comités d'éthique, le rôle des organismes d'accès aux données de santé en matière de gouvernance éthique, et la nécessité de veiller à ce que l'éthique reste un processus vivant et participatif, et ne soit pas perçue dans la construction de l'Espace européen des données de santé comme une simple étape ponctuelle de mise en conformité.

Rappel du caractère national de l'évaluation éthique

Owe LANGFELDT, chargé de mission au sein de l'Unité Santé numérique de la Direction générale de la santé et de la sécurité alimentaire de la Commission européenne a, en début de workshop, contextualisé les défis que représente l'évaluation éthique au sein de l'EEDS. Son introduction a rappelé que, malgré le fait que le système de l'EEDS soulève des enjeux sociétaux et éthiques importants comprenant la préservation de l'autonomie des individus ou encore les finalités pour lesquelles les données peuvent être réutilisées, les évaluations éthiques restent une compétence nationale. Il n'existe pas de procédure d'évaluation éthique harmonisée au sein de l'UE. Ceci expliquant le fait que le règlement renvoie au droit national applicable en la matière au sein de l'article 67 du Reg. EEDS. Owe LANGFELDT a à ce sujet rappelé que le projet pilote de l'EEDS[115] s'est interrogé sur la faisabilité d'un modèle éthique commun, mais que les positions nationales divergentes n'ont pas permis sa réalisation.

Implications éthiques de l'EEDS

A la suite des quatre présentations données par les experts, un débat sur les implications éthiques de l'EEDS a permis de faire émerger 5 thèmes essentiels :

- **La nécessaire mise en place de pratiques cohérentes en matière d'autorisations d'accès aux données dans un paysage aujourd'hui encore très fragmenté.**

Les participants ont souligné le risque que certains Etats membres s'obstinent à appliquer leurs propres règles sans coopération au niveau européen pour arriver à une approche cohérente. L'approche commune à défendre a été discutée au regard de l'articulation avec les ambitions du marché européen. Les apports d'un point de vue sanitaires et sociétaux devant également être réellement pris en compte dans l'évaluation des demandes d'accès.

- **Les risques liés à la coopération en matière de données de santé, notamment au regard des préoccupations liées à la confidentialité conduisant certains secteurs médicaux à refuser de participer à de tels systèmes coopératifs.**

La confiance a été ici considérée comme essentielle pour améliorer la collaboration des acteurs. De

[115] D'octobre 2022 à décembre 2024, le projet pilote HealthData@EU a élaboré une version pilote de l'infrastructure d'utilisation secondaire des données de santé prévue par l'Espace européen des données de santé. Ce projet pilote a été piloté par la Plateforme des données de santé (ou Health Data Hub) et a réuni 12 pays européens. V. https://health-data-hub.fr/page/healthdataeu-pilot.

plus, le lien entre utilisation primaire et utilisation secondaire des données doit être davantage mis en évidence dans la construction de l'EEDS, ce dernier permettant une meilleure qualité des données et donc une meilleure utilisation secondaire. Des efforts restent également à faire en matière de sensibilisation du public afin de ne pas exacerber les inégalités liées à son accès.

- **Les défis techniques liés à la qualité des données, aux métadonnées et à l'accès transfrontalier.**

Il a été souligné ici que les métadonnées sont essentielles à l'utilisation secondaire des données de santé selon les principes FAIR (*Findable, Accessible, Interoperable, Reusable*)[116]. De plus, il a été convenu que toutes les demandes de données ou d'accès à des données, qu'elles soient nationales ou internationales doivent être traitées de manière égale selon les principes communs prévus par le Reg. EEDS. Ceci a été rappelé en réponse à l'inquiétude formulée de voir certaines régions de l'UE dotées de systèmes de gouvernance de l'utilisation secondaire des données de santé plus réticentes à partager les données de santé détenues demandées par certaines régions présentant des systèmes moins développés.

- **La définition de la structure et du rôle des Organismes d'accès aux données de santé (ORAD).**

Il a été défendu que les ORAD[117] s'insèrent dans le paysage existant en s'appuyant notamment sur les infrastructures existantes, tout en soulignant le défi de coordination des différents acteurs. Si le modèle décentralisé apparaît comme étant le plus adapté, certaines inquiétudes à sa mise en place ont été soulignées : cela ne doit pas conduire à un paysage illisible. Une approche stratégique et coordonnée au niveau européen de la mise en œuvre de l'EEDS en matière d'évaluation éthique est plébiscitée afin d'éviter une mise en œuvre fragmentée du règlement.

- **L'élargissement par le Reg. EEDS du champ des détenteurs de données, des catégories de données et des cas d'utilisation de ces dernières.**

Les cas d'utilisation des données de santé visés ici étaient notamment ceux de l'exploitation des données d'assurance ou l'entrainement des systèmes d'intelligence artificielle. Cet élargissement des cas d'usage des données impliquant une grande quantité de données mais aussi de multiples acteurs, a souligné le défi lié à la capacité des ORAD à avoir la ressource humaine adaptée pour traiter de questions éthiques complexes.

Conclusions et résultats

Le rapport résumant le workshop souligne dans ses conclusions qu'un alignement entre les Etats membres est nécessaire afin de garantir la fiabilité et le respect de l'éthique au sein de l'EEDS. Pour ce faire, quatre messages clés peuvent être retenus :

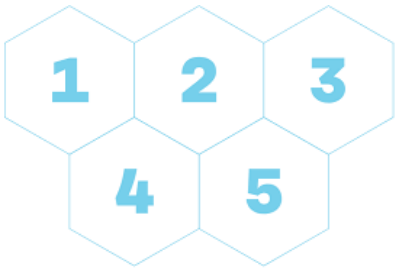
- Trouver un équilibre entre l'harmonisation et le respect des compétences nationales en parvenant à un alignement des pratiques entre les Etats membres.
- Faire de la solidarité en matière de données un principe clé en guidant les décisions relatives à la gouvernance des données de santé par la question fondamentale de la garantie du bénéfice sociétal et de réponse aux objectifs de santé publique.
- Assurer la confiance des personnes et des professionnels en garantissant la confidentialité et la sécurité des données de manière visible dans la mise en œuvre de l'EEDS.

[116] Décrits en 2016, les principes FAIR sont des principes favorisent l'accès et la réutilisation des données de la recherche.

[117] La structuration, les missions et les obligations des organismes responsables de l'accès aux données de santé sont décrites aux articles 55, 57 et 58 du Reg. EEDS.

- Renforcer les capacités et l'expertise des organes de gouvernance pour naviguer dans le paysage éthique et technique complexe que l'EEDS implique.

Le rapport mentionne enfin que les résultats de l'atelier seront analysés plus en détail dans le cadre de la tâche 4.2 du Work Package 4 de TEHDaS2 afin de servir de référence pour la planification de la mise en œuvre du Reg. EEDS.



27.05.2025

D7.1 Guideline on how to use data in a secure processing environment

par Franck AZNAR

Diplomé en biotechnologies, biologie moléculaire et cellulaire ; titulaire du DU EDiHL

La ligne directrice définitive 7.1[118] du groupe de travail TEHDAS 2[119], intitulée « comment utiliser les données dans un environnement de traitement sécurisé ? » publiée fin 2025 à l'occasion de la consultation publique vise à accompagner les utilisateurs de données de santé de la phase de planification préalable à leur demande d'accès aux données de santé jusqu'à la clôture du projet une fois leur analyse effectuée.

L'environnement de traitement sécurisé

Un environnement de traitement sécurisé (ci-après, ETS) est défini comme un espace de travail numérique hautement contrôlé, physique ou virtuel, garantissant un haut niveau de sécurité et de confidentialité, à travers lequel seuls les participants autorisés par l'organisme responsable de l'accès aux données (ci-après, ORAD) peuvent analyser des données de santé personnelles, et ce dans la limite des finalités définies dans l'autorisation de traitement qui leur est délivrée.

Ce nouveau mécanisme de traitement de données de santé de l'espace européen des données de santé (EEDS) coexiste avec les dispositifs traditionnels d'accès et de traitement de données pour la recherche et l'innovation, il ne les remplace pas (voir la ligne directrice D6.2 pour plus d'informations). À ce titre, la combinaison ou l'analyse conjointe de données obtenues via l'EEDS avec des informations issues d'un autre cadre n'est autorisée qu'à la condition d'être explicitement déclarée dans la demande d'accès aux données et validée par l'ORAD dans l'autorisation de traitement des données de santé, conformément à l'article 68§1, point b) du règlement sur l'EEDS.

Au plus tard le 26 mars 2027, les exigences techniques et organisationnelles, ainsi que les exigences en matière de sécurité de l'information, de confidentialité, de protection des données et d'interopérabilité applicables aux ETS seront adoptées par la Commission européenne à travers l'adoption d'actes d'exécution (voir Art.73§5 EEDS), définissant par

[118] Ligne directrice définitive 7.1, disponible ici.

[119] Instituée par la Commission européenne, « Toward European Health Data Space 2 » (TEHDAS 2) est la deuxième action conjointe ayant comme objectif de définir des lignes directrices relatives à la mise en œuvre du règlement « Espace européen des données de santé » (EEDS).

ailleurs les outils et fonctionnalités préinstallés pour les utilisateurs dans les différents ETS.

Préparer et anticiper son projet dans l'ETS

Préalablement aux spécifications actuellement non-adoptées, la ligne directrice 7.1 avance quelques conseils pratiques concernant les modalités et spécificités relatives à l'ETS à prendre en considération pour l'utilisateur de données de santé afin de mener à bien son traitement de données, lui permettant ainsi d'informer l'ORAD de ses besoins dès sa demande d'accès aux données de santé (p.15-16).

Dans la suite de cette ligne directrice sont détaillées les règles à respecter concernant le dialogue entre l'utilisateur des données et le fournisseur de l'ETS (p.17) et les mesures relatives à l'identification des individus autorisés au traitement lors de leur accès à l'ETS, suivant la politique du « Zero Trust » (p.18).

De plus le groupe de travail propose une description de l'infrastructure interne et des règles générales relatives à l'utilisation des ETS, avec notamment la possibilité pour les utilisateurs de données d'installer des logiciels spécifiques, en plus de ceux préinstallés, afin de mener à bien leur traitement. Il y est également fait mention des règles de responsabilités légales, comportementales et administratives qui incombent aux utilisateurs de l'ETS (p.18 à 20).

Le chapitre 11 du document quant à lui détermine les différents responsables du traitement des données, au sens de l'article 4§7 du règlement général sur la protection des données (RGPD), en fonction des activités réalisées lors des différents stades de l'accès et du traitement des données de santé dans le cadre de l'EEDS. Sont également précisées les responsabilités spécifiques qui leur incombent, et notamment celles qui pèsent sur les utilisateurs de données de santé en tant que responsables du traitement des données lorsqu'ils interviennent dans l'ETS, conformément à l'article 74§1 du règlement EEDS (p. 20 à 22).

Dans l'avant dernière partie du document sont mentionnées les actions interdites lors de l'utilisation d'un ETS et les conséquences qui en découlent, ainsi que l'obligation de notification des brèches de sécurité à l'autorité compétente, conformément au RGPD (p. 22-23).

Sont définies *in fine* les conditions relatives à l'exportation des résultats de l'ETS. Il est possible d'archiver les données dans un environnement de traitement avec des capacités limitées, notamment à des fins de reproductibilité et de vérification des résultats par les pairs. Il est rappelé qu'une autorisation de traitement de données, conformément à l'article 68 de l'EEDS, ne peut excéder 10 années consécutives, extensible une seule fois pour une période de 10 années supplémentaires. Une fois l'autorisation expirée, l'ORAD dispose alors de 6 mois pour supprimer l'intégralité des données de santé stockées sur l'ETS. Les résultats doivent être publiés dans les 18 mois suivant la fin du traitement (p.23).

05.09.2025

M7.2 Draft guideline on data minimisation, pseudonymisation, anonymisation and synthetic data

par Franck AZNAR

Diplomé en biotechnologies, biologie moléculaire et cellulaire ; titulaire du DU EDiHL

Lors de cette même consultation publique, le groupe de travail 7.2[120] a publié sa ligne directrice préliminaire M7.2 concernant la minimisation des données, la pseudonymisation, l'anonymisation et les données synthétiques.

Minimisation des données

Dans la première partie du document (p. 8 à 24), le groupe de travail se penche sur la question de la minimisation des données, principe fondamental énoncé à l'article 5§1, c) du règlement général sur la protection des données (RGPD) comme suit « les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Le groupe de travail met ainsi en avant le respect de ce principe tout au long de l'intégralité du cycle de vie des données, définissant en ce sens plusieurs recommandations et bonnes pratiques à destination des différents acteurs impliqués. Parmi ces recommandations, on retiendra notamment la réduction du volume des différents jeux de données en fonction des finalités de traitement, et ce en limitant nécessairement la granularité et les variables disponibles, avec une attention particulière portée aux identifiants indirects (âge, nationalité, appartenance ethnique, lieu de travail, niveau de revenus, etc..).

Le document précise la recommandation sus-mentionnée par le biais de cinq dimensions : « Qui ? ; Quoi ? ; Quand ? ; Où ? ; Comment ? » (voir **schéma relatif à la minimisation des données – page suivante**), permettant d'apprécier le spectre des critères essentiels afin d'établir une minimisation efficiente des données (p.13 à 19).

La pseudonymisation comme pierre angulaire

Dans la seconde partie du document la pseudonymisation des données est abordée, telle que définie à l'article 4§5 du RGPD. La pseudonymisation est une transformation, dans laquelle les identifiants personnels directs sont remplacés par de nouveaux identifiants appelés pseudonymes. Elle permet une utilisation secondaire des données de santé électroniques dans un environnement de traitement sécurisé, sous condition prévue par l'article 68§1, c) du règlement relatif à l'Espace européen des données de santé (EEDS).

Le groupe de travail liste dans ce chapitre les avantages de la pseudonymisation par rapport à l'anonymisation, à savoir un degré de qualité et de fidélité des données plus élevé, la possibilité de lier différents jeux de données entre eux et l'aspect réversible de la pseudonymisation.

Concernant la possibilité de lier différents jeux de données appartenant à différents détenteurs de données, c'est par l'intermédiaire de l'organisme responsable de l'accès aux données (ORAD) ou d'un détenteur de données de confiance que sera délivrée, suite à une évaluation des risques, une autorisation de traitement de données permettant ou non la liaison des jeux de données, utilisant les identifiants directs en amont de la pseudonymisation (p.26) – (Pour davantage d'informations sur la liaison des différents jeux de données voir le document M7.5[121] du TEHDAS 2).

Les auteurs énoncent ensuite différents scénarios impliquant tous les acteurs

[120] Ligne directrice préliminaire 7.2, disponible ici.

[121] Ligne directrice préliminaire 7.5, disponible ici.

lors des différentes phases de l'utilisation secondaire des données de santé (voir schéma récapitulatif des cas d'usage généraux) et émettent des recommandations générales, notamment en termes de métadonnées (voir ligne directrice D5.1[122], de mesures techniques, organisationnelles et de gestion des risques associées à la pseudonymisation (p.28 à 33). Une pseudonymisation réversible est nécessaire dans le cas d'une constatation significative relative à la santé d'une personne physique (voir article 58§3 EEDS) ou pour l'application du droit d' « opt-out » (voir article 71 EEDS).

Aller plus loin dans la protection des données

Le groupe de travail a été amené à discuter en détail, dans ce dernier chapitre dédié à l'anonymisation et à la génération de données synthétiques, de différentes techniques qui permettent une protection complémentaire à la minimisation des données et aux données pseudonymisées. Il y est précisé que ces techniques d'anonymisation et de génération de données synthétiques seront souvent rendues nécessaires afin, entre autres, de garantir un niveau de protection des données élevé empêchant les risques de ré-identification notamment dans le cadre d'entraînement de modèles d'IA d'apprentissage automatique, ou lors de l'exportation de données des environnements de traitement sécurisés, ou encore afin de permettre aux demandeurs de données de santé de tester divers algorithmes informatiques, préalablement à la demande de traitement des données, sur des échantillons de jeux de données publiquement disponibles (voir ligne directrice D5.1 section 8.2.4).

Le document présente différents cas d'utilisation des données de santé et en ce sens différentes méthodologies et outils utiles au développement d'une architecture « la plus robuste qui soit » en matière d'anonymat, de génération de données synthétiques, et d'évaluation des risques associés (p.37 à 40).

Les règles générales relatives à l'établissement d'une documentation obligatoire lors de l'utilisation de techniques d'anonymisation des jeux de données et de génération de données synthétiques sont également définies (p.40-41).

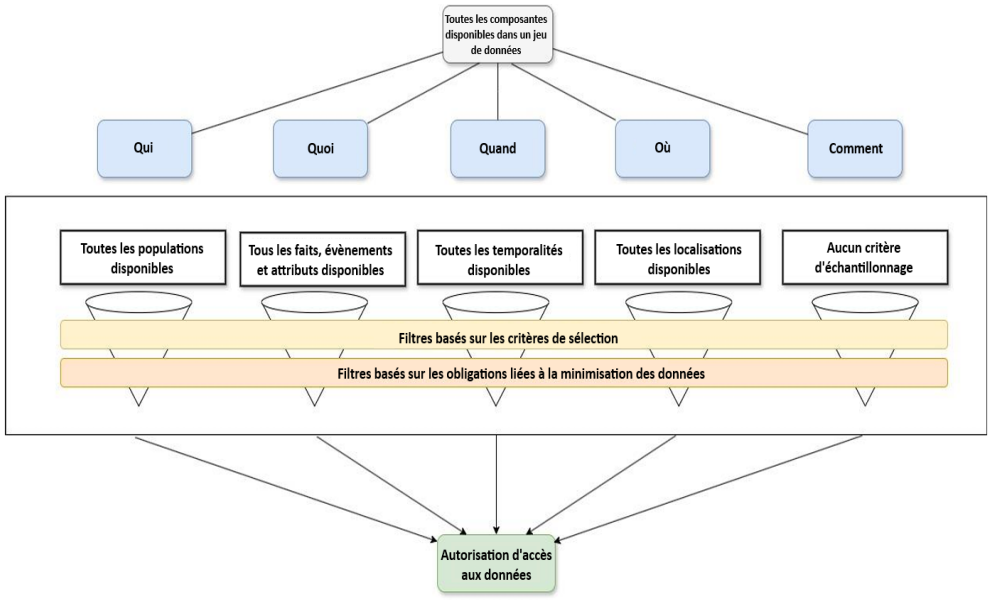


Schéma relatif à la minimisation des données définissant les différentes dimensions liées à la minimisation des données dans le cadre de l'EEDS

[122] Ligne directrice définitive 5.1, disponible ici.

Enfin, dans la dernière partie du document, sont présentées différentes techniques existantes d'anonymisation et de génération de données synthétiques (p.41-45), ainsi que différents outils supposés nécessaires afin d'aider les différents acteurs impliqués à vérifier, et évaluer automatiquement (ou semi-automatiquement) la viabilité des mesures de protection des données ayant été mises en œuvre sur un jeu de données (p.45 à 47).

Un arrêt attendu :

La Cour dans son arrêt *CEPD contre CRU*, C-413/23 P, du 4 septembre 2025[123] a été amenée à se prononcer sur plusieurs questions relatives aux données à caractère personnel. Après avoir réaffirmé, conformément à une jurisprudence constante, les critères caractérisant les données à caractère personnel, à savoir le fait que les données à caractère personnel se rapportent à une personne physique en raison de « leur contenu, de leur finalité ou de leur effet » *(voir arrêt Nowak, C-434/16[124])* et le fait qu'elles se rapportent à une personne physique « identifiée ou identifiable » *(voir arrêt Breyer, C-582/14[125]),* la Cour consacre le caractère relatif (ou contextuel) de l'effet de la pseudonymisation sur l'identifiabilité des données à caractère personnel.

On notera avec intérêt la formulation retenue selon laquelle « l'existence d'informations supplémentaires permettant d'identifier la personne concernée n'implique pas à elle seule, que des données pseudonymisées doivent être considérées comme constituant en toute hypothèse et pour toute personne, des données à caractère personnel ».

En conséquence, laissant ouverte la question du caractère contextuellement identifiable des données pseudonymisées, la Cour nous amène à nous attendre, vraisemblablement, à l'apparition future d'une vaste jurisprudence en la matière, évoluant et se précisant, au gré des nouvelles réglementations et des nouvelles technologies.

Il n'est pas interdit de penser, sous réserve d'une confirmation par la CJUE de cette interprétation, si elle en est saisie, que les utilisateurs de données de santé autorisés par l'ORAD, auraient la possibilité de télécharger, conformément à l'article 73§2 tiret 2 du règlement EEDS des données de santé électroniques pseudonymisées ne comportant aucun élément à caractère personnel au sens de l'interprétation retenue dans l'arrêt CRU. En attendant, la version définitive du projet de lignes directrices M7.2 apportera sans doute des éléments éclairants et déterminants. Une telle possibilité aurait été inenvisageable si la Cour s'était prononcée en faveur du caractère dit « absolu » de la pseudonymisation.

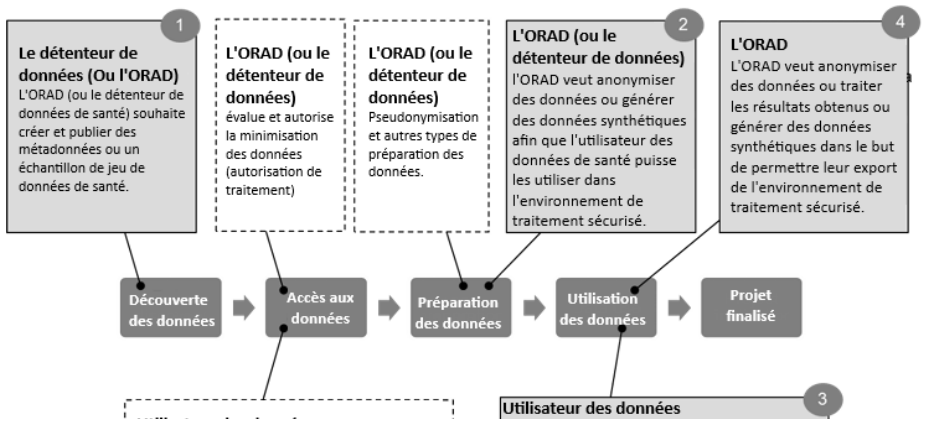


Schéma récapitulatif des cas d'usage généraux dans lesquels interviendraient minimisation, pseudonymisation, anonymisation des données et génération de données synthétiques en fonction des différentes phases de l'utilisation secondaire des données de santé et des différents acteurs impliqués

[123] Arrêt CRU contre CEPD, C-413/23 P, disponible ici.

[124] Arrêt Nowak, C-434/16, disponible ici.

[125] Arrêt Breyer, C-582/14, disponible ici.

Commentaire des propositions TEHDaS2 clarifiant les modalités d'examen des finalités de réutilisation, de notification des constatations significatives et portant sur les infrastructures techniques de traitement des données

par Winnie DONGBOU WAMBA

Doctorant en Droit public, EDT-R-IRDEIC, Université Toulouse Capitole
Juriste en droit de la protection des données de santé MyData-TRUST

16.09.2025
M5.2 Draft Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data

17.09.2025
M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure

12.09.2025
M7.4 Draft technical, functional and security specifications of Secure Processing Environments

07.09.2025
M8.2 Draft Guideline to Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data

Dans le cadre d'une consultation publique ouverte du 30 septembre au 30 novembre 2025, TEHDAS2[126] a soumis à contributions un ensemble de onze projets de lignes directrices[127], dont quatre retiennent particulièrement notre attention en raison de l'importance des dispositions du Règlement EEDS qu'ils proposent de concrétiser. Il s'agit du projet de ligne directrice M5.2 sur les catégories minimales et les limitations à la réutilisation des données de santé[128], la ligne directrice M8.2 sur l'obligation de notification aux personnes physiques des constatations importantes liées à leur santé, issues de l'utilisation secondaire[129], ainsi que les projets de spécifications techniques M7.3 et M7.4 portant respectivement sur l'infrastructure informatique commune[130] et sur les environnements de traitement sécurisés[131].

Ces projets de lignes directrices et de spécifications techniques abordent des questions essentielles à l'opérationnalisation effective de l'EEDS : la frontière entre finalités autorisées et usages prohibés, y compris l'harmonisation de l'évaluation des demandes d'accès (I), la primauté de l'intérêt

[126] L'action conjointe TEHDAS2 (Towards a European Health Data Space-2) a pour objectif d'accompagner la Commission Européenne dans la conception de lignes directrices visant à opérationnaliser l'utilisation secondaire des données de santé.
[127] Tous les 11 projets de lignes directrices sont disponibles ici https://tehdas.eu/public-consultations/#public-consultation.
[128] TEHDAS2, M5.2 Draft Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data, 16 September 2025.
[129] TEHDAS2, M8.2 Draft Guideline to Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data, 7 September 2025.
[130] TEHDAS2, M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure, 17 September 2025.
[131] TEHDAS2, M7.4 Draft technical, functional and security specifications of Secure Processing Environments, 12 September 2025.

du participant à la recherche à travers la notification des constatations significatives (II), et à la configuration technique et organisationnelle de l'infrastructure indispensable aux échanges entre autorités compétentes (III), à l'accès, au partage et la sécurité des données de santé (IV).

I. LA BARRIERE POREUSE ENTRE FINALITES AUTORISEES ET USAGES PROHIBES

La ligne directrice M5.2 vise essentiellement à guider les Organismes d'accès aux données de santé (ORAD, en anglais *Health Data Access Bodies* – HDAB) dans l'interprétation des articles 53 et 54 du Règlement EEDS, qui définissent respectivement les finalités autorisées et les usages prohibés de l'utilisation secondaire des données de santé électroniques. Elle énumère six finalités licites au titre de l'article 53(1) dont les finalités d'intérêt public et de recherche scientifique, qui nous intéresseront particulièrement en raison de leur frontière floue avec certains usages prohibés.

A. Les clarifications conceptuelles attendues sur les finalités d'intérêt public et de recherche scientifique

Le projet de ligne directrice propose une lecture restrictive de l'intérêt public en soulignant que la finalité doit relever des domaines de la santé publique ou de la santé au travail tels que définis par le Règlement (UE) 1338/2008 et par les standards de l'Organisation mondiale de la santé[132]. Le document insiste sur le fait que l'intérêt public au sens de l'EEDS doit s'entendre comme un concept fonctionnel, étroitement lié à des compétences d'autorité publique[133]. Cette précision est utile, car elle évite l'instrumentalisation du concept par des acteurs qui invoqueraient un intérêt public diffus pour accéder à des données sensibles.

Concernant la clarification de la finalité de recherche scientifique, le projet de ligne directrice procède en deux temps. il observe d'abord que ce concept n'est pas entièrement défini dans les actes du droit dérivé de l'Union, et qu'il convient de la rapprocher de la définition extensive donnée au considérant 159 du RGPD, laquelle englobe le développement et la démonstration technologiques, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé[134]. Il introduit ensuite une distinction subtile entre « recherche scientifique » stricto sensu et « activités d'innovation »[135], reconnaissant que ces dernières couvrent un spectre allant de la recherche translationnelle à des activités de développement de produits. Les risques d'une lecture trop extensive de la « recherche scientifique », ne sont pas explicitement adressés, mais le projet de ligne directrice propose néanmoins des garde-fous opérationnels en exigeant des ORAD qu'ils vérifient la cohérence entre les qualifications du demandeur et l'objectif déclaré[136].

B. La difficile frontière des usages prohibés : marketing et produits préjudiciables

L'article 54 du Règlement EEDS prohibe cinq catégories d'usages : les décisions préjudiciables aux personnes (a), les décisions discriminatoires à l'égard de groupes (b), les activités de publicité et de marketing (c), le développement de produits ou services préjudiciables (d), et les activités contraires aux dispositions éthiques nationales (e). Le projet de ligne directrice M5.2 consacre des développements substantiels à ces interdictions, sans cependant parvenir à dissiper toutes les zones d'ombre[137].

Nous proposons de les résumer en trois principaux points : (1) l'asymétrie informationnelle. Un

[132] Projet M5.2, §. 6.1, p. 14.
[133] *Ibid.*, pp. 14-21.
[134] *Ibid.*, pp. 27-28.
[135] *Ibid.*, p. 29.
[136] *Ibid.*, §. 6.7.4, p. 30.
[137] Projet M5.2, §. 9.

demandeur disposant de véritables intentions discriminatoires ne les révélera jamais dans sa demande, rendant le contrôle *ex ante* par l'ORAD inefficace à prévenir les usages détournés les plus préjudiciables ; (2) la temporalité défavorable du contrôle : les violations seront découvertes seulement lors du monitoring *ex post*, lorsqu'un préjudice sera probablement déjà constaté ; (3) l'insuffisance de la solution offerte : les clauses d'engagement recommandées pour éviter les usages prohibés ne fonctionnent que sur base de la bonne foi des utilisateurs des données, mettant ainsi en évidence le décalage entre la promesse protectrice de l'EEDS et sa réalité opérationnelle.

C. Les pistes de réflexion additionnelles : l'aveu d'une « œuvre » inachevée

La ligne directrice M5.2 se distingue par la lucidité avec laquelle elle assume le caractère inachevé de son travail. Sa section 9, intitulée « *Areas of further exploration* », énumère sept chantiers ouverts qui mériteront un approfondissement via les résultats de la consultation publique. Sont ainsi identifiés : (1) l'alignement continu entre les ORAD quant à l'évaluation des demandes (§9.1), qui suppose la mise en place de mécanismes de coordination — comparables, en matière de protection des données, au rôle du Comité européen de la protection des données ; (2) la clarification de la frontière entre innovation et marketing (§9.2), dont la ligne directrice admet qu'elle constitue un point imprécis ; (3) l'interprétation de l'interdiction du développement des produits préjudiciables dans le contexte de la recherche médicale impliquant des substances contrôlées (§9.3), question particulièrement sensible pour la recherche sur les addictions et les psychédéliques thérapeutiques ; (4) la définition d'une procédure européenne standard pour l'évaluation des demandes par les ORAD (§9.4), ce qui revient à reconnaître l'insuffisance d'une harmonisation seulement par les principes ; (5) l'organisation d'un soutien éthique et juridique aux ORAD (§9.5), enjeu central pour assurer la capacité de ces organismes à évaluer les demandes d'accès ; (6) le traitement des décisions automatisées et de leurs effets potentiellement préjudiciables (§9.6) ; et (7) la construction d'un système de surveillance permettant d'identifier les usages détournés des données (§9.7).

II. L'INTÉRÊT SUPÉRIEUR DES PARTICIPANTS À LA RECHERCHE : LA NOTIFICATION DES CONSTATATIONS SIGNIFICATIVES

Le projet de ligne directrice M8.2 quant à lui couvre l'une des questions éthiques les plus délicates posées par la réutilisation secondaire des données de santé : que faire lorsque l'analyse de données conduit à la découverte d'une information médicale significative (ci-après « constatation(s) significative(s) ») pour la personne dont les données ont été utilisées ? Les articles 58(3) et 61(5) du Règlement EEDS imposent aux ORAD-une procédure spécifique en matière de constatations significatives, dont la ligne directrice M8.2 précise les contours opérationnels en distinguant préalablement les constatations incidentes de celles qui sont significatives. Les premières se définissent comme des informations révélées fortuitement au cours d'une recherche, en dehors du champ de la question scientifique initiale, et non intentionnellement recherchée par les investigateurs[138]. Les secondes sont des constatations qui présentent une pertinence médicale directe pour la santé de la personne dont les données ont été traitées[139]. Cette définition évite une notification de toute découverte incidente, lequel aboutirait à une surcharge informationnelle préjudiciable à la personne et matériellement insoutenable pour les détenteurs de

[138] Projet M8.2, §. 5.1.

[139] *Ibid.*

données. Il est bien évidemment entendu que la procédure de notification n'est applicable que lorsqu'il est possible d'identifier directement (via des identifiants personnels) ou indirectement (via une pseudonymisation avec accès à la clé de réidentification) la personne concernée[140].

Cette procédure de notification implique trois acteurs dont il convient de préciser les responsabilités. L'utilisateur de données signale la découverte significative à l'ORAD[141], qui la transmet au détenteur de données. C'est le détenteur qui assure, le cas échéant, la notification à la personne concernée ou au professionnel de santé qui la prend en charge[142]. L'ORAD n'est responsable ni de la validation clinique du résultat, ni de la notification directe à l'individu. Il ne joue qu'un rôle d'intermédiaire. La décision de notification est toutefois laissée à l'appréciation du détenteur des données en fonction de ce qui est autorisé ou requis par le droit national[143]. Le projet M8.2 révèle également une tension entre le droit de la personne à ne pas être informée[144] et l'obligation potentielle de notification des constatations découlant de la réutilisation de ses données. A ce sujet, elle laisse le soin aux États membres d'établir des procédures permettant d'assurer que le droit à ne pas être informé est appliqué lors du déclenchement de la procédure de notification[145].

III. LA CONFIGURATION TECHNIQUE ET ORGANISATIONNELLE DE L'INFRASTRUCTURE COMMUNE INDISPENSABLE AUX ÉCHANGES ENTRE AUTORITÉS COMPÉTENTES

Le projet de spécification technique M7.3 présente HealthData@EU, l'infrastructure transfrontalière instituée par l'article 75 du Règlement EEDS, en deux composantes essentielles. D'une part, la plateforme centrale HealthData@EU opérée par la Commission européenne[146] et d'autre part, les points de contact nationaux déployés par les États membres pour connecter leurs environnements nationaux à la plateforme centrale[147]. En effet, chaque État membre désigne un Point de Contact National (PCN) qui sert d'intermédiaire unique entre les systèmes nationaux et la plateforme centrale.

Aucune communication directe entre États membres n'est possible — tout transite obligatoirement par la plateforme centrale[148], ce qui garantit une traçabilité complète mais crée une dépendance technique envers la Commission. Chaque message échangé — qu'il s'agisse d'une demande d'accès aux données, d'une décision de permis ou d'une mise à jour du catalogue — suit un flux identique en douze étapes, au cours duquel il est successivement validé, chiffré, signé, transmis, déchiffré, authentifié et enregistré à des fins d'audit[149]. Deux couches distinctes assurent ce processus : une couche « métier » qui vérifie que le contenu du message est conforme aux exigences du Règlement EEDS, et une couche « transport » qui garantit la sécurité technique de la transmission[150]. À chaque étape, un accusé de réception signé est renvoyé à l'expéditeur, assurant qu'aucun message ne peut être perdu ou contesté.

Avant de se connecter à l'infrastructure, les États membres peuvent tester leurs systèmes via un outil de conformité mis à disposition par la Commission, dont l'usage est recommandé mais non obligatoire[151]. Ce cadre

[140] *Ibid.,* §. 5.3.
[141] *Ibid.,* §. 7.1, step 2.
[142] *Ibid.,* steps 3 and 4.
[143] *Ibid.,* §. 7.2, Figure 1.
[144] Considérant 67 et art. 58(3) du Règlement EEDS.
[145] Projet M8.2, p. 23.
[146] M7.3, §. 2.1.
[147] *Ibid.,* Annexe 2
[148] *Ibid.,* p. 14-15.
[149] *Ibid.,* §. 7.2.
[150] *Ibid,* §. 6.
[151] *Ibid.*, §. 8.

technique, aussi robuste soit-il, laisse entière une question juridique centrale que M7.3 ne tranche pas : en cas de défaillance dans la chaîne de transmission, la responsabilité reste indéterminée entre le point de contact national, la Commission et les ORAD destinataires des demandes d'accès.

IV. L'ARCHITECTURE DES ENVIRONNEMENTS DE TRAITEMENT SÉCURISÉS

Les environnements de traitement sécurisés (ETS) constituent, selon la spécification M7.4, une plateforme virtuelle conçue pour permettre une réutilisation sécurisée des données de santé tout en maintenant la conformité aux obligations de protection et de confidentialité des données[152]. Leur définition juridique est empruntée au Règlement (UE) 2022/868 sur la gouvernance des données, qui les décrit comme des environnements physiques ou virtuels permettant à leur opérateur de déterminer et superviser toutes les actions à effectuer sur les données, de leur accessibilité à leur exportation[153]. Dans le périmètre de l'EEDS, l'article 73 du Règlement (UE) 2025/327 en fixe les exigences de base, que M7.4 décline en dix-huit exigences numérotées (EHDSR-1 à EHDSR-18), articulées autour de trois impératifs : la sécurité des données, l'accès restreint aux seules personnes nominativement désignées dans le permis de données, et le contrôle des sorties garantissant que seuls des résultats agrégés et anonymisés peuvent quitter l'environnement[154].

Le cycle de vie de l'ETS passe par six étapes[155]. L'environnement est d'abord créé sur mesure une fois le permis délivré par l'ORAD, typiquement par le déploiement d'une machine virtuelle isolée. Les données sont ensuite transmises par le détenteur de données vers l'ETS, où l'ORAD procède à leur préparation technique — pseudonymisation, anonymisation, agrégation, etc…— avant de les mettre à disposition du chercheur dans un espace dédié. Le chercheur analyse les données à l'aide des outils fournis par l'ETS, conformément à des exigences strictes[156]. À l'issue de l'analyse, toute extraction de résultats est soumise à validation préalable de l'OADS (EHDSR-12, EHDSR-13), et l'ensemble des données doit être supprimé dans les six mois suivant l'expiration du permis, sans exception pour les sauvegardes (OPR-5 ; art. 68(12) EEDS, cité en M7.4, §4.5.2, p. 26).

Les exigences opérationnelles du projet M7.4 s'organisent en six catégories couvrant la gestion des accès, l'audit et la conformité, la surveillance et la gestion des incidents, la gestion des risques, et la maintenance[157]. Concernant la gestion des accès, chaque utilisateur doit disposer d'une identité unique, non transférable, authentifiée par authentification multifactorielle, et les droits doivent être strictement limités au minimum nécessaire à la réalisation du projet autorisé[158]. Sur le plan de la traçabilité, tous les accès et toutes les opérations effectuées dans l'ETS doivent être journalisés, conservés au minimum un an — et plus longtemps si justifié— et disponibles à tout moment pour vérification et audit[159]. En cas d'incident de sécurité, l'opérateur technique de l'ETS doit notifier l'ORAD dans les 24 heures, fournir un rapport détaillé dans les 72 heures et un rapport final dans le mois, en cohérence avec les exigences de la Directive NIS2[160]

Malgré ces spécifications déjà bien précises, le projet M7.4 laisse ouverte la question des mesures de sécurité organisationnelles et

[152] M7.4, Executive Summary, p. 6.
[153] *Ibid.*, §. 3.1, p. 9, citant DGA, art. 2).
[154] *Ibid.*, §. 3.1, pp. 9-10; §. 4.4, pp. 19-22.
[155] *Ibid.*, §. 3.2, pp. 9-10)
[156] *Ibid.*, §. 4.3.3, p. 18)
[157] *Ibid.*, §. 4.5, pp. 22-41.
[158] *Ibid.*, §. 4.5.2, pp. 27-29.
[159] Voy. EHDSR-6, EHDSR-7, EHDSR-8 ; OPR-16, OPR-17 ; art. 73(1)(e) EEDS, cités dans M7.4, §. 4.5.4, pp. 35-36.
[160] Voy. OPR-18, OPR-19 ; M7.4, §. 4.5.4, p. 36.

techniques communes aux ETS. Il renvoie aux actes d'exécution que la Commission doit adopter en vertu de l'article 73(5) du Règlement EEDS avant mars 2027[161].

Conclusion

La lecture des quatre projets de lignes directrices révèle un important travail abordant à la fois des considérations substantielles (finalités de réutilisation des données, droits des personnes), procédurales (procédure de notification des découvertes, gestion des demandes d'accès) et techniques (infrastructure commun, sécurité) dans une perspective d'harmonisation européenne. Cette harmonisation technique et des pratiques indispensable pour garantir une évaluation uniforme des demandes d'accès et un seuil minimal commun de sécurité des données de santé disponibles au niveau des catalogues nationaux.

Leur soumission à consultation publique permettra sans aucun doute aux experts, aux professionnels de santé, aux organisations de patients et aux chercheurs de participer à la construction d'un espace de données de santé dont le pilier fondamental est l'innovation en santé sans le sacrifice de la protection des individus.

AUTRES PUBLICATIONS TEHDaS 2

17. 09.2025

M4.1.1 Draft guideline on fees related to the EHDS regulation

Second section: 4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

7.09.2025

M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse

6.05.2025

D6.2 Guideline for data users on good application and access practice

17.09.2025

D6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access

17.09.2025

D6.4 Technical Specifications for Data Access Application Management System (DAAMS) for Health Data Access Bodies (HDABs)

17.09.2025

M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure

12.09.2025

M7.4 Draft technical, functional and security specifications of Secure Processing Environments

[161] M7.4, §. 4.4, p. 19 ; EHDSR-18.

La Commission européenne propose une simplification du cadre règlementaire applicable aux dispositifs médicaux

Le 16 décembre 2025, la Commission européenne a présenté une proposition de règlement visant à réviser de manière ciblée les deux règlements de l'Union européenne relatifs aux dispositifs médicaux (règlement (UE) 2017/745, dit « MDR ») et aux dispositifs médicaux de diagnostic in vitro (règlement (UE) 2017/746, dit « IVDR »). Cette initiative s'inscrit dans une démarche de simplification du cadre réglementaire européen destinée à le rendre plus efficace, plus proportionné et mieux adapté aux évolutions technologiques, tout en maintenant un niveau élevé de protection de la santé publique.

La Commission justifie cette révision par les difficultés rencontrées depuis l'entrée en application du MDR et de l'IVDR : complexité des procédures, délais de certification importants, capacités limitées des organismes notifiés, coûts élevés de mise en conformité et risques pesant sur la disponibilité de certains dispositifs, en particulier pour les petites et moyennes entreprises.

La proposition prévoit notamment une simplification de certaines obligations réglementaires, un recours accru aux outils numériques, une plus grande proportionnalité des exigences au regard du niveau de risque des dispositifs ainsi qu'une amélioration de l'efficacité des procédures d'évaluation de conformité. Elle vise également à soutenir l'innovation et la compétitivité du secteur européen des technologies de santé tout en préservant les garanties de sécurité et de performance applicables aux dispositifs médicaux.

Le texte comporte enfin plusieurs dispositions destinées à mieux articuler le cadre applicable aux dispositifs médicaux avec les autres législations européennes récentes, notamment en matière d'intelligence artificielle.

À ce stade, la proposition est en cours d'examen par le Parlement européen et le Conseil.

DOCUMENTS DE RÉFÉRENCE

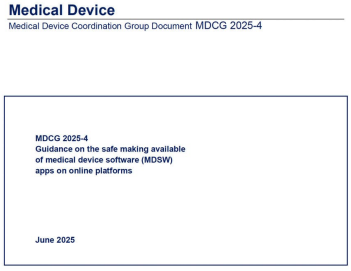
- **Fiche d'information de la Commission européenne** – Présentation synthétique des principales mesures de simplification proposées pour les dispositifs médicaux et les dispositifs médicaux de diagnostic in vitro
- **Proposition de règlement *COM(2025)* 1023 final** – Texte de la proposition de révision ciblée du MDR et de l'IVDR
- **Questions & Answers de la Commission européenne** – Questions-réponses détaillant les objectifs et les effets attendus de la réforme

Aperçu général du MDCG et de ses guides

Le *Medical Device Coordination Group* (MDCG) est le groupe de coordination institué par les règlements européens relatifs aux dispositifs médicaux (art. 103) et aux dispositifs médicaux de diagnostic in vitro (art. 98). Composé de représentants des autorités compétentes des États membres et présidé par la Commission européenne, il contribue à une mise en œuvre harmonisée de ces règlements au sein de l'Union européenne.

Dans ce cadre, le MDCG publie régulièrement des guides d'orientation (« guides MDCG ») destinés à accompagner l'application pratique des règlements MDR et IVDR. Ces guides abordent de nombreuses questions relatives à l'interprétation et à la mise en œuvre du cadre européen applicable aux dispositifs médicaux. Bien que dépourvus de caractère juridiquement contraignant, ils constituent aujourd'hui des références importantes pour l'interprétation et l'application du cadre juridique de l'Union européenne applicable aux technologies de santé.

*Les contributions qui suivent présentent trois guides récents du MDCG consacrés aux logiciels médicaux et à l'intelligence artificielle, portant respectivement sur la qualification et la classification des logiciels, leur mise à disposition sur les plateformes en ligne et l'articulation entre les règlements relatifs aux dispositifs médicaux et l'*AI Act.



L'encadrement de la mise à disposition des applications qualifiées de dispositifs médicaux sur les plateformes en ligne. Commentaire du guide MDCG 2025-4

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

L'intégration croissante des technologies numériques dans le domaine de la santé transforme en profondeur les paradigmes de la prise en charge médicale. Les applications logicielles bouleversent notre mode de vie et occupent une place de plus en plus prépondérante dans les parcours de soins, couvrant un spectre extrêmement vaste d'utilisations, allant des algorithmes complexes destinés à piloter des pompes à insuline aux applications capables de détecter et de diagnostiquer des cancers de la peau.

La disponibilité directe de ces applications sur des plateformes de téléchargement grand public soulève toutefois des défis réglementaires inédits. L'accès facilité pour les patients et les professionnels de santé exige une vigilance accrue quant à la sécurité, la performance et la conformité de ces produits aux exigences du règlement (UE) 2017/745 relatif aux dispositifs médicaux (« MDR » acronyme anglais pour *medical device regulation*)[162] et du règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[163].

C'est dans ce contexte de convergence entre le droit des produits de santé et le droit du numérique qu'a été publié, le 16 juin 2025, le guide MDCG 2025-4 *« Guidance on the safe making available of medical device software (MDSW) apps on online platforms »*. Approuvé par le Groupe de coordination en matière de dispositifs médicaux (« MDCG »), ce document vise à clarifier les rôles, les responsabilités et les

[162] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, *JOUE* L. 117 du 5 mai 2017.

[163] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, *JOUE* L. 117 du 5 mai 2017.

obligations d'information des fournisseurs de plateformes d'applications. Ce texte s'attache particulièrement à articuler les exigences du MDR et de l'IVDR avec celles introduites par le règlement (UE) 2022/2065 sur les services numériques, plus connu sous le nom de Digital Services Act (« DSA »)[164].

L'analyse de ce guide révèle l'émergence d'une architecture réglementaire stratifiée, où les obligations de conformité ne reposent plus exclusivement sur les fabricants, mais s'étendent désormais aux intermédiaires technologiques. Il convient d'examiner en détail les dispositions de ce guide, en dégageant des perspectives opérationnelles pour les acteurs de l'écosystème numérique en santé, tout en s'inscrivant dans la continuité des analyses portant sur le droit européen de la santé numérique.

I. LA QUALIFICATION JURIDIQUE DES OPERATEURS DE PLATEFORMES : UNE DISTINCTION DETERMINANTE POUR L'IMPUTATION DES RESPONSABILITES

L'un des apports majeurs du guide MDCG 2025-4 réside dans la clarification de l'applicabilité simultanée de plusieurs cadres juridiques de l'Union européenne à un même produit numérique.

La mise à disposition ou la mise en service d'un logiciel qualifié de dispositif médical (*Medical Device Software*, ci-après « MDSW ») ne peut intervenir que si le produit satisfait à l'ensemble des législations d'harmonisation applicables.

Afin d'appréhender les responsabilités respectives, le guide rappelle la terminologie réglementaire du cycle de vie du produit. La « mise sur le marché » correspond à la première mise à disposition d'un dispositif sur le marché de l'Union. Dans l'écosystème des applications, le téléchargement initial ou l'intégration (*upload*) du MDSW par le fabricant sur la plateforme correspond à cette étape cruciale. Par la suite, la « mise à disposition sur le marché » englobe toute fourniture d'un dispositif destiné à être distribué, consommé ou utilisé, la période durant laquelle l'application est accessible via la plateforme relevant de cette définition. Ces définitions permettent de scinder l'acte technologique d'hébergement en actes juridiques distincts déclenchant des responsabilités spécifiques.

Le guide envisage ainsi deux configurations réglementaires principales pour les fournisseurs de plateformes, selon qu'ils agissent en tant que simples intermédiaires ou en tant qu'opérateurs économiques de la chaîne de distribution.

Dans la première configuration, la plateforme joue un rôle d'infrastructure technique reliant les fabricants de MDSW aux patients. Selon l'article 3 du DSA, une plateforme en ligne est définie comme un service d'hébergement qui, à la demande d'un destinataire du service, stocke et diffuse des informations au public. Lorsque le fournisseur de la plateforme propose exclusivement des applications développées par des tiers, il agit uniquement en tant que service d'intermédiation. Sous ce régime, la plateforme facilite la conclusion de contrats à distance entre les consommateurs et les professionnels mais n'est pas considérée comme un distributeur ou un importateur au sens du MDR ou de l'IVDR. Ce statut lui permet de bénéficier des exemptions de responsabilité prévues par le DSA pour les contenus hébergés, à condition qu'elle ne joue pas un rôle actif dans la distribution et qu'elle respecte ses obligations de diligence.

La seconde configuration se présente lorsque le fournisseur de la plateforme

[164] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *JOUE* L. 277 du 27 octobre 2022.

s'implique directement dans la chaîne d'approvisionnement. Si la plateforme met à disposition son propre MDSW, ou si elle agit de manière à transférer la propriété ou les droits d'utilisation directs à l'utilisateur, elle revêt la qualification d'opérateur économique, à savoir de distributeur ou d'importateur. À titre d'exemple, le guide mentionne que si le fabricant de l'application est basé en dehors de l'Union européenne et que la plateforme est basée dans l'Union, cette dernière assume le rôle d'importateur. Dans ce scénario, l'applicabilité protectrice du DSA s'efface au profit des obligations strictes de la législation sectorielle (articles 13 ou 14 du MDR/IVDR[165]). L'importateur doit alors s'assurer que le fabricant a formellement désigné un mandataire au sein de l'Union, et le distributeur doit vérifier de manière proactive la sécurité et les performances du dispositif.

II. LES OBLIGATIONS DE TRANSPARENCE ET D'IDENTIFICATION : UNE MISE EN ŒUVRE DU PRINCIPE « KNOW YOUR BUSINESS CUSTOMER »

La sécurité des patients naviguant sur les plateformes numériques repose fondamentalement sur la transparence de l'information.

À cet effet, le MDCG 2025-4 impose aux plateformes, même lorsqu'elles n'agissent qu'en tant que services d'intermédiation, de concevoir leurs interfaces de manière à ce que les fabricants puissent se conformer à leurs obligations d'information.

Conformément aux articles 30 et 31 du DSA, qui consacrent le principe du « *Know Your Business Customer* » (« KYBC »), les plateformes doivent recueillir et afficher des informations précises avant d'autoriser un professionnel à proposer ses produits. L'interface de la plateforme doit impérativement permettre aux fabricants de fournir leurs coordonnées complètes (nom, adresse, numéro de téléphone et adresse électronique), les éléments permettant une identification sans ambiguïté des produits proposés, tout signe distinctif identifiant le professionnel (marque déposée, logo), ainsi que les informations relatives à l'étiquetage et au marquage conformes à la législation de l'Union (Chapitre III de l'Annexe I du MDR/IVDR).

L'obligation d'inclure le Single Registration Number (« SRN ») et l'Identifiant Unique des Dispositifs (« UDI-DI ») revêt une importance stratégique. Le SRN relie directement l'acteur économique à la base de données européenne EUDAMED, tandis que l'UDI-DI constitue la clé de voûte de la traçabilité des dispositifs, essentielle en cas de rappel de produit ou de signalement d'incidents graves. Par ailleurs, l'exigence d'un lien vers l'eIFU (*electronic Instructions for Use*) souligne la transition vers une dématérialisation complète de la documentation médicale, garantissant un accès permanent aux instructions cliniques.

Une des recommandations les plus pragmatiques du guide concerne l'architecture de l'information au sein des plateformes elles-mêmes. Pour pallier le risque de confusion chez le consommateur entre une application de bien-être et un véritable dispositif médical, le MDCG recommande fortement de créer une délimitation claire dans les bibliothèques d'applications.

Cette catégorie distincte « Dispositif Médical » ne devrait être proposée comme option aux développeurs qu'une fois qu'ils ont fourni l'ensemble des informations de conformité obligatoires énumérées précédemment. Cette mesure opère comme un mécanisme de filtrage ex-ante, empêchant un développeur de revendiquer de manière fallacieuse une finalité médicale

[165] Les articles 13 et 14 de ces deux règlements sont respectivement consacrés aux obligations générales des importateurs et à celles des distributeurs.

sans avoir préalablement satisfait aux rigueurs réglementaires.

III. LES MÉCANISMES DE VÉRIFICATION ET DE SURVEILLANCE : DE L'ÉVALUATION PRÉALABLE A L'INJONCTION DE RETRAIT

La protection des patients requiert une dynamique de vérification continue. Le guide MDCG 2025-4 détaille les devoirs de vérification des plateformes à travers deux phases temporelles distinctes, assorties de mécanismes d'action corrective.

Avant même de permettre à un professionnel de proposer son application MDSW, la plateforme doit procéder à une évaluation préalable. Le niveau d'exigence juridique requis ici est celui des « meilleurs efforts ». La plateforme doit s'efforcer d'évaluer si les informations requises (coordonnées, SRN, UDI-DI, etc.) sont fiables, complètes et rendues disponibles pour les utilisateurs. Bien que le DSA n'impose pas à la plateforme de se substituer aux autorités compétentes, l'incapacité d'une plateforme à démontrer qu'elle a déployé ses meilleurs efforts pourrait compromettre son exemption de responsabilité en tant qu'hébergeur.

L'obligation de surveillance se poursuit au stade post-publication. Une fois que le professionnel est autorisé à proposer ses produits, le fournisseur de la plateforme est tenu d'effectuer des contrôles aléatoires. Pour cette surveillance, la norme juridique glisse vers l'exigence d'« efforts raisonnables ». La plateforme doit vérifier si les produits proposés ont été identifiés comme illégaux en croisant les données avec des bases de données officielles en ligne, librement accessibles et lisibles par machine. Cette disposition implique opérationnellement que les plateformes d'applications intègrent des requêtes automatisées vers les bases de données institutionnelles, telles qu'EUDAMED ou les registres des autorités nationales compétentes, afin d'identifier les certificats suspendus ou les produits rappelés.

Le cœur de la régulation des contenus illicites repose sur le mécanisme d'alerte et d'action. Les plateformes d'applications doivent mettre en œuvre des mécanismes permettant à toute entité de signaler la présence d'un contenu illégal. La réception d'un tel signalement est réputée conférer au fournisseur une « connaissance ou conscience effective » de l'illicéité du contenu. Dès l'acquisition de cette connaissance, la plateforme doit prendre des « décisions rapides et diligentes » concernant le retrait du contenu pour conserver son immunité d'intermédiaire. De surcroît, le guide rappelle que les autorités nationales compétentes ont le pouvoir d'émettre des injonctions spécifiques directement à l'encontre des fournisseurs de plateformes pour contraindre la suppression d'un contenu illégal.

Enfin, le guide réserve un traitement particulier aux « Très Grandes Plateformes en Ligne » (Very Large Online Platforms – « VLOPs »), désignées par la Commission européenne.

Conformément aux articles 34 et 35 du DSA, ces acteurs doivent procéder, au moins une fois par an, à des évaluations des risques systémiques découlant de la conception ou du fonctionnement de leur service, y compris la diffusion de contenus illicites tels que des dispositifs médicaux non conformes. Ils sont par la suite tenus de mettre en œuvre des mesures d'atténuation proportionnées, transférant ainsi une part de la politique de prévention des risques aux départements de conformité de ces entreprises.

IV. INTERDEPENDANCES NORMATIVES : L'ARTICULATION AVEC L'IA ACT ET L'ESPACE EUROPÉEN DES DONNÉES DE SANTÉ

L'analyse de l'opérationnalisation du guide MDCG 2025-4 ne saurait être

complète sans la replacer dans le macro-écosystème du droit européen du numérique en santé. Le guide s'inscrit dans une architecture réglementaire complexe où interagissent de multiples textes fondateurs.

La publication du guide MDCG 2025-4 intervient de manière quasi concomitante avec celle du guide MDCG 2025-6[166], publié le 19 juin 2025, qui aborde spécifiquement l'interaction entre le MDR/IVDR et le nouveau règlement sur l'Intelligence Artificielle (IA Act)[167]. De nombreuses applications MDSW intègrent aujourd'hui des modèles d'apprentissage automatique. Sous l'IA Act, ces logiciels médicaux, dès lors qu'ils nécessitent l'intervention d'un organisme notifié au titre du MDR, sont classés comme des systèmes d'IA à haut risque. Pour les plateformes d'applications, cette superposition réglementaire signifie que la vérification de conformité s'alourdit. Le marquage CE de l'application ne devra plus seulement attester de la performance clinique, mais également de la robustesse algorithmique, de l'absence de biais discriminatoires et de la transparence de l'IA. L'information transparente exigée à l'égard du patient devra ainsi s'étendre aux paramètres de l'IA, afin d'assurer que l'utilisateur final comprenne les limites du diagnostic généré par l'application.

Par ailleurs, la question du traitement des données de santé par ces applications renvoie inévitablement aux exigences de l'Espace Européen des Données de Santé (EEDS)[168]. L'adoption du règlement sur l'EEDS instaure de nouvelles normes d'interopérabilité pour les dossiers médicaux électroniques et les applications de bien-être revendiquant une telle interopérabilité. Une application MDSW téléchargée depuis un magasin d'applications européen devra, à terme, s'insérer de manière sécurisée dans l'infrastructure de santé du patient.

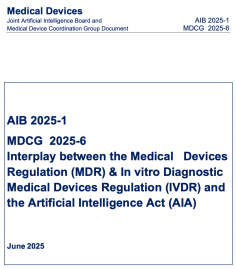
En conclusion, le guide MDCG 2025-4 marque une étape décisive dans la maturation du droit européen de la santé numérique. En clarifiant le statut des plateformes de téléchargement en ligne, il comble un vide juridique qui permettait jusqu'alors à certaines applications logicielles de se soustraire à la rigueur de la matériovigilance. En liant les obligations sectorielles du MDR et de l'IVDR aux obligations horizontales de régulation de l'internet portées par le DSA, les instances européennes créent un filet de sécurité où la responsabilité est partagée entre le concepteur médical et l'hébergeur technologique. Les plateformes en ligne ne peuvent plus prétendre à une neutralité aveugle ; elles sont désormais contraintes d'exercer un rôle de vigie sanitaire, assumant des devoirs de vérification préalable, de surveillance continue et de réaction immédiate face aux contenus illicites. Cette structuration est la condition essentielle pour préserver la confiance des citoyens et garantir que l'innovation numérique ne sacrifie jamais l'exigence clinique.

MDCG 2025-4 - *Guidance on the safe making available of medical device software (MDSW) apps on online platforms*, June 2025

[166] AIB 2025-1 / MDCG 2025-6, *Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AI ACT)*, June 2025.

[167] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JOUE* du 12 juillet 2024.

[168] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* du 5 mars 2025.


Medical Devices
Joint Artificial Intelligence Board and Medical Device Coordination Group Document
AIB 2025-1
MDCG 2025-6

AIB 2025-1
MDCG 2025-6
Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA)
June 2025

L'articulation opérationnelle entre le règlement sur les dispositifs médicaux et la législation sur l'intelligence artificielle. Commentaire du Guide MDCG 2025-6

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

L'intégration croissante et inéluctable des technologies d'intelligence artificielle (« IA ») au sein des dispositifs médicaux bouleverse en profondeur le paysage technologique et réglementaire européen de la santé. Jusqu'à récemment, l'encadrement de ces innovations numériques reposait exclusivement sur le règlement (UE) 2017/745 relatif aux dispositifs médicaux (« MDR » acronyme anglais pour *medical device regulation*)[169] et le règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[170]. Bien que ces deux textes fondateurs imposent des exigences particulièrement strictes en matière de sécurité, de performance clinique et de gestion des risques liés aux logiciels dispositifs médicaux, ils n'ont pas été originellement conçus pour appréhender les vulnérabilités spécifiques, évolutives et inédites inhérentes aux systèmes algorithmiques complexes. L'opacité des réseaux de neurones profonds, la dérive des données d'apprentissage, les biais cognitifs encodés ou encore les menaces avancées en matière de cybersécurité constituent autant de défis que l'approche traditionnelle de la conformité médicale peinait à endiguer de manière exhaustive.

Afin de combler ces lacunes normatives tout en garantissant un niveau particulièrement élevé de protection des droits fondamentaux, de la santé et de la sécurité des citoyens de l'Union européenne, le législateur a adopté le règlement (UE) 2024/1689 fixant des règles harmonisées concernant l'intelligence artificielle, communément désigné sous l'acronyme « *AI Act* »[171]. L'entrée en vigueur de ce texte à vocation transversale instaure de fait un modèle de double conformité pour les fabricants de dispositifs médicaux intégrant de l'IA, dispositifs désormais catégorisés sous l'appellation de « *Medical Device Artificial Intelligence* » (« MDAI »). Cette dualité réglementaire, bien qu'absolument justifiée sur le plan de la politique de sécurité publique européenne, engendre une complexité opérationnelle majeure pour les opérateurs économiques. Ces derniers doivent désormais naviguer entre des corpus juridiques aux philosophies distinctes, dont les terminologies, les exigences

[169] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, *JOUE* L. 117 du 5 mai 2017.

[170] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, *JOUE* L. 117 du 5 mai 2017.

[171] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JOUE* du 12 juillet 2024.

documentaires et les cycles d'évaluation se superposent, créant un risque tangible de paralysie administrative et d'engorgement des organismes notifiés.

C'est précisément dans ce contexte d'incertitude juridique, et en réponse à une attente pressante de la part de l'industrie des technologies médicales, que le Bureau de l'intelligence artificielle (« AIB ») et le Groupe de coordination des dispositifs médicaux (« MDCG ») ont publié, en juin 2025, le document d'orientation conjoint AIB 2025-1 / MDCG 2025-6, intitulé « *Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AI ACT)* ». Ce guide stratégique, structuré sous la forme d'une foire aux questions, constitue la pierre angulaire de la nouvelle architecture de mise en conformité. Il a pour vocation première d'expliciter l'application simultanée et complémentaire de ces textes, en parfaite adéquation avec l'approche du nouveau cadre législatif européen, afin d'assurer que l'innovation médicale ne soit pas entravée par des redondances procédurales injustifiées.

L'analyse exégétique de ce guide révèle une volonté manifeste des autorités européennes de rationaliser les efforts de mise en conformité. Le législateur encourage activement l'intégration des nouvelles exigences de l'AI Act au sein des processus de gestion de la qualité et des architectures documentaires déjà exigés par le MDR et l'IVDR. Toutefois, cette synergie, évidente sur le plan théorique, se heurte à des défis pratiques considérables lorsqu'il s'agit de décliner de manière purement opérationnelle des concepts novateurs tels que la gouvernance algorithmique des données, l'explicabilité des modèles, la surveillance humaine par conception, ou encore la qualification juridique des modifications substantielles apportées aux systèmes d'apprentissage continu.

La présente analyse s'attache à décrypter les mécanismes de qualification et de classification des MDAI, les stratégies d'optimisation de la fusion des systèmes de gestion de la qualité (« SMQ » pour système de management de la qualité) et de la documentation technique, ainsi que les nouvelles obligations pesant sur le cycle de vie complet de ces dispositifs médicaux de nouvelle génération. De la conception rigoureuse des jeux de données d'entraînement jusqu'à la surveillance post-commercialisation proactive, cette étude intègre également les dynamiques réglementaires adjacentes. Seront également abordés les liens avec l'Espace européen des données de santé (EEDS)[172] et les conséquences de la nouvelle directive sur la responsabilité du fait des produits défectueux[173] afin d'en définir des repères clairs et utiles sur le terrain.

I. PERIMETRE D'APPLICATION ET HEURISTIQUE DE CLASSIFICATION DES DISPOSITIFS MDAI

A. Précisions terminologiques : une indispensable traduction des rôles opérationnels

La toute première étape de la mise en conformité conjointe exige une maîtrise absolue des chevauchements lexicaux et des divergences terminologiques entre la législation sur l'IA et la législation sectorielle médicale. Le guide MDCG 2025-6 prend le soin de lever d'emblée toute ambiguïté concernant l'identification des opérateurs économiques et des différents acteurs de la chaîne de soins. Sur

[172] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* du 5 mars 2025.

[173] Directive (UE) 2024/2853 du Parlement européen et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, JOUE du 18 novembre 2024.

le plan strictement juridique, l'entité qualifiée de « fabricant » au sens de l'article 2 du MDR et de l'IVDR correspond très exactement à l'entité qualifiée de « fournisseur » (*provider*) selon les dispositions de l'AI Act. Il incombe par conséquent au fabricant du dispositif médical d'assumer l'intégralité des obligations incombant au fournisseur du système d'IA, regroupant ainsi les responsabilités de conception, de validation et de mise sur le marché sous une seule et même entité juridique.

Une distinction encore plus critique sur le plan de la responsabilité est opérée concernant les entités situées en bout de chaîne de déploiement. L'AI Act introduit le concept novateur de « déployeur », défini de manière extensive à l'article 3, paragraphe 4 comme toute personne physique ou morale, autorité publique, agence ou tout autre organisme qui utilise un système d'IA sous son autorité, à l'exception d'une utilisation dans le cadre d'une activité personnelle non professionnelle. Le guide MDCG 2025-6 précise expressément que ce concept spécifique à l'AI Act ne saurait en aucun cas être confondu avec la notion d'« utilisateur » telle qu'elle est définie et appréhendée sous le MDR et l'IVDR.

Afin de clarifier cette dichotomie essentielle pour la mise en œuvre des obligations réglementaires, il convient de se référer à la typologie de ces acteurs de santé :

Terme selon le MDR / IVD	**Terme équivalent ou distinct selon l'AI Act**	**Définition opérationnelle dans le secteur médical**
Fabricant (*Manufacturer*)	Fournisseur (*Provider*)	L'entité juridique qui conçoit, développe et met sur le marché le logiciel médical intégrant l'IA, assumant l'entière responsabilité de la double conformité.
Aucun équivalent direct	Déployeur (*Deployer*)	L'établissement de santé, l'hôpital, la clinique ou l'autorité de santé publique qui acquiert le MDAI, l'intègre dans son infrastructure informatique clinique et en gère l'exploitation sous sa propre autorité.
Utilisateur (*User*)	Non applicable directement au sens du déployeur	Le professionnel de santé (médecin, radiologue, infirmier) qui manipule directement l'interface du dispositif pour établir un diagnostic, ou le patient lui-même dans le cas de thérapies numériques (DTx).

Cette distinction s'avère fondamentale en pratique, car elle détermine de manière univoque la répartition des responsabilités en matière de transparence algorithmique, de fourniture des notices d'utilisation spécifiques et d'obligations de surveillance humaine. Le fabricant doit concevoir son système non seulement pour qu'il soit cliniquement efficace entre les mains de l'utilisateur final, mais également pour qu'il fournisse au déployeur les métriques de fonctionnement (logs) et la transparence nécessaires à la gestion des risques institutionnels et éthiques.

B. Le mécanisme de déclenchement : quand un MDAI devient-il une IA à haut risque ?

Le cœur névralgique de l'articulation entre les deux cadres législatifs réside dans la détermination du niveau de risque du système d'IA. L'AI Act a été structuré selon une approche proportionnée, n'imposant ses obligations les plus contraignantes qu'aux seuls systèmes d'IA qualifiés de « haut risque ». Selon l'article 6, paragraphe 1 de l'AI Act, et tel qu'explicité en détail par le guide MDCG 2025-6, un dispositif MDAI revêt la qualification de système d'IA à haut risque si, et seulement si, deux conditions juridiques cumulatives sont strictement remplies.

Premièrement, le MDAI doit constituer un composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union énumérée à l'annexe II de l'AI Act (laquelle inclut le MDR et l'IVDR), ou le système d'IA doit être lui-même un dispositif médical au sens de ces mêmes règlements. Le guide précise par ailleurs que la Commission européenne élabore des lignes directrices horizontales pour affiner ce concept de « composant de sécurité », mais son application dans le domaine médical est généralement évidente dès lors que le logiciel a une finalité diagnostique ou thérapeutique.

Deuxièmement, condition déterminante, le dispositif médical concerné doit être soumis à une procédure d'évaluation de la conformité réalisée par une tierce partie, à savoir un organisme notifié, conformément aux dispositions de classification du MDR ou de l'IVDR. Cette règle d'assujettissement conditionnel crée une architecture réglementaire où l'intervention d'un organisme notifié agit comme l'interrupteur exclusif déclenchant les obligations de l'AI Act relatives au haut risque.

Le tableau de classification fourni par le MDCG permet de cartographier cette dynamique d'application avec précision.

Classification	Notified Body Involved?	AIA High-Risk (Art. 6(1)) conditions fulfilled?
MDR Class I (non-sterile, non-measuring, non-reusable surgical)	❌ No	❌ No
MDR Class I (sterile, measuring, reusable surgical)	✅ Yes	✅ Yes
MDR Class IIa, IIb, III	✅ Yes	✅ Yes
MDR Annex XVI[10]	✅ Yes	✅ Yes
IVDR Class A (non-sterile)	❌ No	❌ No
IVDR Class A)	✅ Yes	✅ Yes
IVDR Class B, C, D	✅ Yes	✅ Yes
In-house device according to Art. 5(5) MDR/IVDR	❌ No	❌ No

10 Note: Except for non-invasive devices which are classified as Class I in accordance with 'Guidance on qualification and classification of Annex XVI products - A guide for manufacturers and notified bodies'.

L'analyse scrupuleuse de cette matrice de classification met en exergue des points d'attention stratégiques majeurs pour les fabricants. Un logiciel médical intégrant de l'IA et classé en classe I sous le MDR échapperait techniquement à la qualification de haut risque de l'AI Act. Toutefois, il convient de rappeler que la règle 11 de l'annexe VIII du MDR tend aujourd'hui à classifier la quasi-totalité des logiciels d'aide à la décision clinique en classe IIa ou supérieure, rendant l'échappatoire de la classe I purement marginale en pratique, sauf exceptions très spécifiques ou logiciels intégrés à des dispositifs de classe I mesurants.

Il est également indispensable de souligner que l'AI Act s'applique de plein droit aux produits ne revendiquant aucune destination médicale, mais qui relèvent du champ d'application du MDR par l'intermédiaire de son Annexe XVI, tels que les équipements de stimulation cérébrale à visée non médicale ou certains logiciels esthétiques. Dès lors que ces produits d'imitation médicale intègrent une IA et requièrent l'intervention d'un organisme notifié en raison de leur profil de risque inhérent, ils basculent inévitablement dans la catégorie des systèmes d'IA à haut risque de l'AI Act. À l'inverse, les algorithmes diagnostiques développés, fabriqués et utilisés exclusivement au sein d'un même établissement de santé (bénéficiant de la clause d'exemption « *in-house* » de l'article 5 paragraphe 5 du MDR ou de l'IVDR) échappent à l'obligation de certification par un organisme notifié. Par effet domino, ils échappent logiquement à la qualification de système d'IA à haut risque de l'article 6 paragraphe 1 de l'AI Act, créant ainsi un environnement réglementaire allégé pour la recherche et l'innovation intra-hospitalière, bien que la conformité aux exigences générales de sécurité et de performance demeure impérative.

C. L'indépendance stricte de la classification des risques : une dichotomie maintenue

Une confusion persistante parmi les opérateurs économiques, et parfois même au sein des directions des affaires réglementaires, consiste à présumer qu'une qualification d'« IA à haut risque » au titre de l'AI Act entraîne mécaniquement une surclassification du dispositif médical sous le MDR ou l'IVDR. Le guide MDCG 2025-6 réfute formellement et définitivement cette hypothèse. La classification d'un système d'IA comme étant à haut risque en vertu de l'article 6 paragraphe 1 de l'AI Act n'implique en aucun cas que le dispositif médical ou le dispositif médical de diagnostic in vitro doive basculer dans une classe de risque supérieure selon les règles de classification de l'annexe VIII du MDR ou de l'annexe VIII de l'IVDR.

La relation de causalité est strictement unilatérale : c'est exclusivement la classification MDR/IVDR qui, en déterminant la nécessité de recourir à un organisme notifié, engendre la qualification AI Act de haut risque. L'AI Act n'a donc aucune incidence sur la détermination de la classe de risque médicale. Néanmoins, la qualification AI Act impose un niveau de contrôle réglementaire, de transparence algorithmique et de surveillance humaine considérablement accru, augmentant la complexité de l'évaluation de la conformité sans pour autant modifier l'étiquette de classe (qu'il s'agisse d'un dispositif IIa, IIb ou III) du dispositif médical.

De surcroît, le guide rappelle avec force que même si un dispositif MDAI n'est pas qualifié de haut risque sous l'AI Act (par exemple un dispositif *in-house*), le fabricant ou le fournisseur reste impérativement tenu de respecter certaines obligations fondamentales de ce texte transversal. Sont notamment visées les dispositions de l'article 5, qui énumèrent les pratiques d'IA strictement interdites au sein de l'Union européenne, ainsi que les obligations de l'article 50 relatives à la transparence, qui imposent par exemple d'informer les utilisateurs lorsqu'ils interagissent avec certains systèmes d'IA de type agent

conversationnel (chatbot) ou système de reconnaissance des émotions, obligations dont l'application est totalement indépendante de la classification MDR/IVDR.

D. Dispositions transitoires : la gestion du calendrier d'application et des dispositifs hérités

L'approche opérationnelle nécessite de prendre en compte avec la plus grande rigueur le calendrier d'application du nouveau cadre. Si l'AI Act est officiellement entré en vigueur de manière globale en 2024, les dispositions spécifiques relatives aux systèmes d'IA à haut risque relevant de l'Annexe II (qui inclut explicitement le MDR et l'IVDR) ne s'appliqueront pleinement et de manière opposable qu'à partir du 2 août 2027. Le guide MDCG 2025-6 apporte à ce titre des clarifications indispensables sur la gestion épineuse des dispositifs dits « hérités » (*legacy devices*).

Si un dispositif médical intégrant une IA a été mis sur le marché de l'Union ou mis en service avant cette date fatidique du 2 août 2027, les exigences contraignantes de l'AI Act pour les systèmes à haut risque ne s'appliquent pas de manière rétroactive. Cependant, cette protection transitoire est assortie d'une condition résolutoire majeure : si ce système d'IA hérité fait l'objet d'une modification significative de sa conception ou de sa finalité à compter du 2 août 2027, il perd instantanément le bénéfice de cette exemption et bascule sous l'empire complet et immédiat de l'AI Act, incluant toutes les obligations afférentes aux systèmes d'IA à haut risque de l'Annexe I. En revanche, tout dispositif médical intégrant une IA mise sur le marché ou mis en service pour la toute première fois à partir de cette date pivot du 2 août 2027 devra naître en pleine conformité avec les deux cadres législatifs, imposant aux équipes de développement d'intégrer ces doubles contraintes dès les premières phases de conception.

II. FUSION STRATÉGIQUE ET DOCUMENTAIRE : L'INTÉGRATION DES SYSTÈMES DE GESTION DE LA QUALITE (SMQ)

A. Le principe de flexibilité : l'article 8 paragraphe 2 de l'AI Act comme levier d'efficience réglementaire

La mise en œuvre d'une double conformité stricte, si elle devait être gérée en silos étanches, conduirait inévitablement à une paralysie administrative des fabricants de technologies médicales et à l'engorgement définitif des organismes notifiés, lesquels opèrent déjà sous une tension systémique depuis l'entrée en application du MDR et de l'IVDR. Pleinement conscient de ce risque majeur pour la compétitivité et la capacité d'innovation de l'industrie européenne, le législateur a introduit un mécanisme d'efficience déterminant à l'article 8 paragraphe 2 de l'AI Act. Ce paragraphe fondamental permet aux fabricants de dispositifs médicaux de choisir d'intégrer les processus de test, les mécanismes de *reporting*, les informations spécifiques et la documentation exigés par la législation sur l'IA directement et organiquement dans les procédures documentaires déjà établies en vertu du MDR ou de l'IVDR.

Le guide MDCG 2025-6 insiste de manière particulièrement appuyée sur cette disposition libératoire. Il encourage très vivement les fabricants de MDAI à exploiter cette flexibilité procédurale afin d'éviter les redondances de tests, de réduire les charges administratives supplémentaires et de garantir la cohérence structurelle de leurs processus internes. Sur le plan purement opérationnel, cela signifie qu'un fabricant n'est en aucun cas tenu d'élaborer un dossier technique isolé et spécifique à l'AI Act, ni de maintenir un système de gestion de la qualité (SMQ) parallèle et déconnecté de la norme ISO 13485. Une documentation technique unique et un SMQ intégré, astucieusement conçus pour démontrer la conformité aux exigences

générales de sécurité et de performance du MDR/IVDR tout en absorbant de manière granulaire les exigences spécifiques liées à l'IA, constituent la voie royale, pragmatique et recommandée vers la conformité. Toutefois, le guide formule une mise en garde explicite : cette fusion documentaire et cette rationalisation des procédures ne dispensent en rien le fabricant d'une démonstration de conformité exhaustive. Le système MDAI doit répondre de manière démontrable, auditable et sans équivoque à toutes les exigences matérielles applicables des deux règlements européens simultanément.

B. L'extension conceptuelle du système de gestion de la qualité : au-delà du risque médical classique

Les articles 10 du MDR et de l'IVDR imposent d'ores et déjà la mise en œuvre, le maintien et l'amélioration continue d'un SGQ strictement proportionné à la classe de risque et au type spécifique du dispositif médical Dans une approche en miroir, l'article 17 de l'AI Act introduit une obligation symétrique pour les systèmes d'IA à haut risque, exigeant la mise en place d'un SMQ couvrant au moins treize aspects procéduraux obligatoires, lesquels doivent également être mis en œuvre de manière proportionnée à la taille de l'organisation du fournisseur. Le guide MDCG 2025-6 explicite de manière très claire que les obligations du SMQ prévues par l'AI Act sont ciblées très spécifiquement sur la nature algorithmique du système et sont donc intrinsèquement complémentaires au SMQ global du dispositif médical exigé par les textes sectoriels.

Afin que le SMQ existant d'un fabricant de dispositifs médicaux (généralement adossé à la norme ISO 13485) devienne pleinement conforme à l'AI Act, il convient de procéder à une refonte de la politique qualité pour y incorporer de nouveaux macro-processus. Les ajouts opérationnels indispensables, qui nécessitent souvent l'implication d'ingénieurs en science des données et d'experts en éthique algorithmique, incluent notamment :

1. La gouvernance et la gestion fine des données : l'établissement de protocoles de niveau ingénierie stricts régissant la provenance, la collecte, le nettoyage, la représentativité statistique et l'évaluation continue des biais au sein des jeux de données d'entraînement, de validation et de test.
2. La conservation des enregistrements : la mise en place de capacités techniques avancées de journalisation automatique (logs) inaltérables, permettant la traçabilité complète des événements et du comportement de l'algorithme tout au long du cycle de vie opérationnel du système.
3. La transparence et la surveillance humaine : l'intégration de processus ergonomiques garantissant que la conception de l'interface utilisateur permet aux professionnels de santé d'exercer un contrôle critique effectif, de comprendre le cheminement de la décision algorithmique et, de manière cruciale, de pouvoir contourner ou annuler les décisions de l'IA si le contexte clinique l'exige.
4. La stratégie de conformité réglementaire intégrée : l'adaptation du plan de développement logiciel pour que chaque jalon de conception et de vérification intègre conjointement et harmonieusement les impératifs de conformité du MDR et de l'AI Act.

Il convient de noter que l'élaboration de normes harmonisées européennes et internationales pertinentes (notamment par le Comité technique mixte 21 du CEN/CENELEC[174]) est actuellement en

[174] Le comité technique mixte 21 (souvent abrégé JTC21 pour Joint Technical Committee 21) est un groupe de travail créé conjointement par les deux principaux organismes européens de normalisation :

cours à la date de rédaction de ce commentaire. Ces futurs standards viendront cristalliser ces nouvelles exigences sous forme de spécifications auditables. Dans l'intervalle, la réingénierie des processus qualité doit impérativement s'inspirer des lignes directrices horizontales publiées par la Commission européenne afin de garantir un alignement précoce avec les attentes des évaluateurs.

C. Gestion des risques et du cycle de vie : l'intégration des risques liés aux droits fondamentaux

Tant le cadre du MDR/IVDR (notamment via l'application de la norme harmonisée ISO 14971 relative à l'application de la gestion des risques aux dispositifs médicaux) que l'AI Act (au travers de son article 9) imposent un système de gestion des risques structuré comme un processus itératif, systématique et continu, s'étendant sur l'intégralité du cycle de vie du dispositif, des premières phases de conception pré-clinique jusqu'au démantèlement post-commercialisation. Néanmoins, l'intégration de l'AI Act contraint les fabricants à élargir considérablement le périmètre classique de l'analyse des risques médicaux, créant un véritable défi conceptuel pour les ingénieurs qualité.

En effet, l'évaluation ne doit plus se limiter exclusivement aux risques cliniques directs pesant sur le patient ou l'utilisateur (tels que la mauvaise attribution d'un traitement due à un faux positif). L'AI Act impose d'identifier, d'analyser et d'atténuer les « risques connus et raisonnablement prévisibles que le MDAI à haut risque peut poser pour les droits fondamentaux » (considérant n°65). Le guide MDCG 2025-6 précise ainsi que les fabricants doivent intégrer dans leurs matrices de risques, l'évaluation des biais dans les données d'apprentissage pouvant mener à une discrimination interdite (risque éthique et légal), la robustesse du système d'apprentissage automatique face aux cyberattaques sophistiquées (risque sécuritaire), et la fiabilité de l'interface homme-machine au regard de la surveillance humaine.

De plus, ce processus enrichi de gestion des risques doit intégrer des mesures organisationnelles garantissant un usage fiable en milieu clinique réel. Cela implique la documentation des mesures d'atténuation qui dépassent la simple modification du code source, pouvant inclure la mise en place de programmes de formation spécifiques et obligatoires destinés aux déployeurs et aux utilisateurs. Il s'agit d'une évolution paradigmatique : le fabricant est désormais tenu de s'assurer que l'environnement de déploiement dispose de la maturité et des compétences nécessaires pour interagir avec l'IA sans engendrer de nouveaux risques systémiques liés à la dépendance technologique ou à l'automatisation excessive.

III. EXIGENCES DOCUMENTAIRES ET REGLES D'ECHANTILLONNAGE DES ORGANISMES NOTIFIES

La constitution de la documentation technique, qui sert de fondement probatoire à toute évaluation de la conformité, obéit également au principe primordial de l'intégration et de la rationalisation. Les annexes II et III du MDR et de l'IVDR imposent déjà la fourniture de descriptions extrêmement détaillées de l'architecture logicielle, de la destination médicale, des méthodes de traitement des données cliniques, ainsi que des stratégies complètes

---

le CEN (comité européen de normalisation) le CENELEC (comité européen de normalisation électrotechnique). Sa mission principale est d'élaborer des normes européennes harmonisées spécifiquement dédiées à l'intelligence artificielle. La Commission européenne a formellement mandaté ce comité pour traduire les obligations juridiques de l'AI Act en spécifications techniques et opérationnelles claires.

de gestion des risques et des résultats de l'évaluation clinique. De son côté, l'article 11 et l'annexe IV de l'AI Act exigent des éléments complémentaires fortement axés sur la redevabilité algorithmique, l'explicabilité du modèle et la traçabilité de sa construction. Ces éléments incluent une documentation approfondie des choix de conception de l'architecture du réseau de neurones, la description des ressources informatiques déployées pour les phases d'entraînement et de test, les métriques précises de performance algorithmique, ainsi que les pratiques détaillées de gouvernance des données employées.

Le guide MDCG 2025-6 confirme et sécurise la position selon laquelle les fabricants doivent établir un ensemble unique et cohérent de documentation technique démontrant la satisfaction croisée de toutes ces exigences. Une interrogation opérationnelle majeure pour l'industrie concernait la méthodologie d'évaluation de cette volumineuse documentation par les organismes notifiés, telle que définie par l'annexe VII de l'AI Act, et particulièrement son articulation avec les règles d'échantillonnage strictes prévues par le MDR/IVDR.

Le guide apporte une réponse univoque et particulièrement rassurante : les règles d'échantillonnage de la procédure d'évaluation de la conformité qui régissent le dispositif médical restent pleinement applicables à la partie IA du système. Par conséquent, pour les dispositifs relevant de la classe IIa ou IIb (sous le MDR) ou des classes B ou C (sous l'IVDR), l'organisme notifié évaluera la documentation technique spécifique à l'AI Act en suivant les mêmes règles d'échantillonnage représentatif par catégorie ou par groupe générique de dispositifs, telles que minutieusement définies dans le document d'orientation MDCG 2019-13[175]. Cette précision réglementaire constitue une avancée décisive pour l'industrie des technologies médicales. Elle permet d'éviter une évaluation systématique, individuelle et chronophage de chaque variante logicielle mineure d'un algorithme d'IA au sein d'une même gamme de produits, limitant ainsi de manière significative l'explosion des coûts d'audit et la congestion des délais d'accès au marché européen.

IV. GOUVERNANCE DES DONNÉES : LA FONDATION JURIDIQUE ET TECHNIQUE DE LA FIABILITÉ ALGORITHMIQUE

A. L'article 10 de l'AI Act et la taxonomie réglementaire des données

Si le MDR exige déjà que les données cliniques utilisées pour l'évaluation des performances soient robustes, fiables et représentatives de la population visée afin de démontrer la sécurité du dispositif (conformément à l'Annexe XIV du MDR et détaillé dans le document MDCG 2020-1[176]), l'AI Act, par le biais de son article 10, s'aventure beaucoup plus loin dans la granularité et la rigueur de l'ingénierie des données. La gouvernance des données n'est plus considérée uniquement comme un moyen de valider une allégation médicale en fin de processus ; elle devient une exigence essentielle, autonome et préalable, conditionnant la légalité même du développement du système d'IA (**Page suivante**).

[175] MDCG 2019-13 Rev.1, *Guidance on sampling of MDR Class IIa / Class IIb and IVDR Class B / Class C devices for the assessment of the technical documentation*, December 2024.

[176] MDCG 2020-1, *Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software*, March 2020.

L'AI ACT impose une taxonomie juridique stricte des données utilisées au cours du cycle de vie du modèle d'apprentissage. Afin d'harmoniser les pratiques, l'article 3 de l'AI ACT définit réglementairement les concepts fondamentaux de la science des données, que le guide MDCG rappelle :

Type de données (Art. 3 AI Act)	Définition et utilité dans le développement du MDAI
Données d'entraînement (*Training data*)	Données utilisées pour entraîner le système d'IA par l'ajustement (*fitting*) de ses paramètres apprenants (ex: les poids d'un réseau de neurones).
Données de validation (*Validation data*)	Données utilisées pour fournir une évaluation du système d'IA entraîné et pour ajuster ses hyperparamètres non apprenants, afin de prévenir les phénomènes de surapprentissage (*overfitting*) ou de sous-apprentissage (*underfitting*).
Ensemble de données de validation	Un ensemble de données distinct ou une partie de l'ensemble de données d'entraînement, utilisé par le biais d'une séparation fixe ou variable (*split*).
Données de test (*Testing data*)	Données utilisées pour fournir une évaluation totalement indépendante du système d'IA afin de confirmer les performances attendues avant sa mise sur le marché ou sa mise en service.

Le guide MDCG 2025-6 souligne avec insistance que ces différents ensembles de données de formation, de validation et de test doivent, en vertu de l'AI Act, être « *d'une grande qualité, pertinents, suffisamment représentatifs et, dans la mesure du possible, exempts d'erreurs et complets au vu de la destination prévue* » (considérant n°67). L'obligation d'avoir des jeux de données dotés de propriétés statistiques appropriées impose aux fabricants de documenter minutieusement et scientifiquement les protocoles de collecte de ces données.

Les données d'entraînement et de test doivent refléter de manière exhaustive et proportionnée les caractéristiques de la population cible. Cela inclut des variables telles que l'âge, le sexe, le genre, la race, l'origine ethnique, la localisation géographique, ainsi que les comorbidités spécifiques au contexte clinique visé. Cette exigence drastique est d'une importance vitale pour maîtriser le risque de dérive des données, s'assurer de la généralisation des performances du modèle au-delà de l'échantillon d'apprentissage, et éviter des défaillances dramatiques de précision lors d'un déploiement dans des contextes cliniques non anticipés par les développeurs.

B. Atténuation des biais algorithmiques et respect inconditionnel des droits fondamentaux

La nouveauté radicale et philosophiquement marquante de l'AI Act réside dans l'obligation positive d'examiner en profondeur les ensembles de données et de mitiger les biais algorithmiques susceptibles d'affecter la santé, d'avoir une incidence négative sur les droits fondamentaux ou de conduire à une

discrimination prohibée par le droit de l'Union européenne. Dans le domaine de la santé numérique, un algorithme d'analyse dermatologique entraîné de manière disproportionnée sur des phototypes clairs et affichant des performances significativement dégradées sur des peaux foncées constitue l'archétype du biais discriminatoire et d'un risque inacceptable pour l'équité des soins et la sécurité des patients.

Les fabricants de dispositifs MDAI doivent concevoir des processus statistiques et d'assurance qualité permettant la détection et la correction précoce de ces biais dès la phase de constitution des bases de données. De surcroît, le guide MDCG 2025-6 met en avant l'importance cruciale des exigences de journalisation (logging) automatique imposées par l'AI Act. Ces capacités techniques intégrées visent à faciliter la traçabilité des décisions de l'IA et l'identification rétrospective de situations où des biais latents se manifesteraient uniquement lors de l'exploitation post-commercialisation par le déployeur, ou à la suite d'une modification logicielle en conditions réelles.

C. L'interaction stratégique avec le RGPD et l'Espace européen des données de santé

La gestion, la collecte et le traitement de ces gigantesques volumes de données médicales, par nature éminemment sensibles, posent immédiatement le défi de l'articulation avec le Règlement général sur la protection des données (« RGPD »). Le guide MDCG 2025-6 précise de manière sans équivoque que les pratiques de gouvernance et de gestion des données à caractère personnel doivent être pleinement conformes aux dispositions du RGPD, incluant le respect des principes de minimisation et de transparence quant à la finalité initiale de la collecte auprès du patient. Toutefois, l'AI Act, conscient des nécessités techniques de l'apprentissage automatique, introduit une dérogation exceptionnelle et ciblée à son article 10 paragraphe 5. Cette disposition autorise le traitement de catégories particulières de données à caractère personnel (telles que les données révélant l'origine ethnique ou les données concernant la santé) s'il est strictement et techniquement nécessaire à des fins exclusives de détection et de correction des biais algorithmiques, et ce, sous réserve de la mise en place de garanties de sécurité renforcées comme la pseudonymisation avancée ou le chiffrement de bout en bout.

Néanmoins, l'accès à des jeux de données de santé massifs, parfaitement représentatifs et de haute qualité, tels qu'exigés par l'AI Act, constituera sans aucun doute le principal goulot d'étranglement pour les développeurs d'IA en Europe. C'est précisément à ce stade qu'intervient le récent règlement (UE) 2025/327 relatif à l'Espace européen des données de santé (EEDS ou EHDS), une initiative législative phare souvent mise en exergue dans l'écosystème de la santé numérique.

Comme le soulignent avec pertinence les travaux de l'Action conjointe TEHDAS[177], l'EEDS a pour vocation de structurer et de fluidifier l'utilisation secondaire des données de santé à l'échelle continentale, en s'appuyant sur un réseau interconnecté d'Organismes responsables de l'accès aux données de santé (« HDAB »). En fournissant aux industriels et aux chercheurs un accès réglementé, sécurisé et standardisé à des données harmonisées issues des dossiers médicaux électroniques de toute l'Union, l'infrastructure de l'EEDS constituera le carburant vital permettant aux fabricants de satisfaire aux lourdes exigences de représentativité et d'absence d'erreurs de

[177] L'action conjoint TEDHAS (*Towards the European Health Data Space*) est une initiative européenne majeure visant à accompagner les Etats membres et la Commission européenne dans le développement et le partage transfrontalier des données de santé pour une utilisation secondaire, c'est-à-dire pour la recherche, l'innovation et l'élaboration de politiques de santé.

l'article 10 de l'AI Act. Cette interdépendance législative démontre que la robustesse des modèles d'IA européens dépendra intrinsèquement de l'opérationnalisation réussie de l'EEDS et du respect de l'éthique européenne de la donnée.

V. PRECISION, ROBUSTESSE, CYBERSECURITE ET L'INTERFACE AVEC L'EVALUATION CLINIQUE

A. La traduction de l'évaluation clinique en exigences algorithmiques quantifiables

Bien que l'AI Act n'utilise pas explicitement la nomenclature médicale classique d'« évaluation clinique » (propre au MDR) ou d'« évaluation des performances » (propre à l'IVDR), il n'en instaure pas moins des obligations de résultat strictes en matière d'exactitude, de robustesse algorithmique et de cybersécurité, qui se superposent et se confondent directement avec les objectifs de preuve clinique du MDR. Le guide MDCG 2025-6 clarifie ce point en indiquant que les critères de performance de l'AI Act doivent être interprétés et traités comme des composantes intégrales de l'évaluation clinique exigée par le cadre médical.

Sur le plan purement opérationnel, cela implique que le plan d'évaluation clinique ou le plan d'évaluation des performances du dispositif doit être significativement étendu. Il ne suffit plus de démontrer que le logiciel aide à diagnostiquer une pathologie ; le plan doit désormais intégrer les protocoles statistiques de validation des réseaux neuronaux, définir des seuils de tolérance scientifiquement justifiés pour les faux positifs et les faux négatifs, et inclure des analyses de sensibilité du modèle face à des données bruitées ou de qualité dégradée (robustesse). La démonstration de la performance algorithmique devient ainsi le prérequis indispensable à la démonstration du bénéfice clinique global.

B. Le croisement des investigations cliniques et des tests en conditions réelles

Une des zones de friction potentielles majeures entre les deux textes résidait dans les exigences de test *in vivo* avant la mise sur le marché. D'une part, le MDR impose la réalisation d'investigations cliniques pour valider l'efficacité et la sécurité d'un dispositif médical en conditions d'utilisation réelles. D'autre part, l'AI Act introduit un nouveau concept juridique : les « tests en conditions réelles » obligatoires pour les systèmes d'IA à haut risque avant leur commercialisation, tel que prévu par son article 60.

Le document d'orientation du MDCG apporte ici une clarification opérationnelle majeure qui soulagera considérablement les promoteurs d'études. Il affirme de manière catégorique que lorsqu'un MDAI fait l'objet d'une investigation clinique ou d'une étude de performance en vertu des dispositions du MDR ou de l'IVDR, ce processus rigoureux est juridiquement qualifié et formellement accepté comme équivalent à un test en conditions réelles au sens de l'AI Act.

L'AI Act prévoit en effet explicitement que de tels tests en conditions réelles sont autorisés « sans préjudice du droit de l'Union ou du droit national relatif aux essais en conditions réelles de systèmes d'IA à haut risque qui sont des dispositifs médicaux » (article 60). Cette équivalence conceptuelle prévient la nécessité absurde pour le fabricant de devoir soumettre deux protocoles d'expérimentation distincts à des comités d'éthique de la recherche ou à des autorités compétentes différentes. Elle garantit ainsi une continuité logique et temporelle dans le recueil des preuves cliniques et des performances algorithmiques.

C. La sécurité par la conception : la cybersécurité à l'ère de l'intelligence artificielle

La robustesse d'un système MDAI ne se limite pas à la précision de ses prédictions cliniques dans un environnement contrôlé ; elle englobe de manière indissociable sa résilience face aux perturbations extérieures et aux actes de malveillance. Si le MDR et l'IVDR imposent déjà des exigences générales de sécurité des systèmes d'information (complétées de longue date par les orientations spécifiques du MDCG 2019-16 sur la cybersécurité des dispositifs médicaux[178]), l'AI Act apporte une focalisation extrêmement ciblée sur les menaces structurelles inhérentes à l'architecture même de l'IA.

Les fabricants ont l'obligation de mettre en œuvre une démarche de cybersécurité dès la conception (*security by design*) qui soit spécifiquement capable de contrer les vecteurs d'attaque propres à l'apprentissage automatique. Le guide MDCG attend des fabricants qu'ils préviennent et documentent les parades contre des menaces telles que :

- l'empoisonnement du modèle (*Model poisoning*) : l'altération malveillante ou la corruption des données d'entraînement visant à introduire des failles ou à dégrader subrepticement la performance de l'algorithme diagnostique.
- les attaques adversariennes (*Adversarial attacks*) : la manipulation des prédictions de l'algorithme en phase d'inférence, par l'introduction de modifications infimes et souvent imperceptibles pour l'œil humain dans les données d'entrée (par exemple, l'ajout d'un bruit calculé sur une radiographie, conduisant l'IA à ignorer une tumeur).

Les dossiers techniques doivent démontrer de manière irréfutable que le modèle IA est capable de détecter ces anomalies de manière proactive au cours de son exploitation, ou *a minima* de conserver un comportement de sécurité résiduel contrôlé en cas de compromission avérée des données, afin de ne pas mettre en danger la vie du patient.

VI. TRANSPARENCE, EXPLICABILITE ET SURVEILLANCE HUMAINE : REPENSER L'ERGONOMIE DE LA DECISION MEDICALE

L'intégration de l'intelligence artificielle en pratique clinique quotidienne soulève un enjeu de confiance majeur de la part du corps médical, de plus en plus réticent face aux outils prescripteurs, et des patients. L'approche européenne postule fermement que la technologie, aussi avancée soit-elle, doit demeurer un outil d'assistance à la décision et non un oracle médical inviolable. Cette philosophie humaniste se traduit juridiquement par de lourdes obligations en matière de transparence (définies à l'article 13 de l'AI Act) et de contrôle humain (définies à l'article 14 de l'AI Act).

L'AI Act impose une obligation juridiquement contraignante aux développeurs : concevoir les MDAI à haut risque de manière à ce que leur fonctionnement global soit suffisamment transparent pour permettre aux « déployeurs » d'interpréter correctement les résultats générés et d'utiliser le système de manière pleinement appropriée. Cette notion de transparence va bien au-delà de la simple fourniture d'une notice d'utilisation classique conforme aux exigences générales de sécurité et de performance du MDR. La documentation fournie doit expliciter avec pédagogie les caractéristiques de performance, les capacités réelles de l'IA,

[178] MDCG 2019-16 Rev.1, *Guidance on Cybersecurity for medical devices*, July 2020.

mais surtout ses limites inhérentes et ses angles morts.

Le fonctionnement en « boîte noire » absolue est formellement proscrit dans les environnements de soins à haut risque. L'architecture du modèle doit intégrer, par conception, des niveaux d'explicabilité (*XAI - Explainable AI*) permettant aux médecins, qui restent les utilisateurs finaux de la donnée, de comprendre la logique sous-jacente ou les paramètres déterminants ayant conduit à une prédiction clinique donnée (par exemple, via des cartes de chaleur sur une image médicale identifiant les zones ayant focalisé l'attention de l'algorithme).

Corollaire de cette transparence, la surveillance humaine imposée par l'article 14 de l'AI Act exige que l'interface homme-machine soit ergonomiquement conçue pour permettre à une personne physique d'exercer un véritable contrôle critique sur la machine. Concrètement, le professionnel de santé doit disposer de l'autonomie et des moyens techniques nécessaires pour ignorer, outrepasser, ou annuler purement et simplement une recommandation de l'IA sans subir de contrainte technique ou de lourdeur applicative, assurant ainsi que la responsabilité de la décision médicale finale demeure incontestablement humaine. De plus, les systèmes d'IA conçus pour interagir directement avec des personnes physiques (tels que des agents conversationnels médicaux de triage ou des applications de thérapie comportementale) doivent être obligatoirement accompagnés d'une information claire, signifiant au patient qu'il interagit avec un système d'intelligence artificielle, à moins que cette nature algorithmique ne soit évidente compte tenu du contexte d'utilisation.

VII. ÉVOLUTION DU PRODUIT ALGORITHMIQUE : MODIFICATION SUBSTANTIELLE (AI ACT) VERSUS CHANGEMENT SIGNIFICATIF (MDR)

L'une des problématiques réglementaires les plus épineuses, abondamment débattue dans la littérature spécialisée et directement adressée par le MDCG, concerne le cycle de vie du logiciel après sa certification initiale. Les algorithmes d'IA, particulièrement ceux fondés sur des modèles d'apprentissage profond (*Deep Learning*) et d'apprentissage continu (*Continuous Learning*), ont pour vocation naturelle d'être réentraînés avec de nouvelles données et mis à jour fréquemment afin d'optimiser et d'affiner leurs performances diagnostiques ou prédictives au fil du temps.

Dans ce contexte évolutif, le MDR utilise le concept de « changement significatif » apporté à la conception ou à la finalité prévue, qui déclenche automatiquement la nécessité d'une nouvelle évaluation et d'une approbation par l'organisme notifié (conformément aux dispositions transitoires et aux procédures de l'annexe IX). Parallèlement et sur un plan sémantique très proche, l'AI Act introduit la notion de « modification substantielle ». Le risque systémique d'un désalignement conceptuel entre ces deux définitions est d'imposer aux fabricants des évaluations redondantes, longues et coûteuses pour la moindre mise à jour logicielle de routine ou d'amélioration mineure du modèle, tuant ainsi l'agilité inhérente et indispensable au développement de logiciels médicaux modernes.

Afin de résoudre cette quadrature du cercle réglementaire et de préserver la compétitivité de l'industrie, le guide MDCG 2025-6, en s'appuyant sur l'Annexe IV de l'AI Act, valide formellement l'utilisation et la pertinence des plans de contrôle des changements prédéterminés (*PCCP - Predetermined Change Control Plans*). Selon cette doctrine opérationnelle particulièrement attendue, si les modifications futures du MDAI (par exemple, des réentraînements planifiés de l'algorithme sur des jeux de données d'architecture similaire pour améliorer la

précision de 2%) ont été préalablement définies, minutieusement documentées, analysées en termes de risques résiduels, et surtout validées par l'organisme notifié lors du moment précis de l'évaluation initiale de la conformité, la situation change radicalement.

L'implémentation ultérieure de ces changements pré-approuvés et encadrés par l'enveloppe du PCCP, et qui figurent dans la documentation technique requise à l'annexe IV de l'AI Act, ne constitue pas une « modification substantielle » au sens juridique de l'AI Act, pas plus qu'un « changement significatif » au titre du MDR. Ce mécanisme d'anticipation réglementaire est le seul garant d'un cycle de vie logiciel viable sur le marché européen. L'industrie s'attend désormais à ce que des forums internationaux harmonisés, tels que l'International Medical Device Regulators Forum (« IMDRF ») abondamment cité dans les travaux sectoriels, publient très rapidement des orientations complémentaires plus détaillées afin de normaliser la rédaction et l'évaluation de ces précieux PCCP par les organismes notifiés.

VIII. SURVEILLANCE APRES COMMERCIALISATION ET GESTION DU RISQUE JURIDIQUE

Une fois le dispositif MDAI marqué CE et déployé au sein des infrastructures de santé sur le marché européen, la procédure de conformité ne s'arrête pas ; elle entre au contraire dans sa phase d'observation la plus critique et la plus exigeante. L'AI Act vient renforcer de manière drastique la portée, la profondeur et les capacités d'investigation du système de surveillance après commercialisation (*Post-Market Surveillance, « PMS »*) déjà imposé par le chapitre VII du MDR.

La surveillance algorithmique doit impérativement être proportionnée à la nature hautement dynamique et évolutive de l'IA. Pour les systèmes d'IA dits « apprenants en continu », qui adaptent dynamiquement leurs poids synaptiques ou leur comportement post-déploiement en fonction des nouvelles données cliniques traitées dans les établissements de santé, le PMS est élevé au rang d'instrument exclusif et central de sécurisation clinique.

Les fabricants ont l'obligation légale de mettre en place des canaux de télémétrie robustes et sécurisés permettant de rapatrier et d'analyser les données de journalisation issues des environnements d'exploitation des déployeurs. L'objectif est de détecter en temps quasi réel l'apparition de phénomènes délétères tels que la dérive de performance, les apparitions insidieuses de biais discriminatoires qui n'auraient pas été détectés lors des tests de représentativité initiaux, ou les failles de cybersécurité émergentes. Lorsqu'un risque systémique ou une anomalie clinique est identifié grâce à ce monitorage continu, des actions correctives de sécurité doivent être implémentées et communiquées de manière diligente et transparente à toutes les parties prenantes pertinentes, incluant les patients, les professionnels utilisateurs, les établissements déployeurs, ainsi que les autorités compétentes et les organismes notifiés.

Cet enchevêtrement complexe d'obligations de surveillance de la donnée trouve également un écho direct et menaçant dans l'évolution parallèle du droit de la responsabilité civile européen. Les dysfonctionnements d'un algorithme diagnostique ayant causé un retard de prise en charge, un préjudice corporel, ou la corruption du dossier médical d'un patient tomberont de plein droit sous le coup de la nouvelle directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux. La doctrine juridique a récemment et abondamment mis en exergue que cette refonte majeure inclut désormais expressément et sans équivoque les logiciels autonomes et les systèmes d'intelligence artificielle dans sa définition stricte du « produit ».

Plus fondamentalement, pour pallier l'asymétrie d'information structurelle dont

souffrent les victimes face à l'opacité des boîtes noires algorithmiques, la directive prévoit des mécanismes redoutables de présomption de défectuosité et d'inversion de la charge de la preuve. Dans ce contexte contentieux hautement inflammable, si un fabricant est assigné en justice et qu'il refuse ou s'avère incapable de fournir les données de journalisation (logs) exigées par l'AI Act pour expliquer le cheminement décisionnel de l'IA, le juge pourra présumer que le produit était défectueux au sens de la directive. Le maintien d'un PMS rigoureux, couplé aux obligations de transparence documentaire et de conservation des enregistrements exigées conjointement par l'AI Act et le MDR, ne constitue donc pas seulement une obligation de conformité administrative. Il représente le bouclier juridique primaire et indispensable du fabricant pour se défendre efficacement en cas de contentieux sériel sur la responsabilité des produits de santé numériques.

CONCLUSION : L'AVÈNEMENT DE LA CONFORMITÉ SYSTÉMIQUE PAR CONCEPTION

L'adoption conjointe et simultanée du règlement sur les dispositifs médicaux (MDR/IVDR) et de la loi sur l'intelligence artificielle (AI Act), orchestrée sur le plan purement opérationnel par les orientations pragmatiques du guide MDCG 2025-6, marque assurément une étape décisive dans la maturité de la réglementation européenne de la santé numérique. Le législateur européen a définitivement acté le fait que le logiciel médical n'est plus un simple automate déterministe prédictif. Il est désormais perçu, à juste titre, comme une entité évolutive, vulnérable aux biais de ses concepteurs, et potentiellement génératrice de risques systémiques dépassant largement le strict cadre de la sécurité clinique individuelle, pour empiéter sur le terrain des droits fondamentaux et de la sécurité des données.

L'étude du document MDCG 2025-6 révèle une ingénierie réglementaire exigeante mais qui tente sincèrement de rester pragmatique, dont la philosophie centrale repose sur l'intégration des obligations plutôt que sur leur superposition. En incitant fortement les fabricants à fusionner leurs systèmes de gestion de la qualité, leur documentation technique, leurs évaluations cliniques et leurs protocoles de contrôle des changements, le Groupe de coordination des dispositifs médicaux offre une voie de passage étroite mais praticable pour éviter la fragmentation administrative et l'asphyxie économique de l'industrie technologique européenne de la santé.

Cependant, cette simplification d'ordre formel et procédural ne saurait occulter l'élévation substantielle du niveau d'exigence technique et scientifique requis pour opérer sur ce marché. La gouvernance absolue et traçable des données d'entraînement, l'éradication proactive et documentée des biais discriminatoires, la résilience aux attaques sophistiquées de cybersécurité par la conception, ainsi que la garantie d'une interface suffisamment transparente pour permettre le maintien du libre arbitre et du jugement critique du médecin prescripteur, constituent désormais le socle minimal, non négociable, d'accès au marché intérieur européen.

Pour les fabricants de technologies médicales, le passage d'une culture historique de la certification ponctuelle d'un dispositif figé à une culture de la conformité algorithmique systémique et continue s'impose comme un impératif de survie. Dans ce processus de transformation industrielle, la synergie avec des dispositifs d'infrastructures majeurs, tels que l'Espace européen des données de santé, sera déterminante pour alimenter légalement ces algorithmes voraces en données de haute fiabilité et représentativité. À l'aube de l'application pleinement contraignante des dispositions de l'AI Act prévue en août 2027 pour les dispositifs médicaux, qu'ils soient hérités (et modifiés) ou de conception nouvelle, la capacité de l'industrie, des

hôpitaux déployeurs et des organismes notifiés à s'approprier collectivement les clés de lecture de ce guide MDCG conditionnera non seulement la compétitivité et l'agilité de l'innovation médicale européenne, mais garantira surtout le maintien d'une confiance inaltérable des professionnels de santé et des patients dans la médecine algorithmique de demain.

MDCG 2025-6 FAQ on Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), June 2025


Medical Device
Medical Device Coordination Group Document MDCG 2019-11 rev. 1

MDCG 2019-11 Rev.1
Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR

October 2019
June 2025 rev.1

Lignes directrices relatives à la qualification et à la classification des logiciels dans le cadre du règlement (UE) 2017/745 et du règlement (UE) 2017/746. Analyse opérationnelle de la révision MDCG 2019-11 rev. 1

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

Le paysage réglementaire européen applicable aux technologies médicales traverse une période de mutation systémique, propulsée par une numérisation exponentielle des parcours de soins et par l'émergence d'outils algorithmiques d'une complexité inédite. Dans ce contexte de transformation où le droit tente d'épouser le rythme de l'innovation technologique, le Groupe de coordination en matière de dispositifs médicaux (« MDCG ») a publié, en juin 2025, la révision 1 de ses lignes directrices MDCG 2019-11[179].

Ce document, fondamental pour l'écosystème de la santé numérique, est expressément consacré à la qualification et à la classification des logiciels dispositifs médicaux (ci-après désignés par l'acronyme anglophone « MDSW », pour *Medical Device Software*) au titre du règlement (UE) 2017/745 relatif aux dispositifs médicaux (« MDR » acronyme anglais pour *medical device regulation*)[180] et du règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[181].

[179] MDCG 2019-11 rev.1, *Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746*, June 2025.

[180] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, *JOUE* L. 117 du 5 mai 2017.

[181] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et

Publiée près de six ans après la version originelle d'octobre 2019, cette mise à jour réglementaire était particulièrement attendue par les fabricants, les éditeurs de logiciels, les organismes notifiés et les établissements de soins.

Si l'architecture globale et la philosophie du texte demeurent inchangées, cette révision introduit des clarifications sémantiques profondes et des précisions opérationnelles majeures qui traduisent une volonté ferme d'adaptation du droit de l'Union européenne aux réalités technologiques contemporaines. L'intégration explicite de l'intelligence artificielle au sein du périmètre de qualification, la prise en compte exigeante des architectures logicielles modulaires, l'attention inédite portée aux logiciels de prévention en vertu de la Règle 11 de classification, et l'articulation stratégique avec le nouveau règlement sur l'Espace européen des données de santé[182] (« EEDS ») constituent les axes cardinaux de cette évolution doctrinale.

L'analyse exhaustive de cette révision révèle un glissement paradigmatique : le passage d'une approche réglementaire historiquement centrée sur le support physique vers une régulation purement fonctionnelle, intrinsèque à la nature de la donnée et à l'action opérée sur celle-ci.
L'abandon définitif de la notion de « logiciel autonome » (*standalone software*) au profit d'une qualification fondée exclusivement sur la finalité médicale revendiquée par le fabricant en est l'illustration la plus éclatante.
La présente analyse propose un décryptage approfondi des nouveautés introduites par la révision de juin 2025 du guide MDCG 2019-11. Il s'agit d'examiner les implications pratiques, juridiques et opérationnelles pour les opérateurs de la santé numérique, en démontrant comment ces lignes directrices s'insèrent dans un corpus juridique européen de plus en plus dense, marqué par la convergence entre le droit des produits de santé, le droit des données et la régulation de l'intelligence artificielle.

I. L'ÉVOLUTION DU CHAMP D'APPLICATION ET LA REDÉFINITION CONCEPTUELLE DU LOGICIEL DISPOSITIF MÉDICAL

La première évolution notable de la révision de ce guide réside dans la clarification rigoureuse du champ d'application du document et la redéfinition des contours techniques et juridiques de ce qui constitue un logiciel dispositif médical. Le législateur européen et le MDCG actent ici la dématérialisation croissante des solutions de santé.

A. L'abandon de la notion de logiciel autonome au profit d'une approche fonctionnelle

Une clarification sémantique aux conséquences opérationnelles majeures est l'abandon explicite et définitif du terme « logiciel autonome » (*standalone software*), un concept hérité de l'ère des anciennes directives 93/42/CEE[183] et 98/79/CE[184]. La révision de juin 2025 consacre le principe directeur selon lequel un logiciel doit être qualifié et classifié en fonction de sa destination propre, de manière totalement indépendante de sa localisation physique, de son environnement d'exécution ou de son support d'hébergement.

abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, *JOUE* L. 117 du 5 mai 2017.

[182] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* du 5 mars 2025.

[183] Directive 93/42/CEE du Conseil du 14 juin 1993 relative aux dispositifs médicaux, *JOCE* L. 169 du 12 juillet 1993.

[184] Directive 98/79/CE du Parlement européen et du Conseil du 27 octobre 1998 relative aux dispositifs médicaux de diagnostic in vitro, *JOCE* L. 331 du 7 décembre 1998.

Que le logiciel soit physiquement embarqué dans un dispositif matériel lourd comme un scanner IRM, qu'il opère sur un serveur distant via une architecture en nuage (*Cloud computing*), qu'il prenne la forme d'une application mobile téléchargée directement par un patient sur son smartphone, ou qu'il soit intégré en tant que micro-service au sein d'un vaste système d'information hospitalier, la méthode et la rigueur de la qualification demeurent strictement identiques.

Cette approche fonctionnelle oblige les fabricants à se concentrer exclusivement sur la nature de l'action effectuée sur les données. Selon les termes précis du guide, un logiciel est défini comme un ensemble d'instructions qui traite des données d'entrée pour créer des données de sortie. Si la création ou la modification de ces données de sortie est régie par une finalité médicale telle que définie à l'article 2, point 1, du MDR (diagnostic, prévention, suivi, prédiction, pronostic, traitement ou atténuation d'une maladie), le logiciel revêt irréfutablement la qualification de MDSW.

Cette dématérialisation de la pensée réglementaire permet de capturer efficacement l'ensemble des architectures modernes, et tout particulièrement les solutions en mode SaaS (*Software as a Service*), qui dominent aujourd'hui le marché de la santé numérique et échappaient parfois à une qualification aisée sous l'ancien paradigme.

B. L'intégration formelle de l'intelligence artificielle et l'articulation avec l'AI Act

Face à la prolifération exponentielle des algorithmes d'apprentissage automatique (*machine learning*), des réseaux de neurones profonds et des grands modèles de langage (*Large Language Models*) déployés en santé, le guide MDCG 2019-11 révisé inclut désormais explicitement l'Intelligence Artificielle Dispositif Médical (« MDAI » - *Medical Device Artificial Intelligence*) dans son champ d'application.

Cette reconnaissance formelle marque une étape cruciale dans la taxonomie réglementaire européenne, actant que l'IA n'est plus une technologie émergente périphérique mais une composante centrale des dispositifs médicaux logiciels.

La qualification d'un système d'IA en tant que MDSW obéit aux mêmes règles fondamentales que les logiciels algorithmiques traditionnels : elle dépend intrinsèquement de sa destination médicale. Toutefois, cette inclusion textuelle opère une jonction directe et complexe avec le règlement (UE) 2024/1689 sur l'intelligence artificielle (communément appelé AI Act)[185], entré en vigueur durant l'été 2024.

Les fabricants de MDAI se trouvent désormais confrontés à un défi d'ingénierie réglementaire sans précédent. Ils doivent concevoir leur stratégie de mise sur le marché de manière bicéphale, en satisfaisant simultanément aux exigences générales de sécurité et de performances de l'Annexe I du MDR ou du IVDR, et aux obligations strictes de transparence, de gouvernance des données, d'explicabilité et de contrôle humain imposées aux systèmes d'IA à haut risque par l'AI Act.

L'accent mis sur la MDAI reflète une préoccupation aiguë des autorités de régulation quant à la nature probabiliste, évolutive et parfois opaque de ces systèmes. Le guide souligne de manière implicite que le traitement de données d'entrée complexes, telles que des images radiologiques en haute résolution, des séquences génomiques ou des données textuelles non structurées issues de dossiers patients, dans le but de générer des

[185] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JOUE* du 12 juillet 2024.

prédictions diagnostiques ou des recommandations thérapeutiques, constitue une action sur la donnée qui dépasse de très loin la simple recherche, l'archivage ou la compression sans perte (**page suivante**).

Une telle action qualifie irréfutablement ces outils d'IA de dispositifs médicaux.

Critère d'évaluation	Approche antérieure (Directives / MDCG initial)	Approche MDCG 2019-11 rev.1 (Juin 2025)	Impact Opérationnel pour l'industrie
Localisation du logiciel	Importance accordée au caractère « autonome » ou embarqué du logiciel.	Indifférence totale de la localisation (Cloud, mobile, serveur local, embarqué).	Obligation d'évaluer la fonction algorithmique pure, abstraction faite de l'infrastructure d'hébergement.
Nature de la technologie	Traitement uniforme des logiciels déterministes et des algorithmes complexes.	Inclusion explicite et traitement spécifique de la MDAI (Medical Device AI).	Nécessité d'aligner le dossier technique MDR avec les exigences de l'AI Act (explicabilité, gouvernance des données).
Action sur la donnée	Frontière parfois floue entre recherche simple et aide à la décision.	Distinction claire : l'altération de la représentation des données à des fins cliniques est un acte médical.	Les moteurs de recherche utilisant le traitement du langage naturel (NLP) pour influencer une décision clinique sont des MDSW.

C. La clarification réglementaire des produits de l'Annexe XVI sans finalité médicale

La section 3.1 du guide révisé a été substantiellement enrichie pour clarifier l'applicabilité des règles de qualification et de classification aux logiciels relatifs aux produits listés à l'Annexe XVI du Règlement (UE) 2017/745. Ces produits, bien que structurellement dépourvus de finalité médicale[186], sont soumis aux exigences de sécurité et de performance du MDR en raison de leur profil de risque physiologiquement similaire à celui des dispositifs médicaux traditionnels.

La révision du guide établit une distinction opérationnelle et juridique fondamentale pour les éditeurs de logiciels intervenant dans ce secteur particulièrement lucratif mais historiquement sous-réglementé.

Le texte distingue désormais deux scénarios distincts.

D'une part, si un logiciel est spécifiquement conçu et destiné à fournir des informations permettant de déterminer la finalité non médicale ou esthétique d'un produit de l'Annexe XVI, ce logiciel est lui-même qualifié de produit de l'Annexe XVI et se trouve soumis de plein droit au MDR. C'est typiquement le cas d'un algorithme de modélisation 3D avancée utilisé par un chirurgien plasticien pour prédire et visualiser les résultats d'une rhinoplastie ou pour aider un patient à sélectionner la taille et la forme spécifiques d'un implant mammaire esthétique.

D'autre part, si le logiciel se contente de piloter techniquement ou d'influencer directement les performances matérielles d'un équipement de l'Annexe XVI, sans fournir d'information ou d'aide à la décision quant à sa finalité esthétique, ce

[186] A l'instar des équipements de liposuccion esthétique, des lasers d'épilation à lumière pulsée, des équipements de stimulation cérébrale non médicale ou des implants de comblement dermique à visée purement esthétique.

logiciel n'est pas qualifié de produit de l'Annexe XVI de manière indépendante. Il est, en revanche, considéré comme une partie intégrante de cet équipement ou comme un accessoire de celui-ci, et suit par conséquent le régime d'évaluation de la conformité du matériel qu'il pilote.

Cette clarification sémantique est d'une importance capitale. Elle colmate les brèches juridiques potentielles pour les applications logicielles proliférant dans le secteur de l'esthétique et de la modification corporelle, obligeant les développeurs de ces outils de simulation ou de paramétrage à se soumettre à des évaluations cliniques (ou plutôt, dans ce contexte, à des évaluations démontrant la sécurité et l'absence de risque clinique inacceptable) rigoureuses avant toute mise sur le marché européen.

II. L'EXIGENCE ABSOLUE DE LA DESTINATION ET LA MAITRISE OPÉRATIONNELLE DE LA MODULARITÉ

Le cœur battant de la conformité réglementaire d'un dispositif médical, qu'il soit matériel ou logiciel, réside dans sa déclaration de destination (*intended purpose*). La révision du guide MDCG 2019-11 insiste de manière appuyée et répétée sur l'importance cruciale de la rédaction de cette destination, particulièrement dans le contexte des architectures logicielles complexes, interconnectées et modulaires.

A. La formulation de la destination médicale comme clé de voûte de la conformité

Le guide souligne qu'une formulation claire, exhaustive et sans ambiguïté de la destination est le prérequis absolu et non négociable pour une qualification et une classification correctes du logiciel. La destination, telle que définie conjointement par l'article 2, point 12, du MDR et de l'IVDR, englobe l'utilisation prévue selon les indications fournies par le fabricant sur l'étiquetage, dans les instructions d'utilisation, dans les documents promotionnels ou commerciaux, et de manière absolument cruciale, telles que spécifiées dans l'évaluation clinique pour les dispositifs médicaux ou dans l'évaluation des performances pour les dispositifs de diagnostic in vitro.

La nouveauté opérationnelle réside dans la mise en garde explicite formulée par le MDCG à l'attention des industriels : une destination ambiguë, excessivement large, générique ou mal définie peut inéluctablement conduire à une sur-classification pénalisante sur le plan commercial, ou pire, à une sous-classification erronée, entraînant des risques de non-conformité majeurs lors des audits menés par les organismes notifiés ou lors des inspections des autorités compétentes. Le fabricant a l'obligation impérieuse de s'assurer que chaque fonctionnalité du logiciel ayant une prétention ou un but médical est expressément couverte et justifiée par la déclaration de destination.

Concrètement, l'exigence imposée par l'article 7 du MDR et de l'IVDR rappelle que toute allégation relative à la finalité médicale prévue du MDSW doit être soutenue par un niveau de preuve clinique approprié et irréfutable. Si le département marketing d'un fabricant met en avant, sur le site internet du produit ou dans une brochure commerciale, une fonctionnalité offrant un bénéfice thérapeutique prédictif ou diagnostique, mais que cette fonctionnalité est absente de la destination officielle documentée et n'est pas corroborée par les données de l'évaluation clinique, le logiciel enfreint les exigences fondamentales des règlements. Dans une telle situation, le logiciel ne peut légalement être revêtu du marquage CE en tant que dispositif médical, et s'expose à des mesures de police sanitaire incluant le retrait immédiat du marché européen. Cette exigence impose un alignement total et permanent entre les équipes d'ingénierie, les affaires réglementaires, la direction

médicale et les services commerciaux de l'entreprise.

B. L'opérationnalisation rigoureuse des architectures modulaires (Section 7)

La tendance technologique lourde et irréversible en santé numérique est le développement de systèmes d'information hospitaliers (« SIH »), de dossiers patients informatisés (« « DPI) et de plateformes de santé vastes et multifonctionnels, où des fonctionnalités administratives (facturation, gestion des lits), logistiques et purement médicales (aide à la prescription, analyse d'images) cohabitent au sein d'un même environnement logiciel.

Pour faire face à cette complexité architecturale, la Section 7 du guide, consacrée aux modules, a fait l'objet d'une mise à jour et d'une élaboration conceptuelle substantielle.

Le guide entérine et précise la possibilité pour un fabricant de diviser un produit logiciel global en plusieurs modules distincts, certains étant qualifiés de MDSW en raison de leur finalité clinique, et d'autres non. Toutefois, cette approche de conception modulaire n'est pas une simple facilité administrative ; elle exige une rigueur architecturale absolue et une traçabilité sans faille.

Les nouvelles directives opérationnelles adressées aux fabricants concernant la modularité imposent un cadre strict :

1. L'indépendance de la conformité réglementaire : chaque module individuel qualifié de MDSW doit satisfaire de manière totalement indépendante aux exigences réglementaires de sécurité et de performance qui lui sont applicables, comme s'il s'agissait d'un dispositif autonome. L'évaluation clinique et la gestion des risques doivent être documentées pour chaque module médical de façon isolée.
2. L'alignement global du système : la fonctionnalité collective de l'ensemble des composants interconnectés - qu'ils soient médicaux ou non médicaux - doit s'aligner parfaitement sur la destination déclarée globale du système, sans introduire de contradictions opérationnelles, de failles de sécurité ou de risques inacceptables pour le patient ou l'utilisateur.
3. Des frontières architecturales imperméables : le fabricant doit fournir, dans sa documentation technique, une représentation architecturale d'une grande précision, délimitant visuellement et techniquement les frontières exactes entre les modules MDSW et les modules non-MDSW. Les interfaces (API, flux de données, protocoles d'échange) entre ces différents modules doivent faire l'objet d'une analyse de risque spécifique et exhaustive.
4. La gestion systémique des risques d'interface : une défaillance d'un module non-médical (par exemple, un module de gestion des identités provoquant une corruption de la base de données, ou un module de facturation saturant la mémoire du serveur) ne doit en aucun cas compromettre la sécurité, la disponibilité continue, ou l'intégrité clinique des données utilisées par le module médical (par exemple, un algorithme de calcul de dose d'insuline ou un outil d'aide à la décision thérapeutique). L'évaluation des risques, selon la norme ISO 14971, doit expressément et obligatoirement prendre en compte ces interactions inter-modules et démontrer la mise en place de mesures de mitigation efficaces.

Cette clarification détaillée sur la modularité offre une flexibilité stratégique précieuse aux éditeurs de logiciels de santé. Elle leur permet de circonscrire et de limiter

le périmètre fastidieux et coûteux du marquage CE aux seules fonctionnalités véritablement médicales, allégeant ainsi significativement le fardeau réglementaire de la maintenance des fonctionnalités administratives de leurs logiciels. Cependant, cet allègement n'est consenti qu'à la condition expresse que la ségrégation technique, documentée par le respect strict de normes telles que l'IEC 62304 sur le cycle de vie du logiciel[187], soit démontrée comme infaillible devant l'organisme notifié.

III. L'ÉVOLUTION DE LA CLASSIFICATION SOUS L'EMPIRE DE LA RÈGLE 11 : LE TOURNANT DE LA PRÉVENTION (SECTION 4.2.1)

L'un des apports conceptuels et opérationnels les plus déterminants de la révision de juin 2025 concerne la Règle 11 de l'Annexe VIII du MDR. Cette règle constitue, depuis l'entrée en application du règlement, la clef de voûte de la classification des logiciels médicaux en Europe.

Contrairement aux règles applicables au matériel physique, qui évaluent les risques liés au contact invasif ou à l'échange d'énergie, la Règle 11 a été spécifiquement conçue pour capturer les risques indirects inhérents aux logiciels. Le préjudice ne provient pas d'une défaillance mécanique, mais des conséquences délétères d'une information inexacte, incomplète ou erronée fournie par l'algorithme, conduisant le clinicien ou le patient à prendre une mauvaise décision de gestion médicale.

A. L'élargissement de la sous-règle 11a et l'intégration formelle de la « prévention »

La Règle 11 précise, dans sa construction tripartite, que les logiciels destinés à fournir des informations utilisées pour prendre des décisions à des fins diagnostiques ou thérapeutiques relèvent par défaut de la classe IIa. Des exceptions rehaussent cette classification si de telles décisions peuvent entraîner la mort ou une détérioration irréversible de l'état de santé (classe III), ou une détérioration grave de l'état de santé ou nécessiter une intervention chirurgicale majeure (classe IIb).

La nouveauté juridique majeure de la révision du guide réside dans l'ajout d'une clarification explicite concernant les dispositifs logiciels destinés à prévenir le risque de maladie au sein du périmètre d'application de cette sous-règle 11a.

Jusqu'à la publication de ce document révisé, une vaste zone grise réglementaire subsistait quant à la classification exacte des logiciels relevant de la médecine prédictive et préventive. De nombreux fabricants tentaient stratégiquement de classer des applications de prévention avancées (par exemple, des algorithmes prédisant le risque de survenue d'un diabète gestationnel, analysant des biomarqueurs pour anticiper un risque cardiovasculaire, ou évaluant des données génomiques pour déterminer une prédisposition oncologique) dans la catégorie résiduelle de la classe I (sous-règle 11c). Leur argumentaire reposait sur le fait que ces outils ne posaient pas de diagnostic clinique formel et ne proposaient pas de thérapie immédiate, échappant ainsi, selon eux, aux rigueurs de la sous-règle 11a.

La révision du guide MDCG coupe net à cette interprétation minimaliste. Le document précise désormais, sans

[187] La norme IEC 62304 est la norme internationale de référence qui définit les processus de cycle de vie du développement des logiciels de dispositifs médicaux. Son objectif principal est de minimiser les risques pour les patients en imposant une rigueur stricte dans la manière dont le logiciel est conçu, testé, publié et maintenu. Dans le cadre du marquage CE dispositif médical, démontrer la conformité à la norme IUEC 62304 est un moyen privilégié par les fabricants pour prouver aux autorités et aux organismes notifiés que le logiciel a été développé de manière sûre, traçable et contrôlée.

équivoque, qu'un dispositif logiciel destiné à prévenir le risque de maladies ou de pathologies en analysant des paramètres physiologiques (le guide cite expressément l'exemple de l'analyse du placement des vertèbres dorsales ou de la rigidité artérielle) doit être considéré comme fournissant des informations utilisées pour prendre des décisions à des fins de diagnostic, la prévention s'assimilant ici à la détection potentielle précoce de pathologies.

En conséquence directe, ces logiciels de prévention clinique relèvent *a minima* de la classe IIa, rendant obligatoire l'intervention d'un organisme notifié pour l'évaluation de leur conformité avant le marquage CE.

De plus, le guide rappelle que si l'information préventive s'avère erronée (faux négatif) et peut conduire à une inaction médicale entraînant *in fine* une détérioration grave de l'état de santé du patient (par exemple, un logiciel prédisant un risque nul d'infarctus chez un patient à très haut risque, conduisant à l'arrêt injustifié d'une surveillance cardiologique), la classification algorithmique doit logiquement être rehaussée en classe IIb, voire en classe III selon la sévérité du préjudice anticipé.

Sous-règle (Règle 11)	Domaine d'application clarifié (Juin 2025)	Impact sur la classification	Obligation d'Organisme Notifié
Sous-règle 11a	Décisions diagnostiques, thérapeutiques ET prévention du risque de maladie.	Classe IIa minimum (IIb ou III selon la gravité du préjudice potentiel).	OUI (Impact majeur pour les ex-Classe I de prévention).
Sous-règle 11b	Surveillance des processus physiologiques (et paramètres vitaux si danger immédiat).	Classe IIa (ou IIb si danger immédiat).	OUI
Sous-règle 11c	Toutes les autres finalités médicales mineures ne relevant pas du diagnostic, du traitement ou de la prévention clinique.	Classe I (catégorie devenue résiduelle et exceptionnelle)	NON (Autocertification possible, sous réserve d'absence de fonction de mesure).

B. La confirmation du cadre d'évaluation des risques de l'IMDRF

Le guide réaffirme avec force et renforce opérationnellement l'utilisation du cadre conceptuel élaboré par l'IMDRF (*International Medical Device Regulators Forum*) pour évaluer le risque inhérent aux logiciels médicaux. L'Annexe III du document MDCG fournit une matrice d'équivalence permettant d'aligner les catégories de risque de l'IMDRF avec les classes du MDR issues de la Règle 11.

Cette méthodologie d'évaluation impose au fabricant de croiser systématiquement deux variables fondamentales lors de la rédaction de son dossier de gestion des risques :

- L'importance de l'information fournie par le logiciel pour la décision de santé : le logiciel aide-t-il directement à traiter ou diagnostiquer (impact majeur) ? Concourt-il à diriger la gestion clinique (impact modéré) ? Ou sert-il simplement à éclairer et informer la gestion clinique (impact mineur) ?
- L'état de la situation de soins ou l'état du patient : la situation médicale est-elle critique (urgence vitale), sérieuse (maladie chronique grave) ou non grave ?

En clarifiant explicitement que la « prévention » est assimilée sur le plan réglementaire à une aide à la décision diagnostique, le MDCG harmonise la lecture de la Règle 11 à travers toute l'Europe. Cette doctrine empêche fermement le contournement réglementaire par l'usage d'allégations purement « préventives », de « suivi de style de vie » ou de « bien-être » lorsque la fonction intrinsèque et le mécanisme d'action de l'outil relèvent bel et bien d'une analyse clinique prédictive agissant sur le parcours de soin du patient.

IV. L'ÉMERGENCE DES THÉRAPEUTIQUES NUMÉRIQUES (DTX) ET L'EXEMPLE DE LA CLASSE I

Pour faciliter l'appropriation des règles de qualification et de classification, le MDCG a considérablement enrichi la section 3.2 du guide avec de nouveaux exemples concrets illustrant la frontière complexe entre les logiciels relevant du MDR et ceux qui en sont exclus.

A. Les logiciels destinés à « traiter » : la consécration des DTx (Section 3.2)

Une attention institutionnelle particulière a été accordée aux dispositifs thérapeutiques numériques (*Digital Therapeutics* ou « DTx »). Ces logiciels innovants ne se contentent plus d'observer, de surveiller une condition médicale ou d'aider un médecin à formuler un diagnostic ; ils visent activement et de manière autonome à traiter ou atténuer une maladie ou un trouble chez le patient.

Parmi les exemples novateurs introduits dans la version de juin 2025, on relève des cas d'usage reflétant l'état de l'art de la psychiatrie et de la neurologie numérique :

- traitement ciblé de la dyslexie : le guide cite un MDSW spécifiquement destiné à traiter les enfants atteints de dyslexie en améliorant l'analyse visio-orthographique des mots écrits. Le logiciel modifie activement et dynamiquement la présentation des éléments visuels à l'écran pour entraîner le cerveau de l'enfant à traiter simultanément un plus grand nombre d'éléments distincts lors de la fixation oculaire, accélérant ainsi la vitesse de reconnaissance des mots pendant la lecture. En opérant une action directe sur le processus cognitif et neurologique du patient à des fins thérapeutiques correctives, le logiciel se qualifie indéniablement de MDSW.
- aide au traitement de la schizophrénie : un autre exemple frappant concerne un MDSW permettant aux patients atteints de schizophrénie de suivre quotidiennement leurs symptômes et de recevoir des interventions médicales personnalisées basées sur leurs réponses à des évaluations. Le patient interagit avec divers modules thérapeutiques axés sur l'observance médicamenteuse, la régulation de l'humeur, le fonctionnement social, et surtout, la gestion active des hallucinations auditives. La fourniture d'interventions psycho-éducatives personnalisées et réactives dans le but exclusif de soulager ou de gérer les symptômes d'une pathologie psychiatrique lourde caractérise sans ambiguïté l'intention thérapeutique du logiciel.
- réalité virtuelle et réhabilitation neurologique : sont également formellement cités des logiciels recommandant des exercices de réadaptation musculo-squelettiques personnalisés pour soulager la douleur, ou des systèmes fonctionnant de concert avec des casques de réalité virtuelle immersifs pour traiter le syndrome complexe du membre fantôme chez

les personnes amputées. Dans ce dernier cas, le logiciel crée un avatar numérique simulant en temps réel les mouvements du membre manquant pour tromper le cortex cérébral et atténuer la douleur neuropathique.

Ces exemples illustrent la prise en compte mature par les régulateurs européens de la thérapie cognitivo-comportementale numérique et de la neuro-réhabilitation en tant qu'interventions médicales à part entière, soumises au même niveau d'exigence clinique qu'une molécule pharmacologique.

B. Le nouvel exemple de Classe I : Une catégorie devenue l'exception (Annexe IV)

Afin d'équilibrer l'élévation générale de la classification induite par l'interprétation stricte de la Règle 11, le MDCG a pris soin d'ajouter un nouvel exemple de logiciel relevant spécifiquement de la classe I dans l'Annexe IV du document.

Bien que le maintien de logiciels en classe I devienne exceptionnel sous l'empire du MDR, la doctrine réglementaire rappelle que cette classe d'autocertification reste réservée aux logiciels présentant un profil de risque absolument minime, dont les informations fournies n'influencent pas directement, ni de manière significative, une décision de diagnostic ou d'acte thérapeutique (relevant ainsi de la sous-règle 11c résiduelle).

L'ajout de cet exemple pratique vise à guider avec précision les fabricants de petites applications d'accompagnement (par exemple, de simples outils de saisie de journal de bord sans analyse prédictive, ou des logiciels de communication de base entre professionnels de santé n'altérant en rien la donnée médicale transmise) dans leur processus d'auto-certification. Cette précision est vitale pour éviter un engorgement inutile et préjudiciable des organismes notifiés, déjà sous forte tension capacitaire en Europe.

V. L'ARTICULATION STRATÉGIQUE ET JURIDIQUE AVEC L'ESPACE EUROPÉEN DES DONNÉES DE SANTE

L'une des mises à jour les plus structurantes de la révision figure à l'Annexe I, section c.1 du guide. Le document intègre désormais formellement les implications du nouveau règlement (UE) 2025/327 relatif à l'EEDS, un texte législatif majeur et entré en vigueur en un temps record. Cette actualisation minutieuse témoigne d'un changement de paradigme fondamental vers une réglementation de la santé davantage axée sur la donnée, sa portabilité et son interopérabilité.

A. Le défi réglementaire des dossiers médicaux électroniques

L'Annexe I c.1 aborde la question épineuse de la qualification et de la classification des systèmes d'information en santé, et plus spécifiquement des systèmes de dossiers médicaux électroniques (« DME », ou « EHR » pour *Electronic Health Record*).

Historiquement, sous les anciennes directives, les dossiers patients informatisés étaient majoritairement considérés comme de simples bases de données de stockage, d'archivage ou d'outils administratifs. À ce titre, ils échappaient généralement à la qualification de dispositif médical, la simple action d'archivage étant expressément exclue par l'étape 3 de l'arbre de décision de qualification du MDCG.

Toutefois, la réalité technologique a rattrapé le droit. Les DME modernes ne sont plus de passives bases de données ; ils intègrent de plus en plus des fonctionnalités actives d'aide à la décision clinique, des moteurs de règles générant des alertes d'interactions médicamenteuses en temps réel, ou des modules d'analyse de cohortes pour le suivi épidémiologique automatisé.
En outre, le règlement EEDS, dans son chapitre II, impose désormais de nouvelles

exigences drastiques de certification et d'autodéclaration de conformité (marquage CE spécifique EEDS) pour tous les systèmes de dossiers médicaux électroniques commercialisés sur le marché européen.

Le présent guide clarifie les frontières juridiques et techniques entre ces deux cadres réglementaires massifs - le MDR pour la sécurité clinique et l'EEDS pour l'interopérabilité des données - :

- **Interopérabilité et Cybersécurité** : l'accent est mis sur la capacité du logiciel médical à interagir de manière fluide et sécurisée avec le système de santé élargi. Les fabricants de MDSW qui revendiquent dans leurs spécifications une interopérabilité avec les systèmes DME doivent désormais démontrer leur conformité non seulement aux exigences du MDR (notamment en matière d'ingénierie logicielle et de validation clinique), mais également aux exigences applicables de l'EEDS.
- **Intégrité de la décision clinique** : le guide souligne avec insistance que l'interaction complexe entre un module MDSW (par exemple, un algorithme d'aide au diagnostic) et un dossier médical régi par l'EEDS ne doit compromettre en aucune circonstance l'intégrité des données de santé transitant sur le réseau, ni la cybersécurité du système global hospitalier, ni, in fine, la validité de la décision clinique prise par le praticien sur la base de ces données échangées.
- **Gouvernance de l'utilisation primaire des données** : l'EEDS vise à faciliter l'utilisation primaire des données (pour la continuité des soins transfrontaliers) par la standardisation des formats d'échange (comme le format européen d'échange de dossiers de santé électroniques - EEHRxF). Un fabricant de MDSW extrayant des données d'un DME pour alimenter son algorithme doit s'assurer de la qualité intrinsèque et sémantique de ces données d'entrée. Si le logiciel utilise des données corrompues, mal formatées ou incomplètes issues d'un registre EEDS pour générer une recommandation de traitement vitale, le risque d'erreur diagnostique doit être scrupuleusement anticipé et mitigé dans le dossier de gestion des risques du MDR.

L'intégration des préceptes de l'EEDS dans le guide MDCG oblige les éditeurs de logiciels médicaux à abandonner la logique des systèmes fermés pour adopter une posture de conception en « écosystème ouvert et sécurisé ». Un MDSW n'est plus évalué de manière isolée en laboratoire, mais en tant que nœud d'un vaste réseau européen de partage de données de santé, entraînant des responsabilités accrues en matière d'adoption de standards (ex. HL7 FHIR) et de cyber-résilience face aux menaces.

La révision 1 du guide MDCG 2019-11, publiée en juin 2025, ne se contente pas de procéder à un simple toilettage administratif d'un texte vieux de six ans ; elle acte de manière spectaculaire l'alignement définitif du cadre réglementaire européen sur la réalité technologique foisonnante du marché de la santé numérique.

Pour les fabricants de logiciels dispositifs médicaux, cette révision impose une analyse d'écart urgente et rigoureuse de l'ensemble de leur portefeuille de produits et de leur Système de Management de la Qualité (« SMQ »). Les implications opérationnelles jalonnent l'ensemble du cycle de vie du dispositif :

1. **Refonte de la stratégie réglementaire et de la destination** : l'intransigeance renforcée sur la règle 11, et tout particulièrement la requalification formelle de la « prévention » en acte

d'aide au diagnostic, témoigne de la primauté absolue accordée par le régulateur européen à la sécurité des patients face aux dérives possibles des allégations marketing. De nombreux logiciels de prévention, jusqu'alors confortablement installés en classe I, devront migrer vers la classe IIa, nécessitant la constitution de dossiers techniques complexes, des évaluations cliniques robustes en vie réelle (RWD) et l'intervention coûteuse d'organismes notifiés.

2. **Maîtrise de l'ingénierie modulaire** : l'élaboration détaillée sur la modularité (Section 7) offre une voie de passage pragmatique aux industriels développant des plateformes hospitalières complexes. Cependant, cette souplesse réglementaire est conditionnée à une excellence en matière d'ingénierie logicielle (IEC 62304) : la ségrégation technique entre les modules médicaux et non médicaux doit être documentée, auditée et prouvée comme étant infaillible.
3. **Mise en conformité croisée (MDR, AI Act, EEDS)** : en abandonnant la notion géographique de « logiciel autonome » au profit d'une analyse fonctionnelle centrée sur l'algorithme, en intégrant formellement l'intelligence artificielle (MDAI) dans son périmètre, et en tissant des liens réglementaires serrés avec l'AI Act et le règlement sur l'Espace européen des données de santé, le MDCG impose une vision holistique. Le fabricant ne répond plus seulement au MDR ; il devient un acteur de la donnée européenne, responsable de l'explicabilité de ses algorithmes et de la cybersécurité des flux d'informations transitant par les dossiers médicaux électroniques.

En définitive, pour l'écosystème de la santé numérique en Europe, ce guide révisé constitue une boussole incontournable. Il exige une maturité réglementaire transversale, où l'ingénierie informatique, l'expertise en cybersécurité, l'éthique de la gouvernance des données et l'évaluation clinique doivent fusionner dès l'idéation du produit. Si le fardeau de la preuve imposé à l'industrie est particulièrement lourd, il constitue la condition politique et juridique sine qua non pour asseoir la confiance absolue des professionnels de santé et des patients dans les technologies qui façonneront la médecine prédictive, préventive et personnalisée de demain.

Le défi du fabricant n'est plus seulement de concevoir un code informatique performant, mais de garantir son intégrité au sein d'un espace de santé européen devenu unifiant, complexe et hautement interconnecté.

MDCG 2019-11 rev.1 - Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746.

L'évaluation clinique commune des dispositifs médicaux à l'épreuve de la pratique

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

L'intégration européenne dans le domaine de la santé numérique et des technologies médicales franchit une nouvelle étape décisive avec l'adoption, le 17 octobre 2025, du règlement d'exécution (UE) 2025/2086 de la Commission européenne[188]. Ce texte, particulièrement attendu par l'écosystème de l'innovation médicale, établit les règles de procédure détaillées applicables à l'interaction au cours des évaluations cliniques communes (ci-après « ECC ») des dispositifs médicaux (« DM ») et des dispositifs médicaux de diagnostic in vitro (« DMDIV ») au niveau de l'Union européenne. Il s'inscrit dans le prolongement direct et opérationnel du règlement (UE) 2021/2282 concernant l'évaluation des technologies de la santé (ci-après « règlement ETS » ou « HTA Regulation »)[189], qui vise à harmoniser les méthodologies d'évaluation à l'échelle des Vingt-Sept.

Historiquement, l'évaluation des technologies de la santé au sein de l'Union européenne se caractérisait par une fragmentation institutionnelle et méthodologique préjudiciable. Les Etats membres opéraient selon des doctrines disparates, imposant aux développeurs de technologies de la santé (« DTS ») de soumettre de multiples dossiers cliniques pour accéder aux différents marchés nationaux. Cette duplication des efforts non seulement générait une charge administrative et financière considérable pour l'industrie, mais retardait également l'accès des patients aux innovations médicales cruciales. Si le règlement ETS est entré en application de manière échelonnée depuis le 12 janvier 2025 pour les médicaments contenant de nouvelles substances actives en oncologie et les thérapies innovantes, le présent règlement d'exécution 2025/2086 vient parachever l'édifice juridique permettant d'étendre ce mécanisme centralisé aux technologies médicales les plus innovantes et complexes.

La philosophie sous-jacente à ce nouveau cadre normatif est double. D'une part, il s'agit de garantir que les évaluations cliniques communes soient menées selon les standards scientifiques les plus rigoureux, en mutualisant l'expertise clinique et épidémiologique des Etats membres. D'autre part, il convient de préserver la souveraineté des Etats membres quant aux décisions relatives à la tarification, au remboursement et à l'organisation de leurs systèmes de soins, des prérogatives qui demeurent une compétence strictement nationale en vertu du principe de subsidiarité. L'évaluation clinique commune se limite ainsi à l'analyse de la sécurité, de l'efficacité et de la valeur clinique ajoutée, sans empiéter sur l'évaluation économique (coût-efficacité)

[188] Règlement d'exécution (UE) 2025/2086 de la Commission du 17 octobre 2025 établissant, conformément au règlement (UE) 2021/2282 concernant l'évaluation des technologies de la santé, les règles de procédure applicables à l'interaction au cours des évaluations cliniques communes de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro au niveau de l'Union, à l'échange d'informations concernant l'élaboration et la mise à jour de ces évaluations et à la participation à ces dernières, ainsi que des modèles pour ces évaluations cliniques communes, *JOUE* du 20 octobre 2025.

[189] Règlement (UE) 2021/2282 du Parlement européen et du Conseil du 15 décembre 2021 concernant l'évaluation des technologies de la santé et modifiant la directive 2011/24/UE, *JOUE* L. 458 du 22 décembre 2021.

qui reste l'apanage des agences nationales telles que la Haute Autorité de santé (HAS) en France ou le G-BA en Allemagne.

Le texte délimite avec une grande précision les obligations incombant aux développeurs, le rôle central du groupe de coordination des États membres, la fonction de secrétariat assurée par l'Agence européenne des médicaments (« EMA »), ainsi que la contribution indispensable des organismes notifiés et des experts individuels. L'analyse de ce règlement révèle une architecture procédurale sophistiquée, rythmée par des délais impératifs et structurée autour de modèles de dossiers standardisés.

Toutefois, la transition d'un système d'évaluation national à un modèle supranational soulève des défis opérationnels et stratégiques majeurs pour les fabricants de dispositifs médicaux. À l'aune des thématiques portées par le droit européen du numérique en santé, ce commentaire propose une analyse exhaustive et doctrinale du règlement d'exécution (UE) 2025/2086, en décryptant ses mécanismes juridiques, ses implications pratiques pour les industriels (notamment face à l'intégration de l'intelligence artificielle), et les garanties procédurales entourant la protection des données et le secret des affaires.

I. L'ARCHITECTURE DE LA SÉLECTION : CIBLER L'INNOVATION DE RUPTURE ET LE BESOIN MÉDICAL NON SATISFAIT

L'évaluation clinique commune n'a pas vocation à s'appliquer à l'exhaustivité des dispositifs médicaux mis sur le marché européen. Une telle approche engorgerait instantanément le système. Le mécanisme repose sur un processus de sélection rigoureux, visant à concentrer les ressources de l'Union sur les technologies présentant le plus fort potentiel d'impact sur la santé publique et l'organisation des soins.

A. Les critères d'éligibilité matérielle et la dimension numérique

Conformément à l'articulation entre le règlement ETS et le présent règlement d'exécution, le champ d'application matériel de l'évaluation clinique commune est circonscrit aux dispositifs médicaux à haut risque. Sont ainsi concernés les dispositifs médicaux relevant des classes IIb et III au sens du règlement (UE) 2017/745 (« MDR » acronyme anglais pour *medical device regulation*)[190], ainsi que les dispositifs médicaux de diagnostic in vitro de classe D au sens du règlement (UE) 2017/746 (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[191]. Cette limitation aux classes de risque les plus élevées témoigne d'une volonté de proportionnalité dans l'action de l'Union.

Cependant, l'appartenance à ces classes de risque constitue une condition nécessaire mais non suffisante. La sélection s'opère *in fine* sur la base de critères cumulatifs ou alternatifs stricts, reflétant les priorités de santé publique et technologiques de l'Union. Les dispositifs retenus doivent répondre à l'un ou plusieurs des critères suivants :

- premièrement, la réponse à des besoins médicaux non satisfaits ou la qualification de premier de leur catégorie thérapeutique (« *first-in-class* ») ;
- deuxièmement, et c'est ici que le droit des dispositifs médicaux croise le droit du numérique en santé, l'intégration de logiciels fondés sur

[190] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, *JOUE* L. 117 du 5 mai 2017.

[191] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, *JOUE* L. 117 du 5 mai 2017.

l'intelligence artificielle (« IA »), les technologies d'apprentissage automatique (*machine learning*) ou des algorithmes complexes. Cette inclusion spécifique de l'IA démontre la prise de conscience par le législateur européen de la nécessité d'évaluer de manière rigoureuse et centralisée les dispositifs médicaux numériques (Software as a Medical Device - SaMD), dont les performances algorithmiques peuvent avoir des répercussions cliniques majeures ;

- troisièmement, la présence d'une dimension transfrontalière pertinente, une valeur ajoutée significative à l'échelle de l'Union, ou des implications majeures pour l'organisation des systèmes de soins et les patients.

B. Le rôle du groupe de coordination et la procédure de recommandation

L'article 7, paragraphe 4, du règlement (UE) 2021/2282 confie à la Commission la compétence d'adopter, au moins tous les deux ans, une décision d'exécution actant la sélection définitive des dispositifs soumis à l'évaluation clinique commune. Cette décision souveraine est toutefois organiquement conditionnée par une recommandation préalable du groupe de coordination des États membres sur l'évaluation des technologies de la santé.

Ce groupe de coordination ne statue pas de manière isolée ou arbitraire ; il fonde ses recommandations sur l'expertise technique des groupes d'experts désignés au titre de l'article 106, paragraphe 1, du règlement (UE) 2017/745[192]. L'EMA, agissant en qualité de secrétariat de l'ETS, joue ici un rôle de courroie de transmission central. Le règlement d'exécution 2024/2699 lui impose de fournir à la Commission les informations sur les avis scientifiques de ces groupes d'experts au plus tard 15 jours après la fin de chaque trimestre[193].

L'article 2 du règlement 2025/2086 institue une obligation d'information proactive. Dès l'adoption de la recommandation par le groupe de coordination, le secrétariat de l'ETS a l'obligation d'informer les développeurs de technologies de la santé quant à la sélection ou la non-sélection de leur dispositif. En cas de sélection, cette notification doit impérativement être assortie des raisons ayant conduit à cette recommandation. Cette exigence de motivation est fondamentale : elle garantit le respect du droit à une bonne administration et offre aux industriels la visibilité stratégique indispensable pour anticiper la préparation de leur dossier clinique complexe. À l'inverse, si un dispositif examiné n'est pas retenu, le développeur en est également

---

[192] Cet article précise : *« 1. La Commission, au moyen d'actes d'exécution et en concertation avec le GCDM, veille à ce que des groupes d'experts soient désignés pour évaluer l'évaluation clinique dans les différentes disciplines médicales, conformément au paragraphe 9 du présent article, et pour communiquer leurs points de vue sur l'évaluation des performances de certains dispositifs médicaux de diagnostic in vitro, conformément à l'article 48, paragraphe 6, du règlement (UE) 2017/746 et, au besoin, pour des catégories ou groupes de dispositifs, ou pour des dangers particuliers liés à des catégories ou groupes de dispositifs, dans le respect des principes des compétences scientifiques, de l'impartialité, de l'indépendance et de la transparence les plus élevées. Les mêmes principes s'appliquent lorsque la Commission décide de désigner des laboratoires spécialisés conformément au paragraphe 7 du présent article ».*

[193] Article 3, paragraphe 2 du règlement d'exécution (UE) 2024/2699 de la Commission du 18 octobre 2024 établissant, en application du règlement (UE) 2021/2282 du Parlement européen et du Conseil, les règles de procédure détaillées applicables à la coopération du groupe de coordination des États membres sur l'évaluation des technologies de la santé et la Commission avec l'Agence européenne des médicaments sous forme d'échange d'informations en ce qui concerne l'évaluation clinique commune des médicaments, des dispositifs médicaux et des dispositifs médicaux de diagnostic in vitro et en ce qui concerne la consultation scientifique commune sur les médicaments et les dispositifs médicaux, *JOUE du 21 octobre 2024.*

informé afin de préserver la sécurité juridique de ses opérations de mise sur le marché nationales.

II. LA SYNERGIE PROCÉDURALE : L'INTÉRACTION ENTRE LA CERTIFICATION ET L'ÉVALUATION

L'un des apports doctrinaux et opérationnels majeurs du règlement d'exécution 2025/2086 réside dans sa volonté d'arrimer la procédure d'évaluation clinique commune au calendrier de la certification de conformité (marquage CE), tout en préservant l'étanchéité et la stricte confidentialité de ce dernier processus. Ce séquençage est le point névralgique de la réforme, car il conditionne le délai d'accès au marché.

A. La gestion de la confidentialité et le lancement de l'évaluation

Le considérant 3 du règlement rappelle une contrainte juridique forte : la confidentialité inhérente au processus de certification par les organismes notifiés interdit à la Commission de lancer l'adoption de la décision de sélection avant l'achèvement complet dudit processus. La divulgation prématurée d'informations relatives à un dispositif en cours de certification constituerait une violation du secret des affaires et pourrait fausser le jeu de la concurrence.

Toutefois, le considérant 4 expose la nécessité d'un équilibre. Pour éviter que l'ECC n'accuse un retard qui serait in fine préjudiciable aux patients et à la compétitivité du marché européen, l'évaluation doit impérativement débuter dès que le certificat de conformité est formellement délivré au titre du MDR ou de l'IVDR. Ce lancement « en flux tendu » impose une coordination logistique et informationnelle inédite entre des acteurs jusqu'alors cloisonnés : les organismes notifiés, l'EMA (secrétariat de l'ETS) et les développeurs.

B. Les obligations de notification et le rôle pivot d'EUDAMED

L'article 4 du règlement d'exécution crée une obligation de communication en temps réel à la charge des organismes notifiés. Ces derniers doivent informer le secrétariat de l'ETS des résultats du processus de certification pour tout dispositif figurant dans la recommandation du groupe de coordination. Cette notification (octroi du certificat, refus, ou retrait de la demande) doit intervenir dans un délai extrêmement bref de sept jours.

En miroir, l'article 3 impose au développeur de technologies de la santé dont le dispositif a été recommandé de fournir au secrétariat de l'ETS le certificat de conformité et la notice d'utilisation certifiée, également dans un délai de sept jours suivant la délivrance ou la requête du secrétariat. De surcroît, le sous-groupe sur les évaluations cliniques communes (sous-groupe ECC) peut exiger du développeur des informations additionnelles jugées nécessaires pour la détermination du périmètre de l'évaluation.

Cependant, le législateur européen, conscient de la charge administrative pesant sur l'industrie – une préoccupation vivement relayée par MedTech Europe – a introduit un principe de *« dites-le-nous une fois »* (en anglais *once-only principle*). L'article 3, paragraphe 4, et l'article 4, paragraphe 3, mentionnent que les organismes notifiés et les DTS sont dispensés de cette transmission documentaire directe si les informations requises sont déjà dûment et pleinement accessibles dans la base de données européenne sur les dispositifs médicaux (« EUDAMED »), conformément aux articles 33 du MDR et 30 de l'IVDR.

Cette disposition consacre le rôle central d'EUDAMED comme clé de voûte de l'écosystème réglementaire européen de la santé. D'un point de vue pratique pour les fabricants, la maîtrise des composants de l'Identification Unique des Dispositifs (ou *unique device identification* -UDI) – tels que le Basic UDI-DI, l'UDI-DI et l'UDI-PI

– devient cruciale, car toute erreur de catégorisation ou de hiérarchisation dans EUDAMED pourrait bloquer la conformité et retarder le déclenchement de l'ECC. L'automatisation des transferts de données via des interfaces machine-to-machine vers EUDAMED apparaît ainsi comme un levier stratégique indispensable pour sécuriser ce flux d'informations critiques.

C. Le traitement des situations exceptionnelles

Le règlement anticipe l'éventualité de discordances politiques ou scientifiques entre la recommandation du groupe de coordination et la décision finale de la Commission. Lorsque la Commission décide, dans des cas particuliers justifiés (article 7, paragraphe 4 du règlement ETS), de sélectionner un dispositif médical qui n'avait pas été recommandé initialement, l'article 2, paragraphe 2, du règlement d'exécution entre en jeu. Le secrétariat de l'ETS notifie immédiatement le DTS de cette décision inopinée.

Le développeur est alors astreint aux mêmes obligations de transmission documentaire dans les sept jours, assurant ainsi qu'aucun dispositif d'intérêt public majeur n'échappe à l'évaluation clinique commune pour des raisons purement procédurales ou de désaccord institutionnel préalable.

III. LA DÉTERMINATION DU PÉRIMÈTRE DE L'ÉVALUATION : LA CRISTALLISATION DES BESOINS CLINIQUES EUROPÉENS

La phase de détermination du périmètre de l'évaluation (« *scoping* ») constitue le cœur stratégique et scientifique de l'ECC. Elle a pour objet de déterminer avec précision les questions de recherche auxquelles le rapport clinique final devra répondre, conditionnant ainsi l'utilité pratique du rapport pour les autorités nationales de remboursement. Si le périmètre est mal défini, l'évaluation risque de ne pas répondre aux exigences spécifiques d'un Etat membre, forçant ce dernier à exiger des évaluations nationales complémentaires, ce qui ruinerait l'objectif même du règlement.

A. La méthodologie PICO et l'élaboration de la proposition

Le règlement d'exécution 2025/2086 structure cette phase fondamentale autour de la méthodologie PICO (Population de patients, Intervention, Comparateurs, Résultats de santé ou Outcomes).

La procédure s'enclenche formellement à l'article 7 : dès que le sous-groupe ECC désigne un évaluateur et un coévaluateur parmi les experts des Etats membres, le secrétariat informe le développeur du début du processus. L'article 11 précise ensuite que l'évaluateur, assisté de son coévaluateur, est chargé d'élaborer une première « proposition de périmètre ».

La construction de ce cadre de référence s'appuie sur la notice d'utilisation certifiée transmise par le fabricant, mais également sur l'historique réglementaire du dispositif. En effet, l'évaluateur doit obligatoirement consulter le document final de consultation scientifique si le dispositif a fait l'objet d'une consultation scientifique commune préalable (JSC - *Joint Scientific Consultation*) au titre des articles 16 à 21 du règlement ETS. L'avis scientifique initial rendu par les groupes d'experts du MDR est également intégré à la réflexion.

La difficulté institutionnelle inhérente au processus de *scoping* européen réside dans la disparité historique des pratiques cliniques et des comparateurs exigés à travers les différents Etats membres. Afin d'atteindre l'objectif explicite du considérant 16 — à savoir traduire les besoins légitimes de tous les Etats membres par le *« plus petit nombre possible d'ensembles de paramètres de l'évaluation »* — la proposition initiale est partagée via la plateforme informatique de l'ETS avec l'ensemble des membres du sous-groupe ECC. Sur la base de leurs retours, une proposition consolidée est

établie, censée synthétiser l'exigence clinique européenne.

B. L'implication des experts et la finalisation du périmètre

Le processus de *scoping* intègre formellement la consultation d'experts indépendants pour ancrer l'évaluation dans la réalité clinique et le vécu des patients. L'article 11, paragraphe 3, impose au secrétariat de l'ETS de partager la proposition consolidée avec des experts cliniques et des représentants de patients préalablement sélectionnés, leur offrant la possibilité d'apporter des contributions substantielles.

L'article 12 encadre strictement la temporalité de cette phase. La finalisation du périmètre s'opère lors d'une réunion de consolidation du sous-groupe ECC. Le délai de rigueur est fixé à 60 jours maximum après la réception des informations post-certification, ou 10 jours après l'adoption de la décision de la Commission portant sélection du dispositif, l'échéance la plus tardive s'appliquant.

Afin de garantir le respect du principe du contradictoire et de clarifier les attentes méthodologiques, l'article 13 octroie une prérogative essentielle au développeur : ce dernier peut solliciter une « réunion d'explication du périmètre de l'évaluation » en présence du sous-groupe ECC. Cette réunion doit se tenir dans les 20 jours suivant la finalisation du périmètre.1 Sur le plan opérationnel, cette étape est vitale pour les équipes d'accès au du fabricant, car elle permet de dissiper les ambiguïtés sur les comparateurs exigés et de structurer l'analyse des données cliniques en conséquence.

IV. LE FARDEAU PROBATOIRE ET LES CONTRAINTES TEMPORELLES : LE DÉFI DU DOSSIER A 100 JOURS

Une fois le périmètre formellement figé, la charge de la preuve repose intégralement sur le développeur, qui doit démontrer la valeur clinique de son dispositif au regard des multiples paramètres PICO retenus. Cette étape cristallise les plus vives inquiétudes de l'industrie.

A. La règle couperet des 100 jours

L'article 14 du règlement d'exécution fixe un délai de 100 jours, courant à compter de la notification de la demande de la Commission, pour que le développeur soumette sous forme numérique le dossier complet de l'évaluation clinique.

Ce délai de 100 jours représente un défi opérationnel colossal. Dans la pratique, le périmètre PICO consolidé au niveau européen peut intégrer des sous-populations de patients ou des comparateurs (souvent des traitements médicamenteux ou des chirurgies alternatives) qui n'étaient pas les comparateurs primaires étudiés lors des essais cliniques originaux menés par le fabricant pour l'obtention de son marquage CE.

Le fabricant se trouve alors dans l'obligation de produire, en un peu plus de trois mois, de nouvelles synthèses de données.

Face à cette contrainte temporelle sévère, la réalisation de nouveaux essais cliniques est matériellement impossible. Les industriels devront impérativement s'appuyer sur des revues systématiques de la littérature de dernière minute, des méta-analyses en réseau et des comparaisons indirectes de traitements pour combler les vides probatoires entre leurs données cliniques et les exigences du PICO européen.

Les analystes du secteur anticipent que les entreprises, en particulier les PME dont les ressources réglementaires sont limitées, devront massivement recourir à l'intelligence artificielle générative et à des outils analytiques avancés pour simuler de multiples PICO, cartographier les preuves existantes et automatiser la rédaction des

trames documentaires dans les temps impartis[194].

Le législateur a toutefois prévu une soupape de sécurité, bien que minime. L'article 14, paragraphe 3, permet au secrétariat de l'ETS, avec l'accord des évaluateurs, de prolonger ce délai initial de 30 jours maximum dans des cas dument justifiés.

B. Les exigences formelles et le dialogue itératif

Le format du dossier n'est pas libre. L'annexe I du règlement 2025/2086 définit un modèle impératif extrêmement détaillé pour les dispositifs médicaux, aligné sur les principes stricts de la médecine factuelle. Le développeur doit documenter l'historique des révisions, fournir une synthèse des données probantes ventilées par paramètre PICO, justifier méthodologiquement tout écart par rapport aux orientations du groupe de coordination, et caractériser minutieusement l'état pathologique, la population visée, et le parcours de soins actuel en Europe. S'il omet des données pour un PICO spécifique, il a l'obligation d'en expliquer les raisons.

Le règlement organise ensuite un dialogue itératif, soumis à des délais drastiques, pour pallier les éventuelles lacunes du dossier soumis. A la suite de la soumission, la Commission dispose de 15 jours ouvrables pour confirmer si le dossier respecte les exigences formelles de l'article 9 du règlement ETS.

Si la Commission identifie des informations manquantes lors de cette vérification (la « deuxième demande »), l'article 14, paragraphe 4, n'octroie au développeur que 15 jours pour les fournir. Ce délai est même réduit à 7 jours si la Commission estime que seules des « informations mineures » font défaut. De plus, au cours de la phase d'évaluation elle-même, les évaluateurs peuvent exiger des clarifications ou des analyses supplémentaires (article 14, paragraphe 5). Le délai pour répondre est fixé par les évaluateurs eux-mêmes en fonction de la complexité de la demande, mais il ne peut être inférieur à 7 jours ni excéder 30 jours.

Ces fenêtres de tir d'une extrême brièveté exigent des industriels de maintenir des équipes d'experts cliniques et de statisticiens mobilisées et en alerte maximale tout au long de la procédure d'évaluation.

V. LA PHASE D'ÉVALUATION : L'ÉLABORATION DES RAPPORTS, LES GARANTIES DE TRANSPARENCE ET LA PROTECTION DU SECRET DES AFFAIRES

La traduction de l'évaluation clinique en un livrable opposable s'effectue par la rédaction du rapport d'évaluation clinique commune et de son rapport de synthèse. Cette phase confronte les impératifs de transparence publique aux exigences légitimes de protection des intérêts commerciaux.

A. La rédaction et les droits limités de l'industriel

L'article 16 encadre la rédaction des projets de rapports par l'évaluateur et le coévaluateur, en utilisant les modèles standardisés des annexes III, IV et V. Au cours de ce processus, l'avis des experts individuels (cliniciens et patients) est à nouveau sollicité, et les projets sont transmis au sous-groupe ECC pour recueil d'observations.

Le règlement octroie une garantie procédurale au développeur, mais en circonscrit strictement la portée. Conformément à l'article 16, paragraphe 4, le secrétariat de l'ETS transmet les projets

[194] Costello Medical, *Navigating the Challenges of Joint Clinical Assessment for Advanced Therapy Medicinal Products: Harmonising or Hampering HTA?*, https://www.costellomedical.com/what-we-do/value-and-access/challenges-for-advanced-therapy-medicinal-products/, dernier accès le 25 avril 2026.

révisés au développeur. Ce dernier ne dispose alors que de 7 jours pour réagir. Son intervention est cantonnée à deux actions exclusives :

1. Signaler les inexactitudes « purement techniques ou factuelles ».
2. Identifier les informations qu'il considère comme confidentielles, à charge pour lui de démontrer rigoureusement leur « caractère commercialement sensible ».

Il est fondamental de souligner que ce délai et ce cadre juridique interdisent au fabricant de contester le fond des conclusions scientifiques ou méthodologiques de l'évaluation à ce stade. La relecture est un simple contrôle de matérialité et de confidentialité.

B. L'intégration des données de vie réelle en cours d'évaluation

La nature des dispositifs médicaux implique une génération continue de données cliniques via les études de suivi clinique après commercialisation (SCAC ou en anglais PMCF). L'article 16, paragraphe 5, appréhende cette dynamique en prévoyant un mécanisme d'inclusion des données nouvelles survenant pendant l'évaluation.

Si le développeur soumet de nouvelles données cliniques de sa propre initiative, le sous-groupe ECC met « tout en œuvre » pour les prendre en considération. La contrainte devient absolue si ces nouvelles données parviennent au secrétariat au plus tard 60 jours après la confirmation par la Commission de la conformité formelle du dossier initial : dans ce cas, le sous-groupe a l'obligation d'intégrer ces données à son analyse. Cette disposition est favorable à l'industrie, lui permettant de consolider son dossier avec les résultats d'essais cliniques fraîchement publiés.

C. La finalisation temporelle des rapports

L'article 17 fixe la temporalité globale de la phase d'évaluation. Le sous-groupe ECC est tenu de finaliser les projets révisés dans les 165 jours suivant la confirmation de la recevabilité du dossier par la Commission. Une fois finalisés, ces documents sont transmis au groupe de coordination pour approbation formelle. En vertu de l'article 12, paragraphe 2, du règlement ETS, ce groupe dispose de 30 jours pour les endosser (**Page suivante**).

Le tableau ci-dessous résume les différentes phases d'évaluation et le calendrier qui y est associé :

Phase de la procédure d'ECC	Acteur responsable	Délai prescrit ou imparti
Finalisation du périmètre (*Scoping*)	Sous-groupe ECC	Max. 60 jours après réception des données post-certification
Soumission du dossier clinique	Développeur (DTS)	100 jours après la demande formelle (extensible de 30 jours)
Vérification de recevabilité	Commission européenne	15 jours ouvrables après la soumission du dossier
Intégration obligatoire de données nouvelles	Sous-groupe ECC	Données reçues max. 60 jours après la confirmation de recevabilité
Relecture pour confidentialité/erreurs	Développeur (DTS)	7 jours après réception des projets de rapports révisés
Finalisation des rapports	Sous-groupe ECC	165 jours après la confirmation de recevabilité du dossier
Approbation finale	Groupe de coordination	30 jours après réception des rapports finalisés.

De la soumission du dossier recevable jusqu'à l'approbation finale, la phase d'évaluation s'étend donc sur une durée maximale de 195 jours (165 + 30). Ce calendrier serré démontre la volonté de l'Union de ne pas entraver l'accès au marché, tout en exerçant une pression capacitaire immense sur les agences nationales d'évaluation. Pour soutenir cet effort massif, l'Agence exécutive européenne pour la santé et le numérique (« HaDEA ») a d'ailleurs signé en janvier 2025 un contrat-cadre de 35 millions d'euros avec un consortium de 21 pays européens (mené par l'INAMI-RIZIV belge) chargé de mener matériellement ces évaluations et consultations conjointes[195].

D. Le traitement des données : Secret des affaires et RGPD

La publication des rapports d'ECC et des rapports de synthèse constitue l'aboutissement de la procédure, assurant la transparence requise par le public et les professionnels de la santé. Cependant, le règlement encadre minutieusement cette divulgation pour protéger le secret des affaires. L'article 21 précise que la publication n'intervient qu'après examen par la Commission de l'avis du sous-groupe ECC concernant les requêtes de confidentialité formulées par le développeur.

Afin de prévenir tout contentieux, la Commission doit fournir au développeur, avant publication, la liste des informations qu'elle refuse de considérer comme confidentielles, en l'informant explicitement de son droit de former un recours administratif ou juridictionnel contre ce refus d'expurgation.

En matière de protection des données à caractère personnel (« RGPD »), l'article 22 désigne la Commission comme

[195] HaDEA, *From theory to practice: implementing the EU Health Technology Assessment Regulation*, 22 January 2025.

responsable du traitement. Il établit des règles strictes : l'identité et les données de santé des patients impliqués dans les ECC ne sont jamais publiées. Les données personnelles des experts et représentants sont conservées pour une durée n'excédant pas 15 ans après la cessation de leur participation (ou 3 ans s'ils n'ont pas été sélectionnés). Enfin, l'indépendance de l'expertise est garantie par l'obligation, pour chaque expert individuel, de signer un accord de confidentialité et de faire l'objet d'une évaluation rigoureuse de ses intérêts déclarés (conflits d'intérêts) par la Commission (article 8 et 9).

VI. L'ADAPTABILITÉ DU CADRE : LES MISES A JOUR DE L'ÉVALUATION ET L'ENJEU DE L'INTÉLLIGENCE ARTIFICIELLE

L'évaluation d'un dispositif médical n'est pas un acte statique, mais s'inscrit dans un continuum lié au cycle de vie du produit. Ce principe est particulièrement pertinent pour les dispositifs numériques intégrant des algorithmes d'intelligence artificielle adaptative (*machine learning*), dont les performances et l'impact clinique peuvent évoluer de manière significative après leur déploiement initial en vie réelle.

L'article 19 du règlement d'exécution 2025/2086 orchestre les modalités de mise à jour des évaluations cliniques communes. Une réévaluation peut être déclenchée selon deux voies distinctes. Soit elle était explicitement requise dans le rapport d'évaluation clinique initial (par exemple, dans l'attente des résultats finaux d'un registre de cohorte ou d'une étude à long terme), soit elle est sollicitée à l'initiative du développeur lui-même, qui transmet de nouvelles données probantes susceptibles d'améliorer son évaluation. Dans ce second scénario, le groupe de coordination dispose d'un pouvoir discrétionnaire pour inclure, ou non, cette mise à jour dans son programme de travail annuel.

D'un point de vue procédural, le sous-groupe ECC s'attache à désigner les mêmes évaluateurs et experts que lors de l'évaluation originelle, afin de capitaliser sur la connaissance préexistante du dossier. Une étape décisionnelle cruciale intervient alors : le sous-groupe doit statuer sur la nécessité, ou non, de modifier le périmètre de l'évaluation (le PICO). Si le périmètre clinique demeure inchangé, le processus de révision s'enclenche immédiatement sur la base du dossier mis à jour (délais de 165 jours pour les rapports). À l'inverse, si l'évolution des pratiques médicales ou des caractéristiques du dispositif justifie une mise à jour du périmètre, une nouvelle phase de *scoping* est ouverte, nécessitant la consultation des Etats membres (avec un délai de 60 jours pour finaliser ce nouveau périmètre). La finalisation des rapports actualisés s'étend alors jusqu'à 345 jours à compter de la décision de mise à jour par le groupe de coordination.

L'intégration de ce mécanisme de mise à jour est fondamentale pour l'industrie. Elle permet d'adapter l'évaluation des logiciels dispositifs médicaux (SaMD) qui, de par leur nature, font l'objet d'itérations fréquentes (mises à jour logicielles, amélioration des algorithmes d'IA) altérant potentiellement leur profil clinique.

Conclusion

Le règlement d'exécution (UE) 2025/2086 marque une rupture doctrinale et opérationnelle majeure dans l'appréhension de l'innovation médicale au sein de l'Union européenne. En substituant un processus d'évaluation clinique rationnel et centralisé à la myriade de procédures nationales, la Commission européenne entend positionner l'Europe comme un marché unifié et prévisible, capable de valoriser et d'absorber rapidement les thérapies les plus disruptives, à l'instar des dispositifs embarquant de l'intelligence artificielle.

La codification méticuleuse des délais procéduraux, des obligations de transparence institutionnelle et des droits de la défense accordés aux développeurs – notamment via le respect du contradictoire

et la protection des secrets d'affaires – démontre une volonté manifeste de sécuriser juridiquement le dispositif. Par ailleurs, l'arrimage de ce processus à l'infrastructure numérique de la base de données EUDAMED consacre l'interopérabilité des systèmes d'information réglementaires à l'échelle de l'Union.

Toutefois, l'efficience théorique de ce cadre réglementaire se heurtera inévitablement à l'épreuve de la réalité opérationnelle. Les réserves émises par les acteurs de l'industrie, notamment MedTech Europe, mettent en lumière le risque d'une charge administrative asymétrique. L'extrême rigidité des délais impartis aux développeurs (la règle des 100 jours), combinée à l'étendue potentielle et hétérogène des périmètres d'évaluation (PICO) générés par la synthèse des besoins de vingt-sept Etats membres, exigera un changement de paradigme stratégique profond au sein des entreprises. Le recours aux outils numériques d'analyse prédictive et à l'intelligence artificielle pour générer les preuves cliniques indirectes requises deviendra un impératif de survie, tout particulièrement pour les PME.

Il appartiendra aux premières évaluations cliniques communes de dispositifs médicaux, dont les prémices étaient prévues pour le premier trimestre 2026, de démontrer si ce nouvel édifice normatif parvient effectivement à concilier l'exigence de rigueur scientifique des autorités de santé avec l'agilité indispensable au déploiement de l'innovation médicale au bénéfice des patients européens.

Règlement d'exécution n° 2025/2086/UE du 17 octobre 2025 établissant, conformément au règlement n° 2021/2282/UE concernant l'évaluation des technologies de la santé, les règles de procédure applicables à l'interaction au cours des évaluations cliniques communes de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro au niveau de l'Union, à l'échange d'informations concernant l'élaboration et la mise à jour de ces évaluations et à la participation à ces dernières, ainsi que des modèles pour ces évaluations cliniques communes, *JOUE* n° L 2025/2086 du 20/10/2025.

COMPLÉMENT UTILE

HTA CG, Annual Work Programme 2025, 28 November 2025, document de programmation du *Health Technology Assessment Coordination Group* précisant les priorités de mise en œuvre du règlement (UE) 2021/2282 sur l'évaluation des technologies de santé, notamment en matière d'évaluations cliniques conjointes et de consultations scientifiques conjointes au niveau de l'Union européenne.

EUROPEAN RESPIRATORY SOCIETY

*Fondée en 1990, la European Respiratory Society (ERS) est la principale société savante européenne dédiée à la santé respiratoire. Basée à Lausanne, elle rassemble plus de 35 000 cliniciens, chercheurs, professionnels de santé et experts issus de plus de 160 pays. L'ERS contribue au développement des connaissances scientifiques dans le domaine des maladies respiratoires, soutient la recherche et la formation médicale continue, et élabore des recommandations cliniques destinées à harmoniser les pratiques et à améliorer la prise en charge des patients. Elle publie notamment plusieurs revues scientifiques de référence, dont l'*European Respiratory Journal (ERJ).

Marieke L. DUIVERMAN et *al.*, « European Respiratory Society Clinical Practice Guideline on Telemedicine in Home Mechanical Ventilation », *European Respiratory Journal*, 2025

La *European Respiratory Society (*ERS) a publié en 2025 ses premières lignes directrices consacrées à l'utilisation de la télémédecine dans le cadre de la ventilation mécanique à domicile. Ces recommandations s'inscrivent dans un contexte de développement des soins à distance pour les patients atteints d'insuffisance respiratoire chronique nécessitant une assistance ventilatoire prolongée.

Les auteurs soulignent que les outils de télésurveillance permettent un suivi continu des paramètres ventilatoires, une détection plus précoce des anomalies techniques ou cliniques et une adaptation plus réactive de la prise en charge. Les données disponibles suggèrent également un potentiel de réduction de certaines hospitalisations évitables ainsi qu'une amélioration de la coordination entre les équipes spécialisées et les patients suivis à domicile.

Les recommandations mettent toutefois en évidence l'hétérogénéité des preuves scientifiques actuellement disponibles et soulignent la nécessité de disposer d'infrastructures numériques adaptées, de garanties en matière de protection des données et d'une formation suffisante des professionnels de santé. Elles insistent également sur la poursuite des travaux de recherche afin de mieux documenter l'impact de ces dispositifs sur les résultats cliniques et l'organisation des soins.

Ces lignes directrices constituent une étape importante dans l'encadrement du recours à la télémédecine pour le suivi des patients sous ventilation mécanique à domicile et témoignent de la place croissante des outils numériques dans la prise en charge des pathologies respiratoires chroniques.

Droit français

Principes d'évaluation de la CNEDiMTS

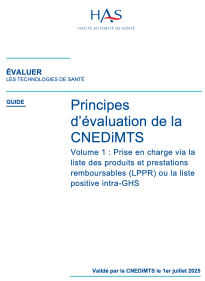
La Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS) a publié une série de quatre volumes consacrés à l'évaluation des dispositifs médicaux numériques (DMN) en vue de leur prise en charge par l'Assurance maladie. Ces documents détaillent les critères d'évaluation et les niveaux de preuve attendus pour démontrer leur intérêt clinique.

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 1 : Prise en charge via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS (1er juillet 2025)

par Marie DESMEULES

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



Le 1er juillet 2025, la commission spécialisée de la Haute Autorité de Santé (H.A.S.), dite Commission Nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS), a publié un guide actualisé sur ses principes d'évaluation, au sein duquel se recoupent quatre volets, dont le premier porte sur les demandes de prise en charge des dispositifs médicaux via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS (groupes homogènes de séjours).

Ce texte poursuit l'idée d'expliciter aux industriels, aux conseils nationaux professionnels de spécialités (CNP), ainsi qu'aux patients et usagers, les principes d'évaluation mis en œuvre par la commission dès que des dossiers lui sont soumis dans le cadre d'une demande d'inscription d'un dispositif médical pour une prise en charge via la LPPR ou la liste positive intra-GHS.

La notion de dispositif médical (D.M.) est précisée par le **règlement européen n° 2017/745/UE** comme « *tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises* ». Leur prise en charge, et donc, leur remboursement par l'assurance maladie, dépend du résultat des évaluations effectuées par la CNEDiMTS, qui sera publié sous la forme d'un avis. Celui-ci répond notamment aux questions suivantes :

** Ce D.M., qu'il soit utilisé à l'hôpital ou en ville, doit-il être pris en charge par la solidarité nationale ?*

** Quelle est la valeur ajoutée du D.M. pour le patient, c'est-à-dire le progrès thérapeutique (au sens large) qu'il apporte par rapport aux thérapeutiques existantes ?*

** Quel est l'effectif de la population pour laquelle le remboursement est justifié et pour laquelle le D.M. représente une valeur ajoutée ?*
** Quel est l'impact de ce D.M. sur la santé publique ?*

Pour répondre à ces interrogations, une évaluation de la CNEDiMTS est réalisée. À titre liminaire, il est souligné qu'en complément des exigences posées par le marquage CE des dispositifs médicaux (qui est une procédure obligatoire attestant de la conformité du produit aux exigences de sécurité, de performance et de bénéfices cliniques), ceux-ci font l'objet d'évaluations complémentaires pour pouvoir être pris en charge. Elles se matérialisent sous deux formes :

1. les **modalités de financement** qui prennent en compte le secteur (ambulatoire, utilisation lors d'actes médicaux ou liée à un handicap) et le type de produit (ceux financés à travers des prestations intra GHS (ce qui équivaut aux prestations d'hospitalisation) ou hors GHS) ;
2. les **types d'inscription sur la LPPR**, dont deux modalités coexistent :
   - L'**inscription sous description générique** qui ne nécessite pas d'évaluation par la CNEDiMTS, mais dont le renouvellement d'inscription nécessite des évaluations périodiques.

Durée de l'inscription : 10 ans

   - L'**inscription sous nom de marque**, qui suppose une évaluation du bien-fondé de la demande, en veillant notamment au respect des conditions de forme tenant à la qualité du dossier et de son contenu.

Durée de l'inscription : 5 ans

De fait, le guide formalise les principes généraux applicables aux évaluations après demandes d'inscription sur la LPPR, et dont leur application est visible sur **deux étapes** :

- **Étape 1** : appréciation de la suffisance ou de l'insuffisance du service attendu ou rendu (SA/SR) par le D.M. afin de déterminer s'il peut être remboursé ou non. Cette appréciation se fait sur la base de deux critères cumulatifs (ou le cas échéant, sur des spécifications techniques et conditions particulières de prescription et d'utilisation) :
  - *l'intérêt du produit* : permet de mesurer l'apport du D.M. en fonction de son effet à l'échelle individuelle et du contexte physiopathologique et de la stratégie de prise en charge de référence du patient.
  - *l'intérêt de santé publique* : permet de mesurer l'apport du D.M. à l'échelle collective, et ce, au regard de divers facteurs tels que : l'épidémiologie de la pathologie (incidence et prévalence), l'impact des D.M. sur la santé publique (effets potentiels-prévisibles, adéquation avec les objectifs des programmes de santé publique), les populations cibles du D.M. susceptibles d'être prises en charge et d'être éligibles au remboursement.

Remarque : l'insuffisance est constatée si : efficacité faible, pas de pertinence clinique, non adéquation aux référentiels CNEDiMTS, association injustifiée de D.M. au sein d'un même conditionnement, etc.

Étape 2 : si le SA/SR est suffisant, alors l'appréciation portera ensuite sur le niveau d'amélioration de celui-ci (ASA/ASR), qui permettra la fixation du prix du D.M., ou plus largement, des seuls produits inscriptibles sur la liste LPPR. Cette évaluation se réalise par rapport à des actes ou prestations comparables précisément désignés et considérés comme une référence selon les données actuelles de la science (DAS). Autrement dit, il s'agit de mettre en évidence le bénéfice supplémentaire apporté par le nouveau produit par rapport aux traitements

thérapeutiques spécifiquement indiqués. La commission devra alors s'appuyer sur des données cliniques analysées selon les critères de la médecine fondée sur la preuve ; et choisir le comparateur convenable à l'étude, selon la stratégie de référence et les DAS. Ainsi, le niveau d'ASA/ASR pourra être déterminé sur la base des résultats cliniques ; éléments probatoires apportés par le demandeur d'inscription ; montrant la supériorité clinique du D.M. par rapport au comparateur. À l'issue de cette évaluation, la commission attribue, en raison d'une amélioration constatée (efficacité, réduction de risque, commodité d'emploi, qualité de vie, impact organisationnel, etc.), un niveau d'ASA/ASR (niveau I : amélioration majeure, niveau II : amélioration importante, niveau III : amélioration modérée, niveau IV : amélioration mineure). Sinon, à défaut d'éléments de preuve suffisants, la commission prononce l'absence d'ASA/ASR.

Dans le cadre de ces multiples évaluations, la CNEDiMTS peut avoir recours à une expertise extérieure pour un éclairage sur le contexte physiopathologique, sur la stratégie thérapeutique de référence et sur la pratique clinique, et ceci, formulé dans un rapport écrit. Elle peut également faire appel d'une part, au CNP pour une consultation alternative ou complémentaire à l'expertise extérieure, lequel se positionne en fonction des pratiques professionnelles et des recommandations ; et d'autre part, aux patients et usagers dont la participation est protéiforme : présence de membres associatifs choisis, audition, ou contribution spontanée d'association après le remplissage d'un questionnaire générique. L'implication de ces derniers offre une vision plus large de l'impact de la maladie, de l'état de santé, etc.

Remarques : la qualité de vie est un critère important pour la CNEDiMTS (notamment pour l'évaluation de l'ASA/ASR), complémentaire à celui de la morbi-mortalité, mais qui reste difficile à établir faute de données ou en raison de la faiblesse méthodologique du recueil de ce paramètre dans les études cliniques qui lui sont soumises. Ce critère peut être mesuré par le biais d'échelles validées (génériques ou spécifiques). De plus, sa pertinence dépend de la finalité du D.M.. Il peut donc aussi bien se présenter comme critère de jugement principal que comme critère de jugement secondaire, ce qui peut évoluer après avoir mené des études post-inscription. L'impact organisationnel d'une technologie de santé concerne ses effets cliniques, notamment sur la qualité de vie, avec des répercussions positives ou négatives, à l'échelle individuelle ou collective. Sa reconnaissance repose sur les incidences portées au processus de soins, aux compétences requises pour la mise en œuvre de ce dernier, à la société et à la collectivité. Tout comme le critère de la qualité de vie, son évaluation est limitée par le manque de données, la faiblesse méthodologique des études et le défaut de transposabilité au contexte national.

En outre, l'évaluation repose donc sur l'apport de preuves, toutes de nature variée (méthodes ou critères). Parmi elles se distinguent :

Les investigations cliniques, élément de preuve principal, adaptées aux revendications du demandeur. À défaut de pouvoir fournir de telles preuves, l'industriel devra justifier et argumenter cette impossibilité. Les attentes et exigences de la CNEDiMTS varient en fonction de la catégorie de D.M., de son cycle de vie, des possibilités de recrutement limitées.

Les critères de jugement :

*critère principal : son identification est proposée en conformité avec l'objectif principal de l'étude et son choix est cohérent avec la pathologie traitée et avec les revendications de l'industriel. Celui-ci peut avoir des objets de natures différentes.

*critères intermédiaires ou de substitution : présentent un intérêt lorsque le critère de l'étude clinique met du temps à être établi.

*critères centrés sur le patient : recueil direct de données cliniques prélevées auprès des patients (lesquels assurent ce recueil) via des outils spécifiques : les PROs et les PROMs.

La pertinence clinique de l'effet : c'est-à-dire une mise en balance entre l'effet

obtenu par le D.M. et le traitement de référence.

L'équivalence : cela suppose que le produit évalué doit être utilisé dans des indications et conditions similaires au produit dont l'industriel revendique l'équivalence.

Par ailleurs, il faut noter que l'évaluation revêt un certain particularisme en matière de D.M.C. (D.M. connectés : intègrent des fonctionnalités numériques, peuvent être connectés à un réseau et sont utilisés à des fins de diagnostic, thérapeutiques, de compensation du handicap ou de surveillance). La CNEDiMTS accepte leur inscription sur la LPPR si et seulement si les conditions suivantes sont remplies : dispositifs marqués CE, D.M. à usage individuel, candidats à un financement individualisé par l'assurance maladie, et D.M. ne faisant pas l'objet d'activités de télésurveillance médicale. En dehors de ceci, les critères d'évaluation demeurent identiques à ceux appliqués pour les autres produits faisant l'objet d'une évaluation. Toutefois, les résultats de l'évaluation peuvent être influencés par les spécificités technologiques et leurs impacts sur la santé des individus, sur l'accès aux soins ou encore sur la qualité de la prise en charge.

De manière générale, les demandes d'inscription doivent être en cohérence avec les revendications de l'industriel, et dans le cas des D.M.C., cela entre également en cohérence avec les demandes du fournisseur de la solution technologique. Il est d'ailleurs conseillé aux industriels d'anticiper l'établissement de leur stratégie, en matière d'indications, notamment pour le programme de développement clinique qui en découle, car cela renforce la cohérence du dossier médico-technique, et donc, de la demande. Pour ce faire, la H.A.S. propose un double accompagnement par le biais : de rendez-vous pré-dépôt, qui consistent à renseigner les industriels sur les aspects technico-réglementaires nécessaires à la constitution du dossier ; et de rencontres précoces, qui sont des entretiens visant à répondre aux interrogations des industriels relatives au développement clinique du produit de santé concerné ou à la réalisation d'une étude médico-économique, si une évaluation de l'efficience du produit est envisagée. Dans les deux situations, la CNEDiMTS est absente puisque ces entretiens sont optionnels, non liants, confidentiels et gratuits.De plus, aux termes de l'inscription (5 ans sur la LPPR), les demandes de renouvellement de celle-ci sont formulées par les industriels, à la suite de quoi la CNEDiMTS effectue son évaluation. Une évaluation qui peut aussi résulter de la propre initiative de la commission ou après demande des ministres chargés de la sécurité sociale et de la santé. Celle-ci repose sur la fourniture de nouveaux éléments, de nouvelles données cliniques, en raison de l'évolution du contexte médical. Un processus qui se distingue de la demande d'études post-inscription faite par l'autorité de contrôle afin de confirmer l'intérêt du D.M. pour le patient, en conditions réelles et à long terme, et de répondre éventuellement aux interrogations soulevées lors de la première évaluation

En définitive, ce guide consolide et clarifie les exigences posées par la CNEDiMTS au cours de son évaluation pour les demandes d'inscription sur la LPPR ou la liste positive intra GHS. Une évaluation qui se structure autour de la détermination de la suffisance ou de l'insuffisance du service attendu ou rendu par le dispositif médical, et puis de son amélioration, au regard de données cliniques prouvées et comparables. Il met en exergue l'importance de l'évaluation scientifique et médicale dans la détermination du remboursement des produits de santé, qui passe essentiellement par le bien-fondé du dossier médico-technique constitué par le demandeur, sur lequel pèse une charge probatoire significative.

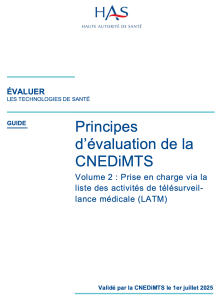
HAS, *Principes d'évaluation de la CNEDiMTS. Volume 1 : Prise en charge via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS*, 1er juillet 2025.

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 2 : Prise en charge via la liste des activités de télésurveillance médicale (LATM)

par Lukas MARA

Étudiant en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



En juillet 2025, la Haute Autorité de santé a publié le volume 2 de ses principes d'évaluation de la CNEDiMTS, consacré aux modalités d'inscription des activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du Code de la sécurité sociale. Instituée par la loi de financement de la sécurité sociale pour 2022, cette liste constitue désormais le cadre de droit commun de la prise en charge par l'Assurance maladie. Le document rappelle d'emblée que la télésurveillance médicale n'est pas un simple outil numérique. Elle repose sur l'association d'un dispositif médical numérique (DMN) et d'une organisation de soins structurée, impliquant l'analyse des données transmises et l'adaptation de la prise en charge par les professionnels de santé. C'est donc une activité intégrée au parcours de soins qui est évaluée, et non seulement la performance technique du dispositif.

L'inscription sur la liste est subordonnée à un avis préalable de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS). Avant l'examen de l'intérêt de l'activité, plusieurs conditions doivent être remplies : le DMN doit bénéficier d'un marquage CE pour l'indication revendiquée, conformément au règlement (UE) 2017/745, et être conforme aux référentiels de sécurité et d'interopérabilité définis par l'Agence du numérique en santé (ANS). Ces prérequis garantissent la conformité technique du dispositif avant toute analyse médico-économique.

Ainsi, deux modalités d'inscription sont distinguées. La procédure sous ligne générique permet d'intégrer des solutions répondant à des critères prédéfinis, sans évaluation individuelle approfondie. À l'inverse, l'inscription sous nom de marque concerne une solution déterminée et donne lieu à une analyse spécifique par la CNEDiMTS, laquelle dispose d'un délai de 90 jours pour rendre son avis.

La démonstration de l'intérêt attendu constitue le point central de la procédure d'inscription.

Concrètement, la demande d'inscription doit toujours reposer sur une comparaison. Lorsque aucune activité de télésurveillance n'est encore remboursée pour l'indication visée, la référence est le suivi médical habituel. En revanche, si une activité est déjà prise en charge, la nouvelle activité doit démontrer qu'elle apporte un bénéfice au moins équivalent, voire supérieur. Le choix de ce comparateur est donc déterminant dans la construction du dossier.

L'intérêt attendu est apprécié selon trois axes principaux. La commission étudie d'abord l'amélioration clinique de l'état de santé du patient, en particulier la mortalité, la morbidité, la qualité de vie et les risques associés au dispositif. Des critères de jugement centrés sur le patient, comme les Patient Reported Outcome Measures (PROMs), peuvent être utilisés pour quantifier le bénéfice perçu. En second lieu, elle apprécie le gain significatif dans

l'organisation des soins, qu'il s'agisse d'économie de ressources, d'amélioration de la coordination ou de sécurisation du parcours, sans perte de chance pour le patient. Enfin, un intérêt de santé publique peut être reconnu lorsqu'il existe un besoin thérapeutique non satisfait ou un problème collectif identifié. Ces différents facteurs déterminent non seulement l'inscription sur la liste, mais aussi le montant du forfait de prise en charge.

Le guide identifie également plusieurs situations susceptibles de conduire à un avis défavorable. L'absence de données cliniques spécifiques constitue à cet égard un obstacle majeur. De plus, les recherches sur une autre technologie ne suffisent pas sans preuve rigoureuse d'équivalence, pas plus que des performances techniques isolées ne permettent d'établir un bénéfice pour la prise en charge. Par ailleurs, l'indication pour laquelle le remboursement est demandé doit être cohérente avec la population effectivement incluse dans les études cliniques. À défaut, la commission peut limiter son évaluation à la seule population étudiée.

Ainsi, l'inscription est accordée pour une durée maximale de 5 ans. Son renouvellement, loin d'être automatique, suppose la production de nouvelles données, notamment issues d'études post-inscription pour confirmer l'intérêt de l'activité en conditions réelles d'utilisation. Dans le même temps, la CNEDiMTS procède à une estimation de la population cible, sur la base de données épidémiologiques françaises, afin d'anticiper les volumes de prise en charge et d'éclairer l'impact budgétaire.

Enfin, le guide insiste sur l'articulation entre le cadre européen et la décision nationale de remboursement. Si le marquage CE permet la mise sur le marché au sein de l'Union européenne, il ne vaut pas reconnaissance automatique d'un droit à la prise en charge. À travers ses développements méthodologiques, la HAS rappelle que l'accès au remboursement repose sur une appréciation propre au système de santé français, fondée sur la démonstration d'un intérêt clinique, organisationnel ou de santé publique. Ce rappel est loin d'être théorique
: il invite les acteurs à penser, dès la phase de développement, la cohérence entre leur stratégie réglementaire européenne et les exigences spécifiques de l'évaluation nationale.

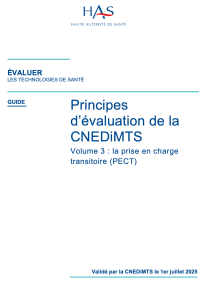
HAS, *Principes d'évaluation de la CNEDiMTS. Volume 2 : Prise en charge via la liste des activités de télésurveillance médicale (LATM)*, 1er juillet 2025

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 3 : la prise en charge transitoire (PECT)

par Amina MOUSTOIFA

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



Le 1er juillet 2025, la Haute Autorité de Santé (HAS) vulgarise dans un guide les principes d'évaluation de la Commission nationale d'évaluation des dispositifs médicaux et de technologies de santé (CNEDiMTS) dans le cadre d'une demande d'une prise en charge transitoire (PECT). La CNEDiMTS est une commission spécialisée de la HAS. Son rôle principal est de formuler des recommandations et de rendre des avis avec un regard scientifique sur les dispositifs médicaux.

Pour être tout à fait clair, le guide explique les méthodes d'évaluation de la CNEDiMTS lors d'un contrôle d'éligibilité d'une candidature pour une PECT. Ce

référentiel s'adresse principalement aux futurs porteurs de projets afin qu'ils saisissent les attentes de la CNEDiMTS et réduire les risques d'erreurs.

La PECT est mise en place par l'article 40 de la loi n° 2019-1446 du 24 décembre 2019. La prise en charge transitoire est, comme son nom l'indique, temporaire. Il s'agit d'un dispositif pour la prise en charge des produits de santé et de prestations associées ayant une finalité thérapeutique ou de compensation du handicap.

À ceci près que la PECT ne doit pas être confondue avec la prise en charge anticipée numérique (PECAN). La PECAN est une évaluation faite par la CNEDiMTS dans le périmètre des dispositifs médicaux numériques à visée thérapeutique ou utilisées en télésurveillance médicale. Donc, la PECAN relève d'une autre procédure à part entière distincte de l'évaluation au titre de la PECT. Toutefois, un dispositif médical intégrant une composante numérique peut recourir à la PECT lorsqu'il s'agit d'un logiciel ayant une fonction médicale, par exemple un implant. L'article L162-48 du code de la sécurité sociale pose deux conditions cumulatives à ce dispositif :

1- Le dispositif médical numérique doit avoir des fonctionnalités de télésurveillance médicale
2- Les fonctionnalités du dispositif médical numérique doivent se limiter à la télésurveillance numérique

Sous cet angle précis, le PECT peut intervenir dans le domaine du numérique au titre des dispositifs médicaux ayant une composante numérique.

L'objectif de la PECT est qu'à terme le produit de santé ou la prestation visée puisse intégrer la liste des produits et prestations remboursables (LPPR). Pour savoir quels produits et prestations sont éligibles à la PECT, il faut se référer aux décrets n°2021-204 du 23 février 2021 et n°2023-232 du 30 mars 2023.

La demande de PECT est conditionnée à 15 critères cumulatifs prévus aux articles R.165-90 et L.165-1-5 du code de la sécurité sociale. La demande est évaluée à la fois par le gouvernement et par la CNEDiMTS.

Le gouvernement est le premier à examiner la demande. Son contrôle s'apparente à une vérification formelle consistant à déterminer si la demande remplit 8 des 15 conditions prévues par le Code de la sécurité sociale.

Préalablement, lorsque les ministres en charge de la santé et de la sécurité sociale reçoivent une demande de PECT, ils se concertent avec le service d'évaluation des dispositifs (SED) de la HAS. Ce dernier travaille également avec la direction de la sécurité sociale. À proprement parler, il s'agit d'un filtrage préalable à l'évaluation des critères techniques par la CNEDiMTS.

À la réception du dossier, le SED et la direction de la sécurité sociale vérifient sa recevabilité administrative et scientifique. Dans l'hypothèse où le dossier n'est pas complet, le demandeur, après une notification, a 15 jours pour le compléter. S'il ne le fait pas, la demande est réputée abandonnée. Néanmoins, si le demandeur n'a pas la capacité de compléter son dossier dans le délai imparti, il peut retirer sa demande. Ainsi, ce retrait ne fera pas obstacle au dépôt ultérieur du même dossier.

Cela posé, le SED de la HAS et la direction de la sécurité sociale examinent ces 8 critères :

1- Le dispositif médical doit disposer du marquage CE ;
2- Le demandeur s'engage à réaliser une demande d'inscription à la LPPR dans un délai de 12 mois à compter de sa demande de PECT ;
3- Le demandeur s'engage à informer sans délai, par tout moyen, les ministres chargés de la santé et de la sécurité sociale de sa demande de prise en charge au titre de la LPPR ;
4- Le produit ou la prestation n'a pas déjà fait l'objet d'un refus de PECT ou d'une PECT à laquelle il a été mis fin

selon les cas prévus par II et III de l'article R.165-95 du Code de la sécurité sociale, qui sont :

- L'intervention d'une décision d'inscription ou de refus d'inscription à la LPPR
- Le retrait de la demande d'inscription à la LPPR par l'industriel
- Le retrait du marquage CE dans l'indication
- Les dispositifs médicaux qui relèvent d'une décision de l'Agence nationale de sécurité du médicament et des produits de santé au regard de l'article L.5312-1 du Code de la santé publique
- L'absence de dépôt d'une demande à la LPPR dans les 12 mois suivant sa demande de PECT
- Une condition d'éligibilité n'est plus remplie

5- Le dispositif médical a déjà été refusé au titre d'une demande de PECT par les ministres chargés de la santé et de la sécurité sociale dans la même indication. Autrement dit, une nouvelle demande du même produit ou de la même prestation pour la même indication n'est pas recevable ;

6- Le produit ne fait pas l'objet, dans l'indication considérée, d'une prise en charge financière au titre des prestations d'hospitalisation mentionnées à l'article L.162-22-6 du code de la sécurité sociale ;

7- Lorsque le produit ou la prestation intègre un dispositif médical numérique répondant à la définition mentionnée au premier alinéa du II de l'article L.162-48, ce dernier est conforme aux règles relatives à la protection des données personnelles ainsi qu'aux référentiels mentionnés à l'article L. 1470-5 du Code de la santé publique, comme expliqué plus tôt ;

8- Pour les dispositifs médicaux, le produit n'a pas fait l'objet d'une décision de suspension ou d'interdiction par l'Agence nationale de sécurité du médicament et des produits de santé (ANSM).

Partant de là, si la demande remplit toutes les conditions, l'industriel reçoit une notification favorable concernant sa demande de la part des ministères en charge de la santé et de la sécurité sociale.

Une fois l'étape préalable validée par les autorités ministérielles, la demande est confiée à la CNEDiMTS. Cette dernière dispose de 60 jours pour donner un avis favorable ou défavorable. La décision rendue par la Commission n'est pas attaquable et n'a pas de phase contradictoire. En effet, la décision finale revient aux ministres de la Santé et de la Sécurité sociale, qui ont 10 jours pour rendre une décision.

Durant ces 60 jours, la CNEDiMTS examine la demande de PECT au regard de ses principes. Dans ce guide, la HAS explique chacun de ces sept principes en collaboration avec la CNEDiMTS.

Tout d'abord, « le produit et la prestation sont destinés à traiter une maladie grave ou rare ou à compenser un handicap ». Pour ce critère, la Commission vérifie que le produit de santé ou la prestation associée vise bien, au choix :

- Une maladie grave
- Une maladie rare
- À compenser un handicap.

Au titre de la gravité et de la rareté de la maladie, elle retient plusieurs éléments d'appréciation. Sous l'angle précis de la gravité, la Commission s'appuie sur les facteurs de morbi-mortalité, de handicap, de complications et de risques. Tout comme pour la rareté de la maladie et la compensation d'un handicap, la Commission analyse les études cliniques, les données épidémiologiques ou encore à travers le calcul d'une population cible.

Ensuite, le produit de santé ou la prestation visée doit répondre à « un besoin médical non ou mal couvert ». Pour cela, il faut qu'il n'y ait pas de « comparateurs pertinents ». Entre autres pour évaluer cette condition, la CNEDiMTS passe en revue les alternatives existantes exposées dans la demande. L'objectif est de vérifier si ces alternatives sont pertinentes et/ou permettent de couvrir un besoin médical au regard des données actuelles de la science ou des recommandations professionnelles.

L'essentiel est que le porteur de projet expose clairement dans sa demande toutes les alternatives disponibles. Néanmoins, la Commission précise que l'existence d'alternatives pertinentes ne suffit pas à écarter la demande de PECT, puisqu'elle prend aussi en compte d'autres éléments comme l'offre de soins, la demande ou encore le rapport bénéfices et risques.

De plus, le produit de santé ou la prestation ne doit pas seulement « traiter une maladie grave ou rare ou à compenser un handicap », le dispositif doit également « apporter une amélioration significative de l'état de santé ou de la compensation du handicap des patients ».

Autrement dit, les indications considérées par l'industriel seront approfondies par le service de la Commission sur la base des données scientifiques transmises par le demandeur. L'analyse se fonde sur des critères d'inclusion, de présomption d'amélioration de la qualité de vie du patient ou l'optimisation de son parcours de soins.

De surcroît, le produit ou la prestation associée doit être innovant « au regard des technologies de santé utilisées dans les indications revendiquées ». En d'autres termes, le dispositif ne peut pas se limiter à une simple amélioration, l'innovation doit être caractérisée. Le guide donne l'exemple :

- D'un nouveau mode d'action modifiant la prise en charge d'une pathologie ou d'un handicap
- D'une réorganisation radicale du système d'information
- L'introduction d'une nouvelle technologie ou prestation dans une classe existante

La CNEDiMTS souligne l'importance de détailler les indications considérées dans la demande pour leur permettre de ne pas passer à côté du caractère innovant de certains produits pouvant porter à confusion.

Dans la continuité immédiate, le cinquième critère rejoint le troisième car il exige une efficacité cliniquement pertinente du produit ou de la prestation. À cela près que, cette cinquième condition approfondit son analyse en examinant les effets indésirables au regard de l'effet apporté par le dispositif. Ici, le bénéfice doit être important au regard des effets indésirables.

Au demeurant, pour apprécier les risques, la Commission s'attache à étudier toutes les données cliniques disponibles, le marquage CE fourni et les données de matériovigilance en France et à l'international par l'industriel. Le demandeur doit préciser le stade de développement du dispositif. La CNEDiMTS réalise également un contrôle in concreto en prenant en compte le contexte épidémiologique et physiopathologique.

La sixième condition rappelle l'importance de l'inscription à la LPPR. En effet, il faut que dans l'indication visée, des études déjà en cours et capables de fournir dans les 12 mois suivant la demande de PECT, des données suffisantes et robustes pour que la CNEDiMTS puisse rendre un avis favorable d'inscription à la LPPR. Plus précisément, ces études servent à lever les doutes laissés par les données préliminaires afin de permettre de se prononcer sur une présomption d'efficacité et de sécurité au moment de l'évaluation.

En ultime analyse, le septième critère précise le fait que la procédure de PECT ne s'adresse pas à tous les dispositifs médicaux. À ce titre, un dispositif médical

numérique ayant une visée thérapeutique ou étant utilisé dans le cadre des activités de télésurveillance médicale prévues à l'article L.162-48 du code de la sécurité sociale, fait l'objet d'une autre procédure à part entière, la prise en charge anticipée des dispositifs médicaux numériques dite PECAN. Cette procédure est également soumise au contrôle de la CNEDiMTS.

Dès lors, à l'issue de l'évaluation de la demande au regard de ses principes, la Commission rend un avis éligible ou un avis non éligible. Cet avis est transmis aux ministres en charge de la santé et de la sécurité sociale. Ces derniers disposent d'un délai de 10 jours pour faire droit ou non à la demande.

En cas d'octroi de la PECT par les ministres, le demandeur est notifié de la décision de ces derniers. Ensuite, il doit proposer un montant maximal de la compensation qu'il revendique au regard de son produit ou de la prestation associée dans un délai de 10 jours. Cela posé, lorsque les ministres accusent réception de la décision de l'industriel, ils ont 45 jours pour accueillir ou rejeter le montant proposé. Ils peuvent également faire une contre-offre. Dans ce cas de figure, le demandeur bénéficie de 10 jours, à compter de la notification de la décision des ministres, pour consentir ou s'opposer au montant révisé. Dans l'hypothèse d'un refus, la demande de la PECT est réputée abandonnée. Dans le cas d'une réponse positive, un arrêté est publié.

Pour conclure, la PECT permet l'accès transitoire à des dispositifs innovants et certains dispositifs médicaux comportant une composante numérique. Dans le champ du numérique en santé, la voie privilégiée pour les dispositifs médicaux numériques reste la PECAN, toutefois, la PECT conserve un champ propre. Partant de là, le guide de la Haute Autorité de Santé contribue à clarifier les critères d'éligibilité et les exigences d'évaluation. Il traduit, pour les porteurs de projets, la volonté de la CNEDiMTS d'encadrer l'innovation numérique par un cadre juridique et scientifique rigoureux.

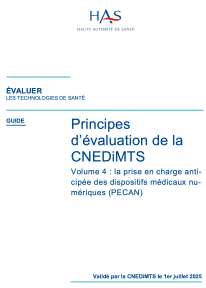
HAS, *Principes d'évaluation de la CNEDiMTS. Volume 3 : la prise en charge transitoire (PECT)*, 1er juillet 2025

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 4 : la prise en charge anticipée des dispositifs médicaux numériques (PECAN)

par Mélanie SOUSA BARBEIRO

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



Introduction

Le numérique occupe une place centrale dans le système de santé, et les dispositifs médicaux numériques (DMN), en particulier ceux intégrant de l'intelligence artificielle, connaissent un développement rapide. Pour accompagner ces innovations tout en garantissant un haut niveau d'exigence, le législateur a mis en place un dispositif d'accès précoce. Ce mécanisme permet la mise à disposition de technologies prometteuses avant l'achèvement complet de leur développement clinique, favorisant ainsi l'innovation tout en préservant la sécurité des patients.

Dans ce contexte, le document *« Principes d'évaluation de la CNEDiMTS (Volume 4) : Prise en charge anticipée (PECAN) »*, validé en juillet 2025 par la Haute Autorité de santé (HAS), présente les

critères et raisonnements utilisés par la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS) pour formuler ses avis. En clair, il s'agit guide méthodologique ou d'une note de référence qui explicite les principes et critères d'évaluation de la CNEDiMTS pour les dispositifs médicaux numériques (DMN) dans le cadre de la prise en charge anticipée (PECAN).

Ce guide se concentre sur deux axes principaux : le cadre réglementaire de l'accès précoce et les critères d'éligibilité ainsi que les exigences méthodologiques applicables aux dispositifs médicaux numériques. L'idée est de comprendre les enjeux liés à l'évaluation anticipée et de clarifier les conditions dans lesquelles ces innovations peuvent être mises à disposition des patients.

I. ENCADREMENT JURIDIQUE ET PROCÉDURAL DE L'ACCÈS PRECOCE AUX DISPOSITIFS MÉDICAUX NUMÉRIQUES

Le document décrit d'abord les fondements juridiques et procéduraux de la PECAN **(A)**, avant de présenter la procédure d'évaluation structurée et transparente mise en place par la CNEDiMTS **(B)**.

A. Fondements légaux et cadre réglementaire de la prise en charge anticipée (PECAN)

Instaurée par l'article 58 de la loi de financement de la sécurité sociale pour 2022, la PECAN permet aux DMN d'accéder plus rapidement au remboursement, que ce soit pour un usage thérapeutique relevant de la LPPR ou pour des activités de télésurveillance relevant de la LATM. L'idée est d'offrir un accès anticipé à des innovations qui peuvent réellement apporter un bénéfice, sans sacrifier les standards scientifiques sur lesquels reposent les décisions de prise en charge. La CNEDiMTS intervient systématiquement pour éclairer ces décisions.

Le dispositif repose sur un équilibre précis : la prise en charge est temporaire, limitée à douze mois, et non renouvelable. L'entreprise doit ensuite déposer une demande d'inscription en droit commun dans un délai de six mois pour un produit destiné à la LPPR, ou de neuf mois pour un dispositif de télésurveillance. Certaines situations empêchent l'accès à la PECAN : il n'est ainsi pas possible d'obtenir deux prises en charge anticipées pour la même indication, ni de solliciter le dispositif en cas de suspension liée à un signalement de matériovigilance, ou lorsqu'un autre mode de financement est déjà mobilisé. Un nouveau dépôt n'est envisageable que si le précédent refus résulte exclusivement d'un manque de données en cours d'acquisition.

Par ailleurs, l'Agence du Numérique en Santé intervient lorsque la certification portant sur la protection des données personnelles, l'interopérabilité, la sécurité ou l'exportabilité est requise. Cette vérification, fondée sur l'article L.1470-5 du code de la santé publique, est cumulative à l'examen de la CNEDiMTS, notamment pour les DMN manipulant des données de santé ou connectés à des accessoires de collecte physiologique.

Ces bases juridiques et procédurales définissent le cadre, mais c'est la procédure d'évaluation qui garantit la rigueur scientifique et la transparence des décisions.

B. Organisation et déroulement de l'évaluation par la CNEDiMTS, garantissant rigueur et transparence

Le processus débute par le dépôt du dossier auprès des ministères, avec transmission simultanée à la CNEDiMTS. Une vérification de complétude est effectuée immédiatement : si des pièces manquent, le demandeur dispose de trente jours pour régulariser son dossier, sinon la demande est considérée comme abandonnée.

L'évaluation scientifique menée par la CNEDiMTS, sans phase contradictoire, doit aboutir à un avis dans un délai maximal de soixante jours. Les ministères disposent ensuite de trente jours supplémentaires pour arrêter la décision de prise en charge. Tous les avis sont publiés en ligne, favorables ou défavorables, afin de garantir lisibilité et transparence.

La CNEDiMTS peut faire appel à un expert externe, après validation de sa déclaration publique d'intérêts, pour compléter l'éclairage scientifique ou clinique. L'expert n'assiste ni à la délibération ni au vote, assurant une séparation claire entre expertise et décision. Les avis, même défavorables, sont conçus comme des outils d'amélioration : ils détaillent les points à renforcer et orientent les entreprises vers une stratégie plus solide, sans jamais remettre en cause l'intérêt intrinsèque du dispositif.

Avec ce cadre et cette procédure en place, l'attention se tourne maintenant vers les critères d'éligibilité et les exigences méthodologiques qui conditionnent l'accès des DMN à la PECAN.

II. CONDITIONS D'ÉLIGIBILITE ET EXIGENCES MÉTHODOLOGIQUES APPLICABLES AUX DISPOSITIFS MÉDICAUX NUMÉRIQUES

Le volume 4 des Principes d'évaluation de la CNEDiMTS précise les conditions d'éligibilité (A), puis les exigences méthodologiques (B) applicables aux dispositifs médicaux numériques, y compris pour les dispositifs intégrant de l'intelligence artificielle.

A. Les conditions d'accès nécessitant marquage CE, présomption d'innovation et cohérence du dossier

Plusieurs critères d'éligibilité sont applicables aux dispositifs médicaux numériques.

Le premier critère est la conformité du marquage CE, qui doit correspondre exactement à l'indication revendiquée. Toute discordance conduit automatiquement à un avis défavorable. Ce prérequis administratif est indispensable pour que la CNEDiMTS puisse examiner le dossier sur le plan scientifique.

Un autre critère est la présomption d'innovation. Cette dernière repose sur deux conditions. La première exige que le dispositif apporte un bénéfice clinique ou organisationnel, appuyé par des données initiales pertinentes : réduction des hospitalisations non programmées, amélioration de la qualité de vie, optimisation du parcours de soins, ou meilleure observance. Lorsque l'innovation concerne l'organisation, il faut démontrer qu'elle ne dégrade pas la qualité des soins, condition systématiquement vérifiée par la Commission.

La seconde condition concerne l'avancement des études : elles doivent être suffisamment avancées pour permettre une évaluation complète dans les six ou neuf mois suivant la décision PECAN. La méthodologie, la cohérence entre critères et bénéfices, le comparateur choisi, l'adéquation de la population et le réalisme du calendrier sont évalués. Les refus les plus fréquents concernent l'absence de données spécifiques, des protocoles peu solides, des critères inadaptés ou un désalignement entre l'étude et le dossier PECAN.

Enfin, le dossier doit être complet et structuré : description du DMN, mode d'action, estimation de la population cible, stratégie de référence, données de matériovigilance, premières preuves cliniques, protocoles finalisés, calendrier de résultats et pièces administratives. Si la PECAN accepte une part d'incertitude liée à l'innovation, elle n'admet pas l'insuffisance méthodologique ou des données imprécises.

Une fois ces conditions vérifiées, il reste à examiner la méthodologie et les exigences

spécifiques, particulièrement pour les DMN intégrant de l'intelligence artificielle.

B. Les exigences méthodologiques relatives aux DMN intégrant de l'intelligence artificielle

L'évaluation repose sur les guides méthodologiques de la HAS : développement clinique, DM connectés, études en vie réelle, évaluation organisationnelle et télésurveillance. L'objectif est d'isoler l'effet propre du dispositif, avec un comparateur pertinent, le contrôle des co-interventions, des critères liés aux bénéfices revendiqués et une population représentative. La transposabilité au système français est également importante, surtout pour des études internationales.

La distinction entre données spécifiques et non spécifiques se voit essentielle. Les données non spécifiques peuvent être utilisées si l'équivalence technique et fonctionnelle est démontrée, notamment pour des versions antérieures du DMN. À défaut, l'hétérogénéité ou l'absence de cohérence méthodologique entraîne souvent un refus, notamment pour des méta-analyses combinant des technologies trop différentes pour être extrapolées.

Pour les DMN intégrant un module d'intelligence artificielle, la documentation doit être particulièrement détaillée : modèle utilisé, données d'entraînement, méthodes de validation interne et externe, gestion des biais, mesures d'explicabilité, traçabilité des versions, performances attendues et stabilité en conditions réelles. Cette exigence vise à sécuriser l'usage clinique des algorithmes évolutifs et à garantir qu'ils n'affectent ni la pertinence des décisions médicales ni la sécurité des patients.

Conclusion

Le guide méthodologique de la CNEDiMTS relatif à la prise en charge anticipée des dispositifs médicaux numériques (PECAN) illustre l'équilibre délicat entre innovation et rigueur scientifique dans le système de santé français. En définissant clairement les fondements juridiques et procéduraux, la HAS offre un cadre structuré et transparent pour l'évaluation des DMN, tout en garantissant que les décisions reposent sur des données fiables et reproductibles.

Les critères d'éligibilité et les exigences méthodologiques détaillés dans le volume 4 permettent de sécuriser l'accès des innovations prometteuses, y compris celles intégrant de l'intelligence artificielle, tout en maintenant la sécurité et la qualité des soins. Ce dispositif d'accès précoce favorise ainsi l'adoption rapide de technologies utiles pour les patients, tout en fournissant aux entreprises un repère méthodologique précis pour renforcer la robustesse de leurs dossiers.

En définitive, la PECAN constitue un outil stratégique pour concilier innovation numérique, protection des patients et transparence dans la décision de prise en charge, renforçant la confiance des acteurs du système de santé et soutenant le développement responsable des DMN en France.

HAS, *Principes d'évaluation de la CNEDiMTS. Volume 4 : la prise en charge anticipée des dispositifs médicaux numériques (PECAN)*, 1er juillet 2025.

RÉFÉRENTIEL :

Harmonisation du bilan médicamenteux. **Recueil des besoins métiers en matière de bilan médicamenteux**

par Clarance JEAN-PIERRE

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Le référentiel d'harmonisation du bilan médicamenteux a été publié en juillet 2025 par la Haute Autorité de santé (HAS). Ce document fait suite à la saisine de la Délégation ministérielle au numérique en santé (DNS) et de la Direction générale de la santé (DGS). Il vise à définir un socle commun d'informations et de pratiques afin d'uniformiser la réalisation du bilan médicamenteux dans les différents secteurs de soins. Le document répond à un objectif de structuration des données et d'amélioration de leur partage entre professionnels de santé. Le référentiel indique que le bilan médicamenteux doit pouvoir être produit sous un format structuré compatible avec les systèmes d'information des professionnels de santé. Cette structuration est nécessaire pour permettre son dépôt dans le DMP. Le DMP est ainsi présenté comme un espace numérique destiné à recevoir et à rendre accessibles les informations issues du bilan, dans le cadre du parcours de soins du patient.

En outre, le référentiel définit un socle minimal d'informations devant figurer dans le bilan médicamenteux. Il comprend notamment l'identification du patient, la liste des traitements en cours, les éléments relatifs à l'observance, les informations issues de la conciliation médicamenteuse ainsi que les recommandations formulées par le professionnel. L'organisation de ces données sous une forme standardisée vise à garantir leur lisibilité et leur utilisation par d'autres professionnels de santé. Cette structuration conditionne également leur intégration correcte dans le DMP.

Par ailleurs, le document précise les exigences techniques nécessaires à cette intégration. En effet, le bilan médicamenteux doit pouvoir être exporté et transmis selon des formats compatibles avec les référentiels nationaux d'interopérabilité. Les logiciels métiers utilisés par les professionnels doivent être en mesure d'assurer le dépôt du document dans le DMP, dans des conditions conformes aux règles nationales applicables aux échanges de données de santé.

Le référentiel prévoit également des éléments assurant la traçabilité du bilan médicamenteux. Celui-ci doit mentionner la date de réalisation, l'identité du professionnel auteur ainsi que le contexte de production. Le bilan médicamenteux peut être mis à jour, et chaque version doit être clairement identifiée dans le DMP. Enfin, le texte rappelle que le dépôt et la consultation du bilan médicamenteux dans le DMP doivent respecter les règles applicables au DMP, notamment celles relatives à l'habilitation des professionnels et aux droits du patient en matière d'accès et de gestion de ses données de santé.

Ainsi, le référentiel organise non seulement le contenu du bilan médicamenteux, mais aussi les conditions de son intégration dans le DMP, en définissant les exigences de structuration, d'interopérabilité et de traçabilité nécessaires à son utilisation dans l'environnement numérique de santé.

HAS, *Harmonisation du bilan médicamenteux. Recueil des besoins métiers en matière de bilan médicamenteux,* 24 juillet 2025.

GUIDE :

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

dans les secteurs sanitaire, social et médico-social

A.V.E.C : Avancer – **V**érifier – **E**stimer – **C**omprendre

par Maïlys CAPELL

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Éditorial

L'intelligence artificielle générative (IAG) en santé : un nouveau défi de responsabilité

En octobre 2025, la Haute Autorité de la Santé (HAS) a franchi une étape décisive dans l'encadrement des technologies numériques en publiant ses « Premières clefs d'usage de l'Intelligence Artificielle (IA) générative en santé ». Ce corpus documentaire, composé d'un guide pédagogique et d'un rapport d'élaboration approfondi, a été officiellement adopté comme Recommandations de Bonne Pratique (RBP) par le Collège de la HAS. Résultat d'une auto-saisine, ce travail a été piloté par la Mission numérique en santé (MNS), sous la conduite de Paul Valois, Julie Marc et Corinne Collignon. Ils ont produit une analyse critique de la littérature scientifique, mené des entretiens avec des experts de l'IA et ont consulté diverses associations de patients. L'objectif est clair : transformer ce qui n'est encore qu'un outil de curiosité en une pratique professionnelle sécurisée, éthique et juridiquement viable.

L'ensemble de ces travaux s'inscrit directement dans le cadre du projet stratégique 2025-2030 de la HAS, dont l'une des thématiques phares est le « Numérique et l'IA en santé ». En publiant ces RBP, la HAS ambitionne de construire un véritable cadre de confiance pour les usages de l'IA. L'enjeu est triple : accompagner les usages pertinents, améliorer les pratiques professionnelles et sécuriser le parcours de soin face à l'apparition des Large Language Models (LLM) dans les secteurs sanitaire, sociaux et médico- sociaux.

L'analyse de ces RBP doit être replacée dans un contexte légal européen en pleine effervescence. Si l'article 168 du TFUE fonde l'action de l'Union en complément des politiques nationales, l'IAG impose aujourd'hui un respect strict d'un corpus de normes complexe, produites à différents niveaux. Ces travaux de la HAS résonnent directement avec le Règlement (UE) 2024/1689 (IA Act) du 13 juin 2024, qui instaure une approche par les risques, et s'articulent avec les exigences de sécurité des Règlements (UE) 2017/745 et 2017/746 relatifs aux dispositifs médicaux. Ce cadre s'appuie également sur le Règlement (UE) 2025/327 relatif à l'Espace européen des données de santé et les garanties de l'article 22 du RGPD (complété par l'article 47 de la loi de 1978) pour encadrer les décisions individuelles automatisées. Enfin, la HAS s'appuie sur la Directive (UE) 2024/2853 sur la responsabilité du fait des produits défectueux pour protéger la liberté de décision des médecins. Face à des outils technologiques qui nous dépassent souvent, il est devenu indispensable de tenter de les maîtriser pour garantir, au final, la sécurité des patients

I. LA DISTINCTION ENTRE IAG « GRAND PUBLIC » ET IAG « MÉTIER »

Le rapport d'élaboration ne s'en cache pas : l'IA est déjà là. On observe un usage sauvage : des praticiens synthétisent des dossiers complexes ou rédigent des

comptes- rendus via des outils non sécurisés, souvent par nécessité, face à la surcharge administrative.

L'un des apports majeurs de l'argumentaire de la HAS est la distinction très nette entre les outils grand public (comme la version gratuite de ChatGPT) et les solutions dites « métier ».

Les IAG grand public sont des « boîtes noires » dont les processus d'entraînement sont opaques et dont les conditions d'utilisation permettent souvent la réutilisation des données communiquées par les utilisateurs pour améliorer le modèle. Pour la HAS, l'usage de ces outils en santé est hautement problématique : non seulement ils ne garantissent pas la confidentialité, mais ils sont sujets à un taux d'hallucination plus élevé. Contrairement aux outils professionnels qui s'appuient sur des bibliothèques de données scientifiques certifiées et des publications médicales relues par des experts, les IA grand public tirent leurs connaissances d'un mélange d'informations piochées partout sur le web. Elles n'ont pas été spécifiquement entraînées pour distinguer une information médicale fiable d'une rumeur ou d'une erreur trouvée sur un forum.

À l'inverse, l'IAG « métier » doit répondre à des exigences de documentation technique, de transparence algorithmique et bénéficier d'un marquage CE dispositif médical dès lors qu'elle intervient dans une finalité diagnostique ou thérapeutique. Le guide rappelle qu'un professionnel de santé ne devrait utiliser que des outils dont il peut identifier l'éditeur et en comprendre le périmètre de sécurité.

II. LA CERTIFICATION ET LE MARQUAGE CE : UN IMPÉRATIF DE SÉCURITE

Dans le secteur de la santé, l'innovation ne peut échapper aux règles de mise sur le marché. Le guide rappelle ainsi une distinction essentielle pour le professionnel de santé : l'outil est-il un simple assistant administratif ou un véritable Dispositif Médical ?

Dès lors qu'une IAG est utilisée dans une finalité médicale — qu'il s'agisse d'aide au diagnostic, de suggestion de traitement ou de surveillance de paramètres physiologiques — elle entre potentiellement dans le champ d'application du Règlement Européen 2017/745. Le marquage CE n'est pas un simple label de qualité, mais une attestation de conformité à des exigences de sécurité et de performance clinique.

Le rapport de la HAS est sans équivoque : si un professionnel utilise une IAG « grand public » dépourvue de marquage CE pour une décision de soin, il s'expose à un risque juridique majeur. En l'absence de certification, l'outil n'a pas été audité par un organisme notifié pour ses performances médicales. Utiliser une IA non certifiée pour interpréter des résultats de biologie ou pour établir un protocole thérapeutique revient, en droit, à utiliser un instrument non homologué.

Le guide engage donc les établissements de santé à une vigilance stricte :

a. **Vérifier la destination de l'outil :** L'éditeur revendique-t-il un usage médical ?

b. **Exiger la documentation technique :** Le professionnel doit avoir accès aux informations prouvant que l'outil a été testé sur des corpus de données cliniques pertinents.

c. **Refuser les « boîtes noires » non documentées :** Si l'éditeur ne garantit pas la traçabilité des sources et la gestion des risques d'erreurs, l'outil doit être cantonné à des tâches de secrétariat ou d'organisation administrative.

La HAS rappelle que le marquage CE est le garant de la « sécurité de résultat », même si la responsabilité finale de l'acte de soin reste humaine. C'est le point de jonction entre le droit des produits défectueux de santé et le droit de la responsabilité médicale.

III. L'ANALYSE JURIDIQUE DE LA MÉTHODE A.V.E.C.

Chaque pilier de la méthode redéfinit les contours de l'obligation de moyens renforcée du professionnel de santé.

a. APPRENDRE. La HAS insiste : on ne peut pas utiliser une IAG sans comprendre son fonctionnement. En droit européen, cela fait écho à l'AI Act qui impose une surveillance humaine. Ne pas se former aux limites de l'IA pourrait demain être qualifié de faute caractérisée en cas d'erreur de traitement.

b. VÉRIFIER. L'IAG peut halluciner, c'est-à-dire inventer des références bibliographiques ou encore des dosages médicamenteux. Le guide rappelle qu'un système d'IAG n'est pas un moteur de recherche. La HAS impose donc une relecture humaine systématique. Juridiquement, cela signifie que la preuve de l'erreur de l'IA ne sera jamais exonératoire d'une responsabilité médicale. La garantie humaine est le seul rempart qui assure que, derrière chaque ligne de code, existe une conscience capable de contredire la machine pour protéger le patient.

c. ESTIMER. Le rapport nous apprend qu'une simple requête consomme une quantité d'eau et d'électricité non négligeable pour refroidir les serveurs. La HAS demande donc aux soignants d'estimer si l'usage de l'IA est réellement nécessaire. Cette sobriété numérique se traduit par des conseils très concrets : supprimer les formules de politesse (bonjour, s'il te plaît) dans les échanges avec la machine afin de réduire la longueur du traitement algorithmique. Plus encore, elle alerte sur la perte de compétence : le risque est celui d'une dépendance cognitive où le praticien perdrait sa capacité d'analyse critique au profit d'une délégation totale à la machine. La recommandation de maintenir des séquences de travail « sans IA », et estimer quand l'IA est un réel gain de temps, est un cri d'alarme pour la préservation de l'intelligence humaine.

d. COMMUNIQUER. L'article L. 1111-4 du Code de la santé publique dispose que le patient doit recevoir une information loyale. La HAS va plus loin : si une IA a été utilisée pour aider au diagnostic ou à la rédaction du compte-rendu, le patient doit le savoir, et cela doit être mentionné dans son dossier médical, conformément à l'article L4001-3 du Code de Santé Publique.

IV. LE RISQUE DES BIAIS DISCRIMINATOIRES : UNE RESPONSABILITE EMERGENTE POUR LES PRATICIENS

Le rapport d'élaboration consacre une section essentielle aux biais algorithmiques. L'UE promeut des valeurs d'égalité et de non-discrimination. Cependant, les LLM sont entraînés sur des bases de données historiques qui reflètent les préjugés de notre société.

La HAS avertit : l'IAG peut reproduire, voire accentuer, des biais de genre, d'origine ou de classe sociale. Par exemple, une IA pourrait suggérer des protocoles de soins moins ambitieux pour certaines populations si les données d'entraînement sont déséquilibrées. Le guide impose donc au professionnel une posture de vigilance éthique. Il ne s'agit plus seulement de vérifier l'exactitude médicale d'une réponse, mais de s'assurer qu'elle ne contient pas une discrimination qui enfreindrait les principes fondamentaux du droit de la santé.

En publiant ces clefs d'usage, la HAS réalise une opération de transfert de responsabilité complexe. Si le guide sécurise les institutions, il place officiellement une charge de contrôle faramineuse sur les épaules du professionnel de santé.

On lui demande d'être, à la fois, médecin, informaticien capable de détecter des biais, et auditeur de conformité

réglementaire (avec la vérification du marquage CE). Est-il raisonnable de faire peser sur l'utilisateur final la responsabilité d'une « boîte noire » dont les mécanismes internes sont protégés, qui plus est, par le secret industriel ? Le guide prône la garantie humaine, mais cette garantie risque de devenir une fiction juridique si le professionnel n'a, ni le temps, ni les outils pour vérifier réellement les propositions de l'IA. Il existe un danger réel de voir apparaître une responsabilité sans faute, ou une obligation de sécurité de résultat déguisée, là où le médecin ne devait être tenu qu'à une obligation de moyens.

V. L'IMPACT SUR LES ÉTABLISSEMENTS SANITAIRES, SOCIAUX ET MÉDICO-SOCIAUX

Le déploiement de l'IAG n'est pas seulement un défi pour le praticien ; c'est un séisme organisationnel pour les Établissements Sanitaires, Sociaux et Médico-Sociaux. Le rapport d'élaboration de la HAS souligne que la mise en place de ces outils doit impérativement s'accompagner d'une réflexion institutionnelle profonde. On ne peut plus laisser l'usage de l'IAG au seul libre arbitre de l'agent.

L'un des points les plus sensibles du rapport d'élaboration concerne la protection des données de santé. En droit français, le secret médical est le socle de la confiance entre le soignant et le patient. La HAS est catégorique : il ne faut fournir aucune donnée identifiante (nom, prénom, NIR, date de naissance) dans une IAG non sécurisée. Le guide souligne que même une information partielle ou incomplète peut, par croisement de données, permettre une ré-identification. Le risque est double : d'une part, la violation du secret professionnel (sanctionnée pénalement) et, d'autre part, l'alimentation des bases de données des éditeurs par des cas cliniques réels, sans consentement des patients. La recommandation de la HAS de privilégier des environnements HDS (Hébergeur de Données de Santé) n'est donc pas une simple option technique, mais une condition de légalité. Pour garantir la sécurité des soins et la protection des données, la HAS préconise que le choix des outils soit centralisé au niveau de la gouvernance de l'établissement. La Direction des Systèmes d'Informations ne doit plus seulement être un support technique, mais un véritable garant de la conformité. C'est elle qui doit s'assurer que l'IAG utilisée est intégrée dans un environnement sécurisé, évitant ainsi l'usage d'outils personnels non autorisés qui expose l'établissement à des cyberattaques ou à des fuites de données massives.

En outre, l'intégration de l'IAG impose de repenser les processus de travail.

Le guide recommande aux établissements de définir des protocoles clairs : pour quelles tâches l'IA est-elle autorisée (rédaction de comptes-rendus, synthèse de littérature…) ? Le rapport précise que cette intégration doit faire l'objet d'un suivi via des indicateurs de performance et de qualité. En droit de la santé, cela renforce la responsabilité de l'établissement en cas de défaut d'organisation si aucun cadre n'a été fixé pour l'usage de ces technologies.

Enfin, la HAS insiste sur la nécessité d'un dialogue entre les directions, les représentants du personnel et les comités éthiques locaux. L'IAG modifie la valeur perçue du travail : si une tâche qui prenait deux heures est désormais réalisée en deux minutes, comment ce temps gagné est-il réalloué au bénéfice du patient ? La réussite organisationnelle réside dans la capacité de l'établissement à transformer ce gain de productivité en temps médical et soignant retrouvé, évitant ainsi que l'IA ne devienne un simple outil de rentabilité comptable au détriment de l'humanité des soins. Elle peut cependant absorber les tâches répétitives pour permettre au soignant de se concentrer sur l'essentiel : l'humain.

Conclusion

Le guide de la HAS d'octobre 2025 marque la fin de l'innocence numérique en matière d'utilisation de l'IA dans le milieu

sanitaire. Il ne s'agit plus de savoir si nous utiliserons l'IAG, mais plutôt de chercher comment tenter de rester maîtres de son usage. La HAS passe donc d'une posture de méfiance à une posture d'accompagnement. Elle ne cherche pas à interdire — ce qui serait illusoire — mais à normaliser. Ce passage vers le bon usage institutionnel implique que les établissements sanitaire, sociaux et médico- sociaux se saisissent de la gouvernance de ces outils. En effet, la responsabilité ne doit plus reposer uniquement sur l'utilisateur isolé, mais sur une stratégie collective de déploiement, qui pourrait passer notamment par la désignation d'un référent IA dans les établissements.

HAS, *Première clefs d'usage de l'IA générative en santé, dans les secteurs sanitaire, social et médico-social. A.V.E.C : Avance – Vérifier – Estimer – Communiquer*, 23 octobre 2025.

*La transformation numérique des établissements de santé se poursuit en 2026 à travers **deux initiatives majeures** : le lancement de la deuxième phase du programme HOP'EN (HOP'EN2) et le déploiement du programme HospiConnect, destiné à renforcer la sécurisation des accès aux systèmes d'information hospitaliers.*

Instruction n° DNS/2025/180 du 29 décembre 2025 relative au lancement de la deuxième phase du programme HOP'EN 2 pour soutenir la transformation numérique des établissements de santé, *BO* du 12/01/2026

Par une instruction du 29 décembre 2025, la Délégation au numérique en santé (DNS) a lancé la deuxième phase du programme HOP'EN (Hôpital numérique ouvert sur son environnement), destinée à poursuivre la transformation numérique des établissements de santé. Cette nouvelle étape vise à accompagner la montée en maturité des systèmes d'information hospitaliers, en favorisant notamment le déploiement de services numériques interopérables, le partage sécurisé des données de santé et la fluidification des parcours de soins**.** Le programme s'inscrit dans la continuité des actions engagées depuis 2019 pour moderniser les infrastructures numériques hospitalières et renforcer l'intégration des établissements dans l'écosystème numérique en santé.

Arrêté du 27 janvier 2026 relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé – HospiConnect, *JORF* n° 0024 du 29 janvier 2026

L'arrêté du 27 janvier 2026 instaure le programme HospiConnect, un dispositif de financement destiné à renforcer la sécurité numérique des établissements de santé. Inscrit dans le cadre du programme CARE (Cybersécurité Accélération et Résilience des Établissements) et complémentaire du programme HOP'EN 2, il vise notamment à soutenir le déploiement de moyens d'identification électronique conformes au référentiel national d'identification électronique, afin de sécuriser l'accès aux systèmes d'information hospitaliers et aux données de santé. Le programme accompagne plus largement le développement de mécanismes d'authentification forte, de gestion des identités et des accès numériques, dans un contexte de renforcement des exigences de cybersécurité et de protection des données au sein du secteur hospitalier.

REPÈRES

Jusqu'en 2022, la télésurveillance médicale était principalement financée dans le cadre de l'expérimentation **ETAPES** (Expérimentations de télémédecine pour l'amélioration des parcours en santé). La loi de financement de la sécurité sociale (**LFSS**) pour 2022 a instauré un cadre pérenne de prise en charge des activités de télésurveillance médicale, codifié à l'**article L. 162-52 du code de la sécurité sociale**. Ce dispositif repose sur une liste des activités de télésurveillance prises en charge par l'Assurance maladie, complétée progressivement par voie réglementaire, ainsi que sur des forfaits destinés à financer leur mise en œuvre.

PRISE EN CHARGE DES ACTIVITÉS DE TÉLÉSURVEILLANCE MÉDICALE

La télésurveillance médicale poursuit son intégration dans le droit commun de l'Assurance maladie. Plusieurs textes publiés en 2025 et 2026 étendent ou adaptent les modalités de prise en charge applicables à différentes pathologies, contribuant ainsi à la diversification progressive des activités de télésurveillance prises en charge.

TÉLÉSURVEILLANCE DU DIABÈTE GESTATIONNEL

Renouvellement de la prise en charge du DMN MYDIABBY jusqu'en 2028

- Arrêté du 27 mars 2026 portant renouvellement d'inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° L 0077 du 31 mars 2026

TÉLÉSURVEILLANCE DES PORTEURS DE MONITEURS CARDIAQUES IMPLANTÉS

Inscription du dispositif CARELINK (Medtronic)

- Arrêté du 24 juillet 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0182 du 7 août 2025
- Arrêté du 24 juillet 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0182 du 7 août 2025

Inscription du dispositif HOME MONITORING SERVICE CENTER (Biotronik)

- Arrêté du 23 juin 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0149 du 28 juin 2025
- Arrêté du 23 juin 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0147 du 26 juin 2026

Inscription du dispositif LATITUDE CLARITY (Boston Scientific)

- Arrêté du 3 mars 2026 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0055 du 5 mars 2026
- Arrêté du 3 mars 2026 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0055 du 5 mars 2026

Inscription du dispositif IMPLICITY IM009 (Implicity)

- Arrêté du 20 mai 2026 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0119 du 22 mai 2026
- Arrêté du 20 mai 2026 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n°0119 du 22 mai 2026

GUIDE DE LA CONSULTATION, « Comment consulter les documents de Mon espace santé »

par Lukas MARA

Étudiant en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Le guide *« Mon espace santé/DMP »* est intéressant pour comprendre les évolutions actuelles du numérique en santé en France. Il présente principalement les nouvelles modalités d'accès aux données médicales et leur gestion par les professionnels de santé et les patients. Ainsi, le guide ne se limite pas à une simple présentation technique de la plateforme. Il expose des enjeux juridiques, organisationnels et éthiques liés à la circulation des données de santé dans un système de soins de plus en plus numérisé.

Le guide rappelle que le vieillissement de la population, l'augmentation des maladies chroniques et la complexification des parcours de soins rendent indispensable une meilleure coordination entre les professionnels de santé. Le numérique apparaît alors comme une réponse à ces difficultés, notamment grâce à la centralisation et au partage sécurisé des données médicales. Mon espace santé est un outil destiné à fluidifier les échanges d'informations entre les acteurs du soin tout en renforçant la place du patient dans la gestion de sa santé. En effet, Mon espace santé succède au Dossier Médical Partagé (DMP), créé initialement en 2004 mais dont le déploiement a longtemps été considéré comme un échec. Il y avait plusieurs difficultés qui empêchaient son adoption massive : les dossiers n'étaient pas créés automatiquement, les professionnels de santé ne les alimentaient pas régulièrement et les logiciels utilisés n'étaient pas suffisamment interopérables. Afin de remédier à ces limites, la loi de 2019 instaure un système d'opt-out avec la création automatique d'un profil pour chaque assuré social, sauf opposition de sa part. Mon espace santé est ensuite généralisé en 2022 comme nouvelle version du DMP, avec une logique davantage centrée sur le patient.

Mon espace santé ne doit plus être perçu comme un simple dossier médical numérique. Le guide insiste au contraire sur le fait qu'il s'agit d'un véritable *« compagnon de santé »*. La plateforme permet notamment au patient d'accéder à ses antécédents médicaux, à ses ordonnances, à ses comptes rendus d'hospitalisation, à ses résultats de biologie ou encore à ses vaccinations. Elle comprend également une messagerie sécurisée, un agenda médical et différents outils de prévention. Cette évolution traduit une volonté claire des pouvoirs publics de mettre en avant un patient acteur, plus autonome dans son parcours de soins.

De surcroît, le guide met en avant le renforcement des droits des patients sur leurs données de santé. En effet, contrairement à l'ancien DMP, certaines informations n'étaient pas nécessairement accessibles au patient. Désormais, le principe repose sur la transparence puisque l'usager peut consulter les données présentes dans son espace santé. Le patient peut consulter l'historique des accès à son dossier, recevoir des notifications lorsqu'un professionnel consulte ses données et masquer certains documents s'il le souhaite. Cette logique rejoint les principes du RGPD et de la protection des données personnelles, particulièrement

importantes lorsqu'il s'agit de données sensibles.

Ensuite, le guide présente les différentes situations dans lesquelles les professionnels de santé utilisent Mon espace santé. Ils peuvent s'en servir avant une consultation, pendant une hospitalisation, aux urgences ou après une prise en charge pour assurer le suivi du patient. Il met aussi en avant plusieurs avantages concrets comme le gain de temps, la réduction des examens réalisés plusieurs fois, une meilleure connaissance des antécédents du patient et une meilleure coordination entre les professionnels. Le développement du numérique en santé répond donc à des besoins concrets pour améliorer l'efficacité des soins.

Le cœur juridique du guide repose sur le mécanisme appelé « **DICAH** », qui correspond aux cinq conditions cumulatives nécessaires pour accéder aux données de santé d'un patient. Ce système est particulièrement intéressant car il illustre la manière dont les exigences juridiques sont traduites techniquement dans les outils numériques de santé.

1. La première condition est la **D**isponibilité du profil Mon espace santé du patient. Le guide précise qu'environ 68 millions de profils ont déjà été créés automatiquement pour les assurés sociaux.
2. La deuxième condition concerne l'**I**dentité Nationale de Santé (INS), présentée comme un identifiant numérique sécurisé permettant de garantir l'identification correcte du patient. Cette identification est importante car elle permet d'éviter les erreurs médicales liées à une confusion entre patients.
3. La troisième condition est le **C**onsentement du patient. Les professionnels de santé ne peuvent accéder qu'aux informations nécessaires à la prise en charge du patient. Celui-ci doit être informé et donner son accord, afin de garantir le respect de sa vie privée et du secret médical. Le guide prévoit également des règles particulières pour les mineurs avec un système de *« connexion secrète »* permettant de protéger certaines informations médicales sensibles. Cela montre l'importance accordée à la confidentialité des données de santé. De plus, en cas d'urgence, un accès exceptionnel appelé *« bris de glace »* est possible lorsque le patient ne peut pas donner son consentement et que sa vie est en danger. Cet accès reste toutefois strictement encadré et doit être justifié.
4. La quatrième condition concerne l'**A**uthentification du professionnel de santé. Le professionnel doit se connecter de manière sécurisée afin de protéger les données médicales du patient.
5. Enfin, la cinquième condition est l'**H**abilitation du professionnel. L'accès aux documents médicaux dépend de la profession du soignant et de son rôle dans la prise en charge du patient, notamment grâce à des outils sécurisés comme la carte CPS ou ProSanté Connect.

Ainsi, le guide montre que Mon espace santé s'inscrit dans une stratégie plus globale de transformation numérique du système de santé français. Les années 2026 et 2027 doivent permettre une intégration encore plus poussée dans les logiciels hospitaliers et les outils métiers des professionnels de santé. L'objectif est de rendre l'accès aux données médicales plus fluide et plus automatique afin d'améliorer la continuité des soins. Ce guide présente donc un intérêt majeur pour comprendre les mutations actuelles du droit du numérique en santé. Il illustre concrètement la manière dont les outils numériques modifient les relations entre patients, professionnels et établissements de santé. Il montre également que le développement du partage des données de santé nécessite un équilibre constant entre efficacité des soins, protection de la vie privée, cybersécurité et

respect des droits fondamentaux des patients.

ANS, *Guide professionnel de santé – Consultation Mon espace santé/DMP*, septembre 2025.

Actualisation des critères de référencement des services et outils numériques dans Mon espace santé

L'arrêté du 19 juin 2025 met à jour les critères applicables au référencement des services et outils numériques au sein du catalogue de Mon espace santé. Il remplace le référentiel de référencement précédemment en vigueur par une nouvelle version destinée à adapter les exigences applicables aux solutions numériques intégrées à l'espace numérique de santé. Cette évolution vise notamment à renforcer les garanties en matière de sécurité, d'interopérabilité, de protection des données et de qualité des services proposés aux usagers.

Arrêté du 19 juin 2025 modifiant l'arrêté du 20 novembre 2023 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé, JORF n° 0147 du 26 juin 2025.

Approbation du référentiel d'utilisation de l'application carte Vitale comme moyen d'identification à distance

L'arrêté du 5 février 2026 approuve le référentiel fixant les critères applicables à l'utilisation de l'application carte Vitale comme moyen d'identification à distance des usagers. Ce référentiel définit les exigences techniques, organisationnelles et de sécurité auxquelles doivent satisfaire les services souhaitant recourir à ce dispositif. Il vise à garantir un niveau élevé de confiance dans les procédures d'identification numérique tout en assurant la protection des données personnelles et la sécurisation des échanges dématérialisés.

Arrêté du 5 février 2026 approuvant le référentiel fixant les critères applicables en vue de la délivrance de l'autorisation d'utilisation de la carte Vitale sous forme d'application mobile comme moyen d'identification à distance des utilisateurs, *JORF* n° 0034 du 10/02/2026.

L'APPLICATION CARTE VITALE COMME MOYEN D'AUTHENTIFICATION À DISTANCE

L'application carte Vitale (apCV) ne constitue plus seulement une version dématérialisée de la carte Vitale. Elle a vocation à devenir un véritable outil d'identification numérique. Des services autorisés pourront ainsi s'appuyer sur l'application pour vérifier à distance l'identité d'un usager lors de démarches en ligne, sans présence physique. Le référentiel approuvé par l'arrêté fixe les garanties de sécurité, d'authentification et de protection des données applicables à cette utilisation.

SANTEXPO 2026

60ème édition

« L'excellence en santé : un engagement pour toutes les générations »

Le numérique en santé

Synthèse

Droit du numérique en santé

Thomas BOUDON
Étudiant en Master Droit de la santé
École de droit de Toulouse, Université Toulouse Capitole

D'après les notes du salon des 19, 20 et 21 mai 2026
Paris Expo, Porte de Versailles • Salon organisé par la Fédération hospitalière de France

GLOSSAIRE DES ABREVIATIONS

Les sigles et acronymes employés dans la synthèse sont rassemblés ci-dessous. Ils sont utilisés de manière uniforme dans le corps du texte, après une première mention développée lorsque la clarté l'exige.

Sigle	Signification
CE	conformité européenne (marquage)
CHU	centre hospitalier universitaire
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (loi américaine de 2018)
CNIL	Commission nationale de l'informatique et des libertés
CRA	règlement sur la cyberrésilience (Cyber Resilience Act)
DPO	délégué à la protection des données (data protection officer)
EDS	entrepôt de données de santé
EHDS	espace européen des données de santé (European Health Data Space)
FHIR	standard d'interopérabilité en santé (Fast Healthcare Interoperability Resources)
HDS	hébergeur de données de santé (certification)
IA	intelligence artificielle
MDR	règlement européen sur les dispositifs médicaux (Medical Device Regulation)
NIS 2	directive « Network and Information Security » 2
OpenEHR	standard ouvert de modélisation et de stockage du dossier de santé
RGPD	règlement général sur la protection des données
SecNumCloud	visa de sécurité national pour les services d'informatique en nuage (« cloud de confiance »)
TFUE	Traité sur le fonctionnement de l'Union européenne
UGAP	Union des groupements d'achats publics
UniHA	réseau coopératif des achats hospitaliers

AVANT-PROPOS

Du 19 au 21 mai 2026 s'est tenue, à Paris Expo – Porte de Versailles, la 60e édition du salon SANTEXPO, organisé par la Fédération hospitalière de France[196]. Placée sous le thème de **« l'excellence en santé »**, cette édition anniversaire a consacré plus de la moitié de sa programmation au numérique en santé, réunissant près de 36 000 participants, quelque 700 exposants et plus de 550 intervenants[197]. C'est à partir des notes prises au fil de ces trois journées, en représentation de l'Université Toulouse Capitole, qu'a été bâtie la présente synthèse.

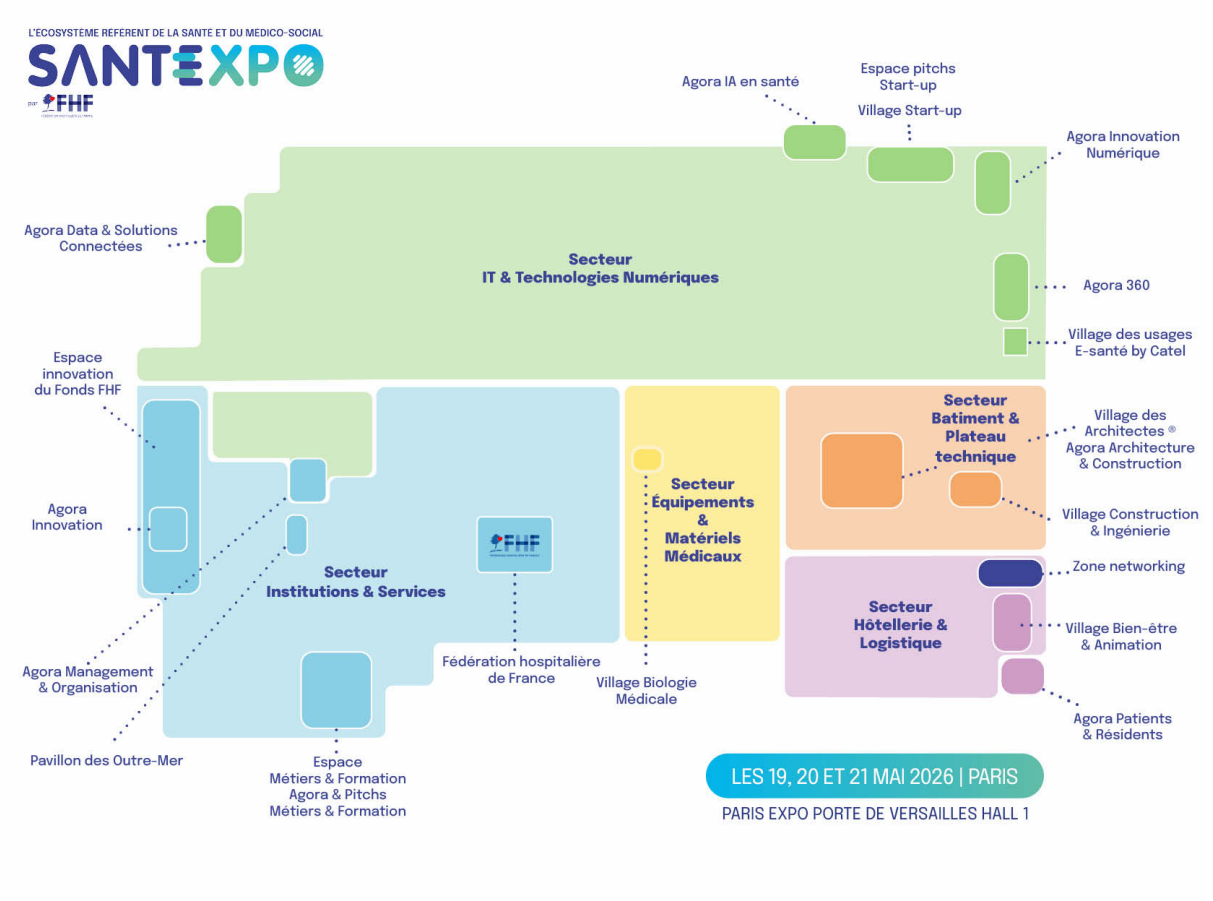


Figure — SANTEXPO 2026 — Plan su salon.

Le présent document n'est pas une restitution exhaustive du salon (objet d'une trace écrite distincte) mais un **exercice de synthèse** répondant à la méthodologie de la dissertation : amorce, délimitation du sujet, intérêt, problématisation, problématique et annonce de plan en introduction ; développement en trois parties articulées par de brèves transitions ; conclusion ouverte. La matière première demeure les notes du salon, mais le propos a été enrichi des enseignements du Master Droit de la Santé et du diplôme d'université *Digital Health Law*, ainsi que de recherches complémentaires. L'appareil de référencement en notes adopte le format de la bibliothèque de l'Université Toulouse Capitole.

Avertissement. La synthèse s'appuie sur des propos d'intervenants rapportés de mémoire et de notes personnelles ; ils n'engagent ni leurs auteurs, ni les organisations citées. Les chiffres et exemples issus du salon sont reproduits à titre documentaire, et les mentions de solutions ou d'éditeurs le sont à titre purement informatif. L'analyse, les rapprochements et les éventuelles erreurs n'engagent que l

eur auteur.

[196] Fédération Hospitalière de France, *SantExpo 2026* (consulté le 30/05/2026).
[197] APMnews, « L'excellence en santé, fil rouge de l'édition 2026 de Santexpo » [en ligne], 5 mai 2026 (consulté le 30/05/2026).

INTRODUCTION

Le 11 février 2024, peu après deux heures du matin, les imprimantes du centre hospitalier d'Armentières se sont mises à cracher une demande de rançon ; quatre-vingt-quinze pour cent du réseau était déjà chiffré, les urgences ont fermé soixante-douze heures, et l'établissement est revenu au papier. Quelques mois plus tard, lors de la soixantième édition du salon SANTEXPO, en mai 2026, un intervenant résumait l'épisode d'une formule qui a fait mouche : *« ce n'est pas un sujet informatique, c'est un sujet de soins »*. La phrase dit l'essentiel. Le numérique a cessé d'être un outil périphérique de l'hôpital pour en devenir le système nerveux, au point qu'une défaillance technique se traduit aujourd'hui en pertes de chances pour le patient, voire en décès.

Cette bascule est l'objet de la présente synthèse. Par « numérique en santé », on entend l'ensemble des technologies (dossiers patients informatisés, entrepôts de données, dispositifs médicaux logiciels, systèmes d'intelligence artificielle, infrastructures d'hébergement) qui transforment la production, la circulation et l'exploitation de l'information de santé. Le champ couvert dépasse le seul hôpital : il embrasse les trois composantes du système de santé français, le secteur sanitaire, le secteur social et le secteur médico-social[198], dont la réunion sous une même bannière demeure, du reste, davantage un horizon qu'une réalité homogène. Sur ce terrain mouvant s'est invité, en quelques années, un corpus de textes européens d'une densité inédite : règlement sur l'espace européen des données de santé (EHDS), règlement sur l'intelligence artificielle (IA), directive « NIS 2 », règlement sur la cyberrésilience (CRA), sans compter le socle que constituent le règlement général sur la protection des données (RGPD) et le règlement relatif aux dispositifs médicaux (MDR).

L'intérêt du sujet tient précisément à cette concomitance. Jamais le législateur de l'Union n'a, en si peu de temps, autant encadré un secteur ; et jamais le calendrier ne s'est fait aussi pressant, l'EHDS devant produire ses principaux effets dès 2029[199]. Or cette pression réglementaire rencontre un système de santé fragile : infrastructures héritées et cloisonnées, établissements publics corsetés par leur statut, financements contraints, disparités territoriales criantes, le tout dans un marché du numérique de santé encore neuf mais déjà férocement disputé, où les solutions les plus performantes sont souvent américaines. La transition n'est donc ni un simple projet de modernisation, ni une affaire de pure conformité : elle est le point de rencontre d'une contrainte juridique exogène, d'une nécessité opérationnelle endogène et d'une vulnérabilité structurelle.

De là naît une tension que les trois jours du salon n'ont cessé d'illustrer. D'un côté, une transformation imposée par le droit de l'Union et aspirée par un marché qui n'attend pas ; de l'autre, un appareil de soins inégalement préparé, dont les acteurs publics doivent composer avec des règles, qu'il s'agisse de la commande publique, de la fonction publique ou du principe de spécialité, pensées pour un autre temps. Entre les deux, des principes que nul ne saurait sacrifier : la souveraineté sur les données, la sécurité des systèmes, le respect des droits des patients.

Dans quelle mesure le système de santé français, dans ses composantes sanitaire, sociale et médico-sociale, est-il juridiquement et structurellement prêt à absorber une transition numérique imposée par le droit de l'Union et portée par un marché concurrentiel, sans sacrifier la

[198] *SantExpo 2026*, préc.

[199] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé, *JOUE* [en ligne], 5 mars 2025 ; entrée en vigueur le 26 mars 2025, application progressive (usage primaire en 2027, usage secondaire en 2029, catégories étendues en 2031) (consulté le 30/05/2026).

souveraineté, la sécurité ni les droits des patients ?

Répondre suppose d'abord de mesurer la force qui pousse à la transformation : une transition à marche forcée, sous la double aiguillon du droit européen et des nécessités du soin (I). Il faut ensuite confronter cet élan à la réalité d'un système inégalement armé pour l'absorber, où la maturité numérique des secteurs le dispute aux contraintes propres à l'acteur public (**II**). Il s'agira enfin de dégager les voies d'un équilibre juridique soutenable, à même de réconcilier souveraineté, performance, sécurité et droits des patients (**III**).

I. Une transition numérique à marche forcée

A. Une contrainte exogène : le droit de l'Union comme moteur

1. L'EHDS et la circulation des données de santé

Au sommet de l'édifice trône le règlement du 11 février 2025 relatif à l'EHDS[200]. Le choix de sa base juridique mérite qu'on s'y arrête, car il est révélateur : l'Union s'est fondée sur l'article 114 du Traité sur le fonctionnement de l'Union européenne (TFUE), relatif au marché intérieur, plutôt que sur l'article 168, qui ne lui reconnaît qu'une compétence d'appui en matière de santé[201]. Autrement dit, c'est par la logique du marché unique, et non par celle de la santé publique, que la Commission européenne a pu imposer un cadre contraignant. La donnée de santé devient une marchandise circulant librement. Et cette qualification commande tout le reste.

Deux usages structurent le règlement. D'abord, l'usage primaire consacre des droits nouveaux au bénéfice du patient : accès à ses données, portabilité, échange transfrontalier de son dossier et de ses prescriptions électroniques, le tout adossé à un format européen reposant sur le standard FHIR[202]. Ensuite, l'usage secondaire ouvre la réutilisation des données à des fins de recherche, d'innovation ou de pilotage des politiques publiques, via un guichet géré par un organisme responsable de l'accès aux données et soumis à autorisation. Son entrée en application est progressive : 2027 pour l'usage primaire, 2029 pour l'essentiel de l'usage secondaire, 2031 pour les catégories étendues[203]. L'échéance, elle, est désormais inscrite dans le marbre. Pour les établissements, le message est clair : l'interopérabilité n'est plus une option mais une obligation, et la certification des plateformes deviendra la condition même de l'accès au réseau européen. On comprend qu'au centre hospitalier universitaire (CHU) de Toulouse, les responsables avouaient se préparer « un peu à l'aveugle », faute d'actes d'exécution encore stabilisés.

2. L'IA Act et le MDR : la régulation des systèmes et des dispositifs

Adopté le 13 juin 2024, le règlement sur l'IA procède d'une tout autre méthode : horizontale, graduée selon le risque, et résolument extraterritoriale[204]. En santé, la plupart des systèmes déployés (aide au diagnostic, tri des patients, codage) basculent dans la catégorie à haut risque de l'annexe III, ce qui emporte des obligations lourdes de documentation, de transparence et de surveillance. Certes, le calendrier de ces obligations a été assoupli, le « Digital

---

[200] Règlement (UE) 2025/327 (EHDS), préc.

[201] *Traité sur le fonctionnement de l'Union européenne*, art. 114 (rapprochement des législations, marché intérieur), retenu comme base juridique du règlement EHDS de préférence à l'art. 168 (compétence d'appui en matière de santé publique).

[202] HL7 International, *HL7 FHIR, Fast Healthcare Interoperability Resources* [en ligne] (consulté le 30/05/2026).

[203] Règlement (UE) 2025/327 (EHDS), préc.

[204] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'IA), *JOUE* [en ligne], 12 juillet 2024 ; v. not. l'annexe III (systèmes à haut risque) et l'art. 40 (normes harmonisées) (consulté le 30/05/2026).

Omnibus » de novembre 2025 ayant repoussé certaines échéances[205], mais la direction ne fait pas de doute.

À ce premier texte se superpose le règlement de 2017 sur les dispositifs médicaux[206]. Dès lors qu'un logiciel poursuit une finalité médicale, il est un dispositif médical, soumis à une classification par niveau de risque et au marquage CE délivré sous le contrôle d'organismes notifiés. Ainsi, la solution d'aide à la décision présentée au salon était marquée CE en classe IIa, ses éditeurs devant articuler conformité au règlement sur les dispositifs et exigences à venir du règlement sur l'IA. Pareille double conformité n'a rien d'académique : un acteur étranger jugé non conforme, OpenEvidence, n'était à la date du salon accessible ni dans l'Union, ni au Royaume-Uni. La régulation produit donc déjà des effets de marché. Elle s'adosse d'ailleurs largement à la normalisation technique : les normes harmonisées, au sens de l'article 40 du règlement sur l'IA, valent présomption de conformité, déplaçant une part du pouvoir normatif vers des organismes privés[207].

3. NIS 2 et le Cyber Resilience Act : la cybersécurité érigée en obligation

Longtemps affaire de bonnes pratiques, la sécurité numérique est devenue une obligation juridique sanctionnée. Promulguée le 14 décembre 2022, la directive « NIS 2 » range la santé parmi les secteurs hautement critiques et classe les établissements, selon leur taille et leur nature, en entités essentielles ou importantes[208]. Trois obligations en découlent : s'enregistrer auprès de l'autorité compétente, notifier les incidents significatifs, et déployer des mesures de gestion des risques déclinées par le référentiel cyber national, qui fixe une vingtaine d'objectifs de sécurité[209]. Quant au CRA, entré en vigueur fin 2024 et applicable par paliers jusqu'en 2027, il complète le dispositif en imposant une sécurité « dès la conception » aux fabricants de produits comportant des éléments numériques, tout au long de leur cycle de vie[210].

Quelques chiffres disent l'urgence. En 2024, les établissements de santé ont déclaré quelque sept cent cinquante incidents, en hausse de près de trente pour cent[211], et l'on a observé une augmentation de cent treize pour cent des accidents vasculaires cérébraux mal pris en charge dans les hôpitaux victimes d'une attaque. La cybersécurité a quitté le champ technique pour entrer dans celui de la sécurité des soins.

---

[205] Commission européenne, *Digital Omnibus*, proposition de simplification du cadre numérique de l'Union [en ligne], 19 novembre 2025 (consulté le 30/05/2026).

[206] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux (MDR), *JOUE* [en ligne], n° L 117, 5 mai 2017 (consulté le 30/05/2026).

[207] Organisation internationale de normalisation, *NF EN ISO/IEC 27001:2023, Systèmes de management de la sécurité de l'information* [en ligne] (consulté le 30/05/2026).

[208] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive NIS 2), *JOUE* [en ligne], n° L 333, 27 décembre 2022 (consulté le 30/05/2026).

[209] Agence nationale de la sécurité des systèmes d'information, *Référentiel cyber France (ReCyF)* [en ligne], 2026 (consulté le 30/05/2026).

[210] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences horizontales de cybersécurité pour les produits comportant des éléments numériques (Cyber Resilience Act), *JOUE* [en ligne], 20 novembre 2024 ; entré en vigueur le 10 décembre 2024, application par paliers jusqu'en décembre 2027 (consulté le 30/05/2026).

[211] Agence du numérique en santé / CERT Santé, *Observatoire des signalements d'incidents de sécurité des SI pour le secteur santé, bilan 2025* [en ligne], 2026 (consulté le 30/05/2026).

B. Une nécessité endogène : efficience, qualité et attractivité

1. Désenclaver et structurer des données silotées

Si le droit pousse, le besoin tire. Producteur de données massives, l'hôpital français les enferme pourtant. Un établissement compte couramment des centaines de logiciels qui ne se parlent pas ; tel centre exploitait encore en 2024 un dossier patient mis en service en 1999. Faute d'urbanisation d'ensemble, les systèmes se sont empilés par strates successives. Sur le remède, le consensus est large : une logique d'interopérabilité « par les interfaces » et un entrepôt de données de santé (EDS) capable de centraliser, d'historiser et d'exposer l'information. Encore faut-il ne pas confondre les fonctions, que se partagent plusieurs familles de standards. Pour l'échange entre systèmes, le pivot s'appelle FHIR[212] : il fait circuler la donnée d'un logiciel à l'autre. Pour le stockage, deux standards complémentaires coexistent : OpenEHR[213], qui modélise et conserve le dossier clinique au fil du soin, et OMOP[214], modèle commun qui range et harmonise la donnée dans l'entrepôt, en vue de l'analyse et de la réutilisation. Les uns communiquent, les autres structurent ; c'est leur articulation qui fait la cohérence de l'ensemble. Et le constat, partout au salon, était le même : sans interopérabilité, l'IA reste inopérante, car un modèle n'a de valeur qu'adossé à des données fiables, structurées et croisées. Recueillie au plus près du soin, la qualité de la donnée conditionne tout l'édifice.

2. Libérer du temps soignant et fluidifier le parcours patient

Vient ensuite l'argument du temps. Près de quatre dixièmes du temps de travail hospitalier seraient absorbés par des tâches répétitives ou administratives. Sur ce point, les promesses de gains sont considérables : comptes rendus et lettres de liaison rédigés par assistance vocale, codage des séjours accéléré, synthèse automatique du dossier. Un centre hospitalier avançait une diminution de quarante pour cent du temps de ses agents administratifs ; un acteur du médico-social, une baisse de soixante pour cent du temps de saisie grâce à la dictée. Au-delà de l'efficience, c'est l'attractivité qui est en jeu : recentrer le soignant sur la relation au patient, dans un contexte de pénurie, constitue un argument de recrutement. Même logique pour la fluidification du parcours (télésurveillance des patients chroniques, anticipation des flux aux urgences, coordination ville-hôpital), à la condition expresse que l'humain conserve la décision finale.

3. Se positionner dans un marché neuf et concurrentiel

Une dernière force, plus diffuse, achève d'entraîner le mouvement : la pression du marché. Jeune mais foisonnant, le numérique de santé voit coexister éditeurs historiques convertis à l'IA, plateformes intégrées et myriade de jeunes pousses. En 2024, la France comptait plusieurs centaines d'entreprises de santé numérique, dont près de deux cents pour la seule Occitanie[215]. Une solution française d'IA médicale (MedGPT) revendiquait sept cent mille connexions mensuelles. Dans ce contexte, ne pas se doter d'outils numériques, c'est risquer de décrocher, et ce sur deux plans. Verticalement (micro-vertical), dans la relation au patient : recourant aux assistants conversationnels grand public, celui-ci en vient à interroger son médecin, qui doit à son tour disposer d'outils spécialisés et fiables. Horizontalement (méso-horizontal), entre acteurs de santé : dans des parcours toujours

---

[212] HL7 International, *HL7 FHIR*, préc.

[213] openEHR International, *openEHR Specifications* [en ligne]. Standard ouvert de modélisation et de persistance du dossier de santé (consulté le 30/05/2026).

[214] Observational Health Data Sciences and Informatics, *OMOP Common Data Model* [en ligne] (consulté le 30/05/2026).

[215] APMnews, art. préc.

plus coordonnés, l'établissement ou le professionnel qui n'échange pas ses données se marginalise, sort des circuits d'adressage et se fait contourner par ceux qui, eux, savent se connecter. Le décrochage n'est donc pas seulement commercial, il est relationnel : rester dans le jeu suppose de rester interopérable. Se positionner devient ainsi un impératif de survie autant qu'un choix de gestion : l'image de l'établissement, sa place dans les réseaux de soins et sa capacité à fidéliser les compétences en dépendent. Sa face sombre, la concentration entre quelques mains étrangères, n'apparaîtra qu'au stade des contraintes. À ces deux échelles s'en ajoute une troisième, plus vaste : celle de la France et de l'Union européenne face à la concurrence internationale. Mais à ce niveau, le numérique cesse d'être un simple atout concurrentiel pour devenir une question de souveraineté, dont la face sombre, la concentration du marché entre quelques mains étrangères, n'apparaîtra qu'au stade des contraintes.

Ces forces convergentes, à savoir l'obligation venue de la Commission européenne, la quête d'efficience et la concurrence, dessinent une dynamique puissante. Encore faut-il que le système soit en état d'en soutenir le choc. Or rien n'est moins sûr : la maturité numérique reste très inégale d'un secteur à l'autre, et l'acteur public se heurte à des contraintes que le marché ignore.

II. UN SYSTÈME INÉGALEMENT ARMÉ POUR L'ABSORBER

A. Une maturité numérique différenciée selon les secteurs

1. Le sanitaire : richesse des données, faiblesse des infrastructures

Côté sanitaire, le paradoxe est saisissant. Les données y sont d'une richesse rare : l'Assistance publique-Hôpitaux de Paris suit huit millions de patients par an, et certains centres disposent de quarante années d'historique exploitable. Mais les infrastructures peinent à suivre. Huit cents applications cohabitent parfois au sein d'un même groupe, le dossier patient demeure peu structuré, et certains progiciels de référence, anciens et éprouvés, n'évoluent plus qu'à grand-peine. On dénombrait cent vingt-cinq EDS autorisés par la Commission nationale de l'informatique et des libertés (CNIL), signe d'une dynamique réelle ; mais le pays ne disposait que de trois supercalculateurs publics, ce qui borne sa capacité d'entraînement de modèles. Richesse de la matière première, pauvreté de l'outillage : le contraste est frappant.

2. Le social et le médico-social : un retard préoccupant

Dès que l'on quitte l'hôpital, le tableau s'assombrit. Le social et le médico-social accusent un retard de numérisation préoccupant, que traduit le déploiement encore embryonnaire du dossier usager informatisé. Quant au programme national de cybersécurité, il ne s'y est ouvert que tardivement : l'appel à projets dédié aux établissements et services sociaux et médico-sociaux n'a été lancé, sous forme expérimentale, qu'en mars 2026, pour une vingtaine de lauréats et moins de deux millions d'euros[216]. Pourtant, les usages prometteurs ne manquent pas (robotique sociale, exosquelettes de prévention des troubles musculo-squelettiques, réalité

[216] Agence du numérique en santé, *Programme CaRE : cybersécurité, accélération et résilience des établissements* [en ligne] (consulté le 30/05/2026).

virtuelle apaisante pour les résidents atteints de troubles cognitifs), mais ils se déploient sur un socle fragile, où la maturité cybersécuritaire reste faible et la mobilisation des acteurs encore timide. Ici, le défi est moins technologique qu'organisationnel et financier.

3. La ville et la coordination des parcours : l'enjeu de la responsabilité populationnelle

Entre l'hôpital et le domicile, la ville constitue le maillon le plus difficile à intégrer. Souvent prisonnières des cabinets libéraux, les données y restent dispersées, ce qui contraint à bâtir des passerelles spécifiques. Or l'enjeu dépasse la seule technique : il s'agit d'assumer une responsabilité populationnelle, c'est-à-dire de penser la santé d'un territoire entier, en stratifiant la population par niveau de risque et en réunissant un consortium ville-hôpital. Déployée dans plusieurs milliers de pharmacies, la téléconsultation assistée répond directement aux déserts médicaux ; la directive de 2011 sur les soins transfrontaliers[217] avait, dès avant l'EHDS, posé les jalons d'une mobilité du patient. Mais la coordination suppose une information fiable, disponible au bon moment et à la bonne personne : exactement ce que le morcellement actuel rend malaisé.

B. Des acteurs publics juridiquement et économiquement contraints

1. Le statut public : commande publique et fonction publique hospitalière

C'est ici que le juriste retrouve son terrain. Établissement public, l'hôpital est un pouvoir adjudicateur, soumis au Code de la commande publique et à ses principes cardinaux : liberté d'accès, égalité de traitement des candidats, transparence des procédures[218]. Dès 2003, le Conseil constitutionnel leur a reconnu valeur constitutionnelle[219]. Ces garanties, précieuses pour le bon emploi des deniers publics, ont un revers : la lenteur. Là où le marché du numérique se renouvelle en quelques mois, la passation d'un marché public s'étire, impose la rédaction de clauses techniques exigeantes (en lien avec le responsable de la sécurité et le délégué à la protection des données, le DPO) et se heurte aux conditions générales d'utilisation, non négociables, des grands fournisseurs. D'où un risque, maintes fois souligné au salon : que « les bonnes solutions arrivent trop tard ».

Pour desserrer cet étau, les établissements peuvent passer par une centrale d'achat. En se fournissant auprès de l'UGAP, établissement public industriel et commercial, ou d'un réseau coopératif hospitalier comme UniHA, qui s'interposent entre les EPS et les industriels, l'acheteur s'épargne sa propre procédure : la mise en concurrence a déjà été faite en amont[220]. Le gain de temps est réel, mais il a une contrepartie. La centrale prélève une commission, et surtout l'établissement choisit dans un catalogue déjà référencé : son éventail se réduit aux solutions retenues par l'opérateur. Le contournement de la lenteur se paie ainsi d'un libre choix plus étroit, et la commodité tend à orienter l'achat autant que le besoin propre de l'établissement. La centrale est donc une réponse ambivalente, dont on retrouvera le versant vertueux, la mutualisation, au stade des solutions.

À la rigidité de l'achat s'ajoute celle de l'emploi. Avec son recrutement par concours et ses grilles, la fonction publique

---

[217] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* [en ligne], n° L 88, 4 avril 2011 (consulté le 30/05/2026).

[218] *Code de la commande publique*, art. L. 3 (principes de liberté d'accès à la commande publique, d'égalité de traitement des candidats et de transparence des procédures, garants de l'efficacité de la commande publique et de la bonne utilisation des deniers publics).

[219] Conseil constitutionnel, décision n° 2003-473 DC du 26 juin 2003 (consécration de la valeur constitutionnelle des principes fondamentaux de la commande publique).

[220] *Code de la commande publique*, art. L. 2113-2 et s. (centrales d'achat).

hospitalière peine à attirer des compétences rares, ingénieurs en données ou spécialistes de la sécurité, que le privé surpaye. Vieillissement des effectifs, dont un tiers a passé la cinquantaine, et débat récurrent sur le poids des fonctions administratives compliquent encore l'équation. Le facteur humain, en définitive, pèse autant que le facteur technique.

2. Des financements et un retour sur investissement incertains, sur fond de disparités territoriales

L'argent commande, et il manque. Contraints, les budgets hospitaliers le sont à l'heure où le retour sur investissement des projets d'IA demeure difficile à objectiver : il faut le mesurer sur quatre registres (opérationnel, économique, qualité des soins et gouvernance) sans se contenter d'une démonstration de laboratoire. Des financements fléchés existent, du programme de cybersécurité doté de sept cent cinquante millions d'euros[221] au volet numérique du Ségur de la santé[222] ; mais un projet pilote réussi ne préjuge en rien d'un passage à l'échelle, lequel coûte cher et tarde à produire ses fruits. Surtout, ces moyens se répartissent inégalement. Un grand CHU et un petit hôpital de proximité ne disposent ni des mêmes équipes, ni de la même capacité d'investissement : la fracture numérique épouse la fracture territoriale, et la première creuse la seconde.

3. Une dépendance technologique extra-européenne : la souveraineté entre impératif et surcoût

C'est alors que réapparaît le marché, sous son visage inquiétant. Près des deux tiers du marché mondial du cloud sont contrôlés par trois acteurs américains, et l'écrasante majorité des grands modèles d'IA sont conçus hors d'Europe. Or le droit américain, par le CLOUD Act de 2018, autorise un accès extraterritorial aux données hébergées par ces entreprises[223]. La souveraineté numérique, c'est-à-dire la localisation des données dans l'Union, leur traitement depuis l'Union, le contrôle opérationnel et la maîtrise contractuelle, n'est donc pas un slogan, mais une réponse à une vulnérabilité juridique réelle, que la loi visant à sécuriser et réguler l'espace numérique a entendu renforcer[224]. Le hic est son coût. Choisir la souveraineté, c'est souvent renoncer aux solutions les plus performantes, et payer plus cher : l'arbitrage se joue entre fiabilité, coût et souveraineté, et il pèse d'autant plus lourd que l'établissement est modeste. La boucle se referme ainsi sur les disparités territoriales.

Le diagnostic est posé : une transition irrésistible se heurte à un système inégalement préparé et à un acteur public bridé. Plutôt que d'y voir une impasse, le droit offre les instruments d'un équilibre, à condition de concilier ce qui paraît d'abord inconciliable : la souveraineté et la performance, puis la valorisation des données, leur sécurité et les droits des patients.

III. UN ÉQUILIBRE JURIDIQUE À CONSTRUIRE POUR UNE TRANSITION SOUTENABLE

A. Concilier souveraineté et performance

1. La maîtrise de l'hébergement et des données

Un premier levier est juridico-technique. En santé, l'exigence portant sur l'hébergement est doublement justifiée. La donnée est sensible, d'abord, au sens où sa divulgation porte gravement atteinte à la vie

[221] Agence du numérique en santé, *Programme CaRE*, préc.
[222] Agence du numérique en santé, *Ségur du numérique en santé* [en ligne] (consulté le 30/05/2026).
[223] États-Unis, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Pub. L. n° 115-141, 23 mars 2018.
[224] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, *JORF* [en ligne], n° 0119, 22 mai 2024 (consulté le 30/05/2026).

privée de la personne[225] ; mais elle est aussi engagée dans le soin, car elle nourrit le diagnostic et la décision thérapeutique. Ce n'est donc pas seulement sa confidentialité qu'il faut garantir, c'est aussi son intégrité et sa disponibilité, dont dépend directement la sécurité du patient. Voilà pourquoi tout hébergement de données de santé est subordonné à la certification HDS[226], à laquelle s'ajoute, pour les usages les plus sensibles, le référentiel SecNumCloud de l'agence nationale de la sécurité des systèmes d'information, qui qualifie le « cloud de confiance »[227]. Le panel s'est étoffé : cloud public souverain, cloud privé régulé (où l'hébergeur s'interdit l'accès aux données et où l'établissement conserve les clés de chiffrement), architectures hybrides. D'ailleurs, la pratique a trouvé un compromis astucieux : tester et entraîner les modèles sur un cloud public, plus rapide et moins onéreux, puis déployer en local la solution retenue, au plus près des données sensibles. Au fond, la souveraineté n'exige pas de renoncer à toute performance ; elle commande de cartographier, pour chaque usage, le niveau de protection juridiquement adéquat.

2. La mutualisation comme réponse

Plus organisationnel, le second levier répond directement aux contraintes du statut public. Rendus obligatoires par la loi de modernisation de notre système de santé de 2016, les groupements hospitaliers de territoire imposent une convergence des systèmes d'information qui mutualise compétences et investissements[228]. Cette logique se prolonge dans les centrales d'achat : l'Union des groupements d'achats publics, établissement public industriel et commercial, et le réseau coopératif hospitalier UniHA jouent le rôle de tiers de confiance entre les établissements et les industriels, et dispensent l'acheteur d'une partie du formalisme[229]. À l'échelle supérieure, le partage de l'innovation entre établissements publics (« briques » réplicables, infrastructures de calcul communes à plusieurs centres universitaires) permet de répartir le coût de la souveraineté et d'atténuer les disparités territoriales. Ce que la rigidité de la commande publique freine d'un côté, la mutualisation le débloque de l'autre.

B. Concilier valorisation, sécurité et droits des patients

1. Une valorisation encadrée et non lucrative de la donnée

Réelle, la valeur des données françaises découle d'un trait que l'on ne soupçonne pas toujours : l'égalité d'accès aux soins produit des jeux de données diversifiés, donc fiables, là où des systèmes plus inégalitaires les biaisent. Encore faut-il valoriser sans dénaturer. À cette fin, le régime de l'usage secondaire de l'EHDS recourt à un système de redevances dont la finalité n'est pas lucrative : on ne vend pas la donnée, on facture un appui méthodologique[230]. En droit interne, l'architecture est connue : Système national des données de santé[231],

---

[225] Règlement (UE) 2016/679 (RGPD), art. 9 (interdiction de principe et protection renforcée du traitement des catégories particulières de données, dont les données concernant la santé).

[226] Ministère chargé de la santé / Agence du numérique en santé, *Certification des hébergeurs de données de santé (HDS)* [en ligne] (consulté le 30/05/2026).

[227] Agence nationale de la sécurité des systèmes d'information, *SecNumCloud : référentiel d'exigences pour les prestataires de services d'informatique en nuage* [en ligne] (consulté le 30/05/2026).

[228] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* [en ligne], n° 0022, 27 janvier 2016 (groupements hospitaliers de territoire, art. L. 6132-1 du *Code de la santé publique*) (consulté le 30/05/2026).

[229] *Code de la commande publique*, art. L. 2113-2 et s. (centrales d'achat). L'Union des groupements d'achats publics (UGAP), établissement public à caractère industriel et commercial, et le réseau coopératif hospitalier UniHA agissent comme centrales d'achat au service des acheteurs publics de santé.

[230] Règlement (UE) 2025/327 (EHDS), préc.

[231] Commission nationale de l'informatique et des libertés, *Le Système national des données de santé (SNDS)* [en ligne] (consulté le 30/05/2026).

Health Data Hub comme guichet[232], réseau régional d'entrepôts. Et la stratégie nationale de réutilisation pour 2025-2028, issue d'un rapport de 2023, en a fait sa boussole, plaçant la confiance au cœur du dispositif[233]. Soulignée par les praticiens du salon, la frontière juridique est nette : une exploitation lucrative ne se conçoit que sur des données anonymisées, sorties du champ du RGPD[234] ; jamais sur des données simplement pseudonymisées. La CNIL, devenue accompagnatrice plus que gendarme, y veille par ses méthodologies de référence, dans la logique de responsabilisation des acteurs.

2. La cybersécurité, condition de la continuité des soins

Certaines exigences ne se négocient pas, et la première est la sécurité informatique. Longtemps réduite à une affaire d'informaticiens, elle se laisse aujourd'hui saisir par une grille à quatre exigences, résumées par l'acronyme DICP : la disponibilité de la donnée, son intégrité, sa confidentialité et la preuve, c'est-à-dire la traçabilité des accès. Ces quatre propriétés ne protègent pas seulement un patrimoine informationnel ; elles conditionnent la possibilité même de soigner. Une donnée indisponible au moment du diagnostic, ou silencieusement altérée, se paie en perte de chances pour le patient. Voilà pourquoi le programme national de cybersécurité ne se contente plus de prévenir l'attaque : il impose d'organiser la survie du SI. Mise en place d'une gouvernance cybersécurité, construction et test d'un plan de continuité et de reprise d'activité, volet numérique du plan blanc, bilans d'impact sur l'activité destinés à identifier les fonctions vitales à rétablir en priorité : l'établissement doit désormais penser le fonctionnement en mode dégradé[235]. L'épisode du centre hospitalier d'Armentières, contraint de revenir au papier durant des semaines, a montré que la question n'est pas de savoir si la panne surviendra, mais comment continuer à soigner lorsqu'elle survient. La cybersécurité a ainsi cessé d'être un sujet technique pour devenir une dimension de la sécurité des soins.

3. Les droits du patient et l'éthique, socle intangible

Reste le ou un socle primordial, celui que nulle promesse d'efficience ne saurait entamer : les droits de la personne et les principes éthiques. Le secret médical, consacré par le Code de la santé publique et réaffirmé par la loi du 4 mars 2002[236], l'information claire, loyale et appropriée, ainsi que le consentement, explicite pour les données sensibles et écrit pour les données génétiques en droit français[237], encadrent strictement la circulation de l'information. Mais le numérique déplace la difficulté : il ne suffit plus de protéger la donnée, il faut garder la maîtrise de la décision qu'elle nourrit. C'est tout le sens de la garantie humaine du recours à l'IA, codifiée à l'article L. 4001-3 du Code de la santé publique depuis la loi de bioéthique de 2021, qui impose information, traçabilité et maintien d'un contrôle humain[238]. La réflexion éthique avait préparé le terrain :

---

[232] Plateforme des données de santé (*Health Data Hub*), *Missions et projet HealthData@EU Pilot* [en ligne] (consulté le 30/05/2026).

[233] MARCHAND-ARVIER (J.), *Faire de la France un pays pionnier de la réutilisation des données de santé*, rapport [en ligne], 2023, fondant la stratégie nationale de réutilisation des données de santé 2025-2028 (consulté le 30/05/2026).

[234] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD), *JOUE* [en ligne], n° L 119, 4 mai 2016 (consulté le 30/05/2026).

[235] Agence du numérique en santé, *Programme CaRE*, préc.

[236] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* [en ligne], 5 mars 2002 ; v. égal. *Code de la santé publique*, art. L. 1110-4 (secret médical).

[237] Règlement (UE) 2016/679 (RGPD), art. 9 (traitement portant sur des catégories particulières de données, dont les données concernant la santé et les données génétiques).

[238] *Code de la santé publique*, art. L. 4001-3 (garantie humaine du recours aux dispositifs médicaux recourant à l'intelligence artificielle), issu

dans leur avis commun de 2022 sur le diagnostic médical et l'IA, le Comité consultatif national d'éthique et le Comité national pilote d'éthique du numérique mettaient en garde contre toute logique de substitution à l'humain et prônaient l'explicabilité des résultats comme la collégialité du regard[239]. Ces exigences prolongent les quatre principes cardinaux de la bioéthique, à savoir l'autonomie, la bienfaisance, la non-malfaisance et la justice, qui en numérique se traduisent en transparence, loyauté et qualité. Encore faut-il les faire vivre : comités d'éthique, coordinateurs de la donnée distincts du DPO, cartographie des usages pour endiguer l'« IA de l'ombre », et surtout formation des professionnels, l'agence nationale estimant que près des trois quarts des incidents seraient évitables par une sensibilisation adéquate. Comme le résumait un dirigeant hospitalier, la sagesse de l'IA vient par la méthode.

CONCLUSION

Le système de santé français n'est pas prêt ; mais il se prépare, et c'est précisément la contrainte européenne qui l'y force. Tel est le paradoxe que révèle SANTEXPO 2026 : le foisonnement normatif de l'Union, souvent vécu comme un fardeau, agit en réalité comme un double ressort. D'un côté, un accélérateur qui impose l'interopérabilité, la sécurité et la traçabilité ; de l'autre, un garde-fou qui hisse les données françaises au rang d'actif de confiance, plus diversifié et mieux protégé que ceux des grands marchés concurrents. La transition est imposée et nécessaire ; le système est inégalement armé, l'acteur public plus contraint que tout autre ; et l'équilibre, lorsqu'il s'esquisse, repose moins sur la technique que sur le droit : souveraineté arbitrée plutôt que proclamée, mutualisation contre fragmentation, valorisation encadrée, sécurité et droits érigés en limites intangibles.

L'horizon, toutefois, demeure incertain. En 2029 puis 2031, les échéances de l'EHDS mettront à l'épreuve la capacité réelle des établissements à tenir le calendrier. L'essor de l'IA agentique, conjugué à la hausse continue de son coût, rouvrira la question de la dépendance technologique et du risque de décrochage européen. Quant au mouvement de simplification amorcé par le « Digital Omnibus », il dira si l'Union sait alléger sa propre charge sans renier ses ambitions. Au-delà des textes et des infrastructures, c'est peut-être la relation entre le patient et le soignant qui sera le plus sûr révélateur de la transition : selon que l'outil numérique libère du temps pour le soin ou s'interpose dans le colloque singulier, il l'aura confortée ou appauvrie. Une certitude demeure : dans un domaine où une panne se mesure en pertes de chances pour le patient, le droit n'est pas l'ennemi de l'innovation, mais la condition de la confiance sans laquelle aucune transition numérique de la santé ne sera humainement et socialement acceptable.

de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique.

[239] Comité consultatif national d'éthique et Comité national pilote d'éthique du numérique, Avis n° 141 du CCNE et n° 4 du CNPEN, « Diagnostic médical et intelligence artificielle : enjeux éthiques » [en ligne], novembre 2022 (consulté le 30/05/2026).

BIBLIOGRAPHIE

Sont recensées ci-dessous les sources citées en notes de bas de page, classées par nature et présentées selon les conventions de la bibliothèque de l'Université Toulouse Capitole.

I. Textes de l'Union européenne

Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé, *JOUE* [en ligne], 5 mars 2025 ; entrée en vigueur le 26 mars 2025, application progressive (usage primaire en 2027, usage secondaire en 2029, catégories étendues en 2031) (consulté le 30/05/2026).

Traité sur le fonctionnement de l'Union européenne, art. 114 (rapprochement des législations, marché intérieur), retenu comme base juridique du règlement EHDS de préférence à l'art. 168 (compétence d'appui en matière de santé publique).

Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* [en ligne], n° L 88, 4 avril 2011 (consulté le 30/05/2026).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD), *JOUE* [en ligne], n° L 119, 4 mai 2016 (consulté le 30/05/2026).

Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux (MDR), *JOUE* [en ligne], n° L 117, 5 mai 2017 (consulté le 30/05/2026).

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'IA), *JOUE* [en ligne], 12 juillet 2024 ; v. not. l'annexe III (systèmes à haut risque) et l'art. 40 (normes harmonisées) (consulté le 30/05/2026).

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive NIS 2), *JOUE* [en ligne], n° L 333, 27 décembre 2022 (consulté le 30/05/2026).

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences horizontales de cybersécurité pour les produits comportant des éléments numériques (Cyber Resilience Act), *JOUE* [en ligne], 20 novembre 2024 ; entré en vigueur le 10 décembre 2024, application par paliers jusqu'en décembre 2027 (consulté le 30/05/2026).

Commission européenne, *Digital Omnibus*, proposition de simplification du cadre numérique de l'Union [en ligne], 19 novembre 2025 (consulté le 30/05/2026).

II. Textes nationaux et droit étranger

Code de la commande publique, art. L. 3 (principes de liberté d'accès à la commande publique, d'égalité de traitement des candidats et de transparence des procédures, garants de l'efficacité de la commande publique et de la bonne utilisation des deniers publics).

Conseil constitutionnel, décision n° 2003-473 DC du 26 juin 2003 (consécration de la valeur constitutionnelle des principes fondamentaux de la commande publique).

Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* [en ligne], n° 0022, 27 janvier 2016 (groupements hospitaliers de territoire, art. L. 6132-1 du *Code de la santé publique*) (consulté le 30/05/2026).

Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* [en ligne], 5 mars 2002 ; v. égal. *Code de la santé publique*, art. L. 1110-4 (secret médical) (consulté le 30/05/2026).

Code de la santé publique, art. L. 4001-3 (garantie humaine du recours aux dispositifs médicaux recourant à l'intelligence artificielle), issu de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique.

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, *JORF* [en ligne], n° 0119, 22 mai 2024 (consulté le 30/05/2026).

Code de la commande publique, art. L. 2113-2 et s. (centrales d'achat). L'Union des groupements d'achats publics (UGAP), établissement public à caractère industriel et commercial, et le réseau coopératif hospitalier UniHA agissent comme centrales d'achat au service des acheteurs publics de santé.

États-Unis, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Pub. L. n° 115-141, 23 mars 2018.

III. Rapports, doctrine et sources institutionnelles

Fédération Hospitalière de France, *SantExpo 2026* [en ligne] (consulté le 30/05/2026).

APMnews, « L'excellence en santé, fil rouge de l'édition 2026 de Santexpo » [en ligne], 5 mai 2026 (consulté le 30/05/2026).

Agence du numérique en santé, *Programme CaRE : cybersécurité, accélération et résilience des établissements* [en ligne] (consulté le 30/05/2026).

Agence du numérique en santé / CERT Santé, *Observatoire des signalements d'incidents de sécurité des SI pour le secteur santé, bilan 2025* [en ligne], 2026 (consulté le 30/05/2026).

MARCHAND-ARVIER (J.), *Faire de la France un pays pionnier de la réutilisation des données de santé*, rapport [en ligne], 2023, fondant la stratégie nationale de réutilisation des données de santé 2025-2028 (consulté le 30/05/2026).

Commission nationale de l'informatique et des libertés, *Le Système national des données de santé (SNDS)* [en ligne] (consulté le 30/05/2026).

Plateforme des données de santé (*Health Data Hub), Missions et projet HealthData@EU Pilot* [en ligne] (consulté le 30/05/2026).

Ministère chargé de la santé / Agence du numérique en santé, *Certification des hébergeurs de données de santé (HDS)* [en ligne] (consulté le 30/05/2026).

Agence nationale de la sécurité des systèmes d'information, *SecNumCloud : référentiel d'exigences pour les prestataires de services d'informatique en nuage* [en ligne] (consulté le 30/05/2026).

Agence du numérique en santé, *Ségur du numérique en santé* [en ligne] (consulté le 30/05/2026).

Agence nationale de la sécurité des systèmes d'information, *Référentiel cyber France (ReCyF)* [en ligne], 2026 (consulté le 30/05/2026).

Comité consultatif national d'éthique et Comité national pilote d'éthique du numérique, *Avis n° 141 du CCNE et n° 4 du CNPEN, « Diagnostic médical et intelligence artificielle : enjeux éthiques »* [en ligne], novembre 2022 (consulté le 30/05/2026).

IV. Normes et standards techniques

HL7 International, *HL7 FHIR, Fast Healthcare Interoperability Resources* [en ligne] (consulté le 30/05/2026).

Observational Health Data Sciences and Informatics, *OMOP Common Data Model* [en ligne] (consulté le 30/05/2026).

OpenEHR International, *openEHR Specifications* [en ligne]. Standard ouvert de modélisation et de persistance du dossier de santé (consulté le 30/05/2026).

Organisation internationale de normalisation, *NF EN ISO/IEC 27001:2023, Systèmes de management de la sécurité de l'information* [en ligne] (consulté le 30/05/2026).

Droit belge

Soutien financier à l'utilisation de la télématique et des dossiers médicaux électroniques par les médecins

L'arrêté royal du 25 juillet 2025 modifie le régime applicable à l'intervention financière accordée aux médecins pour l'utilisation de la télématique et la gestion électronique des dossiers médicaux. Il actualise plusieurs critères conditionnant l'octroi de cette intervention, notamment en lien avec l'utilisation effective des outils numériques de santé, de la facturation électronique, des services MyCareNet ainsi que du partage sécurisé des données de santé. Le dispositif s'inscrit dans la politique de numérisation des pratiques médicales et de renforcement de l'interopérabilité des systèmes d'information en santé.

Arrêté royal modifiant l'arrêté royal du 30 juin 2017 fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux médecins pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux, *M.B* du 25/07/2025.

Extension du soutien financier aux sage-femmes pour l'utilisation de la télématique

L'arrêté royal du 30 octobre 2025 fixe les conditions dans lesquelles les sage-femmes peuvent bénéficier d'une intervention financière de l'INAMI pour l'utilisation de la télématique et la gestion électronique des dossiers des patientes. Le dispositif est subordonné à plusieurs conditions relatives à l'activité professionnelle, à l'adhésion à la convention nationale ainsi qu'à l'utilisation effective d'outils numériques et de la facturation électronique. Cette mesure participe à l'intégration des sage-femmes dans la stratégie de numérisation des soins et au développement des usages numériques au sein des professions de santé.

Arrêté royal fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux sage-femmes pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux en 2025, *M.B* du 30/10/2025.

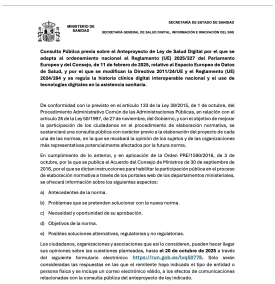
Droit espagnol

Resolución de 1 de diciembre de 2025, de la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, por la que se publica el Convenio con la Sociedad Española de Informática de la Salud, para impulsar la transformación digital del Sistema Nacional de Salud, « BOE » núm. 294, de 08/12/2025

Cette résolution, publiée au Bulletin officiel du 8 décembre 2025, rend publique une convention de coopération conclue entre la Direction générale de la santé numérique et des systèmes d'information du Système national de santé espagnol et la Société espagnole d'informatique de santé (SEIS). L'accord vise à soutenir la transformation numérique du système de santé espagnol au moyen d'actions conjointes de réflexion, d'expertise, de formation et de diffusion des connaissances. Il porte notamment sur l'interopérabilité des systèmes d'information, la gouvernance des données de santé, l'intelligence artificielle, la cybersécurité et les services numériques de santé.

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD (SEIS)

Fondée en 1977, la Société espagnole d'informatique de santé (SEIS) est une association scientifique et professionnelle dédiée au développement du numérique en santé en Espagne. Elle réunit des professionnels de santé, experts en systèmes d'information, chercheurs, administrations publiques et entreprises du secteur afin de promouvoir l'innovation, l'interopérabilité et la transformation numérique du système de santé.



MINISTERIO DE SANIDAD

SECRETARÍA DE ESTADO DE SANIDAD

SECRETARÍA GENERAL DE SALUD DIGITAL, INFORMACIÓN E INNOVACIÓN DEL SNS

Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria.

De conformidad con lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en relación con el artículo 26 de la Ley 50/1997, de 27 de noviembre, del Gobierno, y con el objetivo de mejorar la participación de los ciudadanos en el procedimiento de elaboración normativa, se sustanciará una consulta pública con carácter previo a la elaboración del proyecto de cada una de las normas, en la que se recabará la opinión de los sujetos y de las organizaciones más representativas potencialmente afectados por la futura norma.

En cumplimiento de lo anterior, y en aplicación de la Orden PRE/1590/2016, de 3 de octubre, por la que se publica el Acuerdo del Consejo de Ministros de 30 de septiembre de 2016, por el que se dictan instrucciones para habilitar la participación pública en el proceso de elaboración normativa a través de los portales web de los departamentos ministeriales, se ofrecerá información sobre los siguientes aspectos:

a) Antecedentes de la norma.

b) Problemas que se pretenden solucionar con la nueva norma.

c) Necesidad y oportunidad de su aprobación.

d) Objetivos de la norma.

e) Posibles soluciones alternativas, regulatorias y no regulatorias.

Los ciudadanos, organizaciones y asociaciones que así lo consideren, pueden hacer llegar sus opiniones sobre las cuestiones planteadas, hasta **el 20 de octubre de 2025** a través del siguiente formulario electrónico https://sun.gob.es/bsg59776. Solo serán consideradas las respuestas en las que el remitente haya indicado el tipo de entidad o persona física y en incluya un correo electrónico válido, a los efectos de comunicaciones relacionadas con la consulta pública del anteproyecto de ley indicado.

Consultation publique sur l'avant-projet de loi relatif à la santé numérique

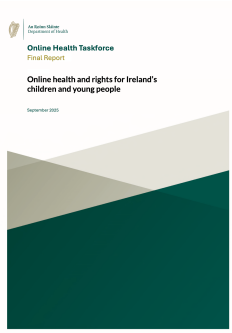
Le ministère espagnol de la Santé lance une consultation publique en vue de l'élaboration d'un avant-projet de loi destiné à adapter le droit espagnol au règlement (UE) 2025/327 relatif à l'Espace européen des données de santé (EHDS). Le texte ne se limite toutefois pas à cette adaptation. Il poursuit plus largement l'objectif de consolider le cadre juridique espagnol en matière de santé numérique et de l'articuler avec les nouvelles exigences européennes. **La consultation publique s'est déroulée du 22 septembre au 20 octobre 2025**.

L'avant-projet prévoit notamment :

- le renforcement de l'interopérabilité de l' « histoire clinique numérique » (« *historia clínica digital interoperable* ») ;
- l'amélioration de l'accès et du contrôle des patients sur leurs données de santé électroniques ;
- l'organisation d'une gouvernance nationale et régionale des données de santé ;
- l'intégration de l'Espagne aux infrastructures européennes prévues par l'EHDS ;
- l'encadrement de l'utilisation des technologies numériques dans le domaine sanitaire, notamment l'intelligence artificielle, la biométrie et les neurotechnologies.

Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria.

Droit irlandais



Department of Health (An Roinn Sláinte), *Online Health Taskforce. Final Report : Online health and rights for Ireland's children and young people*, September 2025

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Instituée en septembre 2024 par le ministère de la Santé irlandais (*Department of Health*) et présidée par l'ancienne sénatrice Jillian van Turnhout, l'Online Health Taskforce (ci-après « OHT ») a remis un rapport final daté de septembre 2025, que la ministre de la Santé Jennifer Carroll MacNeill a rendu public le 12 décembre 2025[240]. Ce rapport propose, dans une perspective de santé publique, une réponse aux défis auxquels sont confrontés les enfants et les jeunes dans l'environnement numérique. Les travaux se sont appuyés sur une *National Youth Assembly on Youth Online Health* tenue le 9 juillet 2025, sur une consultation des parties prenantes qui a recueilli 86 contributions, sur un rapport de l'*Institute of Public Health* consacré à l'exposition des enfants au marketing en ligne de produits nocifs pour la santé,

Established in September 2024 by the Department of Health (*An Roinn Sláinte*) and chaired by former Senator Jillian van Turnhout, the Online Health Taskforce (hereinafter 'OHT') delivered a final report dated September 2025, which the Minister for Health, Jennifer Carroll MacNeill, made public on 12 December 2025[249]. The report sets out, from a public health perspective, a response to the challenges facing children and young people in the digital environment. The work drew upon a *National Youth Assembly on Youth Online Health* held on 9 July 2025, a stakeholder consultation which received 86 submissions, a report by the *Institute of Public Health* on children's exposure to the online marketing of health-harming products, and a review of the international scientific literature. The whole is structured around four

[240] Online Kealth Taskforce, Final Report: Online health and rights for Ireland's children and young people, Department of Health, sept. 2025; Jennifer Carroll MacNeill (ministre de la Santé), communiqué de presse, gov.ie, 12 déc. 2025.

[249] Online Health Taskforce, *Final Report: Online Health and Rights for Ireland's Children and Young People* (Department of Health 2025); Jennifer Carroll MacNeill (Minister for Health), press release (gov.ie, 12 December 2025).

ainsi que sur une revue de la littérature scientifique internationale. L'ensemble s'articule autour de quatre principes fondateurs et de dix recommandations opérationnelles.

I. LES PRINCIPES FONDATEURS : LES DROITS DE L'ENFANT COMME BOUSSOLE

Des droits équivalents en ligne et hors ligne. Le premier principe repose sur une évidence qui reste largement à concrétiser. Dans l'environnement numérique, les enfants et les jeunes doivent bénéficier des mêmes droits que dans le monde physique : santé, vie privée, sécurité, participation, liberté d'expression, accès à l'information et à l'éducation, protection contre les préjudices. Le rapport se réclame ici directement de l'Observation générale n° 25 (2021) du Comité des droits de l'enfant des Nations Unies[241], laquelle avait fixé le cadre.

Cohérence, coopération, agilité. Les trois autres principes prolongent cette exigence. Il est demandé au gouvernement d'assurer une cohérence entre stratégies publiques, cadres législatifs et mécanismes de financement, afin que les espaces en ligne comme hors ligne offrent aux mineurs les conditions de leur épanouissement. Le rapport appelle par ailleurs l'Irlande à porter ces enjeux au niveau international. Enfin, la Taskforce insiste sur la nécessité d'une recherche suffisamment agile pour suivre le rythme des évolutions technologiques.

Les dix recommandations opérationnelles qui suivent se répartissent en cinq domaines d'action.

Le premier insiste sur la nécessité d'une approche fondée sur les droits des enfants et des jeunes, supposant en particulier une co-construction des

foundational principles and ten operational recommendations.

I. THE FOUNDATIONAL PRINCIPLES : CHILDREN'S RIGHTS AS GUIDING COMPASS

Equivalent rights online and offline. The first principle rests on a proposition that remains largely to be put into practice. In the digital environment, children and young people should enjoy the same rights as those afforded to them in the physical world: health, privacy, safety, participation, freedom of expression, access to information and education, as well as protection from harm. The report draws here directly on General Comment No. 25 (2021) of the UN Committee on the Rights of the Child[250], which had set the framework.

Coherence, cooperation, agility. The three other principles take this requirement further. Government is required to ensure coherence across public strategies, legislative frameworks and funding mechanisms, so that both online and offline spaces offer minors the conditions for their development. The report also calls on Ireland to champion these issues at the international level. Finally, the Taskforce insists on the need for a research agenda capable of keeping pace with the speed of technological change.

The ten operational recommendations that follow fall within five areas of action.

The first stresses the need for a children's and young people's rights-based approach, which supposes in particular that solutions be co-designed with minors themselves. The second concerns safety by design, coupled with the introduction of a legally binding age-

[241] Comité des droits de l'enfant des Nations Unies, Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique, CRC/C/GC/25, 2 mars 2021.
[250] UN Committee on the Rights of the Child, 'General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment' UN Doc CRC/C/GC/25 (2 March 2021).

solutions avec les mineurs eux-mêmes. Le deuxième concerne la sécurité dès la conception (*Safety by Design*), qu'accompagne la mise en place d'un système de classification par âge juridiquement contraignant. Le troisième porte sur la littératie numérique critique, que le rapport entend déployer dans l'ensemble du système éducatif. Le quatrième, consacré à l'application effective du droit et à la responsabilité, cible spécifiquement les systèmes de recommandation algorithmique. Quant au cinquième, il traite de l'articulation avec la réglementation européenne et nationale.

II. L'ARTICULATION AVEC LE DROIT DE L'UNION EUROPEENNE

A. Le DSA comme socle, le Digital Fairness Act comme perspective

Le règlement n° 2022/2065/UE du 19 octobre 2022 relatif au marché unique des services numériques[242] (ci-après « DSA »), applicable en Irlande depuis février 2024, constitue le socle du raisonnement. La recommandation n° 3 invite l'Irlande à plaider, à l'échelle européenne, pour que les fournisseurs de produits et services numériques intègrent les principes de *Child Rights by Design* dans la conception de leurs services et algorithmes. Sont visées ici les lignes directrices adoptées par la Commission européenne en juillet 2025 sur le fondement de l'article 28 du DSA, lequel est consacré à la protection des mineurs en ligne[243].

La question des systèmes de recommandation algorithmique est au

classification system. The third addresses critical digital literacy, which the report proposes to roll out across the entire education system. The fourth, devoted to enforcement and accountability, specifically targets recommender systems. As for the fifth, it concerns the articulation between EU and national regulation.

II. ARTICULATION WITH EU LAW

A. The DSA as foundation, the Digital Fairness Act as horizon

Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services[251] (hereinafter 'DSA'), in force in Ireland since February 2024, forms the starting point of the reasoning. Recommendation 3 calls on Ireland to advocate, at European level, for all providers of digital products and services to embed Child Rights by Design principles into the design of their services and algorithms. The intended reference point here is the guidance adopted by the European Commission in July 2025 on the basis of Article 28 of the DSA, which addresses the protection of minors online[252].

The question of recommender systems lies at the heart of Recommendation 6, which calls on platforms to put in place effective risk-mitigation measures, and on regulators to enforce the obligations arising under the DSA, particularly as regards the swift removal of illegal content. The Taskforce goes one step further: should platforms fail to comply with both the DSA and the *Online Safety and Media Regulation Act 2022* (OSMRA), the liability exemption

[242] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive n° 2000/31/CE (règlement sur les services numériques), *JOUE* n° L 277 du 27/10/2022.
[243] Commission européenne, G*uidelines on the protection of minors online under Article 28(1) of the Digital Services Act*, *C(2025)* 4613 final, 14 juillet 2025.
[251] Regulation n° 2022/2065/EU of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] *OJ* L277/1.
[252] European Commission, 'Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act' *C(2025)* 4613 final (14 July 2025).

cœur de la recommandation n° 6, qui appelle les plateformes à mettre en œuvre des mesures effectives d'atténuation des risques, et les régulateurs à faire respecter le DSA, notamment s'agissant du retrait rapide des contenus illicites. La Taskforce pousse le raisonnement un cran plus loin : à défaut pour les plateformes de respecter le DSA et l'*Online Safety and Media Regulation Act 2022* (OSMRA), l'exonération de responsabilité dont elles bénéficient pour les contenus préjudiciables mais légaux mériterait, selon lui, d'être reconsidérée. La prise de position n'est pas anodine. Elle traduit une forme de tension entre l'approche européenne, largement centrée sur les obligations de transparence et d'évaluation des risques systémiques qui pèsent sur les très grandes plateformes (*VLOPs*/*VLOSEs*), et l'ambition irlandaise d'aller au-delà de la seule modération de contenu, pour s'attaquer à la conception même des services. L'Organisation mondiale de la santé (OMS) avait d'ailleurs, dans ses travaux de 2025 consacrés aux déterminants numériques de la santé mentale des jeunes[244], noté cette inflexion, relevant que l'Irlande s'intéressait désormais aux « *addictive design features* » [« caractéristiques de conception addictive »] des plateformes.

La présidence irlandaise du Conseil et le Digital Fairness Act. Le rapport ne se limite pas à une lecture du droit en vigueur. Par sa recommandation n° 9, il exhorte le gouvernement irlandais à se saisir de la présidence du Conseil de l'Union européenne, qui débutera en juillet 2026, pour favoriser une convergence des politiques nationales en la matière. La recommandation n° 10, enfin, soutient le projet de *Digital Fairness Act* (DFA), qui vise à combler les lacunes du droit de la consommation

they benefit from for harmful but legal content ought, in its view, to be reconsidered. That position is a significant one. It reflects a genuine tension between the European approach, which is largely built around transparency obligations and systemic risk assessments imposed on very large platforms (*VLOPs*/*VLOSEs*), and the Irish ambition to move beyond content moderation alone and address the very design of the services themselves. The World Health Organization, in its 2025 work on the digital determinants of youth mental health[253], had already noted this shift, observing that Ireland was now turning its attention to the 'addictive design features' of platforms.

The Irish Presidency of the Council and the Digital Fairness Act. The report does not confine itself to a reading of the existing law. Through Recommendation 9, it urges the Irish Government to seize upon its forthcoming Presidency of the Council of the European Union, which will begin in July 2026, as an opportunity to foster convergence among national policies in this field. Recommendation 10, for its part, supports the *Digital Fairness Act* (DFA) project, which aims to close the gaps left by existing consumer law in tackling online commercial practices. Ireland advocates an ambitious reading: a self-standing regulation conceived as the 'digital twin' of the Unfair Commercial Practices Directive, carrying a general prohibition on unfair digital commercial practices as well as an explicit ban on targeted advertising directed at minors on the basis of sensitive data within the meaning of Article 9 of the GDPR. The report thereby draws, once again, a bridge between consumer protection, personal-data protection and the protection of minors.

[244] Organisation mondiale de la santé (Bureau régional de l'Europe), *Commercial determinants of youth mental health: a policy brief*, OMS, 2025.
[253] World Health Organization Regional Office for Europe, *Commercial Determinants of Youth Mental Health: A Policy Brief* (WHO 2025)

face aux pratiques commerciales en ligne. L'Irlande y défend une lecture ambitieuse : un règlement autonome, conçu comme le « jumeau numérique » de la directive sur les pratiques commerciales déloyales, qui prohiberait les pratiques numériques déloyales et interdirait expressément la publicité ciblée adressée aux mineurs sur la base de données sensibles au sens de l'article 9 du RGPD. Voilà qui fait le pont, déjà esquissé ailleurs dans le texte, entre protection des consommateurs, protection des données à caractère personnel et protection des mineurs.

B. Les convergences avec le règlement européen sur l'IA

Bien que le rapport ne se présente pas comme un texte de transposition du règlement n° 2024/1689/UE du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle[245] (ci-après « RIA » ou « AI Act »), il en croise nettement les préoccupations. Les systèmes de recommandation algorithmique y sont traités comme l'une des sources majeures de risques pour les mineurs : le rapport les définit comme des systèmes d'IA qui profilent le comportement des individus pour déterminer les contenus qui leur sont présentés, afin de maximiser leur engagement. Or cette qualification fonctionnelle n'est pas sans effet au regard du RIA. Appliqués à des enfants, de tels systèmes peuvent basculer dans la catégorie des pratiques manipulatoires prohibées par l'article 5 ; à défaut, ils relèveront au minimum des systèmes à haut risque, avec évaluation de conformité associée.

Le rapport accorde à l'IA générative une attention particulière en relevant la multiplication des contenus d'abus

B. Convergences with the EU AI Regulation

Although the report does not present itself as a text of transposition of Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence[254] (hereinafter 'AI Act'), it clearly intersects with the European legislator's concerns. Recommender systems are treated as one of the main sources of risk to minors: the report defines them as AI systems that profile individuals' behaviour in order to determine what content is shown to them, with a view to maximising engagement. Now that functional classification is not without consequence under the AI Act. When applied to children, such systems may fall within the category of manipulative practices prohibited by Article 5; failing that, they will qualify, at the very least, as high-risk systems subject to conformity assessment.

Generative AI receives particular attention from the report, which notes the rise in AI-generated child sexual abuse material, as well as the emergence of *chatbots* that form pseudo-relationships with children, sometimes of a sexual nature, and give them misleading advice, including in the field of mental health. The *National Youth Assembly* calls, in that context, for the creation and distribution of *deepfakes* to be banned. That request aligns with the transparency obligations which Article 50 of the AI Act now imposes on systems generating synthetic content. Departing from the established instruments, the report finally suggests an original avenue: that of a Digital Child Safety Certification, inspired by the CE marking applied to physical toys[255]. Such a scheme could, in time, dovetail with the conformity

[245] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, *JOUE* n° L 2024/1689, 12 juill. 2024.
[254] Regulation n° 2024/1689/EU of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] *OJ* L2024/1689
[255] Council Directive 88/378/EEC of 3 May 1988 on the approximation of the laws of the Member States concerning the safety of toys [1988] OJ L187/1; Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] *OJ* L170/1.

sexuels sur mineurs générés par IA, ainsi que le développement de *chatbots* qui nouent avec les enfants de fausses relations, parfois à dimension sexuelle, et leur prodiguent des conseils erronés, y compris dans le champ de la santé mentale. La *National Youth Assembly* demande, dans ce contexte, que soit prohibée la création et la diffusion de *deepfakes* ; l'exigence converge avec les obligations de transparence que l'article 50 du RIA impose désormais aux systèmes générant des contenus synthétiques. À rebours des textes existants, le rapport propose enfin une piste originale : celle d'une *Digitale Child Safety Certification*, inspirée du marquage CE applicable aux jouets physiques[246]. Ce dispositif pourrait, à terme, entrer en dialogue avec les procédures d'évaluation de conformité que le RIA prévoit pour les systèmes à haut risque, et ouvrir la voie à une certification intégrée des produits numériques destinés aux mineurs.

C. Le cadre national et le rôle du Coimisiún na Meán

L'Irlande n'est pas démunie face à ces enjeux. L'OSMRA[247] avait déjà, en 2022, institué le Coimisiún na Meán en tant que régulateur de la sécurité en ligne, et introduit un *Online Safety Code* imposant certaines obligations aux plateformes de partage de vidéos établies sur le territoire, particulièrement en matière de vérification d'âge. Plusieurs limites sont cependant pointées du doigt par le rapport. Le champ d'application du dispositif, d'abord, reste étroit et ne couvre qu'une catégorie restreinte de services numériques. La marge d'appréciation laissée aux plateformes, ensuite, apparaît excessive.

Renforcer les moyens et les pouvoirs du Coimisiún na Meán. La

assessment procedures that the AI Act provides for high-risk systems and pave the way for integrated certification of digital products designed for minors.

C. The national framework and the role of Coimisiún na Meán

Ireland is not ill-equipped when it comes to these issues. The OSMRA[256] had already, in 2022, established Coimisiún na Meán as the online safety regulator, and introduced an *Online Safety Code* imposing certain obligations on video-sharing platforms established in Ireland, particularly in relation to age verification. Several shortcomings are nevertheless identified by the report. The scope of the framework, first, remains narrow and covers only a limited category of digital services. The margin of appreciation left to platforms, further, appears excessive.

Strengthening the resources and powers of Coimisiún na Meán. Recommendation 7 calls for the regulator to be given adequate resources, both financial and human. It further suggests conferring upon it broader powers. Among those envisaged are the possibility of geo-blocking online services and VPNs, the option to conditionally disable recommender algorithms as regards minors, and the implementation of robust age verification at the national level, in cooperation with other European regulators and the Commission.

A personal liability for directors and officers. Recommendation 8 is more ambitious still. Drawing inspiration from the precedent set by the *Data Protection Act 2018*[257] in the field of data protection, it proposes amending the OSMRA in order to introduce personal liability for directors and officers of companies

[246] Directive n° 88/378/CEE du Conseil du 3 mai 1988 concernant le rapprochement des législations des États membres relatives à la sécurité des jouets, *JOUE* n° L 187 du 16/07/1988 ; Directive n° 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets, *JOUE* n° L 170 du 30/06/2009.
[247] Irlande, *Online Safety and Media Regulation Act 2022*, Act n° 41 of 2022, promulguée le 10 décembre 2022.
[256] Online Safety and Media Regulation Act 2022.
[257] Data Protection Act 2018, ss 146 and 149.

recommandation n° 7 appelle à doter le régulateur de ressources adéquates, financières comme humaines. Elle suggère également de lui conférer des pouvoirs élargis. Sont notamment visés la possibilité de procéder au géo-blocage de services en ligne et de VPN, celle de désactiver conditionnellement les algorithmes de recommandation à l'égard des mineurs, ou encore la mise en œuvre d'une vérification d'âge robuste au niveau national, en coopération avec les autres régulateurs européens et la Commission.

Une responsabilité personnelle des dirigeants. La recommandation n° 8 est plus audacieuse encore. S'inspirant du précédent établi par le *Data Protection Act 2018*[248] en matière de données, elle propose de modifier l'OSMRA pour instituer une responsabilité personnelle des dirigeants et administrateurs d'entreprises fournissant des produits et services numériques, en cas de manquement aux réglementations de sécurité en ligne affectant la santé, la sécurité ou le bien-être des enfants et des jeunes. La proposition prend place dans un débat européen plus vaste sur la responsabilisation des décideurs au sein des entreprises technologiques.

III. PORTEE DU RAPPORT

Le rapport de l'OHT se distingue par son parti pris : aborder la sécurité en ligne comme une question de santé publique, et non comme un simple problème de régulation des contenus. Il prend d'ailleurs expressément ses distances avec l'idée d'une interdiction générale des smartphones pour les enfants, jugée « trop grossière comme instrument ». Le modèle qu'il propose combine au contraire régulation structurelle des plateformes, littératie numérique et autonomisation des mineurs.

providing digital products and services, where their undertaking breaches online safety regulations affecting the health, safety and wellbeing of children and young people. The proposal fits into the broader European debate on the accountability of decision-makers within technology companies.

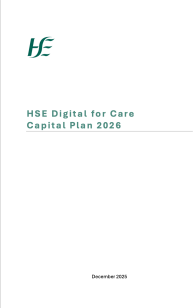
III. SCOPE OF THE REPORT

What sets the OHT report apart is its approach: to treat online safety as a public health issue rather than a narrow problem of content regulation. It explicitly distances itself from the idea of a blanket ban on smartphones for children, deemed 'too blunt an instrument'. The model it puts forward combines instead the structural regulation of platforms, digital literacy and the empowerment of minors.

This report thus illustrates in a remarkable way how a Member State transposes and extends, through soft law instruments, the requirements of the DSA, the GDPR and the AI Act. The recommendations it sets out moreover foreshadow the debates of the forthcoming Irish Presidency of the Council of the European Union (commencing in July 2026), which could thereby elevate the digital health of minors to the status of a European political priority. The digital safety certification of children and the conditional disabling of recommendation algorithms already provide a number of illustrations of this.

[248] Irlande, *Data Protection Act 2018*, Act n° 7 of 2018, sections 146 et 149 (responsabilité personnelle des dirigeants en cas de manquement commis avec leur consentement, leur complicité ou imputable à leur négligence).

Ce rapport montre ainsi de façon remarquable comment un État membre transpose et prolonge, au moyen d'instruments de soft law, les exigences du DSA, du RGPD et du RIA. Les recommandations formulées préfigurent par ailleurs les débats de la prochaine présidence irlandaise du Conseil de l'Union européenne (à compter de juillet 2026), laquelle pourrait ainsi élever la santé numérique des mineurs au rang de priorité politique européenne. La certification de sécurité numérique des enfants ou la désactivation conditionnelle des algorithmes de recommandation en offrent déjà quelques illustrations.



Health Service Executive (HSE), *Digital for Care Capital Plan 2026*, December 2025
et
Department of Health (An Roinn Sláinte), *National Development Plan Review 2025 – Sectoral Investment Plan : Department of Health 2026–2030*, July 2025

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

En l'espace de quelques mois, la santé numérique irlandaise s'est dotée de deux instruments de planification complémentaires qu'il convient de lire ensemble. L'un fixe l'enveloppe de l'année 2026. L'autre en trace la trajectoire pluriannuelle.

Le plan annuel pour 2026. Publié par le *Health Service Executive* (HSE) en décembre 2025, le *Digital for Care Capital Plan 2026* est l'instrument annuel d'investissement numérique en santé. Il découle directement de la stratégie-cadre *Digital for Care: A Digital Health Framework for Ireland 2024–2030*[258], approuvée par le gouvernement et intégrée à la réforme *Sláintecare*. L'enveloppe prévue pour 2026 s'élève à 263 millions d'euros (contre 190 M€ en 2025), dont 70 % fléchés vers les projets de transformation.

Parmi ces projets, plusieurs méritent l'attention. Le dossier patient électronique national (*HSE One Health Record – NEHR*, 36 M€) en constitue le premier poste d'investissement, en vue d'un déploiement dans les six régions sanitaires. On peut citer également l'application mobile *HSE Health App* (mise à disposition du public depuis février 2025), laquelle intègre un

Within the space of a few months, Irish digital health has been equipped with two complementary planning instruments which should be read together. The first sets the financial envelope for 2026. The second maps out its multiannual trajectory.

The annual plan for 2026. Published by the *Health Service Executive* (HSE) in December 2025, the *Digital for Care Capital Plan 2026* is the annual instrument of digital investment in health. It flows directly from the overarching strategy *Digital for Care: A Digital Health Framework for Ireland 2024–2030*[262], which was approved by Government and is integrated into the *Sláintecare* reform. The envelope provided for 2026 comes to €263 million (as against €190 million for 2025), of which 70 percent is earmarked for transformation projects.

Among those projects, several deserve attention. The national electronic patient record (*HSE One Health Record – NEHR*, €36 million) constitutes its leading investment line, with a view to deployment across the six health regions. Mention may also be made of the *HSE Health App* mobile application (made available to the public from February 2025), which carries an explicit

[258] Department of health (Irlande), Digital for Care: A Digital Health Framework for Ireland 2024–2030, Department of Health, May 2024.
[262] Department of Health, *Digital for Care: A Digital Health Framework for Ireland 2024–2030* (Department of Health 2024).

engagement explicite en matière d'obligations européennes (MyHealth@EU/EEDS). S'y ajoutent le dossier de soins partagé (*Shared Care Record*), la prescription électronique (*ePrescribing*), les soins virtuels et le télésuivi, le déploiement de solutions d'IA conformes à la stratégie *AI for Care* (identification d'AVC, radiologie, échocardiogrammes), ainsi qu'un volet cybersécurité adossé à la directive NIS 2[259].

Ce plan illustre bien la dynamique d'intégration du système de santé irlandais dans l'architecture européenne. La référence à MyHealth@EU rattache en effet l'Irlande au dispositif de l'espace européen des données de santé[260] (EEDS). L'*Individual Health Identifier* (IHI) institué par le *Health Identifiers Act 2014* anticipe, de son côté, les exigences d'identification transfrontalière posées par le règlement EEDS. Le volet cybersécurité prolonge enfin cette même dynamique du côté de la protection des systèmes d'information.

La trajectoire pluriannuelle à horizon 2030. Ce plan annuel ne prend tout son sens qu'à la lecture du plan sectoriel de santé publié en juillet 2025 dans le cadre de la révision du *National Development Plan* (NDP). Celui-ci alloue une enveloppe de 9,25 milliards d'euros aux infrastructures de santé et à la numérisation pour la période 2026–2030. Jamais l'État irlandais n'avait consenti un tel investissement en infrastructures de santé publique.
La section 3.3 du plan, intitulée « *Digital for Care* », décline les six principes de la

commitment in relation to European obligations (MyHealth@EU/EHDS). Added to this are the *Shared Care Record*, *ePrescribing*, virtual care and remote monitoring, the deployment of AI solutions aligned with the *AI for Care* strategy (stroke identification, radiology, echocardiograms), and a cybersecurity strand anchored on the NIS 2 Directive[263].

This plan illustrates the gradual integration of the Irish health system into the European digital health architecture. The reference to MyHealth@EU does in fact anchor Ireland within the apparatus of the European Health Data Space[264] (EHDS). The *Individual Health Identifier* (IHI) established by the *Health Identifiers Act 2014*, for its part, anticipates the cross-border identification requirements laid down by the EHDS Regulation. The cybersecurity strand, finally, extends the same dynamic on the side of information-system protection.

The multiannual trajectory to 2030. This annual plan only takes on its full meaning when read against the health sectoral plan published in July 2025 as part of the revision of the *National Development Plan* (NDP). The latter allocates an envelope of €9.25 billion to health infrastructure and digitalisation for the period 2026–2030. Never before has the Irish State committed such an investment in public health infrastructure.
Section 3.3 of the plan, entitled '*Digital for Care*', sets out the six principles of the overarching strategy adopted in May 2024: the patient as empowered partner, digital modernisation of the workplace, digitally connected care, data-driven services, the digital-health innovation

[259] Directive n° 2022/2555/UE du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive NIS 2), *JOUE* n° L 333 du 27/12/2022.
[260] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* n° L 2025/327 du 5/03/2025.
[263] Directive n° 2022/2555/EU of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) [2022] *OJ* L333/80
[264] Regulation n° 2025/327/EU of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] *OJ* L2025/327

stratégie-cadre adoptée en mai 2024 : le patient responsable de sa santé, la modernisation numérique du milieu de travail, les soins connectés, les services fondés sur les données, l'écosystème d'innovation en santé numérique et les fondations sécurisées. Le programme *Digitally Enabled and Connected Care*, qui concentre les financements dans le dossier de santé électronique national, la prescription électronique, le *National Shared Care Record* et les soins virtuels, est doté à lui seul d'une enveloppe supérieure à un milliard d'euros. Le volet *Secure Foundations & Digital Enablers* bénéficie quant à lui d'un investissement compris entre 500 millions et un milliard.

Sont identifiés expressément, comme moteurs réglementaires de cette transformation, les obligations découlant du règlement EEDS, de la directive NIS 2, du RIA et du *Health Information Act 2026*. Le plan est clair sur ce point : tout retard dans ces investissements exposerait l'Irlande à des risques de non-conformité. On mentionnera enfin l'ouverture, en 2026, du *National Children's Hospital Ireland* (NCHI), pensé comme le premier hôpital public entièrement numérique du pays : un jalon emblématique de la stratégie.

L'ampleur de l'effort consenti apparaît toutefois à la mesure du retard accumulé. Selon l'indicateur de la Décennie numérique 2025 relatif à l'accès aux dossiers de santé électroniques[261], l'Irlande occupe la dernière place (25 %) parmi les vingt-neuf pays évalués, loin de la moyenne européenne (83 %) et des 100 % atteints par l'Estonie, dont l'infrastructure X-Road est pourtant opérationnelle depuis 2001. Ce n'est donc pas tant d'un rattrapage qu'il s'agit que d'un démarrage, certes intensif.

ecosystem, and secure foundations. The *Digitally Enabled and Connected Care* programme, which funds the national electronic health record, ePrescribing, the *National Shared Care Record* and virtual care, is alone provided with an envelope exceeding one billion euros. The *Secure Foundations & Digital Enablers* strand, for its part, benefits from an investment of between €500 million and €1 billion.

The plan expressly identifies, as regulatory drivers of this transformation, the obligations flowing from the EHDS Regulation, the NIS 2 Directive, the AI Act and the *Health Information Act 2026*. The plan is unambiguous on this point: any delay in these investments would expose Ireland to non-compliance risks. Mention should finally be made of the opening, in 2026, of the *National Children's Hospital Ireland* (NCHI), conceived as the first fully digital public hospital in the country: an emblematic milestone within the strategy.

The scale of the commitment made is, however, commensurate with the scale of the lag accumulated. According to the Digital Decade 2025 indicator on access to electronic health records[265], Ireland occupies last place (with a score of 25 percent) among the twenty-nine countries assessed, a considerable distance from the European average (83 percent) and from the 100 percent reached by Estonia, whose X-Road infrastructure has nonetheless been operational since 2001. It is therefore less a matter of catching up than of a belated start, albeit one now pursued intensively.

[261] Communication de la Commission européenne sur l'état d'avancement de la décennie numérique, *COM(2025)*290 final du 16/06/2025.
[265] European Commission, 'Digital Decade Report 2025' SWD(2025) 290 (June,16 2025)/


Number 10 of 2026
Health Information Act 2026

Health Information Act 2026, No. 10 of 2026, signed into law by the President of Ireland on 30 April 2026

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Déposé en juillet 2024 par le *Ministère de la Santé* devant le *Dáil Éireann*, le *Health Information Bill 2024* (ci-après « HIA » ou « la loi ») a été longuement débattu et amendé, puis adopté en première lecture par le *Dáil Éireann* le 19 novembre 2025, avant d'être transmis devant le *Seanad Éireann*. Après examen et amendements, le texte a finalement été adopté par les deux chambres et promulgué par le Président de la République le 30 avril 2026 sous le titre de Health Information Act 2026 (n° 10 of 2026)[266].

La loi porte une ambition considérable. Elle se veut l'instrument par lequel l'Irlande donne effet, dans son ordre juridique interne, au règlement n° 2025/327/UE relatif à l'espace européen des données de santé (ci-après « EEDS » ou « règlement EHDS »). Le texte s'inscrit par ailleurs dans le prolongement du *Health Identifiers Act 2014*[267] et de la réforme *Sláintecare*, et confère au *Health Service Executive* (Direction des services de santé ; ci-après « HSE ») un rôle pivot dans l'architecture nationale de gestion des données de santé électroniques.

Introduced in July 2024 by the *Department of Health* to *Dáil Éireann*, the *Health Information Bill 2024* (hereinafter 'HIA' or 'the Act') was debated at length and amended, then passed at first reading by *Dáil Éireann* on 19 November 2025, before being referred to the *Seanad Éireann*. Following examination and amendments, the text was finally passed by both Houses and signed into law by the President of Ireland on 30 April 2026 under the title of Health Information Act 2026 (No. 10 of 2026)[273].

The Act carries considerable ambition. It is intended as the instrument by which Ireland gives effect, in its domestic legal order, to Regulation (EU) 2025/327 on the European Health Data Space (hereinafter 'EHDS' or 'EHDS Regulation'). The Act also fits within the line of the *Health Identifiers Act 2014*[274] and of the *Sláintecare* reform, and confers on the *Health Service Executive* (hereinafter 'HSE') a pivotal role in the national architecture governing electronic health data.

[266] Irlande, *Health Information Act 2026*, n° 10 of 2026 ; Bill n° 61 of 2024 déposé le 19 juill. 2024 devant le Dáil Éireann ; texte adopté en première lecture le 19 nov. 2025 et transmis devant le Seanad Éireann, promulgué par le Président de la République d'Irlande le 30 avril 2026.
[267] Irlande, *Health Identifiers Act 2014*, Act n° 15 of 2014.
[273] Health Information Act 2026 (No 10 of 2026); originating as the Health Information Bill 2024 (Bill No 61 of 2024) introduced on 19 July 2024 before Dáil Éireann; passed First Stage on 19 November 2025 and referred to Seanad Éireann; signed into law by the President of Ireland on 30 April 2026.
[274] Health Identifiers Act 2014.

I. L'OBLIGATION DE PARTAGE DES DONNEES DE SANTE (PARTIE 2)

La Partie 2 de la loi pose le principe d'un *duty to share* [« devoir de partage »] entre prestataires de soins. Aux termes de la section 7, tout prestataire qui assure le soin d'un patient est tenu de transmettre à ses confrères intervenant dans la même prise en charge les données de santé personnelles pertinentes, nécessaires et proportionnées, dans un format numérique conforme aux lignes directrices d'interopérabilité fixées par le HSE.

On reconnaîtra ici l'esprit du chapitre II du règlement EHDS, qui régit l'utilisation primaire des données de santé électroniques. Le droit du patient vient compléter le dispositif : la section 8 lui permet d'exiger le transfert gratuit de ses données vers un autre prestataire, dans un délai d'un mois. Ce délai s'aligne expressément sur celui de l'article 15 du RGPD[268] pour l'exercice du droit d'accès, et de l'article 20 du RGPD[269] pour l'exercice du droit à la portabilité. Des mesures de sauvegarde sont enfin prévues à la section 9 en cas de cessation d'activité d'un prestataire.

II. LE DOSSIER DE SANTE ELECTRONIQUE NATIONAL (PARTIE 3)

La Partie 3 constitue le cœur du dispositif de transposition. La section 10 habilite le HSE à créer, pour chaque patient, un dossier de santé électronique national (*Electronic Health Record*, ci-après « EHR »), après analyse d'impact relative à la protection des données (*data*

I. THE DUTY TO SHARE PERSONAL HEALTH DATA (PART 2)

Part 2 of the Act establishes the principle of a 'duty to share' among healthcare providers. Pursuant to section 7, any healthcare services provider responsible for the care of a patient is required to transmit to other providers involved in the patient's treatment the relevant, necessary and proportionate personal health data, in a digital format compliant with the interoperability guidelines laid down by the HSE.

The provision echoes the approach of Chapter II of the EHDS Regulation, which governs the primary use of electronic health data. The patient's own right completes the mechanism: section 8 allows the patient to request the free-of-charge transfer of their data to another provider, within one month. That timeframe expressly mirrors the one laid down by Article 15 of the GDPR[275] for the exercise of the right of access, and by Article 20 of the GDPR[276] for the axercise of the right to data portability. Finally, section 9 provides for safeguarding measures in the event of the cessation of activity of a provider.

II. THE NATIONAL ELECTRONIC HEALTH RECORD (PART 3)

Part 3 constitutes the core of the transposition framework. Section 10 empowers the HSE to create, for each patient, a national Electronic Health Record (hereinafter 'EHR'), following a data protection impact assessment conducted in consultation with the *Data Protection Commission* (DPC). Section

[268] Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 (règlement général sur la protection des données), *JOUE* n° L 119 du 4/05/2016.
[269] *Ibid*.
[275] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] *OJ* L119/1
[276] *ibid*

protection impact assessment) réalisée en concertation avec la *Data Protection Commission* (DPC). La section 10(3) apporte une précision importante : aucun patient ne pourra se voir refuser un service de santé au motif qu'il ne dispose pas d'un EHR. On retrouve ici la logique de l'article 3, paragraphe 10, du règlement EHDS, qui prohibe toute discrimination fondée sur l'exercice des droits relatifs aux données de santé.

Contenu du dossier de santé électronique (EHR). La section 11 dresse la liste des catégories de données appelées à figurer dans l'EHR. On y retrouve sans surprise les rubriques énumérées à l'article 14 et à l'annexe I du règlement EHDS : résumé patient, prescriptions, dispensations, imagerie médicale, résultats de laboratoire et lettres de sortie. Le législateur irlandais est cependant allé plus loin que le texte européen. Trois catégories supplémentaires sont expressément mentionnées : les données relatives aux maladies rares (intégration aux Réseaux européens de références[270]), celles qui portent sur le statut fonctionnel du patient, et celles que ce dernier fournit lui-même. Cet ajout anticipe les catégories prioritaires que le règlement EHDS prévoit de rendre accessibles à terme dans le cadre de MyHealth@EU.

Identification du patient. Elle repose sur le *personal public service number* (PPSN), numéro d'identification personnel utilisé par l'administration irlandaise. La section 12 impose son enregistrement par tout prestataire de santé, mais prohibe simultanément le refus de soins en cas d'absence de PPSN. Le mécanisme est destiné à assurer la liaison avec l'*Individual Health Identifier* (IHI) institué par le *Health Identifiers Act 2014*, dans la perspective des exigences d'identification

10(3) contains an important refinement: no patient may be refused a health service on the ground that they do not hold an EHR. One finds here the logic of Article 3(10) of the EHDS Regulation, which prohibits any discrimination based on the exercise of rights in relation to health data.

Content of the EHR. Section 11 lists the categories of data intended to be recorded in the EHR. One recognises here, unsurprisingly, the headings enumerated in Article 14 and Annex I of the EHDS Regulation: patient summary, e-prescriptions, e-dispensations, medical imaging, laboratory results, and discharge reports. The Irish legislator has, however, gone further than the European text. Three additional categories are expressly referred to: data relating to rare diseases (integrating European reference networks[277]), data concerning the functional status of the patient, and data provided by the patient themselves. That addition anticipates the priority categories that the EHDS Regulation is to make accessible in due course through MyHealth@EU.

Patient identification. It rests upon the Personal Public Service Number (PPSN), the personal identification number used by the Irish public administration. Section 12 requires its recording by every healthcare services provider while, at the same time, prohibiting the refusal of care in cases where no PPSN is available. The mechanism is intended to ensure articulation with the *Individual Health Identifier* (IHI) established by the *Health Identifiers Act 2014*, with a view to the cross-border identification requirements set down by the EHDS Regulation.

[270] Directive n° 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* n° L 88 du 4/04/2011, art. 12.
[277] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] *OJ* L88/45, art 12.

transfrontalière posées par le règlement EHDS.

III. L'ACCES AU DOSSIER ET LES DROITS DU PATIENT (SECTIONS 13 A 16)

Le régime d'accès à l'EHR a été pensé autour de quatre catégories de bénéficiaires : le patient lui-même ; une « personne appropriée » qui agit pour son compte (parent, tuteur, ou encore représentant décisionnel au sens de l'*Assisted Decision-Making (Capacity) Act 2015*[271]) ; le prestataire de soins, aux fins du traitement en cours ; enfin les agents du HSE (Health Service Executive ; Direction des services de santé), à des fins de maintenance technique.

La section 14 reconnaît au patient un droit de restreindre l'accès à tout ou partie de son EHR, à la condition qu'il ait reçu un avertissement explicite sur les conséquences potentielles de cette restriction sur sa prise en charge. Il s'agit d'un mécanisme d'*opt-out* qui reprend la logique de l'article 8 du règlement EHDS. Une exception a néanmoins été prévue : la section 14(4) permet l'accès aux données restreintes lorsque les intérêts vitaux du patient l'exigent, avec traçabilité et notification en retour. Soulignons enfin la mise en place, à la section 15, d'une notification automatique et en temps réel de tout accès à l'EHR, conformément à l'exigence de transparence portée par l'article 9, du règlement EHDS.

IV. L'UTILISATION PRIMAIRE ET SECONDAIRE DES DONNEES DE SANTE ELECTRONIQUE

La section 18 autorise le HSE à conclure des accords réciproques avec des prestataires établis dans des pays tiers, pour l'échange sécurisé d'informations contenues dans l'EHR, après consultation de la DPC (Data

III. ACCESS TO THE RECORD AND THE RIGHTS OF THE PATIENT (SECTIONS 13 TO 16)

The regime of access to the EHR has been designed around four categories of beneficiaries: the patient themselves; an 'appropriate person' acting on the patient's behalf (parent, guardian, or decision-making representative within the meaning of the *Assisted Decision-Making (Capacity) Act 2015*[278]); the healthcare services provider, for the purposes of the treatment in progress; and, finally, HSE personnel, for purposes of technical maintenance.

Section 14 recognises the patient's right to restrict access to all or part of their EHR, on condition that they have received an explicit warning as to the potential consequences of such restriction for their treatment. The mechanism is one of opt-out, which takes up the logic of Article 8 of the EHDS Regulation. An exception has nonetheless been provided for: section 14(4) permits access to restricted data where the patient's vital interests so require, with traceability and notification back to the patient. One should further underline the arrangement put in place at section 15, which provides for automatic, real-time notification of any access to the EHR, in line with the transparency requirement laid down by Article 9 of the EHDS Regulation.

IV. THE PRIMARY AND SECONDARY USE OF ELECTRONIC HEALTH DATA

Section 18 authorises the HSE to conclude reciprocal agreements with third-country healthcare providers for the secure exchange of information contained in the EHR, following consultation with the DPC. Here lies a

[271] Irlande, *Assisted Decision-Making (Capacity) Act 2015*, Act n° 64 of 2015.
[278] Assisted Decision-Making (Capacity) Act 2015.

Protection Commission ; Commission de protection des données). Voici une amélioration notable : l'Irlande prépare ainsi le terrain à une interconnexion avec MyHealth@EU qui pourrait, à terme, dépasser le seul cadre des États membres. La disposition vient compléter, de ce point de vue, l'article 14 du règlement EHDS sur l'accès transfrontalier.

La Partie 4 et l'utilisation secondaire. C'est le deuxième pan du dispositif. La Partie 4 de la loi encadre la collecte d'informations de santé par le HSE auprès de « personnes pertinentes », à des fins d'intérêt public : santé publique, planification des services et statistiques. Plusieurs garanties balisent le dispositif. Le texte exige en particulier une évaluation préalable de la nécessité de recourir à des données personnelles plutôt qu'anonymisées (section 22(4)), une analyse d'impact, une pseudonymisation, des mesures de limitation d'accès, ainsi qu'une formation ciblée des agents amenés à manipuler ces données. On notera, à cet égard, qu'au stade du Seanad le texte initial a été amendé pour supprimer la condition de subsidiarité qui imposait au HSE de démontrer, préalablement à toute demande, que les données ne pouvaient être obtenues par d'autres moyens en temps utile et de manière effective. La suppression de cette condition élargit sensiblement les pouvoirs de collecte du HSE à des fins secondaires et mérite d'être signalée. La définition de la « health information » à la section 2 a, dans le même mouvement, été étendue aux informations relatives à la fourniture et à l'évaluation des services de santé. Par ailleurs, les finalités d'utilisation secondaire visées aux sections 17(b)(ii) et 22(2) ont été élargies pour inclure « la planification intégrée des services, la gestion des performances et l'utilisation efficiente et efficace des ressources dans le domaine de la santé » ; ce dernier ajout n'étant pas neutre au regard des exigences de proportionnalité posées par l'article 9 du RGPD.

significant avenue: Ireland is in this way preparing the ground for an interconnection with MyHealth@EU that may, in time, extend beyond the sole framework of the Member States. The provision thus complements Article 14 of the EHDS Regulation on cross-border access.

Part 4 and secondary use. This is the second strand of the framework. Part 4 of the Act governs the collection of health information by the HSE from 'relevant persons', for public-interest purposes: public health, service planning, and statistics. Several safeguards frame the mechanism. The Act requires, in particular, a prior assessment of the necessity of resorting to personal data rather than anonymised data (section 22(4)), an impact assessment, pseudonymisation, access-restriction measures, and targeted training for officers who come to handle such data. It should be noted, in this regard, that at the Seanad stage the original text was amended so as to remove the subsidiarity-type condition which had required the HSE to demonstrate, prior to any request, that the data could not be obtained 'by alternative means in a timely and effective manner'. The removal of that condition appreciably widens the HSE's collection powers for secondary purposes, and deserves to be flagged. The definition of 'health information' at section 2 has, in the same vein, been extended to encompass information relating to the provision and evaluation of health services; and the secondary-use purposes referred to in sections 17(b)(ii) and 22(2) have been broadened to include 'integrated service planning, performance management and the efficient and effective use of resources in the area of health' — the latter addition not being a neutral one when measured against the proportionality requirements laid down by Article 9 of the GDPR.

The HSE may not, under any circumstances, re-identify the patients whose data have been collected (section 24(2)), and is to publish, every eighteen

Le HSE ne peut en aucun cas ré-identifier les patients dont les données ont été collectées (section 24(2)), et doit publier tous les dix-huit mois un rapport sur l'utilisation des données obtenues. On retrouve, en filigrane, les grandes lignes du chapitre IV du règlement EHDS consacré à l'utilisation secondaire, appuyées sur les bases juridiques nationales de traitement des données sensibles au sens de l'article 9, paragraphe 2, points g), h) et i), du RGPD.

On signalera enfin que la section 21, qui régit l'élaboration par le HSE des lignes directrices d'application de la loi, intègre désormais la *Health Information and Quality Authority* (HIQA) parmi les autorités obligatoirement consultées. L'ajout fait écho au rôle reconnu à la HIQA dans la stratégie *AI for Care* commentée infra, en particulier dans la préparation du *National Guidance for the Responsible and Safe Use of AI in Health and Social Care*.

On retiendra surtout de cette loi qu'elle place l'Irlande parmi les premiers États membres à avoir mené à terme un processus législatif formel de « mise en œuvre » du règlement EHDS, avant même l'expiration du délai d'application. L'utilisation primaire et l'utilisation secondaire des données de santé y sont articulées dans un cadre juridique unifié, qui tente de concilier les exigences d'interopérabilité européenne et les spécificités institutionnelles irlandaises, notamment le rôle pivot du HSE et l'ancrage sur le PPSN.

L'adoption définitive du texte clôt la trajectoire législative, mais ouvre celle, plus délicate encore, de la mise en œuvre. L'enjeu n'est pas mince : compte tenu du retard de l'Irlande déjà mesuré par l'indicateur de la Décennie numérique 2025 (v. supra)[272], l'ambition législative portée par la loi ne se traduira dans les faits qu'à la faveur d'un effort

months, a report on the use made of the data obtained. One recognises, in outline, the broad lines of Chapter IV of the EHDS Regulation concerning secondary use, supported by the national legal bases for the processing of sensitive data within the meaning of Article 9(2)(g), (h) and (i) of the GDPR.

It should finally be noted that section 21, which governs the elaboration by the HSE of the guidelines giving effect to the Act, now includes the *Health Information and Quality Authority* (HIQA) among the bodies that must be consulted. The addition echoes the role conferred on HIQA in the *AI for Care* strategy discussed below, in particular as regards the preparation of the *National Guidance for the Responsible and Safe Use of AI in Health and Social Care*.

Most notably, the Act places Ireland among the first Member States to have brought to completion a formal legislative process for the transposition of the EHDS Regulation, even before the expiry of the implementation deadline. Primary and secondary use of health data are articulated there within a unified legal framework, which seeks to reconcile the European interoperability requirements with the institutional specificities of Ireland, notably the pivotal role of the HSE and the reliance on the PPSN.

The final adoption of the text closes the legislative trajectory but opens the more delicate one of implementation. The stakes are not minor: given Ireland's considerable lag, as already measured by the 2025 Digital Decade indicator (see above)[279], the legislative ambition carried by the Act will only bear fruit in practice were accompanied by a technical implementation effort and a level of citizen take-up of an entirely different order.

[272] Commission européenne, *COM(2025)* 290 final, *préc.* ; *v. supra*, « Infrastructures numériques de santé ».
[279] European Commission, 'Digital Decade Report 2025' (n 13); *see further the discussion under 'Digital Health Infrastructure' above.*

d'implémentation technique et d'appropriation citoyenne d'une toute autre ampleur.

Department of Health (An Roinn Sláinte) & Health Service Executive (HSE), *AI for Care – The Artificial Intelligence (AI) Strategy for Healthcare in Ireland 2026–2030*, March 2026

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Fruit d'une commande conjointe du ministère de la Santé (*Department of Health*, ci-après « DoH ») et du HSE, la stratégie *AI for Care* est la toute première stratégie nationale irlandaise dédiée à l'intégration de l'intelligence artificielle dans le système de santé. Publiée en 2025 pour la période 2026–2030, elle donne corps à un engagement inscrit au *Programme for Government 2025*[280], lequel prévoyait l'élaboration d'une telle stratégie en cohérence avec le cadre *Digital for Care 2024–2030* et avec la réforme *Sláintecare*. Un *AI Implementation Framework* élaboré par le HSE, qui détaille les modalités opérationnelles de déploiement, vient compléter l'ensemble. Il s'agit de l'un des premiers exercices systématiques, par un État membre, d'articulation entre une politique sectorielle d'IA en santé et les exigences du RIA.

I. LES PRINCIPES DIRECTEURS : LA CONVERGENCE AVEC LE CADRE EUROPEEN

La vision affichée par *AI for Care* consiste à « exploiter l'IA de manière sûre et responsable pour transformer la manière dont nous dispensons des soins efficients et innovants ». Cette vision est étayée par six principes directeurs dont la convergence avec le RIA et, plus largement, l'approche européenne de l'IA digne de confiance est notable.

Jointly commissioned by the Department of Health (*An Roinn Sláinte*, hereinafter 'DoH') and the HSE, the *AI for Care* strategy is the very first national Irish strategy dedicated to the integration of artificial intelligence into the healthcare system. Published in 2025 for the period 2026–2030, it gives substance to a commitment inscribed in the *Programme for Government 2025*[284], which had provided for the development of such a strategy in alignment with the *Digital for Care 2024–2030* framework and with the *Sláintecare* reform. An *AI Implementation Framework* prepared by the HSE, setting out the operational arrangements for deployment, completes the package. This represents one of the first systematic exercises, by a Member State, in aligning a sectoral AI policy in healthcare with the requirements of the AI Act.

I. THE GUIDING PRINCIPLES : CONVERGENCE WITH THE EUROPEAN FRAMEWORK

The vision set out by *AI for Care* is to 'harness AI safely and responsibly to transform how we deliver efficient and innovative healthcare for patients and professionals'. That vision is underpinned by six guiding principles whose convergence with the AI Act and,

[280] Gouvernement d'Irlande, *Programme for Government: Securing Ireland's Future*, janvier 2025.
[284] *Programme for Government: Securing Ireland's Future* (Government of Ireland 2025.

Le principe *Person-Centred place* les résultats de santé et les besoins du public au cœur des décisions relatives à l'adoption de l'IA, tout en postulant un partenariat continu avec les patients. Le principe *Transparent and Trustworthy* fait directement écho aux obligations de transparence posées par les articles 13 et 14 du RIA pour les systèmes à haut risque. Le principe *Human in the Loop*, sans doute le plus significatif du point de vue juridique, emprunte la terminologie même du RIA, dont l'article 14 impose un contrôle humain effectif pour tout système à haut risque. Aussi la stratégie précise que l'IA doit « soutenir les professionnels de santé dans leur prise de décision médicale tout en gardant toujours le praticien au centre des soins au patient » : l'exigence juridique d'un contrôle humain adéquat se voit ainsi traduite dans le langage de la politique de santé.

Deux autres principes viennent prolonger cet alignement. Le principe *Governance and Safety* exige la conformité aux législations nationale et européenne applicables, RIA inclus. Quant au principe *Proven Benefit*, il engage à une évaluation continue des résultats mesurables de l'IA déployée. La stratégie rejoint ainsi l'exigence de surveillance post-commercialisation prévue à l'article 72 du RIA. La référence complémentaire aux principes éthiques de l'OMS[281] relatifs à l'IA pour la santé achève d'inscrire la démarche dans un cadre de gouvernance à plusieurs niveaux : national, européen et international.

more broadly, with the European approach to trustworthy AI, is striking.

The *Person-Centred* principle places health outcomes and the needs of the public at the heart of decisions relating to AI adoption, while postulating continuous partnership with patients. The *Transparent and Trustworthy* principle directly echoes the transparency obligations laid down by Articles 13 and 14 of the AI Act for high-risk systems. The *Human in the Loop* principle, doubtless the most significant from a legal standpoint, borrows the very terminology of the AI Act, Article 14 of which imposes effective human oversight for every high-risk system. The strategy accordingly specifies that AI must 'support clinicians in their clinical decision-making while keeping the clinician at the centre of patient care': the legal requirement of adequate human oversight is thus translated into the language of health policy.

Two further principles carry this alignment forward. The *Governance and Safety* principle demands compliance with applicable national and European legislation, the AI Act included. As for the *Proven Benefit* principle, it commits to ongoing assessment of the measurable outcomes of AI once deployed. The strategy thus meets the post-market monitoring requirement provided for at Article 72 of the AI Act. The complementary reference to the WHO's ethical principles[285] on AI for health completes the inscription of the endeavour within a layered governance framework: national, European and international.

[281] Organisation mondiale de la santé, Ethics and governance of artificial intelligence for health, OMS, Juin 2021 ; mis à jour en oct. 2023 pour intégrer les grands modèles multimodaux.
[285] World Health Organization, Ethics and Governance of Artificial Intelligence for Health (WHO 2021, updated October 2023).

II. QUATRE PILIERS STRATEGIQUES A LA LUMIERE DU RIA

A. AI for Clinical Care

C'est le pilier aux enjeux juridiques les plus denses. Il englobe l'imagerie médicale assistée par IA (détection de fractures, d'AVC, de tumeurs), l'aide à la décision clinique et la documentation clinique automatisée. La stratégie reconnaît expressément que bon nombre de ces solutions sont qualifiées d'« IA en tant que dispositif médical » (*AI-as-a-medical-device*) au titre du règlement n° 2017/745/UE[282] et qu'elles sont, à ce titre, traitées comme des systèmes à haut risque au sens de l'article 6, paragraphe 1, du RIA lu conjointement avec l'annexe I.

Les conséquences sont considérables. Ces solutions sont soumises aux obligations du chapitre III, section 2, du RIA. La gestion des risques (article 9) doit être établie et documentée. La gouvernance des données est encadrée à l'article 10. La documentation technique (article 11), la traçabilité des opérations (article 12), la transparence (article 13), le contrôle humain (article 14) et les exigences de robustesse, de précision et de cybersécurité (article 15) viennent compléter le dispositif. La stratégie mentionne par ailleurs les analyses d'impact sur les droits fondamentaux prévues à l'article 27 du RIA, ainsi que l'inscription des projets sur les registres d'IA visés à l'article 49.

Le rapport illustre sa démarche par une étude de cas intéressante : le déploiement de l'IA en radiologie, dans un hôpital universitaire irlandais, pour la détection de caillots sanguins et de fractures. Les résultats cités font état d'une amélioration du taux de détection des caillots de 100 %, le système opérant

II. FOUR STRATEGIC PILLARS IN LIGHT OF THE AI ACT

A. AI for Clinical Care

This is the pillar whose legal stakes run deepest. It encompasses AI-assisted medical imaging (detection of fractures, strokes, and tumours), clinical decision support, and automated clinical documentation. The strategy expressly acknowledges that a number of these clinical solutions qualify as 'AI-as-a-medical-device' within the meaning of Regulation (EU) 2017/745[286] and are, on that account, treated as high-risk systems within the meaning of Article 6(1) of the AI Act read in conjunction with Annex I.

The consequences are considerable. Those solutions are made subject to the obligations of Chapter III, Section 2, of the AI Act. A risk-management system must be established and documented (Article 9). Data and data governance are regulated at Article 10. Technical documentation (Article 11), record-keeping (Article 12), transparency (Article 13), human oversight (Article 14) and the requirements of accuracy, robustness and cybersecurity (Article 15) complete the framework. The strategy also refers to the fundamental rights impact assessments provided for at Article 27 of the AI Act, together with registration of projects in the EU database of AI systems referred to at Article 49.

The strategy illustrates its approach through an instructive case study: the deployment of AI in radiology, in an Irish teaching hospital, for the detection of blood clots and fractures. The figures cited report an improvement in the clot detection rate of 100 percent, the system operating in support of the radiologist rather than autonomously.

---

[282] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, *JOUE* n° L 117 du 5/05/2017.

[286] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices [2017] *OJ* L117/1.

toutefois en appui du radiologue et non de manière autonome.

B. AI for Operations

Ce pilier concerne l'amélioration de l'efficience opérationnelle du système. Sont envisagées l'automatisation des fonctions support (ressources humaines, finances, chaîne d'approvisionnement), la gestion prédictive de la demande et des capacités, l'automatisation des centres de contact, ou encore l'accélération du déploiement du dossier de santé électronique. À première vue, le profil de risque apparaît moindre que pour les applications cliniques. Il convient cependant de ne pas s'y méprendre. Certains usages (gestion prédictive du flux de patients, allocation automatisée des lits) sont susceptibles de relever de l'annexe III, point 5, du RIA relative aux systèmes à haut risque en matière de santé, dès lors qu'ils influent sur l'accès aux soins ou l'allocation des ressources.

C. AI for Research & Innovation

Le troisième pilier porte sur la mobilisation de l'IA pour accélérer la recherche médicale, optimiser les essais cliniques et améliorer l'audit clinique. Il soulève des questions juridiques spécifiques, notamment quant à l'articulation entre le RIA et le cadre de protection des données. L'utilisation de l'IA pour l'analyse de grands volumes de données de santé ou pour le recrutement automatisé de patients implique en effet, par hypothèse, un traitement au sens de l'article 9 du RGPD. La stratégie prévoit d'ailleurs une rationalisation des procédures de conformité, la préparation des analyses d'impact relatives à la protection des données (AIPD, *DPIA*) figurant parmi les actions prioritaires, ce qui ouvre un champ d'articulation avec le chapitre IV du règlement EHDS relatif à l'utilisation secondaire des données de santé.

B. AI for Operations

This pillar concerns the improvement of the operational efficiency of the system. It contemplates the automation of support functions (human resources, finance, supply chain), predictive management of demand and capacity, the automation of contact centres, and the acceleration of the roll-out of the electronic health record. At first sight, the risk profile appears lower than that of clinical applications. It is advisable, however, not to be misled. Certain uses (predictive management of patient flow, automated bed allocation) are liable to fall within Annex III, point 5, of the AI Act concerning high-risk systems in the health domain, where they influence access to care or the allocation of resources.

C. AI for Research & Innovation

The third pillar concerns the mobilisation of AI to accelerate medical research, optimise clinical trials, and improve clinical audit. It raises legal issues that are specific to it, notably as regards the articulation between the AI Act and the data-protection framework. The use of AI for the analysis of large volumes of health data or for the automated recruitment of patients necessarily implies, by hypothesis, a processing of data within the meaning of Article 9 of the GDPR. The strategy does indeed provide for a streamlining of compliance procedures, the preparation of data protection impact assessments (DPIAs) being among the priority actions, opening up a field of articulation with Chapter IV of the EHDS Regulation on the secondary use of health data.

D. *AI for Public Health*

The fourth and final pillar aspires to integrate AI into population-level screening programmes, epidemiological surveillance, and the formulation of evidence-based public health policies. The strategy cites, by way of example, a Swedish study from 2023 in which AI-

D. AI for Public Health

Le quatrième et dernier pilier ambitionne d'intégrer l'IA dans les programmes de dépistage populationnel, la surveillance épidémiologique et la formulation de politiques de santé publique fondées sur les preuves. La stratégie cite, à titre d'exemple, une étude suédoise réalisée en 2023 dans laquelle le dépistage du cancer du sein assisté par IA aurait permis une hausse de 29 % du taux de détection tout en réduisant de 44 % la charge de travail des radiologues[283]. On voit bien l'intérêt de la méthode. Son application à grande échelle soulève cependant des enjeux considérables en matière d'équité algorithmique et de non-discrimination, lesquels sont au cœur du RIA (considérant 27 et article 10, paragraphe 2, relatif à la prévention des biais).

III. UNE FEUILLE DE ROUTE DANS LE TEMPO DU RIA

La stratégie déploie une feuille de route à trois horizons : « *Now* » (année 1), « *Next* » (années 2–3) et « *Future* » (années 4–5). Elle identifie vingt-six opportunités prioritaires de déploiement de l'IA. Cette séquence mérite d'être mise en regard du calendrier d'application du RIA. Les systèmes à haut risque, qui recouvrent la plupart des applications cliniques du premier pilier, seront soumis aux obligations du chapitre III à compter du 2 août 2026, soit la première année d'exécution de la feuille de route *AI for Care*. La coïncidence temporelle implique que les preuves de concept et les projets pilotes de l'horizon « *Now* » devront intégrer dès leur conception les exigences du RIA en matière de gestion des risques, de qualité des données et de documentation technique.

supported breast cancer screening reportedly enabled a 29 percent increase in the cancer detection rate while reducing the radiologists' workload by 44 percent[287]. One readily appreciates the interest of the method. Its application at scale nevertheless raises considerable issues in terms of algorithmic fairness and non-discrimination, matters which lie at the heart of the AI Act (recital 27 and Article 10(2) on the prevention of bias).

III. A ROADMAP IN STEP WITH THE AI ACT TIMELINE

The strategy deploys a roadmap with three horizons: '*Now*' (year 1), '*Next*' (years 2–3) and '*Future*' (years 4–5). It identifies twenty-six priority opportunities for the deployment of AI. That sequencing deserves to be read against the timeline for the application of the AI Act. High-risk systems, which cover the bulk of the clinical applications of the first pillar, will be subject to the obligations of Chapter III from 2 August 2026, namely the first year of execution of the *AI for Care* roadmap. The temporal coincidence means that the proofs of concept and pilot projects of the '*Now*' horizon will have to incorporate, from the design stage, the AI Act requirements in terms of risk management, data quality and technical documentation.

The *AI Implementation Framework* developed by the HSE sets out the mechanisms of governance, approval and monitoring. It provides, in particular, for the creation of an *AI & Automation Centre of Excellence*, tasked with recording AI projects in a national registry (as required, moreover, by the AI Act) and with ensuring compliance with the guidelines of the Health Information and Quality Authority (HIQA) and of the Department of Public Expenditure,

[283] LANG M. et *al.*, « Artificial intelligence-supported screen reading versus standard double reading in the Mammography Screening with Artificial Intelligence trial (MASAI) », *The Lancet Digital Health*, 2023.
[287] K LANG and others, 'Artificial Intelligence-Supported Screen Reading versus Standard Double Reading in the Mammography Screening with Artificial Intelligence Trial (MASAI)' (2023) *The Lancet Digital Health.*

L'*AI Implementation Framework* développé par le HSE décline les mécanismes de gouvernance, d'approbation et de suivi. Il prévoit notamment la création d'un Centre d'excellence en IA et automatisation (*AI & Automation Centre of Excellence*), chargé d'enregistrer les projets d'IA sur un registre national (ce qu'impose par ailleurs le RIA) et d'assurer la conformité aux lignes directrices de la *Health Information and Quality Authority* (HIQA) et du *Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation* (DPER).

Sont visées, à cet égard, les *Guidelines for the Responsible Use of AI in the Public Service* publiées par le DPER ainsi que le *National Guidance for the Responsible and Safe Use of AI in Health and Social Care* en cours de préparation à la HIQA, lequel doit accompagner la mise en conformité avec le RIA. Le rôle de la HIQA dans cet écosystème se trouve d'ailleurs conforté par la section 21 du *Health Information Act 2026*, qui impose désormais au HSE de la consulter pour l'élaboration de ses lignes directrices (v. *supra*). Une remarque conclusive mérite d'être soulignée : la stratégie reconnaît elle-même la nécessité de demeurer agile face à l'évolution des cadres européens. L'observation n'est pas anodine dès lors que la Commission doit adopter, dans les mois à venir, plusieurs règlements d'exécution précisant les exigences techniques applicables aux systèmes d'IA à haut risque dans le domaine de la santé.

IV. PORTEE DE LA STRATEGIE

La démarche irlandaise appelle plusieurs remarques. En premier lieu, elle témoigne d'une anticipation sectorielle du RIA qui mérite l'attention. Loin de traiter ce texte comme une contrainte, la stratégie en fait un cadre structurant, intégré dès la conception des projets (*compliance by design*). La

Infrastructure, Public Service Reform and Digitalisation (DPER).

Particular reference is made to the *Guidelines for the Responsible Use of AI in the Public Service* issued by the DPER and to the forthcoming *National Guidance for the Responsible and Safe Use of AI in Health and Social Care* being prepared at HIQA, which is to accompany compliance with the AI Act. The role of HIQA in this ecosystem is, moreover, reinforced by section 21 of the *Health Information Act 2026*, which now requires the HSE to consult HIQA in the elaboration of its guidelines (see above). One concluding remark deserves to be underlined: the strategy itself acknowledges the need to remain agile in the face of the evolution of European frameworks. The observation is not trivial, inasmuch as the Commission is required, in the months ahead, to adopt a number of implementing regulations specifying the technical requirements applicable to high-risk AI systems in the health domain.

IV. SCOPE OF THE STRATEGY

The Irish approach calls for a number of comments. First, it bears witness to a sectoral anticipation of the AI Act that commands attention. Far from treating the text as a constraint, the strategy makes of it a structuring framework, embedded from the design stage of projects (*compliance by design*). The approach contrasts with certain more defensive stances, in which compliance with the AI Act is apprehended as a retrospective exercise of adapting existing systems.

Second, the strategy puts in evidence a point of articulation still left unresolved: that between conformity assessment under the Medical Devices Regulation and that required by the AI Act. The category of 'AI-as-a-medical-device' systems is certainly identified, and their classification as high-risk systems under the AI Act is explicitly acknowledged. The practical arrangements for the articulation of the two regimes remain, however, largely

démarche contraste avec certaines approches plus défensives, où la conformité au RIA est appréhendée comme un exercice rétrospectif d'adaptation de systèmes existants.

En second lieu, la stratégie laisse entrevoir un point d'articulation encore en suspens : celui entre l'évaluation de conformité au titre du règlement sur les dispositifs médicaux et celle requise par le RIA. La catégorie des systèmes d'« IA en tant que dispositif médical » est certes identifiée, et leur classification comme systèmes à haut risque au titre du RIA est explicitement reconnue. Les modalités pratiques d'articulation des deux régimes restent cependant largement renvoyées à l'*AI Implementation Framework*. Voilà assurément l'un des enjeux déterminants de la mise en œuvre effective du texte.

La stratégie s'inscrit enfin dans un écosystème réglementaire plus large. Le *Health Information Act 2026* analysé ci-dessus en constitue l'autre jalon majeur, qu'une stratégie nationale de données du HSE, encore à venir, viendra compléter. Qu'observe-t-on ? La stratégie reconnaît explicitement que la donnée constitue le « fondement de l'adoption de l'IA » et établit un lien bidirectionnel entre qualité des données et efficacité des systèmes. Ce faisant, elle trace un pont direct avec le règlement EHDS, dont le chapitre IV organise précisément l'accès à des données de santé de qualité à des fins de recherche, d'innovation et d'élaboration de politiques. À l'approche de la présidence irlandaise du Conseil de l'Union européenne, en juillet 2026, cet ancrage pourrait bien offrir à l'Irlande un socle cohérent pour porter ces sujets au niveau européen.

deferred to the *AI Implementation Framework*. It is, without doubt, one of the determining questions for the effective implementation of the text.

The strategy finally takes its place within a wider regulatory ecosystem. The *Health Information Act 2026* analysed above constitutes its other major milestone, which a forthcoming HSE data strategy will, in due course, complete. What does this reveal? The strategy explicitly acknowledges that data constitutes the 'foundation of AI adoption', and establishes a bidirectional link between data quality and the effectiveness of systems. In so doing, it draws a direct bridge with the EHDS Regulation, whose Chapter IV organises precisely the access to quality health data for the purposes of research, innovation and policymaking. As the Irish Presidency of the Council of the European Union draws near, in July 2026, that anchoring may yet offer Ireland a coherent platform from which to carry these matters at European level.

Droit italien

Direttiva generale per l'attività amministrativa e la gestione, Anno 2026 (Directive générale pour l'activité administrative et la gestion), 2026.

par Maddalena DE CARLO
Etudiante en Master 2 Droit international et comparé, École de droit de Toulouse, Université Toulouse Capitole

Aperçu général de la directive

La directive générale du Ministère italien de la Santé, adoptée en vertu des articles 4 et 14 du décret législatif n° 165/2001, constitue le document stratégique annuel qui structure les priorités de la gestion du Service National de Santé (SSN) pour l'année en cours. Elle établit les orientations globales en matière de santé publique, d'organisation des services, de ressources humaines et de modernisation des infrastructures sanitaires.

Ce document encadre les actions des administrations centrales, des Régions et des Provinces autonomes dans l'exécution de leurs missions, en tenant compte des engagements européens et des financements du PNRR (Piano Nazionale di Ripresa e Resilienza)[288].

Après un "contexte institutionnel" (p. 11) qui rappelle le cadre juridique fondamental, incluant le decreto legge 300/1999, la legge 172/2009 et autres textes de référence, le cœur du document réside dans l'intitulé 2 « Priorité de l'action administrative et de la gestion » (v. p. 12 et s.), lequel repose sur treize objectifs stratégiques majeures présentées de manière fluide et hiérarchisée.

On retiendra plus particulièrement les points suivants :

- **2.1.** « Renforcement des mesures de prévention » (p. 17) (vise à protéger les groupes vulnérables pour un bien-être équitable) ;
- **2.2.** « Promotion de politiques de santé axées sur l'innovation » (p. 17) (renforce les réseaux de recherche et le transfert technologique) ;
- **2.3.** « Renforcement des capacités de surveillance épidémiologique » (p. 18) (améliore la gestion des urgences sanitaires) ;
- **2.4.** « Réduction des inégalités entre les régions » (pp. 19-26)[289]

[288] PNRR -désigne le plan italien de relance et de résilience financé par NextGenerationEU pour répondre aux exigences d'interopérabilité de l'EHDS.

[289] 2.4. Incluant dix-sept sous-points, il aborde la garantie des niveaux essentiels d'assistance (LEA) à travers l'intégration hôpital-territoire, les interventions PNRR, la réduction des listes d'attente et l'utilisation de l'IA dans des conditions de non-discrimination et d'information des patients - en incluant des aspects tels que :
2.4.1 Programmation sanitaire nationale
2.4.4 Rischio Clinico ("Risque clinique")

Sont aussi à relever les sections suivantes :

- **2.5.** « Valoriser les professionnels de santé » (p. 27) (met l'accent sur la reconnaissance des médecins urgentistes) ;
- **2.6.** « Favoriser l'innovation technologique dans les dispositifs médicaux » (p. 30) (modernise les essais cliniques).
- **2.7.** « Simplifier l'accès aux services de santé et renforcer les interventions en santé numérique » (p. 33) (constitue un élément central de la directive dans le domaine de la digitalisation, structurant les priorités stratégiques de modernisation du SSN)[290].

Le document se poursuit avec les priorités restantes de l'intitulé 2 (pp. 37-44), qui couvrent :

- **2.8.** « Implémentation de l'efficacité organisationnel du ministère » ;
- **2.9.** « Sensibilisation des usagers à la santé publique » ;
- **2.10.** « Promotion des modes de vie sains et de la santé mentale » ;
- **2.11.** « Sécurité alimentaire » ;
- **2.12.** « Santé publique vétérinaire », et enfin ;
- **2.13.** « Renforcement du rôle international de l'Italie en matière de politique sanitaire ».

La directive se clôt par une synthèse des objectifs stratégiques :

3. « Synthèse des objectifs stratégiques ;

4. « Destinataires et attribution des ressources adressée aux Centri di responsabilità amministrativa (CRA) » (p. 46) ;

5. « Ressources financières et humaines » (p. 47) ;

6. « Systèmes de monitoring informatisé » (p. 47) ;

7. « Bilan de réalisation des objectifs 2025 » (p. 48) ; et enfin

8. « Dispositions finales » (p. 52), complétés par quatre annexes : tableau récapitulatif des objectifs (Allegato 1, p. 54), effectifs au 1er janvier 2026 (Allegato 2, p. 61), modèles et fiches détaillées d'objectifs (Allegati 3-4, pp. 64-67).

Les orientations stratégiques de la directive en matière de santé numérique

Dans le domaine de la digitalisation, la directive identifie des actions stratégiques précises. Elle énonce clairement que la section 2.7 vise à simplifier l'accès aux services de santé et à renforcer la santé numérique par trois axes prioritaires (p. 33).

1. En développant l'écosystème des données de santé (EDS) en créant un outil centralisé (plateforme) de collecte, d'analyse et de valorisation des données sanitaires au service des professionnels de la santé et du public ;
2. En exploitant le potentiel d'information du dossier de santé électronique (FSE) en tant que système d'alimentation du SDE et d'accès aux services de santé numérique ;

2.4.5 Farmacia dei servizi (" Pharmacie des services").
2.4.10 Numero europeo 116117 ("Numéro européen pour soins non urgents") ou encore,
2.4.11 SiVeAS (système de vérification nationale).

[290] Cette section se déploie en points précis :
2.7.1 « Renforcement du Dossier Médical Électronique » (p. 34) ;
2.7.2 « Mise en œuvre de l'Écosystème des Données Sanitaires " (p. 34) ;
2.7.3 « Renforcement des capacités de collecte, d'analyse et de diffusion des données + soutien à la télémédecine » (p. 35) ;
2.7.4 « Santé numérique et échange de données sanitaires dans le cadre européen » (p. 36) ; 2.7.5 Sunshine Act (p. 36) ;
2.7.6 « Élévation des niveaux de cybersécurité » (p. 37) ;
2.7.7 « Rapport sur l'état sanitaire du pays 2022-2024 » (p. 37). Aspects qui seront développés plus en détail (v. p. 3).

3. En développant les services de télémédecine afin d'accroître l'offre de prestations sanitaires de plus en plus efficaces et rapides, avec une attention particulière accordée aux sujets atteints de pathologies chroniques, y compris par la mise en œuvre de la plateforme nationale.

Le Ministère de la Santé entend poursuivre le renforcement de l'infrastructure numérique du Service National de Santé (SSN) en cohérence avec les investissements PNRR en cours, et dans le but de la mise en œuvre de l'Espace européen des données de santé (EEDS) conformément au Règlement UE 2025/327, entré en vigueur le 26 mars 2025.

« *Fascicolo Sanitario Elettronico*[291] (FSE) »

La directive annonce d'abord que l'Italie doit se doter d'un cadre de gouvernance national pour l'usage des données de santé et distingue, conformément au Règlement sur l'EEDS, l'utilisation primaire[292] et l'utilisation secondaire[293]. Ce cadre doit être aligné sur l'objectif européen de la « décennie digitale 2020-2030[294] », qui vise à garantir à toutes les personnes l'accès à leurs données de santé d'ici 2030.

Dans cette perspective, la directive rattache les objectifs de l' EEDS au PNRR, en particulier à l'Investissement 1.3 « *Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione* » (*Missione 6, Componente 2*). Le Ministère de la Santé y est désigné comme entité chargée de la mise en œuvre, en collaboration avec le Département pour la transformation digitale, notamment pour renforcer le FSE à travers de nouveaux décrets prévus par l'article 12, alinéa 7, du décret-loi n° 179/2012.

La directive prévoit aussi la mise en place d'un cadre juridique spécifique pour la télémédecine, qui doit couvrir à la fois les règles de traitement des données de santé et les modalités de tarification des actes de télémédecine, en coopération étroite avec AGENAS (Agence nationale de santé numérique). L'idée est de sécuriser juridiquement ces pratiques tout en les intégrant dans le financement ordinaire du système. L'ensemble de ces "sous-investissements" a un double objectif : d'un côté, moderniser l'infrastructure technologique du Ministère pour supporter de nouvelles applications numériques ; de l'autre, améliorer la rapidité, l'exhaustivité et la qualité des données, qu'elles soient cliniques ou issues du *Nuovo Sistema Informativo Sanitario* (NSIS[295]) utilisé pour la programmation, le suivi et le pilotage administratif. D'ailleurs, la directive explique que, pour la digitalisation, elle se concentre sur le renforcement du *Fascicolo Sanitario Elettronico* (FSE). Elle rappelle que la numérisation des systèmes de santé est considérée par la Commission

[291] Il s'agit de l'équivalent du Dossier de santé électronique.

[292] Art. 2 p.1 let. d) du Règlement (UE) 2025/327 « utilisation primaire : le traitement de données de santé électroniques pour la fourniture de soins de santé en vue d'évaluer, de maintenir ou de rétablir l'état de santé de la personne physique à laquelle ces données se rapportent, y compris la prescription, la dispensation et la fourniture de médicaments et de dispositifs médicaux, ainsi que pour les services sociaux, administratifs ou de remboursement pertinents ».

[293] Art. 2 p. 1 let. e) « utilisation secondaire », le traitement de données de santé électroniques aux fins énoncées au chapitre IV du présent règlement, autres que les finalités initiales pour lesquelles ces données ont été collectées ou produites »
Chapitre 4, Art. 53 désigne le traitement des données de santé pour des finalités autres que les soins individuels (art. 53). Elle est autorisée pour : a) santé publique ; b) politiques sanitaires ; c) statistiques officielles ; d) formation ; e) recherche scientifique et innovation (IA, dispositifs médicaux) ; f) optimisation des soins.

[294] Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030.

[295] NSIS - Nouveau système d'information sanitaire

européenne comme un élément central pour responsabiliser les citoyens et construire une société plus saine, les données étant vues comme un facteur clé de la transformation numérique et devant être accessibles et partageables dans toute l'UE.

Conformément à la stratégie de la Commission européenne, les données de santé sont présentées comme essentielles non seulement pour la prise en charge individuelle (prévention et soins personnalisés) dans le cadre de leur utilisation primaire, mais aussi pour la recherche, la prévention des maladies et le recours à des outils numériques centrés sur le patient (utilisation secondaire). L'objectif opérationnel du Ministère italien est donc d'étendre et d'uniformiser au niveau national le contenu des documents numériques de santé, leurs fonctionnalités, ainsi que les modalités de consultation par les professionnels du SSN.

La directive insiste sur le fait que cette transformation sera progressive, organisée en plusieurs phases liées entre elles, et que le Ministère jouera un rôle de coordination entre toutes les institutions concernées. De façon plus précise, il lui revient de fixer les fondements juridiques et d'adopter des lignes directrices techniques (règles, guides, codifications, classifications, standards) pour la collecte, la conservation, la consultation et l'échange de données entre Régions et Provinces autonomes, avec l'appui d'AGENAS et du Département pour la transformation digitale.

« Ecosistema dei dati sanitari[296] (EDS) »

La directive présente ensuite l'Écosystème des Données Sanitaires (EDS) comme l'instrument nécessaire pour parfaire l'architecture du FSE, en fournissant des services d'élaboration et de consultation des données extraites des documents du FSE, tant pour l'usage primaire (prévention, diagnostic, soins) que secondaire (programmation, gouvernement, recherche) (p. 34).

Dans le cadre de la directive, l'EDS assure deux fonctions fondamentales : coordination informatique nationale et prestation de services homogènes sur tout le territoire (services aux patients, professionnels, administrateurs, chercheurs). L'objectif est d'optimiser l'utilisation des données pour une assistance plus efficace, appropriée et rapide, tout en offrant aux citoyens une visibilité claire et immédiate de leurs informations sanitaires, dans le plein respect de la confidentialité, de la cybersécurité et de la protection des données personnelles (p. 35).

La directive précise que l'EDS, conformément à l'article 12, alinéa 15-quater du décret-loi n° 179/2012, sera réalisé en collaboration avec le Département pour la Transformation Digitale (DTD) et AGENAS, et intégrera les données alimentant le système FSE provenant de toutes les structures sanitaires et médico-sociales publiques et privées, des entités du Service National de Santé, des professionnels de santé et du système Tessera Sanitaria[297].

Ces données EDS seront validées et extraites par les solutions technologiques identifiées afin d'offrir des services à l'ensemble des opérateurs du SSN et aux patients, principalement pour les finalités de soins et de prévention, mais aussi pour la prophylaxie internationale, le gouvernement et la recherche.

L'EDS est explicitement présenté comme la base nationale de départ pour la mise en œuvre du Règlement UE 2025/327 établissant l'Espace européen des données de santé, dont les objectifs consistent à permettre aux personnes un meilleur contrôle sur leurs données sanitaires, à faciliter une meilleure continuité des soins

[296] Espace européen des données de santé (EEDS).

[297] Système équivalent à celui des services sanitaires à partir de la Carte Vitale.

transfrontières au sein de l'UE, à encourager un marché unique des services et produits de santé numérique, et à garantir un cadre cohérent pour la réutilisation des données pour la recherche, l'innovation, les politiques sanitaires et les activités règlementaires.

Pour atteindre ces objectifs, la directive prévoit la mise en œuvre de règles communes pour les données personnelles, l'identification de standards et formats assurant l'interopérabilité des données, ainsi que l'élaboration d'une gouvernance nationale impliquant d'autres institutions centrales pour la mise en œuvre du règlement au niveau national. Comme dans d'autres sections de la directive, on constate ici que l'adoption de ces règles communes pour atteindre les objectifs européens reste à l'état de projet en cours d'élaboration, sans que des mesures concrètes soient déjà mises en place.

Collecte, analyse, diffusion des données et soutien à la télémédecine

La directive précise de manière plus concrète comment s'exécute la ligne de financement spécifique du PNRR dans le cadre du 2.7.3 *Potenziamento della capacità di raccolta, analisi e diffusione dei dati a livello centrale e supporto alla diffusione della telemedicina* (p. 35).

Elle détaille les priorités d'utilisation des fonds : moderniser l'infrastructure du Système Informatif Sanitaire National et optimiser tous les processus de gestion des données de santé (collecte, traitement, validation, analyse). Les interventions se concentrent sur trois axes : accélérer l'exploitation des données existantes pour mieux suivre les Niveaux essentiels d'assistance - *Livelli Essenziali di Assistenza* (LEA) ; intégrer de nouvelles sources de données via des plateformes dédiées comme le Système Informatif des Soins Primaires et celui des Hôpitaux de Communauté ; soutenir l'innovation avancée, notamment en définissant une base juridique pour l'intelligence artificielle en santé (p. 36).

Pour exploiter pleinement le potentiel des données tout en respectant la protection des données personnelles, des outils technologiques permettront leur diffusion publique sous forme d'Open Data. Ce projet mobilise l'ensemble du territoire italien, administration centrale, Régions, Provinces autonomes, dans une logique de programmation, monitoring et contrôle sanitaires renforcés.

La Plateforme Nationale de Télémédecine (PNT), placée sous l'égide d'AGENAS (Agence nationale pour les services sanitaires nationaux) avec ses Infrastructures Nationales (INT) et Régionales (IRT), garantira l'accès universel aux services essentiels de télémédecine (téléconsultation, téléassistance, télésurveillance, téléconsultation) grâce à des standards d'interopérabilité communs.

Enfin (§ 2.7.4) la directive confirme que le Ministère de la santé italien continuera sa participation aux activités de santé numérique de l'e Health Network, coordonnant les actions pour l'interopérabilité des données sanitaires au niveau UE, tant pour les finalités de soins (usage primaire) que pour l'usage secondaire (gouvernement, recherche), dans le cadre du Règlement sur l'Espace européen des données de santé.

À travers les infrastructures MyHealth@EU, actuellement en phase expérimentale en Italie pour l'usage primaire des données de santé, et HealthData@EU, dont le pays prépare activement la mise en œuvre pour l'usage secondaire, l'Italie se conforme aux obligations du règlement EEDS en désignant ses autorités nationales compétentes pour garantir l'interopérabilité européenne.

Derniers points sur la santé numérique et dispositions ultérieures

La directive conclut la section sur la santé numérique (§ 2.7) par des mesures transversales de transparence, sécurité et reporting, avant de passer à l'efficience organisationnelle (§ 2.8).

Elle prévoit la pleine mise en œuvre du Sunshine Act (decreto legge. 90/2017) pour une transparence totale des relations financières entre l'industrie pharmaceutique/dispositifs médicaux et les acteurs de santé, transposant la legge 62/2022 "*Disposizioni in materia di trasparenza dei rapporti tra le imprese produttrici, i soggetti che operano nel settore della salute e le organizzazioni sanitarie*"[298] via la plateforme nationale « Santé transparence » gérée par AGENAS : publication annuelle des avantages financiers de l'industrie pharma/dispositifs aux professionnels et structures, avec audits et sensibilisation pour restaurer la confiance publique (p. 36). Elle prévoit une publication annuelle des avantages financiers de l'industrie pharma/dispositifs aux professionnels et structures, avec audits et sensibilisation pour restaurer la confiance du public (§ 2.8).

En conclusion, la directive identifie des actions qui constituent des prérequis indispensables pour sécuriser la transformation numérique du SSN, mais ces mesures demeurent programmatiques et non pleinement opérationnelles, reflétant une vision stratégique encore en phase préparatoire au stade de la directive 2026.

Ministère italien de la Santé, *Direttiva generale per l'attività amministrativa e la gestione (ai sensi degli articoli 4 e 14 del decreto legislativo 30 marzo 2001, n. 165), Anno 2026.*

[298] Loi du 31 mai 2022, n° 62 portant les « Dispositions en matière de transparence des relations entre les entreprises productrices, les acteurs du secteur de la santé et les organisations de santé ».

Droit suédois

Reimbursement of Digital Medical Devices in Sweden

par Sarah DE HEER

Doctorante en Droit public, Université de Lund (Suède)

Introduction

Medical devices come in a wide variety, ranging from simple plasters and thermometers to more advanced technology, such as 3D printed prosthetics and digital tools, including mHealth. Medical devices play a vital role in the provision of healthcare activities and services in Sweden. As such, medical devices are widely used in all parts of the healthcare sector ; when providing highly specialised care in hospitals but also for everyday care for patients in the comfort of their own home.

In this piece, the reimbursement of digital medical devices in Sweden will be discussed. This discussion, however, will be restricted to healthcare activities and services provided under the universal system and the publicly funded private healthcare sector. The common denominator is that both are primarily funded through taxes, which means that patients can rely on the reimbursement schemes. Contrarily, the fully private healthcare sector is not funded by the taxpayers' money, and thus the nationwide reimbursement rules are not applicable to this sector.

Since the responsibility of the provision of healthcare activities and services is decentralized, this contribution will, thus, first introduce the Swedish health care system, focusing on both its legislative and governance framework (**Section 2**). As the use of medical devices when receiving healthcare activities and services and the reimbursement of such medical devices are closely connected in Sweden, this piece will also discuss the use of medical devices in the Swedish healthcare system (**Section 3**). After, this contribution will scrutinise the reimbursement of medical devices in general but also concerning consumable medical devices (**Section 4**). Next, this piece will focus on the reimbursement of digital medical devices (**Section 5**). This contribution will also discuss new developments in Sweden (**Section 6**). Last, a conclusion will follow (**Section 7**).

1. THE SWEDISH HEALTHCARE SYSTEM – A BRIEF OVERVIEW

1.1 The Legislative Framework

While healthcare services in Sweden are governed by multiple legislative frameworks, the main act is the Health and Medical Services Act (hälso-och

sjukvårdslagen)[299]. This Act was adopted in 2017, and aims to make the legal framework easier to understand, clearer, and more accessible[300]. The Health and Medical Services Act is a so-called 'targeted framework law', which means that it solely encapsulates provisions on overall goals, responsibilities and guidelines for the healthcare activities.[301] However, dental care, is in principle excluded by the Health and Medical Services Act[302] Rather, dental care is regulated under the Dental Care Act (*tandvårdslagen*)[303].

Additionally, the healthcare sector in Sweden is regulated by other acts, including the Patient Act (*patientlagen*)[304], Patient Data Act (*patientdatalagen*)[305] and the Patient Safety Act (*patientsäkerhetslagen*)[306]. The legislation governing healthcare activities and services in Sweden are so-called obligation, which means that patients do not derive direct rights under the Swedish legal framework. Rather, the law imposes obligations upon healthcare professionals. Nevertheless, based on the legislative framework, patients can still derive expectations of the healthcare activities and services performed by healthcare professionals.

1.1 The Governance Framework

Various actors play a role in providing healthcare activities and services in Sweden, predominantly the Regions (*Regioner*), and in some instances by the municipalities (*kommuner*). The Regions are responsible for ensuring that everyone who resides in their territory has access to quality care[307]. As such, the Regions are mainly responsible for the provision of healthcare activities and services. However, municipalities in Sweden also play a role, as they take care of the healthcare activities and services for, amongst others, individuals who are awarded special support and services under the Act concerning Support and Service for Persons with Certain Functional Impairments (*lag om stöd och service till vissa funktionshindrade*)[308] and housing with special services for people with disabilities[309].

Consequently, the range of medical devices – whether it be digital or not – depends on the Region or municipality one resides. Certain medical devices may be available for the patient's healthcare journey in one Region or municipality, while patients in other Regions or municipalities may not have access to the same medical device.

2. USE OF MEDICAL DEVICES IN SWEDEN

During the provision of healthcare activities and services by healthcare professionals, a plethora of medical devices are used. Most medical devices are used at healthcare facilities by healthcare professionals. However, a substantial part of medical devices is also used by patients either on their own initiative or prescribed by healthcare professionals. As such, patients can use these medical devices in their own homes. These medical devices for the patients' own use include, among others, assistive devices, medical devices

[299] Health and Medical Services Act (*hälso- och sjukvårdslagen (2017:30*).
[300] Regeringen, *En ny hälso- och sjukvårdslag* (Prop. 2016/17:43), 79.
[301] Regeringen, *En ny hälso- och sjukvårdslag* (Prop. 2016/17:43), 80.
[302] 2 Chapter 1 § Health and Medical Services Act.
[303] 1 Chapter 1 § Dental Care Act (*tandvårdslag (1985:125)*).
[304] Patient Act (*patientlag (2014:821)*).
[305] Patient Data Act (*patientdatalag (2008:355)*).
[306] Patient Safety Act (*patientsäkerhetslag (2010:659)*).
[307] 8 Chapter 1 § Health and Medical Services Act. Section 2 also mentions that Regions are to provide healthcare activities and services to those individuals who do not reside in their territory but are entitled to healthcare benefits under the Social Security Coordination Regulation and students on study visits abroad.
[308] 2 § Act on support and services for certain disabled people (*lag (1993:387) om stöd och service till vissa funktionshindrade*).
[309] 8 Chapter 10 § Social Services Act (*socialtjänstlag (2025:400)*).

consumable for personal use, and therapeutic and treatment devices for home use.

In Sweden, healthcare activities and services are to be performed in such a manner that ensures good care is achieved, which in particular includes that the standard of good quality should be achieved[310]. Further, healthcare professionals need to base their work on scientific evidence and proven clinical evidence[311], which is the golden standard in Swedish health care[312]. This also includes the use of medical devices for patient diagnosis and treatment. Specifically for medical devices, Swedish law requires that they need to enable the provision of good care, irrespective of them being used in a healthcare setting or in the patient's own home[313].

The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care (*Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården*)[314] establishes specific national rules on the use of medical devices in health care and dental care. Before using medical devices during the patient's healthcare journey, medical professionals need to have knowledge of, among others, how the medical device operates and the risk of its use by the patient[315], and are to check the medical device before its use on patients[316]. Further, the Regions and municipalities that are responsible for the provision of health care are to establish routines for the use of medical devices, which are aimed at ensuring– among others – that medical devices are used safely and that only safe devices are used during the diagnosis and treatment of patients[317].

3. REIMBURSEMENT OF MEDICAL DEVICES IN SWEDEN

3.1 General Rule

Unlike the use of medical devices, there are no comprehensive reimbursement rules on national level. Seeing the organisational structure of health care in Sweden, where the responsibility of healthcare activities and services are scattered across the Regions and municipalities, the lack of national-wide reimbursement rules is not surprising. Following this decentralised approach, the Regions and municipalities are also responsible for the purchase of medical devices, which is tied to their reimbursement.

The main rule as regards reimbursement is that the use of medical devices for the diagnosis and treatment of patients is reimbursed by the Region or municipality that bears responsibility for health care. Examples include medical devices used for medical imaging, such as a CT scan and MRI, but also medical devices used for the treatment of patients, including kidney dialysis machine and knee implants.

3.2 Consumable Medical Device

There is an exception to the general approach that the rules of reimbursement are governed by the Regions. Certain medical devices used by patients are subsidised by the State under the high-cost protection scheme (*högkostnadsskyddet*).

---

[310] 5 Chapter 1 § Health and Medical Services Act.
[311] 6 Chapter 1 § Patient Safety Act.
[312] Lena Wahlberg and Johannes Persson, 'Importing Notions in Health Law: Science and Proven Experience' 24 (2017) European Journal of Health Law 565, 566.
[313] 5 Chapter 2 § Health and Medical Services Act.
[314] The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care (*HSLF-FS 2021:52 Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården)*.
[315] 3 Chapter 3 § The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care.
[316] 3 Chapter 4 § The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care.
[317] 2 Chapter 2 § The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care.

This scheme is primarily applicable to prescription medicine but also to consumable medical supplies (*förbrukningsartiklar*), which include certain medical devices. Unlike durable medical devices, consumable medical devices are characterised by their limited use.

Under Swedish law, these consumable medical supplies need to be prescribed by a physician *either* for a stoma[318] *or* due to an illness to administer medicine or to self-monitor the medication[319]. Such medical supplies for a stoma are ostomy bag and ostomy belts. Examples of consumable medical supplies to self-administer medication include pen needles for diabetes and inhalation aids, while blood glucose test strips and the blood glucose meter are examples of consumable medical supplies to self-monitor medication.

Under the high-cost protection scheme, patients are to pay a maximum amount per year starting from the first purchase of prescription medicine and consumable medical supplies[320]. In short, the more costs you incur, you will pay less percentage wise until you reach a threshold, after which you will receive prescribed medication and consumable medical supplies free of charge[321].

Which consumable medical devices are included in the high-cost protection scheme and the price thereof is decided by the Dental and Pharmaceutical Benefits Agency (*Tandvårds- och läkemedelsförmånsverket*)[322]. However, the Dental and Pharmaceutical Benefits Agency does not decide which medical devices should be purchased by the Regions.

4. A FOCUS ON DIGITAL MEDICAL DEVICES

The AI Healthcare Map (*AI-vårdkartan*) maps AI initiatives used in the Swedish healthcare system[323], which also includes digital medical devices. The AI Healthcare Map is a work-in-progress and is updated on a continuous basis. The AI Healthcare Map indicates that 197 AI initiatives are implemented across Sweden, with every Regions having at least one AI system in place[324]. Almost all Regions in Sweden even use AI systems to improve the healthcare system, such as AI used for translations between Swedish and other languages, AI predicting sick leave at group level of healthcare professionals, and AI warning that equipment need calibration. Nevertheless, the majority of AI initiatives are medical devices used for the provision of health care. Examples of digital medical devices include the use of AI assisting in detecting breast cancer in Region Scania, AI used as an aid to predict strokes in Region Dalarna, and AI helping in diagnosing people with acromegaly in Region Västerbotten. Where these digital medical devices are used to diagnose and treat patients in the Swedish universal healthcare system, the use of such AI medical devices do not incur costs upon patients. Rather, the costs are paid by the State. Furthermore, various Regions are

[318] 18 § 2nd para. Act on pharmaceutical beneifts etc (*lag (2002:160) om läkemedelsförmåner m.m.*).
[319] 18 § 3rd para. Act on pharmaceutical beneifts etc.
[320] 5 § 2nd para. Act on pharmaceutical beneifts etc.
[321] 4 § Act (1996:1150) on high-cost protection scheme when purchasing pharmaceuticals, etc. (*lag (1996:1150) om högkostnadsskydd vid köp av läkemedel m.m.*)
[322] 7 § Act on pharmaceutical beneifts etc.
[323] AI Sweden, 'AI-vårdkartan' (ai.se/) <https://www.ai.se/sv/sektorsinitiativ/halso-och-sjukvard/ai-vardkartan> accessed 12 February 2026.
[324] AI Sweden, 'Vårdkartan' (https://vardkartan.ai.se/) <https://vardkartan.ai.se/> accessed 12 February 2026.

developing medical devices that could be used for patient care. Thus, it would not be surprising to see an increase in the use of such devices in the future.

However, concerns have been raised as regards AI's place in patient care. Specifically, AI Sweden, the national center for applied artificial intelligence and co-created of the AI Healthcare Map, pointed out that AI development is marked by significant regional inequalities. Five out of 21 Regions represent more than 60% of AI initiative in Sweden, with 4 Regions not having any AI system in place[325]. Furthermore, research from the Swedish Medical Association (*Sveriges läkarförbund*) showed that most of the Regions do not have any guidelines in place on how to use AI in the provision of healthcare[326].

Currently, no digital medical devices are included under the consumable medical supplies, and thereby reimbursed under the high-cost protection scheme. This can change following a decision of the Dental and Pharmaceutical Benefits Agency determining that a digital medical device qualifies as self-administrating or self-monitoring medication. However, it is difficult to see how such a classification would apply to digital medical devices, as they are not characterised by their limited use.

5. RECENT DEVELOPMENTS

As the decentralised approach may form an obstacle to effectively purchasing and evaluating – and thus using – medical devices in the Swedish healthcare sector, all Regions have joined forces and collaborate in the 'Regions' collaboration model for medical technology' (*Regionernas Samverkansmodell för Medicinteknik*). The expert group of the this collaboration model, the Medical Technology Products Council (*Medicintekniska produktrådet*) has adopted the so-called 'National Joint Introduction' (*nationellt ordnat införande*). Its aim is to ensure fair, cost-effective and appropriate use of medical devices across Sweden. The National Joint Introduction is a comprehensive process covering all stages necessary for the nationwide adoption of digital medical devices, including market screening, selection, procurement, and follow-up[327].

This national plan will, thus, ensure that patients have access to the same (digital) medical devices – including its reimbursement – across Sweden, as opposed to the availability of medical devices hinging on in which Region one lives. Another benefit of the National Joint Introduction is that the observed the negative impact of the inequalities of AI initiatives on patient care may be restricted, as digital medical devices, including consumable digital medical devices, are implemented nationwide.

Even though the National Joint Introduction may give an answer to the uniform introduction of digital medical devices, introducing AI into patient care is not without obstacles. The Medical Technology Products Council has specifically addressed concerns related to the safety of using digital medical devices in the healthcare system. To this end, they have adopted a recommendation. Before implementing any AI system, including digital medical devices, into the Region's healthcare system, Regions are recommended to use validation platforms, which ensure that AI systems are safe to use

[325] AI Sweden, 'Ny kartläggning: Stor ojämlikhet i regionernas AI-arbete inom vården' (ai.se/) <https://www.ai.se/sv/nyheter/ny-kartlaggning-stor-ojamlikhet-i-regionernas-ai-arbete-inom-varden> accessed 12 February.

[326] Swedish Medical Associaton, 'Regioner saknar riktlinjer för AI i vården' (slf.se/) <https://slf.se/nyheter/regioner-saknar-riktlinjer-for-ai-i-varden/> accessed 12 February.

[327] Regions' collaboration model for medical technology, 'Ordnat införande' (samverkanmedicinteknik.se/) < https://samverkanmedicinteknik.se/ordnat-inforande> accessed 12 February 2026.

in the healthcare system[328]. The aim of this platform, which are also known as VAI platforms (*VAI-plattformer*) is to validate the AI system's clinical performance within the Region's specific clinical environment[329]. There are in total three VAI platforms, each tailored towards AI applications in a specific area, namely[330].

1. VAI-B (Breast) that evaluates AI systems for breast radiology, including determining the diagnostic performance of AI systems in mammography screening
2. VAI-P (Pathology) that assesses AI systems for the analysis of global Ki-67[331] in breast cancer
3. VAI-S (Stroke) that evaluates AI systems that identify and evaluate various forms of stroke

While the VAI platforms do not cover all possible AI systems – and thus digital medical devices –, it is a promising development, as it may help ensure, and potentially even advance, patient safety in Swedish health care.

Conclusion

Reimbursement of medical devices in Sweden is shaped by the decentralised healthcare system, in which the Regions bear primary responsibility and therefore fund digital medical devices when they are used in patient care. This leads to regional disparities amongst patients, as access and reimbursement depend on whether a Region has adopted such technologies. This may mean that an individual in one Region does not have access to a certain digital medical device in their patient healthcare journey, while a patient in another Region may have access to the same device. The only nationwide reimbursement mechanism, namely the high-cost protection scheme for certain prescribed consumable medical devices, currently does not cover digital medical devices.

At the same time, the expanding role of digital medical devices demonstrates the need for a more uniform approach to ensure equal patient access. The National Joint Introduction seeks to enable nationwide adoption of digital medical devices, while validation platforms aim to ensure that AI-based digital medical devices are safe for use in the Swedish healthcare.

---

[328] Regions' collaboration model for medical technology, 'Rekommendation till regionerna att använda valideringsplattformar för AI-produkter' (samverkanmedicinteknik.se/) <https://samverkanmedicinteknik.se/nyheter/nyheter/2025-03-27-rekommendation-till-regionerna-att-anvanda-valideringsplattformar-for-ai-produkter> accessed 12 February 2026.

[329] The Medical Technology Products Council, *Validering av AI-produkter inom bilddiagnostik före införande och under användning* 2025, 3.

[330] The Medical Technology Products Council, *Validering av AI-produkter inom bilddiagnostik före införande och under användning* 2025, 3-4.

[331] Global Ki-67 is a method to measure the proportion of proliferating cancer cells in a tumor sample. For more information, see C. Boyaci and others, 'Global scoring method of Ki67 immunohistochemistry in breast cancer demonstrates improved concordance using real-world multi-institutional data' (2025) 27 Breast Cancer Research 159.

Droit de l'Union européenne

La notion de données personnelles au regard de la pseudonymisation

par Lili-Marie FERRANDO

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

À l'heure de la révolution du numérique en santé, le partage des données à grande échelle est devenu le socle indispensable d'une médecine personnalisée, prédictive et performante. Cependant, la circulation de ces flux se heurtait jusqu'alors à une interprétation particulièrement rigide du cadre européen de protection des données.

C'est dans ce contexte que la Cour de justice de l'Union européenne (CJUE), dans sa décision du 4 septembre 2025[332], vient de lever un verrou historique en offrant une lecture pragmatique de la pseudonymisation. Par cet arrêt, la Haute juridiction est venue préciser que des données pseudonymisées peuvent perdre leur statut de données personnelles selon le destinataire auquel elles sont transmises. Elle apporte cependant deux conditions majeures : l'impossibilité technique d'identifier la personne via des mesures « raisonnables », et l'incapacité légale du destinataire à obtenir les moyens de réidentification. Cette décision dénote avec l'approche absolue et rigide adoptée jusqu'alors par les autorités de contrôle.

L'affaire s'inscrit dans le cadre de la procédure de résolution bancaire engagée à l'encontre de la *Banco Popular*, un établissement financier espagnol. Le Conseil de résolution unique (CRU) avait mis en œuvre une procédure d'audition des actionnaires et des créanciers. C'est dans ce cadre qu'il a collecté des commentaires et observations des participants dont les identités ont été maintenues confidentielles par le recours à un code alphanumérique unique de 33 caractères, généré aléatoirement au moment de la réponse, qu'il a ensuite pseudonymisés en remplaçant les identités par des codes alphanumériques uniques. Ces commentaires pseudonymisés ont été transmis à un tiers, un cabinet d'audit et de Conseil désigné en tant qu'évaluateur indépendant, mais seul le CRU conservait la clé de correspondance.

En 2019, soit deux ans plus tard, plusieurs participants ont saisi le contrôleur européen de la protection des données (CEPD), reprochant au CRU de ne pas avoir été informés de cette transmission. Le

[332] CJUE, 4 septembre 2025, aff.C-413/23 P, ECLI.EU.

CEPD a adressé un rappel à l'ordre au CRU, estimant que ces données restaient des données à caractère personnel par nature, impliquant une obligation d'information renforcée. Ce dernier a introduit un recours en annulation devant le Tribunal de l'Union qui a annulé la décision du CEPD. C'est dans ce cadre que la Cour de justice a saisie dans le cadre d'un pourvoi.

Bien qu'en l'espèce l'affaire porte sur des données bancaires, la décision était très attendue pour clarifier le régime juridique de la pseudonymisation dans des secteurs sensibles comme celui de la santé.

Il revenait ainsi à la CJUE de trancher une question fondamentale : La qualification de « données personnelles » est-elle absolue ou peut-elle être écartée selon le contexte et le détenteur de l'information ?

En d'autres termes, des données pseudonymisées transmises à un tiers doivent-elles toujours être considérées comme des données personnelles au sens du RGPD et du Règlement UE 2018/1725 ? Cette qualification peut-elle être écartée et si oui, sous quelles conditions techniques et juridiques ?

Par son arrêt en date du 4 septembre 2025, la Cour annule (partiellement) l'arrêt rendu par la juridiction antérieure. Mais elle procède aussi et surtout à une distinction fondamentale entre la nature de la donnée pour l'émetteur et son statut pour le destinataire. Ainsi, une donnée pseudonymisée, peut dans certains cas, ne pas être considérée comme une donnée personnelle à l'égard de son destinataire, sous certaines conditions (appréciation pragmatique et contextuelle). La Cour adopte ainsi une approche casuistique et relative de l'identifiabilité.

Dès lors, il convient d'analyser comment le juge européen est passé d'une approche absolue à une approche relative de la donnée (**I**), avant d'étudier le dualisme du régime juridique qui en découle entre émetteur et destinataire (**II**).

I. DE L'APPROCHE ABSOLUE À UNE APPROCHE RELATIVE : LA « SUBJECTIVISATION » DE LA DONNÉE A CARACTÈRE PERSONNEL

La Cour rompt avec une conception rigide (**A**), pour s'attacher au contexte et à la finalité du traitement, par le prisme d'une conception pragmatique (**B**).

A. Le dépassement de la vision objective

Avant l'arrêt du 4 septembre 2025, prévalait une vision dite « absolue » de la donnée personnelle. En effet, dès lors qu'une clé d'identification existait, peu importe son détenteur, la donnée conservait son caractère personnel pour l'ensemble des acteurs. Cette approche rigide et objective fixait le statut de l'information.

Comme le souligne le Professeur Douville, constituent ainsi des données à caractère personnel des identifiants tels que le nom, l'image, ou encore l'adresse IP « *dès lors que la personne est identifiable à l'aide d'informations supplémentaires*[333] ».

Pour revêtir cette qualification, l'information doit se rapporter à une personne concernée. Dans son arrêt *NOWAK,* la Cour avait déjà dégagé trois critères de rattachement non cumulatifs : le contenu, la finalité et l'effet de l'information. En l'espèce, les opinions exprimées par les créanciers étaient « intimement liées » à ces derniers en tant qu'expression de leurs pensées[334]. Jusqu'à récemment, cette nature personnelle était considérée comme immuable. Cette vision imposait systématiquement l'application du RGPD, entraînant des lourdeurs administratives même si le destinataire des

[333] DOUVILLE, T., « Éthique et données à caractère personnel (Approche française et européenne*) »*, *Revue internationale de droit économique*, 2021 t. XXXV (3), 29-45.

[334] DOUVILLE, T., « La notion de données à caractère personnel après l'arrêt CRU », *Revue trimestrielle de droit commercial et de droit économique*, 2025. 1019. Voir aussi NAFTALSKI, F., *Dalloz IP/IT* 2026, p.158.

données n'avait aucun moyen de savoir qui se cachait derrière tel ou tel code.

La pseudonymisation est un processus réversible défini à l'article 3 (6ème point) du RGPD. Il s'agit d'un traitement permettant que les données ne puissent plus être attribuées à une personne précise « *sans avoir recours à des informations supplémentaires* », à condition que ces dernières soient conservées séparément. À titre d'exemple, la cryptographie à clé secrète permet de lier des données pseudonymisées à l'identité réelle, tant que la clé est stockée de manière sécurisée.

À l'inverse, l'anonymisation, est par principe, irréversible et définitive. Elle détruit définitivement tout lien entre la donnée et l'identité en répondant à trois impératifs : individualisation, corrélation et inférence. Par des techniques de randomisation ou de généralisation, la donnée anonymisée sort instantanément du champ du RGPD.

C'est précisément sur cette distinction que la CJUE apporte une clarification majeure en 2025. Ainsi les données pseudonymisées peuvent désormais perdre leur statut de données personnelles à l'égard du destinataire sous certaines conditions.

B. L'analyse à travers les « yeux » du destinataire

Le point de bascule réside dans le passage d'une approche objective de la donnée à une approche contextuelle, fondée sur le détenteur. La Cour s'appuie sur le considérant 16 du règlement 2018/1725 (équivalent au considérant 26 RGPD) pour affirmer que l'identifiabilité est une notion contextuelle.

Désormais, la donnée est qualifiée à travers son destinataire, sa nature dépend de ce dernier. Dans l'affaire commentée, si le CRU détient la clé de déchiffrement, le cabinet d'audit quant à lui, est juridiquement et techniquement, dépourvu de toute information à caractère personnel. N'ayant accès ni à l'identité des participants, ni aux informations supplémentaires permettant de briser la pseudonymisation mise en place, la donnée change de dimension juridique à son égard. Elle quitte la sphère des données personnelles pour rentrer dans celle des données anonymes.

Comme le souligne le Professeur Douville, cette approche consacre une conception relative :

> *« Ce n'est donc pas parce que des informations supplémentaires permettant d'identifier la personne concernée existent que les informations dont l'attribution à des personnes physiques est discutée dans le cadre d'un traitement de données sont à caractère personnel, tout dépend de qui détient ou peut avoir accès à ces informations supplémentaires. Cette conception relative de la notion de données à caractère personnel s'appuie sur l'interprétation préexistante de la notion de « moyens raisonnablement susceptibles d'être utilisés » et sur la conception dorénavant restrictive de l'expression « toute personne »*[335].

Cette lecture repose sur le critère des « moyens raisonnablement susceptibles d'être utilisés ». Si le destinataire n'a aucun moyen légal ou technique d'accéder à la clé, l'identification n'est plus « raisonnablement envisageable ». La Cour adopte ainsi une interprétation restrictive de l'expression « toute personne », limitant l'analyse aux seuls moyens dont dispose réellement l'entité qui traite la donnée.

Concernant le droit de la santé, cette approche constitue un véritable changement de paradigme. En validant le fait qu'une donnée puisse être anonyme pour celui qui la reçoit sans l'aide pour celui qui l'envoie, la CJUE facilite les échanges. Concrètement, cela sécurise le partage des données massives nécessaires à la médecine de précision ainsi qu'à la recherche, sans pour autant fragiliser la vie privée des patients.

---

[335] DOUVILLE, T., *op cit.* « La notion de données à caractère personnel après l'arrêt CRU », *Revue trimestrielle de droit commercial et de droit économique*, 2025. 1019.

II. LE DUALISME DU RÉGIME JURIDIQUE APPLICABLE : ENTRE SÉCURITÉ DE L'ÉMETTEUR ET SOUPLESSE DU DESTINATAIRE

Si le destinataire bénéficie d'une souplesse nouvelle grâce à l'anonymisation relative (A), l'émetteur quant à lui reste fermement tenu par ses obligations en tant que responsable de traitement (B).

A. Les critères de l'anonymisation relative

Pour que la donnée change de nature aux yeux du destinataire, la Cour ne se contente pas d'une simple promesse de confidentialité. Elle impose un test de réidentification fondé sur « *les moyens raisonnablement susceptibles d'être utilisés* ».

L'anonymisation classique (ou absolue) est irréversible et doit résister à trois impératifs techniques, comme nous avons pu le voir, qui reposent sur des techniques lourdes. L'arrêt crée une anonymisation relative. Ainsi la donnée n'est pas anonyme dans l'absolu, mais elle le devient pour un acteur spécifique selon trois conditions cumulatives. D'abord, on parle de l'impossibilité technique, le destinataire ne dispose d'aucun moyen raisonnable pour identifier les personnes. Ensuite, il y a l'impossibilité légale, qui suppose qu'il n'existe aucune voie de droit permettant au tiers d'accéder aux informations supplémentaires détenues par l'émetteur. Enfin on retrouve l'effort démesuré, c'est l'idée que le coût et le temps nécessaires à une réidentification éventuelle doivent être disproportionnés au regard des technologies disponibles.

Comme l'énonce la Cour, il faut prendre en compte « *l'ensemble des facteurs objectifs, tel que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponible au moment du traitement*[336] ». Si le risque de réidentification est insignifiant ou simplement illicite, le destinataire sort alors du champ d'application du RGPD.

B. Le maintien des obligations du responsable du traitement

Le paradoxe apparent de cette décision réside dans le fait que, bien que les données soient jugées anonymes pour le destinataire (en l'espèce, le cabinet d'audit), le responsable (CRU) est tout de même sanctionné. Ce dualisme s'explique par la nature même de la relation juridique entre le collecteur de données et la personne concernée.

Le statut « personnel » ou « anonyme » d'une donnée est ainsi relatif à son détenteur. Le CRU, en tant qu'émetteur, conserve la clé d'identification, pour lui les données n'ont jamais changé de nature et restent des données à caractère personnel soumises au RGPD. Par conséquent, le fait que la donnée devienne « anonyme » pour un tiers après un transfert, n'efface en aucun cas les obligations initiales du responsable du traitement.

L'obligation d'information, prévue par les articles 14 et 15 du RGPD, naît au moment précis de la collecte. La CJUE rappelle que cette obligation « *s'inscrit dans la relation juridique existant entre la personne concernée et le responsable du traitement*[337] » et porte les informations telles qu'elles ont été transmises aux responsables avant tout transfert à un tiers.

En l'espèce, dès lors que le CRU collectait des noms et des commentaires, il traitait des données personnelles. Il devait ainsi impérativement informer les utilisateurs de l'identité des futurs destinataires, peu importe si ces derniers était incapable de les identifier par la suite.

Ainsi cette décision impose aux responsables de traitement, notamment dans le secteur de la santé, une vigilance accrue. L'anonymisation relative au niveau du destinataire n'est pas une clause

[336] CJUE, aff. C-413/23 P, *opt. cit.*, pt. 79.

[337] *Ibid.*

d'exonération. L'identité des tiers receveurs doit être documentée et communiquée dès la collecte, sous peine de litige, comme en témoigne ledit arrêt. Le responsable du traitement doit continuer de garantir l'exercice des droits car il est le seul maître de la clé de réidentification.

Pour conclure, cet arrêt constitue indéniablement une décision importante pour le droit des données personnelles. En droit de la santé, et plus particulièrement dans le cadre de l'Espace Européen des Données de Santé (EEDS)[338], elle ouvre des perspectives considérables tout en soulevant de nouvelles incertitudes.

L'EEDS, dont l'ambition est de faciliter la circulation des données de santé à des fins de recherche, d'innovation et de soins, repose précisément sur des mécanismes de partage de données à grande échelle entre acteurs multiples. La reconnaissance d'une anonymisation relative par la CJUE pourrait ainsi fluidifier ces échanges.

Toutefois, comme le souligne l'avocate Lorette Dubois, cette avancée pragmatique soulève à elle seule une « *myriade de questions*[339] » aux conséquences pratiques considérables.

D'abord, la question du statut des sous-traitants est particulièrement sensible : les hébergeurs de données de santé recevant des données pseudonymisées pourraient-ils se voir exclus du champ du RGPD ? Une telle exclusion, si elle allégeait leurs obligations formelles, affaiblirait corrélativement les garanties offertes aux patients.

Par ailleurs, la question des transferts de données hors de l'Espace Économique Européen (EEE), fréquents dans le cadre de la recherche médicale internationale, reste, elle aussi en suspens.

Plus fondamentalement, comme le relève l'auteure, « *les notions ont probablement gagné en flexibilité mais la matière perd en sécurité juridique*[340] ». Dans un domaine aussi sensible que celui de la santé, où la réidentification des patients expose à des risques particulièrement graves, cette insécurité appelle une vigilance accrue. Les travaux engagés par le Comité européen de la protection des données sur l'anonymisation et la pseudonymisation, influencés par l'arrêt CRU, ainsi que le projet de règlement *Digital Omnibus* publié en novembre 2025, constituent des développements à suivre attentivement pour les acteurs de l'EEDS.
Ainsi, si l'arrêt CRU ouvre une voie prometteuse pour la médecine de précision et la recherche en santé, il appartient désormais au législateur, ainsi qu'aux autorités de contrôle, de combler les nombreuses « *zones d'ombres et incertitudes* », afin que la flexibilité nouvellement acquise ne se fasse pas au détriment de la protection des données des patients.

CJUE, 4 septembre 2025, *CRE / CRU*, aff. C-413/23 P, ECLI:EU:C:2025:645.

[338] Règlement (UE)2025/327 du Parlement européen et du Conseil du 11 février 2025, *JOUE* L 5 mars 2025

[339] DUBOIS, L., « L'arrêt CRU : un digne épisode de fin pour une série d'anthologie sur la notion de donnée à caractère personnel ? », *Revue Lamy Droit de l'Immatériel*, n° 233, 1er février 2026.

[340] Citation de L. MAISNIER-BROCHE, reprise par l'auteure L. DUBOIS dans « L'arrêt CRU : un digne épisode de fin pour une série d'anthologie sur la notion de donnée à caractère personnel ? », *Revue Lamy Droit de l'Immatériel*, n° 233, 1er février 2026.

La construction prétorienne de la notion de « télémédecine » dans le cadre des soins de santé transfrontaliers

A propos de l'arrêt de la Cour de justice de l'Union européenne du 11 septembre 2025, *UJ c. Österreichische Zahnärztekamme*, aff. C-115/24

par Salaheddine ZAHID

Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Objet de l'arrêt. Par cet arrêt du 11 novembre 2025, UJ c. *Österreichische Zahnärztekammer* (C-115/24), la Cour de justice de l'Union européenne (ci-après « Cour de justice ») précise les contours juridiques de la télémédecine en droit de l'Union, tout en déterminant le régime applicable aux prestations transfrontalières de soins dispensées à distance.

Résumé des faits. Le litige trouve son origine dans la commercialisation, sous la marque « DrSmile », de traitements orthodontiques en délivrant des aligneurs dentaires transparents. UJ, médecin-dentiste établie en Autriche, procédait à certains actes réalisés en présentiels (anamnèse, entretien d'information, scanner 3D de la mâchoire ainsi que des soins préliminaires), tandis que la société allemande *DZK Deutsche Zahnklinik* assurait à distance le suivi orthodontique des patients au moyen d'outils numériques et d'une application dédiée. La chambre autrichienne des médecins-dentistes estimait que cette organisation permettait à une société étrangère (ne disposant pas des autorisations requises par le droit autrichien) d'accéder indirectement à des activités de médecine dentaire en Autriche.

Procédure. La chambre autrichienne des médecins-dentistes introduit une action en cessation assortie d'une demande en référé afin d'interdire à UJ toute participation directe ou indirecte à des activités de médecine dentaire exercées en Autriche par des sociétés étrangères ne disposant pas des autorisations prévues par le droit autrichien. Rejetée en première instance, l'*Oberlandesgericht Graz* (tribunal régional supérieur de Graz, Autriche) accueille la demande d'appel, considérant que UJ agissait en tant qu'auxiliaire d'exécution de l'entreprise allemande. Saisi d'un pourvoi contre cette dernière décision, l'*Oberster Gerichtshof* (Cour suprême, Autriche) sursoit à statuer pour poser des questions préjudicielles à la Cour de justice.

Les questions préjudicielles. La juridiction de renvoi cherchait, pour l'essentiel, à savoir si un traitement médical complexe, mêlant prestations réalisées physiquement dans l'Etat du patient et suivi numérique à distance, pouvait relever de la notion de « télémédecine » au sens de la directive 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers. Elle s'interrogeait, dans un deuxième temps, sur le droit applicable à ces prestations transfrontalières et, dans un troisième, sur l'articulation entre la directive de 2011, la directive 2000/31 (voir *infra*) et la directive 2005/36 (voir *infra*).

Réponses de la Cour de justice. La télémédecine est ainsi « *une notion autonome* » du droit de l'Union, désignant « *exclusivement* » des soins de santé fournis à distance, sans présence physique simultanée du patient et du prestataire, « *au moyen des technologies de l'information et de la communication* » (« TIC »). La Cour précise également qu'un traitement médical complexe peut comprendre des prestations de soins de santé soumises à des régimes juridiques distincts. Enfin, elle en déduit que les prestations de télémédecine doivent être soumises à la législation de l'Etat membre dans lequel le prestataire est établi.

Problématisation et problématique. La Cour de justice se trouve confrontée aux difficultés engendrées par la dématérialisation croissante des prestations de soins de santé au sein du marché intérieur. Le développement de traitements médicaux complexes mêlant prestations numériques et actes réalisés physiquement, remet en cause les critères de rattachement des soins. Et ce, en mettant en tension la libre prestation de services (art. 56 du Traité sur le fonctionnement de l'Union européenne (ci-après « TFUE »), la sécurité des patients et les compétences conservées par les Etats membres en matière d'organisation des systèmes de santé (art. 168, paragraphe 7 du TFUE). Dès lors, la Cour de justice construit, à travers la notion de télémédecine (**I**), un régime autonome applicable aux prestations de soins de santé transfrontalières de télémédecine (**II**).

I. LA CONSTRUCTION PRÉTORIENNE D'UNE CONCEPTION AUTONOME DU DROIT DE L'UNION DE LA TÉLÉMÉDECINE

Une définition autonome. La directive 2011/24/UE ne contient aucune définition explicite de la notion de « télémédecine » et n'opère aucun renvoi au droit des Etats membres pour en déterminer le contenu. La Cour de justice en conclut que le terme « télémédecine » doit recevoir une interprétation uniforme, constituant une « *notion autonome du droit de l'Union* » (§ 62). Dès lors, cette dernière doit être interprétée « *conformément à son sens habituel en langage courant* » et « *du contexte dans lequel [elle] est utilisé[e] et des objectifs poursuivis par la réglementation dont [elle] fait partie* ». Ce considérant méthodologique structure l'ensemble du raisonnement de la Cour de justice, laquelle mobilise successivement les interprétations littérale, contextuelle, téléologique puis historique afin de dégager une véritable conception de la télémédecine dans le droit de l'Union.

Interprétation littérale. Cette interprétation souligne que « *le sens habituel du terme « télémédecine » par son étymologie même, fait référence à des prestations de médecine qui sont fournies à distance* » (§ 63). La Cour rattache cette approche linguistique au libellé de l'article 3, sous d) et e) de la directive 2011/24, dont il ressort qu'un soin dispensé dans le cadre de la télémédecine ne peut relever des « *soins transfrontaliers* » qu'à la condition d'être fourni « *dans un État membre autre que l'État membre d'affiliation* ». La télémédecine apparaît ainsi intrinsèquement liée à la logique de circulation transfrontalière des soins au sein du marché intérieur.

Interprétation contextuelle (§64 à 81). La Cour oppose d'abord la règle générale posée par l'article 3, sous d), première phrase, de la directive selon laquelle « *l' État membre de traitement est celui sur le territoire duquel les soins de santé sont effectivement dispensés* » (§ 64), à l'exception propre à la télémédecine (lieu d'établissement du prestataire), laquelle doit être interprétée strictement afin que « *les règles générales ne soient pas vidées de leur substance* » (§65). De toute évidence, la Cour veille à préserver le principe de rattachement territorial des soins, la télémédecine n'apparaissant que comme une exception fonctionnelle justifiée par les spécificités techniques des « *technologies de l'information et de la communication* » (TIC). Ainsi, « *l'État membre de traitement pour des soins autres que ceux relevant de la télémédecine doit être déterminé sur le fondement du territoire où ces soins sont effectivement dispensés* » (§ 66).

Traitement médical complexe. A partir de la définition des « soins de santé » englobant les services fournis par des professionnels de santé afin « *d'évaluer, maintenir ou rétablir* » l'état de santé des patients (§ 67), la Cour souligne qu'un traitement médical peut comprendre « *une large variété de services de santé* », certains pouvant être réalisés dans différents *États*

membres et par différents professionnels (§ 68). Donc, même lorsqu'un acte réalisé par télémédecine fait partie d'un traitement médical complexe comprenant des soins réalisés physiquement dans l'Etat d'affiliation du patient, un acte effectué par télémédecine peut être considéré, à lui seul, comme un soin de santé transfrontalier et être soumis à des règles juridiques spécifiques (§ 69).

Service de la société de l'information (art. 2 directive 2000/31 et art. 1er, paragraphe premier 1, sous b), directive 2015/1535). La Cour précise que seuls les services de santé effectivement fournis « *à distance* », sans présence physique simultanée du patient et du prestataire, peuvent relever de la télémédecine et, plus largement, des « *services de la société de l'information* » (§ 71 à 74). A l'inverse, les soins réalisés en présence du patient, « *même s'ils impliquent l'utilisation de dispositifs électroniques* », sont exclus de cette qualification (§ 72). Toutefois, la Cour refuse assimiler le traitement médical complexe à un « *service global unique* » au sens de la jurisprudence relative aux plateformes numériques (§ 75 à 77). Par conséquent, chaque acte conserve son autonomie juridique en raison des « *compétences professionnelles spécifiques* » et des « *exigences techniques* » qui lui sont propres (§ 78). Appliquant ce raisonnement au cas en l'espèce, la Cour considère que les actes accomplis physiquement en Autriche par UJ et les prestations réalisées à distance depuis l'Allemagne seront appréciés distinctement, bien qu'ils participent à un seul « *traitement orthodontique* » (§79 à 81).

Interprétation téléologique. La Cour justifie le régime dérogatoire applicable à la télémédecine par « *la nature et [les] spécificités* » de cette pratique (§ 84). Soumettre alors un médecin, exerçant dans l'Etat où il est établi, aux règles applicables dans tous les Etats où se trouveraient ses patients, « *porterait atteinte à la compétence de l'Etat de traitement pour organiser ses soins de santé et exposerait les médecins et les patients à une insécurité juridique* » (§83 à 86 ; v. aussi l'article 168, paragraphes 1 et 7 du Traité sur le fonctionnement de l'Union européenne – TFUE).

Interprétation historique. La Cour rappelle la définition de la télémédecine de la Commission (COM (2008) 689 final) comme la « *fourniture à distance de services de soins de santé* » au moyen des TIC, « *dans des situations où le professionnel de la santé et le patient [...] ne se trouvent pas physiquement au même endroit* » impliquant « *la transmission en toute sécurité de données et d'informations médicales* » (§ 87). Cette conception a ensuite été reprise dans la proposition de directive de 2008 (COM (2008) 414 final) relative à l'application des droits des patients en matière de soins de santé transfrontaliers, laquelle qualifiait notamment de « télémédecine » « *la fourniture d'un service depuis le territoire d'un État membre vers le territoire d'un autre État membre* » (§ 88), distinctement des soins reçus à l'étranger, de l'installation permanente ou de la présence temporaire du praticien.

Par conséquent, la Cour conclut sur l'interprétation de la notion de soins de santé transfrontaliers dispensés dans le cas de la télémédecine que celle-ci est caractérisée par « une prestation d'un service de santé dispensé à un patient par un prestataire de soins de santé établi dans un Etat membre autre que l'Etat membre d'affiliation ~~de ce patient~~, à distance et donc sans la présence physique simultanée au même endroit de ce patient et de ce prestataire, au moyen des technologies de l'information et de la communication » (§90).

II. L'ENCADREMENT JURIDIQUE DE LA TÉLÉMÉDECINE ENTRE LIBRE PRESTATION DE SERVICES ET COMPÉTENCES NATIONALES EN SANTÉ

A. Sur le rapport avec la directive 2000/31 relative aux services de la société de l'information.

Le champ d'application de la directive 2011/24/UE. La directive 2011/24/UE (art. 1er et considérant 10) vise à « *faciliter l'accès à des soins de santé transfrontaliers sûrs et de qualité élevée* », à « *garantir la mobilité des patients* » et à « *promouvoir la coopération en matière de soins de santé entre les États membre* » (§ 95). La Cour souligne que cette directive « *ne se limite pas à édicter des règles en matière de remboursement des coûts des soins de santé transfrontaliers* » (§ 96). En effet, outre les règles relatives au remboursement des soins (§ 97), celle-ci comporte également, pour l'essentiel, des dispositions relatives à la *qualité*, à *la sécurité des soins* et à la *coopération en matière de soins de santé* (§ 97 et 98). La Cour en déduit ainsi que le « *champ d'application de la directive 2011/24 [...] ne se limit[e] pas au remboursement des coûts des soins de santé transfrontaliers* » (§ 99).

Application du droit de l'État membre de traitement. La Cour rappelle que les soins de santé transfrontaliers doivent être dispensés conformément « *à la législation de l'Etat membre de traitement* » ainsi qu'aux « *normes et orientations en matière de qualité et de sécurité* » établies par celui-ci (§ 100). Il en résulte que, en dehors des normes de sécurité fixées par le droit de l'Union, seules les règles de l'Etat membre de traitement ont vocation à s'appliquer (§ 101). Par conséquent, les soins relevant de la télémédecine, étant réputés dispensés dans l'Etat où le prestataire est établi, doivent respecter la législation ainsi que les exigences de qualité et de sécurité de cet Etat membre (§ 102).

Service de la société de l'information. La Cour rappelle que l'application de la directive 2011/24 s'effectue « *sans préjudice* » de la directive 2000/31 relative aux services de la société de l'information (§ 103). De fait, dès lors qu'une prestation de télémédecine peut relever de cette qualification, elle entre également dans le champ d'application de la directive 2000/31. L'article 3 de cette dernière prévoit que les services de la société de l'information doivent respecter les dispositions nationales applicables dans l'Etat membre où le prestataire est établi (§ 104), notamment les « *qualifications ou autorisations* » nécessaires à l'exercice de cette activité (§ 105). Tant la directive 2011/24 que la directive 2000/31 conduisent à appliquer à la télémédecine la législation de l'Etat membre d'établissement du prestataire (§ 106).

B. Sur le rapport avec la directive 2005/36 relative à la reconnaissance des qualifications professionnelles.

L'absence de déplacement dans le cadre de la télémédecine. L'article 5 de la directive 2005/36 ne s'applique qu'en cas de « *déplacement du prestataire vers le territoire de l'Etat membre d'accueil* ». Or, la télémédecine implique précisément qu'aucun déplacement physique n'ait lieu, le service de santé étant fourni « *à distance* » exclusivement au moyen des TIC. Dès lors, la prestation de soins de santé par télémédecine s'effectue sans déplacement du patient ni du prestataire, la Cour relevant ainsi que « *c'est le service de santé qui, en raison de son caractère transfrontalier, « se déplace »* » (§ 111).

L'impossibilité de caractériser un déplacement indirect du prestataire. La Cour écarte l'idée selon laquelle un prestataire établi dans un Etat membre pourrait être regardé comme s'étant déplacé dans un autre Etat membre, du seul fait qu'il y fait réaliser des soins en présentiel par un professionnel lié contractuellement à lui (§ 112). Elle rappelle qu'un « prestataire de soins de santé » est toute entité dispensant légalement des soins sur le territoire d'un État membre (§ 113). Or, *DZK Deutsche Zahnklinik* ne pouvant légalement exercer en Autriche, celle-ci ne saurait être considérée comme le prestataire des soins réalisés physiquement dans cet Etat (§ 114). A l'inverse, UJ, habilitée à exercer

légalement la profession de médecin-dentiste en Autriche, doit être regardée comme le prestataire des soins concernés, indépendamment de l'existence d'un contrat liant ce professionnel et une entité établie dans un autre Etat membre (§ 115). La Cour considère alors qu'il serait « *artificiel* » de considérer que des soins dispensés physiquement en Autriche, l'auraient en réalité été par une société établie en Allemagne (§ 116). Enfin, *« la circonstance que le prestataire exerçant dans l'État membre de résidence du patient ait pu agir au nom du professionnel de santé établi dans un autre État membre ne permet pas de considérer que ce dernier se soit, pour cette seule raison, déplacé dans le premier État membre* » (§ 117).

La Cour conclut donc à l'inapplication de l'article 5 de la directive 2005/36.

CJUE, 11 septembre 2025, *Österreichische Zahnärztekamme*, aff. C-115/24, ECLI:EU:C:2025:694.

Droit français

REGARDS CROISÉS

CE, 10ème et 9ème chambres réunies, 15 octobre 2025, n° 490409, ECLI:FR:CECHR:2025:490409.2025101.

Accès au dossier médical partagé : *« pas sans le consentement initial du patient »* nous dit le Conseil d'État

par Joud GHARZEDDINE

Étudiante en Master 2 Droit des Libertés et titulaire du Master 2 Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

La décision n° 490409 rendue par le Conseil d'État le 15 octobre 2025 porte sur l'équilibre, souvent délicat, qu'il convient d'établir entre l'efficacité et la fluidité de la prise en charge d'un patient et la protection de ses données personnelles. Il s'agissait en l'espèce de savoir si des membres de l'équipe de soins du patient pouvaient accéder et alimenter son dossier médical partagé, alors même qu'ils ne relèvent pas de la catégorie des professionnels de santé.

Saisi par le Conseil national de l'Ordre des médecins, le Conseil d'État avait à statuer sur la légalité de l'arrêté du 26 octobre 2023 du ministre de la santé et de la prévention. Cet arrêté, pris en application de l'article R. 1111-46 du code de la santé publique[341], fixe les règles de gestion des droits d'accès des professionnels, mentionnés à l'article L. 1111-15 et au III de l'article L. 1111-17 de ce même code, au dossier médical partagé du patient. Figure donc en annexe de l'arrêté attaqué une matrice d'habilitation qui définit les droits d'accès aux documents contenus dans ledit dossier médical, en fonction de la catégorie dont relève le professionnel (de santé, du social ou du médico-social).

[341] Cet article dispose que *« L'accès au dossier médical partagé des professionnels mentionnés à l'article L. 1111-15 et au III de l'article L. 1111-17 ainsi que des établissements de santé, établissements ou services sociaux ou médico-sociaux est subordonné au consentement préalable du titulaire selon les modalités prévues aux alinéas suivants. […] Ces professionnels ont accès aux seules données strictement nécessaires à la prise en charge du titulaire du dossier médical partagé dans le respect des règles de gestion des droits d'accès fixées par un arrêté du ministre chargé de la santé, pris après avis de la Caisse nationale de l'assurance maladie, des conseils nationaux des ordres des professionnels de santé, de l'Union nationale des associations agréées d'usagers du système de santé mentionnée à l'article L. 1114-6 et de la Commission nationale de l'informatique et des libertés. »* Nous soulignons.

Plusieurs moyens, ayant trait à la légalité externe comme interne de l'arrêté, sont soulevés par le Conseil national de l'Ordre des médecins. Le premier, portant sur la procédure d'adoption de l'arrêté, est aisément écarté par le Conseil d'État. Cette procédure prévoit que le projet d'arrêté soit soumis à l'avis de divers organismes[342]. Toutefois, une modification ultérieure du projet soumis ne se traduit pas *ipso facto* par l'obligation de procéder à une nouvelle consultation de ces derniers. Le Conseil d'État précise en effet que seule la survenance de questions nouvelles du fait de cette modification est de nature à faire renaitre cette obligation.

Les moyens tirés de la légalité interne font l'objet de développements plus importants qui exigent qu'il soit rappelé, préalablement à leur examen, qu'ils se sont accompagnés d'une demande distincte, d'ordre procédural. Le Conseil national de l'Ordre des médecins avait demandé que soit transmise au Conseil constitutionnel une question prioritaire de constitutionnalité portant sur le paragraphe III de l'article L. 1111-17 du code de la santé publique. Il estimait que ces dispositions portaient atteinte au droit au respect de la vie privée car elles autorisaient tout professionnel participant à la prise en charge d'un patient – nonobstant sa non-appartenance à la catégorie des professionnels de santé – d'accéder à son dossier médical partagé, sous réserve de son consentement[343]. Par une décision du 12 septembre 2024, le Conseil constitutionnel a déclaré cette disposition conforme à la Constitution, estimant qu'elle visait à améliorer la coordination des soins du patient et donc à permettre la poursuite de l'objectif de valeur constitutionnelle de protection de la santé[344]. Ainsi, le consentement donné par le patient pour l'accès à son dossier médical partagé vaut pour l'ensemble de l'équipe des soins.

Se fondant sur cette décision, le juge administratif suprême écarte tout naturellement le moyen tiré de la méconnaissance de la Constitution, validant à son tour l'accès de tous les professionnels concourant effectivement à la prise en charge du patient à son dossier médical partagé. Le Conseil d'État ne nie pas pour autant que la matrice d'habilitation accorde, à l'ensemble desdits professionnels, un *« droit d'accès par défaut »* aux données de santé du patient. Il précise simplement que *« par défaut »* ne signifie pas *« absolu et inconditionné ».* La matrice d'habilitation ne décharge pas ces professionnels de leur obligation d'accéder aux *« seules données strictement nécessaires à la prise en charge du patient »*. En effet, et tel que l'a relevé le Conseil constitutionnel dans la décision précitée, le non-respect de cette obligation peut conduire à l'application des sanctions prévues aux articles L. 1110-4 paragraphe V du code de la santé publique[345] et 226-13 du code pénal[346]. Des considérations

[342] Il s'agit de Caisse nationale de l'assurance maladie, des conseils nationaux des ordres des professionnels de santé, de l'Union nationale des associations agréées d'usagers du système de santé et de la Commission nationale de l'informatique et des libertés.

[343] Le consentement du patient doit être libre et éclairé. Un consentement est libre lorsqu'il est donné sans contrainte et lorsque le patient est en état de l'exprimer. Un consentement est éclairé lorsqu'il est donné à la suite d'une information loyale, claire et adaptée à la capacité de compréhension du patient. De surcroît, il doit être donné *avant* l'ouverture de l'accès au dossier médical partagé, raison pour laquelle nous l'avons qualifié dans la suite de nos propos de consentement *initial.*

[344] Cons. constit, 12 septembre 2024, décision n° 2024-1101 QPC. Cette décision a fait l'objet d'un commentaire dans la deuxième édition de ce Bulletin. Joud Gharzeddine, « Modalités d'accès au dossier médical partagé d'un patient par des professionnels « hors santé » participant à sa prise en charge : une affirmation non équivoque de constitutionnalité », *Bulletin de l'EDiHL*, p. 108.

[345] Conformément à cet article, *« le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende. ».*

[346] Aux termes de cet article, *« la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission*

similaires, se rapportant au principe de minimisation des données, sont mobilisées par le Conseil d'État pour attester de la conformité de l'arrêté attaqué à l'article 8 de la Convention européenne des droits de l'homme et au règlement général sur la protection des données[347].

Toutefois, si cette habilitation collective est validée par le Conseil d'État, l'absence de mention explicite quant à la nécessité de recueillir le consentement initial du patient ne saurait l'être. Cette condition, énoncée à l'article L. 1111-17 du code de la santé publique et rappelée à l'article R. 1111-46 du même code, constitue la pierre angulaire du dispositif tout entier. Elle permet au patient de décider de l'avenir de ses données de santé et de considérer que le droit au respect de sa vie privée et du secret des informations le concernant[348] ait véritablement été respecté. L'omission de la nécessité de recueillir le consentement initial du patient amène le Conseil d'État à considérer que l'arrêté attaqué est entaché d'une erreur de droit, ce qui conduit à son annulation partielle.

Commentaire sous la décision n° 490409 du 15 octobre 2025 du Conseil d'État

par Philippine NEGRAULT

Étudiante en Master 1 Droit du numérique – parcours IA, École de droit de Toulouse, Université Toulouse Capitole

« L'exercice individuel et isolé de la médecine est révolu », ce constat dressé par Laura ESCUDIER[349], dans son commentaire de la décision du 12 septembre 2024[350], illustre la transformation profonde qu'a connue la relation de soin en France. Là où le colloque singulier entre le médecin et son patient constituait le paradigme traditionnel de la pratique médicale, la prise en charge contemporaine mobilise désormais une pluralité de professionnels issus de champs disciplinaires pluriels coopérant autour d'un même patient. Afin d'accompagner cette mutation, le législateur a progressivement structuré le dossier médical partagé (DMP), institué par la loi du 13 août 2004 relative à l'assurance maladie, puis profondément réformé par la loi du 26 janvier 2016. La loi du 24 juillet 2019[351] a ensuite intégré ce dispositif au sein de l'espace numérique de santé, contribuant à élargir son usage et son accessibilité, notamment au profit des professionnels intervenant dans la prise en charge médico-sociale, dans des conditions précisées par les textes réglementaires et le code de la santé publique.

L'arrêté du 26 octobre 2023 du ministre de la santé et de la prévention, pris sur le fondement de l'article R. 1111-46 du code de la santé publique, fixe les règles de gestion des droits d'accès au dossier médical partagé des professionnels mentionnés aux articles L. 1111-15 et L. 1111-17 III du même code. En application de ces

temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. ».

[347] Règlement (UE) 2016/679 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

[348] Conformément à cet article, *« Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant.».*

[349] Jurisprudence du Conseil Constitutionnel, Laura ESCUDIER, pages 229 à 245 (disponible sur Cairn).

[350] Décision n° 2024-1101 QPC.

[351] Loi n° 2019-774.

dispositions, tout professionnel participant à la prise en charge d'une personne peut, sous réserve du consentement de celle-ci préalablement informée, accéder au DMP et l'alimenter, tandis que lorsque ce professionnel est membre d'une équipe de soins au sens de l'article L. 1110-12 du code de la santé publique, cet accès est réputé autorisé à l'ensemble des membres de cette équipe. L'arrêté comporte en annexe une matrice d'habilitation distinguant treize catégories de professionnels de santé selon leurs professions et six catégories de professionnels des secteurs social et médico-social selon leurs fonctions, définissant pour chacune d'elles les droits d'accès à plus de quatre-vingts types de documents composant le DMP. La présentation introductive de cette matrice précise notamment que les droits d'accès sont applicables de plein droit sauf décision contraire du titulaire, et que « les professionnels membres de l'équipe de soins du patient sont réputés autorisés à accéder au DMP du patient préalablement informé et qui n'a pas formulé d'opposition ». C'est l'ensemble de ce dispositif que le Conseil national de l'ordre des médecins a entendu contester, en remettant en cause tant la légalité externe de l'arrêté que sa conformité aux exigences constitutionnelles, conventionnelles et européennes de protection des données personnelles de santé.

Par une requête sommaire enregistrée le 22 décembre 2023 au secrétariat du contentieux du Conseil d'État, complétée par un mémoire le 21 mars 2024 et un mémoire en réplique le 25 février 2025, le Conseil national de l'ordre des médecins a demandé l'annulation pour excès de pouvoir de l'arrêté du 26 octobre 2023 du ministre de la santé et de la prévention fixant les règles de gestion des droits d'accès au dossier médical partagé, pris sur le fondement de l'article R. 1111-46 du code de la santé publique. Il sollicitait également la condamnation de l'État à lui verser la somme de 5000 euros sur le fondement de l'article L.761-1 du code de justice administrative. Entre-temps, le Conseil constitutionnel, par sa décision n° 2024-1101 QPC du 12 septembre 2024, a déclaré conformes à la Constitution les dispositions du III de l'article L. 1111-17 du code de la santé publique, applicables au litige.

Le Conseil d'État, statuant en formation des 9e et 10e chambres réunies, a rendu sa décision le 15 octobre 2025.

Le Conseil d'État rejette la requête du Conseil national de l'ordre des médecins pour l'essentiel mais prononce une annulation partielle de l'arrêté du 26 octobre 2023. Il écarte les moyens tirés de l'irrégularité de la procédure consultative, de l'illégalité de l'article R. 1111-46 du code de la santé publique ainsi que de la méconnaissance de l'article 8 de la Convention européenne des droits de l'homme et des principes de protection des données issus du RGPD. En revanche, il juge que la présentation de la matrice d'habilitation annexée à l'arrêté omet de rappeler l'exigence du consentement initial du patient préalablement à l'ouverture de l'accès au dossier médical partagé pour les membres de l'équipe de soins, ce qui constitue une erreur de droit justifiant l'annulation partielle de l'arrêté.

Dans ce contexte il convient de se demander, dans quelle mesure l'arrêté ministériel fixant les règles d'accès au dossier médical partagé concilie-t-il l'impératif de coordination des soins avec les exigences du consentement éclairé du patient et les principes de protection des données de santé ?Si le Conseil d'État valide dans son principe l'élargissement de l'accès au dossier médical partagé à l'ensemble de l'équipe de soins et juge ce dispositif compatible avec les normes européennes de protection des données personnelles de santé (**I**), il prononce néanmoins une annulation partielle de l'arrêté, révélatrice des tensions persistantes entre la régulation numérique nationale et les standards de protection du consentement éclairé du patient (**II**).

I. LA VALIDATION D'UN ACCÈS ELARGI AUX DONNÉES DE SANTÉ AU SERVICE DE LA COORDINATION DES SOINS

Le Conseil d'État valide l'accès du dossier médical à l'ensemble de l'équipe de soins, en écartant les moyens tirés de l'illégalité des dispositions réglementaires applicables (A), ainsi que la compatibilité de cet encadrement avec les exigences des normes européennes de protection des données personnelles de santé (B).

A. La légalité confirmée d'un accès encadré au dossier médical partagé

La décision commentée s'inscrit dans le prolongement de la décision QPC du 12 septembre 2024, par laquelle le Conseil constitutionnel avait déclaré le III de l'article L. 1111-17 du code de la santé publique conforme à la Constitution. En application de cette décision le Conseil d'État écarte, au point 8 de sa décision, le moyen tiré de la méconnaissance des droits et libertés garantis par la Constitution. Ce faisant, il fait application de l'article 62, alinéa 2, de la Constitution, aux termes duquel les décisions du Conseil constitutionnel « s'imposent aux pouvoirs publics et à toutes les autorités administratives et juridictionnelles ». Dans la décision de septembre 2024, le Conseil constitutionnel avait retenu que le législateur, en adoptant ces dispositions, n'a fait que prévoir des modalités particulières de partage d'informations entre professionnels[352], en poursuivant l'objectif à valeur constitutionnelle de la protection de la santé. Cette validation constitutionnelle du principe même de l'élargissement de l'accès au DMP posait le cadre dans lequel le Conseil d'État allait ensuite examiner la légalité de l'arrêté.

Dans la décision commentée d'octobre 2025, le Conseil d'État rejette, au point 9, l'exception d'illégalité de l'article R. 1111-46 du code de la santé publique soulevée par le CNOM. Le Conseil d'État, en application des articles L. 1110-4 et L. 1110-12 du code de la santé publique, précise que dès lors que le patient a donné son consentement à l'ouverture de son DMP, ce consentement « vaut pour l'ensemble des professionnels membres de cette équipe, qu'ils soient professionnels de santé ou non »[353]. Il convient de relever à cet égard que l'équipe de soins est définie par l'article L. 1110-12 du code de la santé publique, auquel renvoie l'article R. 1111-46, comme un ensemble de professionnels participant directement au profit d'un même patient à la réalisation d'actes diagnostiques, thérapeutiques, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, selon l'une des trois modalités d'organisation qu'il énumère. Cette extension du consentement présente une portée particulière dans la mesure où les informations contenues dans le dossier médical partagé constituent des données de santé au sens du droit de l'Union européenne. Le RGPD qualifie les données relatives à la santé de « catégories particulières de données à caractère personnel » au sens de son article 9, dont le traitement est en principe interdit sauf dans les cas limitativement énumérés par le règlement. Cette qualification traduit la sensibilité particulière de ces informations, qui portent sur l'état de santé physique ou mental d'une personne et peuvent révéler des éléments particulièrement intimes de sa vie privée. Le partage de ces données au sein de l'équipe de soins doit dès lors être encadré par des garanties spécifiques destinées à assurer la confidentialité des informations médicales et à concilier la protection de la vie privée du patient avec les nécessités de la prise en charge thérapeutique.

Le point 13 précise la validation de la matrice d'habilitation elle-même en procédant à un contrôle en deux temps. Le

[352] CC, n° 2024-1101 QPC, 12 sept. 2024.

[353] Paragraphe 9 de l'arrêt commenté.

Conseil d'État vérifie d'abord que la matrice ne confère à aucune catégorie professionnelle un accès à des types de documents qui ne lui seraient « jamais nécessaires ». Cette formulation est notable en ce qu'elle retient un critère de possibilité théorique et non de nécessité systématique, laissant ainsi au professionnel le soin d'apprécier quelles données sont strictement nécessaires à la prise en charge du patient. Il relève ensuite que si l'arrêté mentionne que les droits d'accès sont « applicables de plein droit, sauf si le titulaire du dossier médical partagé en décide autrement », cette applicabilité est encadrée par le principe de nécessité issu de l'article L. 1110-4 du code de la santé publique, auquel renvoie le III de l'article L. 1111-17 et que rappelle l'annexe de l'arrêté, selon lequel un professionnel «ne doit accéder effectivement, parmi les types de documents qui lui sont ouverts par la matrice d'habilitation, qu'aux seules données strictement nécessaires à la prise en charge du patient ».

Cette solution appelle une observation sur la portée du secret professionnel, que le CNOM avait précisément mise en cause en soutenant que des professionnels ne relevant pas de la catégorie des professionnels de santé ne seraient pas soumis aux mêmes règles déontologiques. Gérard Cornu défini le secret professionnel comme « une obligation pour les personnes qui ont eu connaissance de faits confidentiels dans l'exercice ou à l'occasion de leurs fonctions, de ne pas les divulguer hors les cas où la loi impose ou autorise la révélation du secret »[354]. Laura ESCUDIER, dans une analyse de la décision QPC du 12 septembre 2024, précise que le respect du secret médical ne saurait être réservé aux seules professions médicales ou ordinales, ce que le droit positif confirme d'ailleurs expressément[355]. Le code de la santé publique confère en effet au patient un droit au respect de sa vie privée et au secret des informations le concernant qui s'impose, selon les termes mêmes de l'article L. 1110-4, « à tous les professionnels intervenant dans le système de santé ». Le droit au respect de la vie privée est protégé par la Constitution au titre des droits de la personnalité. Le droit à la vie privée constitue un « *droits naturels et imprescriptibles de l'Homme* » protégé par La Déclaration des droits de l'homme et du citoyen de 1789[356]. L'article 226-13 du code pénal sanctionne toute violation du secret professionnel, indépendamment de la nature ordinale ou non de la profession concernée. Le Conseil d'État reprend explicitement ce raisonnement au point 13, en rappelant que la méconnaissance du principe de nécessité dans l'accès aux données du DMP « est susceptible de donner lieu à l'application des peines prévues au paragraphe V de l'article L. 1110-4 du code de la santé publique et à l'article 226-13 du code pénal, et, le cas échéant, de sanctions disciplinaires ».

B. Un encadrement de l'accès compatible avec les normes européennes de protection des données personnelles de santé

Le Conseil d'État était également saisi de moyens tirés de la méconnaissance des normes européennes de protection des données personnelles, fondés respectivement sur l'article 8 de la Convention européenne des droits de l'homme (CEDH) et l'article 5 du RGPD. Ces moyens sont écartés au point 14 de la décision.

S'agissant en premier lieu du moyen tiré de la violation de l'article 8 CEDH, il convient de rappeler que cet article garantit à toute personne le droit au respect de sa vie privée tout en admettant, à son second paragraphe, qu'une ingérence par une autorité publique peut intervenir si elle est

[354] « Vocabulaire juridique », Gérard CORNU, 14e édition, p.954.

[355] Jurisprudence du Conseil Constitutionnel, Laura ESCUDIER, pages 229 à 245 (disponible sur Cairn)

[356] Le rattachement du droit au respect de la vie privée à la Déclaration des droits de l'homme et du citoyen a été réaffirmé dans une décision n° 2014-693 DC du 25 mars 2014.

prévue par la loi, qu'elle poursuit un but légitime et respecte le principe de proportionnalité. Le Conseil d'État reconnaît que le dispositif litigieux constitue une ingérence dans le droit au respect de la vie privée au sens de l'article 8 de la Convention européenne des droits de l'homme. Il écarte toutefois le moyen tiré de sa méconnaissance en relevant que cette ingérence est encadrée par des garanties suffisantes, tenant notamment à la limitation de l'accès aux seuls professionnels participant à la prise en charge du patient, au respect des exigences de confidentialité et à l'existence de sanctions pénales en cas de violation du secret médical, prévues par l'article 226-13 du code pénal.

S'agissant, en deuxième lieu, du moyen tiré de la méconnaissance du principe de minimisation des données consacré à l'Article 5 du RGPD, paragraphe 1, sous c), selon lequel les données à caractère personnel doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées », ce principe impliquant ainsi une proportionnalité entre l'étendue des données collectées ou accessibles et l'objectif poursuivi, le Conseil d'État l'écarte en relevant que le dispositif contesté limite l'accès aux seules informations nécessaires à la prise en charge du patient. Les données en cause, entendues comme toute information se rapportant à une personne physique identifiée ou identifiable, présentent en l'espèce un caractère particulièrement sensible dès lors qu'il s'agit de données de santé, lesquelles bénéficient d'une protection renforcée en droit de l'Union.

Le juge souligne que cet encadrement s'inscrit dans la logique du partage d'informations entre professionnels participant à la prise en charge, telle qu'organisée par l'Article L.1110-4 du code de la santé publique, qui subordonne cet accès à une finalité strictement médicale. Sans ériger expressément cette limitation en application directe du principe de minimisation, le Conseil d'État considère ainsi que les garanties prévues sont de nature à assurer la compatibilité du dispositif avec les exigences du RGPD, en ce qu'elles restreignent l'accès aux seules données strictement nécessaires à la finalité de soin.

S'agissant, en dernier lieu, du moyen tiré de la méconnaissance du principe de limitation de la conservation des données, prévu à l'article 5, paragraphe 1, sous e) du RGPD, selon lequel les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités du traitement, le Conseil d'État en écarte l'examen en relevant que les règles relatives à la conservation des données du dossier médical partagé ne sont pas fixées par l'arrêté contesté, mais relèvent d'autres instruments normatifs. Ce faisant, le juge circonscrit son contrôle à l'acte attaqué, conformément à son office en matière de recours pour excès de pouvoir.

Il convient de préciser que la décision commentée s'inscrit dans un contexte normatif européen en évolution, marqué par l'adoption du règlement du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé, publié au Journal officiel de l'Union européenne le 5 mars 2025 et entré en vigueur le 26 mars 2025 (l'entrée en application des dispositions du règlement est toutefois progressive). Ce règlement vise à établir un cadre harmonisé pour l'utilisation et la circulation des données de santé au sein de l'Union européenne. Il consacre notamment une distinction entre l'utilisation primaire des données de santé, correspondant à leur traitement dans le cadre direct de la prise en charge du patient et de la prestation de soins, et l'utilisation secondaire, qui concerne leur réutilisation à des fins de recherche, d'innovation ou de politiques publiques en matière de santé. Dans cette perspective, le régime du dossier médical partagé, qui limite l'accès aux données aux professionnels impliqués dans la prise en charge du patient et le

conditionne au respect du principe de nécessité, s'inscrit conceptuellement dans la logique d'utilisation primaire des données que l'EHDS entend organiser à l'échelle de l'Union européenne.

Si la légalité du dispositif est ainsi globalement confirmée, le Conseil d'État prononce néanmoins une annulation partielle révélatrice d'une tension entre la logique de régulation retenue par le pouvoir réglementaire et les exigences du consentement éclairé du patient.

II. UNE ANNULATION PARTIELLE RÉVÉLATRICE DES TENSIONS PERSISTANTES ENTRE RÉGULATION ET PROTECTION DU CONSENTEMENT ECLAIRÉ DU PATIENT

Le Conseil d'État réalise une annulation partielle fondée sur une erreur de droit tenant à l'omission de l'exigence du consentement initial du patient (**A**) soulignant des tensions entre la logique de régulation retenue par le pouvoir réglementaire et les standards contemporains de protection des données de santé (**B**).

A. L'erreur de droit caractérisée : l'omission de l'exigence du consentement initial préalable à l'ouverture du DMP

Le Conseil d'État prononce une annulation partielle de l'arrêté du 26 octobre 2023, en relevant une erreur de droit tenant à l'omission, dans la présentation de la matrice d'habilitation, de l'exigence du consentement initial du patient. Au point 10 de sa décision le Conseil d'État précise qu'il résulte des dispositions combinées du III de l'article L. 1111-17 et de l'article R. 1111-46 du code de la santé publique que « le premier accès au dossier médical partagé d'un patient, tant par l'équipe de soins qui le prend en charge que par un professionnel non-membre d'une équipe de soins, nécessite le consentement préalable du patient, dûment informé ». Cette affirmation, d'une portée considérable, établit un double niveau du consentement, structurant l'ensemble du régime d'accès au DMP. Le consentement initial du patient constitue la condition *sine qua non* de l'ouverture de l'accès à son dossier, y compris au bénéfice des membres de l'équipe de soins. Ce n'est qu'une fois ce consentement initial positivement recueilli que l'autorisation étendue à l'ensemble des membres de l'équipe, prévue par l'article R. 1111-46 alinéa 2, peut valablement jouer.

Or, le Conseil d'État constate, au point 11, que la présentation introductive de la matrice d'habilitation est rédigée dans les termes suivants « les professionnels membres de l'équipe de soins du patient sont réputés autorisés à accéder au DMP du patient préalablement informé et qui n'a pas formulé d'opposition ». Cette formulation réduit l'exigence du consentement à une simple absence d'opposition du patient, faisant ainsi basculer le régime d'un mécanisme d'*opt-in*, seul conforme aux dispositions législatives applicables, vers un mécanisme d'*opt-out* que ces mêmes dispositions n'autorisent pas. Par ailleurs, elle omet toute mention de l'obligation de recueil d'un consentement initial positif préalablement à l'ouverture de l'accès au DMP à l'ensemble des membres de l'équipe de soins. Le Conseil d'État en tire la conséquence, au point 12, que « l'auteur de l'arrêté a commis une erreur de droit », et prononce l'annulation de l'arrêté dans cette mesure.

La portée de cette annulation mérite d'être précisément mesurée. Le Conseil d'État prononce en effet une annulation limitée à la seule omission constatée, sans remettre en cause ni la matrice d'habilitation elle-même, ni le principe de l'accès élargi aux professionnels des secteurs social et médico-social membres de l'équipe de soins. En omettant de rappeler une exigence pourtant expressément prévue par les dispositions législatives et réglementaires applicables, l'arrêté a introduit une

formulation susceptible de créer une ambiguïté quant aux conditions d'accès au dossier médical partagé. Une telle omission était de nature à altérer la compréhension, par les professionnels concernés, des modalités de mise en œuvre de leurs obligations et des garanties entourant l'accès aux données de santé du patient, au premier rang desquelles figure l'exigence d'un consentement préalable et éclairé à l'ouverture de cet accès.

B. Les enjeux d'une régulation numérique de la santé à l'épreuve des standards de protection des données de santé

La décision commentée, au-delà de sa portée contentieuse immédiate, révèle des tensions structurelles plus profondes entre la logique de régulation retenue par le Conseil d'État et les standards de protection des données de santé.

Dans un premier temps, les évolutions législatives récentes témoignent d'une volonté de renforcer l'effectivité du dossier médical partagé, notamment en encadrant plus strictement les obligations de renseignement de ce dernier. La décision du Conseil Constitutionnel du 30 décembre 2025 relative à la loi de financement de la sécurité sociale pour 2026[357] illustre toutefois certaines limites encadrant l'introduction de mesures relatives au dossier médical partagé. Le Conseil a en effet censuré certaines dispositions de la loi parmi lesquelles figuraient des mesures relatives aux obligations de renseignement du dossier médical partagé et au régime de pénalité associé. Cette censure repose sur la jurisprudence constante relative aux « cavaliers sociaux », ces dispositions étant regardées comme dépourvues d'effet suffisamment direct sur les dépenses ou les recettes de la sécurité sociale.

Dans un second temps, sur le plan des standards de protection des données, la décision commentée soulève une tension entre la logique de garanties correctives a posteriori retenue par le Conseil d'État et l'exigence de protection dès la conception imposée par l'article 25 du RGPD. En validant la matrice d'habilitation et l'accès élargi au DMP pour les membres de l'équipe de soins, le Conseil d'État se fonde, au point 13, sur un ensemble de mécanismes correctifs reconnus au patient : faculté de clore son dossier, de restreindre l'accès à certaines informations ou de modifier la liste des professionnels habilités. À ces prérogatives s'ajoutent les sanctions pénales, comme vu précédemment, prévues à l'article 226-13 du code pénal et au paragraphe V de l'article L. 1110-4 du code de la santé. Cette architecture repose ainsi sur un contrôle exercé a posteriori par le patient sur l'accès à ses données.

Or, aux termes de l'article 25 du RGPD, le responsable de traitement est tenu de mettre en œuvre, dès la conception du traitement et par défaut, des mesures techniques et organisationnelles appropriées assurant la protection des données personnelles relevant des catégories particulières au sens de l'article 9 du même règlement, parmi lesquelles figurent expressément les données de santé. Dans le cadre du DMP, la Caisse nationale de l'assurance maladie est désignée responsable de traitement par l'article R. 1111-41 du code de la santé publique[358], issu du décret du 4 août 2021[359], sans préjudice des responsabilités susceptibles d'incomber, en qualité de co-responsables au sens de l'article 26 du RGPD, aux établissements de santé et professionnels libéraux participant au renseignement du dossier. Ainsi la caisse nationale de l'assurance maladie « s'assure de la conformité du dossier médical partagé à l'article L. 1111-8 du présent code et aux référentiels d'interopérabilité et de sécurité

[357] Décision n° 2025-899 DC du 30 décembre 2025.
[358] « La Caisse nationale de l'assurance maladie est responsable de traitement au sens de l'article 3 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. ».
[359] Décret n° 2021-1047 du 4 août 2021 relatif au dossier médical partagé.

mentionnés à l'article L. 1470-5 »[360]. C'est donc à ces responsables qu'incombent les obligations de privacy by design et de privacy by default.

Le dispositif retenu par l'arrêté, qui organise un accès par défaut à un ensemble étendu de documents du DMP pour les membres de l'équipe de soins, paraît difficilement conciliable avec la logique de protection intégrée dès la conception que promeut l'article 25 du RGPD. En effet, subordonner la protection effective des données à l'exercice d'un droit d'opposition par le patient revient à faire peser sur ce dernier la charge de la protection de ses propres données sensibles, là où le RGPD impose précisément au responsable de traitement d'assurer cette protection par défaut, indépendamment de toute démarche de l'intéressé. Si le Conseil d'État juge ce dispositif légal au regard du droit positif applicable, la conformité entre la logique corrective retenue et l'esprit des exigences de protection consacrées par le règlement peut être questionnée

[360] Article R1111-41 du Code de la santé publique.

Consultation irrégulière de 441 dossiers médicaux : quand le Conseil d'État rappelle l'importance du consentement des patients pour la recherche

par Joud GHARZEDDINE

Étudiante en Master 2 Droit des Libertés et titulaire du Master 2 Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Par sa décision n° 491701 rendue le 4 juillet 2025, le Conseil d'État clarifie la notion *« équipe de soins »*, précisant les professionnels de santé, du social ou du médico-social qui peuvent être considérés comme y relevant. Cette clarification est fondamentale en ce que si le recueil du consentement du patient[361] est obligatoire préalablement à l'ouverture de l'accès à son dossier médical partagé, une fois donné, les informations y figurant sont *« réputées confiées à l'ensemble de l'équipe »*[362].

En l'espèce, le ministre de l'enseignement supérieur et de la recherche et le ministre de la santé et de la prévention – requérants devant le Conseil – demandaient l'annulation de la décision disciplinaire visant M. A., professeur des universités-praticien hospitalier exerçant à l'hôpital Henri Mondor. Ladite décision l'avait en effet déchargée de toute responsabilité et ce, malgré la consultation irrégulière de 441 dossiers médicaux entre le 1er janvier et le 31 août 2020. La juridiction disciplinaire avait considéré que M. A. appartenait à l'équipe de soins, telle que définie par l'article L. 1110-12 du code de la santé publique[363]. Elle se fondait pour se faire sur sa participation *« aux réunions de l'équipe médico-soignante du service de chirurgie cardiaque et au dispositif de permanences et d'astreintes de ce service »* et sa qualité de *« responsable de la recherche »* au sein dudit service. Elle en déduit que les informations disponibles dans les dossiers médicaux consultés étaient réputées confiées à l'*ensemble* de l'équipe de soins et partant, à M. A.

Le Conseil d'État est, quant à lui, d'un tout autre avis. Il lui parait inexact de considérer que M. A. appartenait à l'équipe de soins, en ce qu'il n'avait pas consulté les dossiers médicaux à l'occasion d'une prise en charge *effective* des patients concernés, mais en vue de réaliser une étude sur la morbi-mortalité des patients du service. De surcroît, sa responsabilité en matière de recherche au sein du service ne le dispense pas de l'obligation prévue à l'article L. 1122-1 du code de la santé publique[364], soumettant la conduite de tout protocole de recherche impliquant la consultation des dossiers médicaux de patients au recueil préalable de leur consentement. Ainsi, en estimant que la juridiction disciplinaire a inexactement qualifié les faits de l'espèce, le Conseil d'État apporte une clarification nécessaire quant aux professionnels pouvant être entendus comme relevant effectivement de *« l'équipe de soins »* et ceux qui, n'y appartenant pas, restent soumis à l'obligation de recueillir leur consentement.

CE, 5ème chambre, 04 juillet 2025, n° 491701, ECLI:FR:CECHS:2025:491701.20250704.

[361] Le consentement du patient doit être libre et éclairé. Un consentement est libre lorsqu'il est donné sans contrainte et lorsque le patient est en état de l'exprimer. Un consentement est éclairé lorsqu'il est donné à la suite d'une information loyale, claire et adaptée à la capacité de compréhension du patient.

[362] Cela est précisé au III de l'article L. 1110-4 du code de la santé publique qui dispose que *« Lorsque ces professionnels appartiennent à la même équipe de soins, au sens de l'article L. 1110-12, ils peuvent partager les informations concernant une même personne qui sont strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social. Ces informations sont réputées confiées par la personne à l'ensemble de l'équipe. ».*

[363] Aux termes de cet article, *« l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes (...) ».* Nous soulignons.

[364] Cet article dispose que *« Préalablement à la réalisation d'une recherche impliquant la personne humaine, une information est délivrée à la personne qui y participe par l'investigateur ou par un médecin qui le représente. (...) ».*

En matière de données de santé, le RGPD s'applique tant que le risque concret de réidentification subsiste

par Laure DUGRAVOT

Étudiante en Master 1 Droit du numérique – parcours IA, École de droit de Toulouse, Université Toulouse Capitole

La protection des données de santé revient à préserver, dans une économie du numérique portée par la valorisation massive des données, l'intégrité de la vie privée des personnes, et plus particulièrement la confidentialité de ces données. A ce titre, la doctrine évoque les données comme « l'or noir du numérique ». Les données médicales représentent une matière première pour les acteurs des industries pharmaceutiques, parapharmaceutiques et des études de marché en santé, qui s'organisent pour en extraire des informations statistiques commercialisables.

C'est ce sens que le Conseil d'État a rendu une décision le 13 février 2026.

Le groupe Cegedim a un modèle économique reposant sur la collecte et la valorisation de données provenant des cabinets médicaux et des officines pharmaceutiques. À travers ses filiales, dont la société GERS, le groupe exploitait deux bases de données. Une première base de données dite « Thin », alimentée par les données recueillies auprès des médecins utilisant le logiciel de gestion Crossway édité par Cegedim Santé, et une seconde base dite « Gers Etudes clients », alimentée par des données collectées auprès d'officines pharmaceutiques. Fin mars 2021, la société GERS disposait, dans la base « Thin » de données relatives à 13,4 millions de consultations associées à 4 millions de codes patients et la base « Gers Etudes Clients », quant à elle, d'environ 78 millions d'identifiants de clients pour les 8 500 pharmacies dont elle recueillait les données. À partir de ces données, le groupe a réalisé des études quantitatives et a commercialisé des données statistiques dans le domaine de la santé auprès de clients publics et privés. Les données ainsi collectées étaient pseudonymisées. En ce sens, les données relatives aux patients ne mentionnaient qu'un code patient, substitué au nom, et celles relatives aux acheteurs en pharmacie, qu'un code client. Les sociétés du groupe soutiennent que la pseudonymisation aurait eu pour effet de rendre les données anonymes. Ce faisant, elles contestaient la qualification de données à caractère personnel retenue par la Commission nationale de l'informatique et des libertés (ci-après « CNIL »), et les obligations en découlant, notamment celles imposées par l'article 66 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « LIL »), qui soumet les traitements de données de santé, lorsqu'ils ne recueillent pas le consentement des personnes concernées, à une autorisation préalable de la CNIL ou à la conformité à un référentiel établi par celle-ci.

La CNIL, à l'issue de contrôles engagés portant sur la mise en œuvre de ces deux bases de données, a prononcé, par trois délibérations distinctes, plusieurs amendes administratives au groupe: une amende de 800 000 € à l'encontre de la société GERS par délibération du 28 août 2024, une amende de 200 000 € à l'encontre de la société GERS venant aux droits de la société Santestat par délibération du même jour, et une amende de 800 000 € assortie de la publication nominative de la délibération pendant deux ans à l'encontre de la société Cegedim Santé par délibération du 5 septembre 2024. Ces trois sociétés ont chacune introduit des recours en annulation devant le Conseil d'État, demandant à titre subsidiaire la réformation des délibérations attaquées et le renvoi d'une question préjudicielle à la Cour de justice de l'Union européenne (ci-après « CJUE ») sur

l'interprétation de l'exigence tenant à la mise en œuvre de moyens raisonnables pour écarter le risque de réidentification. Les requêtes, présentant à juger des questions semblables, ont été jointes par le Conseil d'État pour être tranchées par une seule décision.

Ainsi, les juges du quai de l'horloge ont été amenés à se prononcer sur les conditions auxquelles une donnée de santé pseudonymisée peut être regardée comme ayant été rendue anonyme, et partant, soustraite aux obligations du régime de protection spécifique imposée aux acteurs qui exploitent les données des patients.

Par une décision rendue le 13 février 2026, le Conseil d'État considère qu'« une donnée ne peut être considérée comme ayant été rendue anonyme par une pseudonymisation que si le risque d'identification est insignifiant, une telle identification étant irréalisable en pratique, notamment parce qu'elle impliquerait un effort démesuré en termes de temps, de coût et de main d'œuvre ». En se fondant sur les dispositions de l'article 4, §5 du RGPD, telles qu'interprétées par la CJUE dans son arrêt du 7 mars 2024, OC c/ Commission (aff. C-479/22), le Conseil d'État confirme l'appréciation de la CNIL. *In fine*, les données litigieuses, bien que pseudonymisées, n'étaient pas anonymisées, le risque de réidentification étant avéré. Les trois requêtes sont en conséquence rejetées.

Si le Conseil d'État fixe les conditions auxquelles une donnée de santé pseudonymisée peut être regardée comme anonyme (I), cette qualification emporte des conséquences sur le régime applicable aux acteurs de la santé, en confirmant tant les exigences de la gouvernance publique des données de santé que les obligations pesant sur les concepteurs de logiciels médicaux (II).

I. LA QUALIFICATION JURIDIQUE DES DONNÉES DE SANTÉ PSEUDONYMISÉES

La détermination de l'anonymisation des données de santé pseudonymisées est expressément proportionnée à la sensibilité des données de santé (A), dont l'application concrète révèle les vulnérabilités du système de santé face au risque de réidentification (B).

A. La précision des conditions de l'anonymisation des données de santé proportionnées à leur sensibilité

Les données de santé sont une catégorie particulière de données à caractère personnel dont la sensibilité justifie un niveau de protection renforcé. L'article 4, §15 du RGPD définit ces données comme « des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». L'article 9 prévoit que leur traitement est en principe interdit, sauf exceptions. Cette interdiction est l'expression la protection de confidentialité de la relation médicale et la protection de l'intimité corporelle des patients. C'est dans ce contexte que le Conseil d'État fixe le principe de l'anonymisation, en reprenant la formulation de la CJUE dans son arrêt du 7 mars 2024, *OC c/ Commission* (C-479/22). Ainsi, « une donnée ne peut être considérée comme ayant été rendue anonyme par une pseudonymisation que si le risque d'identification est insignifiant, une telle identification étant irréalisable en pratique, notamment parce qu'elle impliquerait un effort démesuré en termes de temps, de coût et de main-d'œuvre ». Le seuil retenu n'est pas celui du risque « faible » ou « résiduel ». En raison de la nature des données de santé, le seuil du risque retenu est « **insignifiant** » c'est-à-dire pratiquement inexistant.

Dans le domaine de la santé, la réidentification d'un patient n'est pas une atteinte neutre à sa vie privée. Celle-ci elle peut entraîner des discriminations à l'assurance, à l'emploi, ou encore une

rupture de confiance dans le système de soins. La Haute Autorité de Santé et le législateur français ont depuis longtemps reconnu, à travers le secret médical prévu par l'article L.1110-4 du code de la santé publique, que la confidentialité des informations médicales est une condition structurelle de la relation de soin elle-même. Un patient qui ne peut pas avoir la certitude que ses données médicales resteront confidentielles peut renoncer à consulter, à déclarer certaines pathologies, ou à adhérer à un traitement. En soumettant les données de santé pseudonymisées à l'exigence d'insignifiance du risque, la logique du secret médical dans l'espace numérique est prolongée.

Le Conseil d'État applique par ailleurs un critère objectif en précisant que « la circonstance que les sociétés ne procèdent elles-mêmes à aucune inférence de données est sans incidence sur l'appréciation des possibilités d'identification ». Ce faisant, il consacre une approche cohérente avec la jurisprudence de la CJUE dans l'affaire *Patrick Breyer* (C-582/14), selon laquelle ce qui importe n'est pas la capacité propre du responsable de traitement à réidentifier mais la possibilité concrète de toute personne d'y parvenir par des moyens raisonnablement accessibles. Les bases de données circulant entre acteurs privés, celles-ci peuvent faire l'objet de cyberattaques ou être recoupées avec des registres publics, indépendamment de la volonté initiale de leur producteur. En refusant de renvoyer une question préjudicielle à la CJUE, le Conseil d'État souligne la position stable du droit européen sur ce point.

B. Le rappel de l'exigence d'une évaluation *in concreto* du risque

Le Conseil d'État, confirmant l'analyse de la CNIL, procède à une évaluation factuelle du risque de réidentification. Les bases de données litigieuses contenaient, au-delà du code pseudonymisant, un ensemble d'informations comme l'âge, le sexe, la catégorie socio-professionnelle, les pathologies, les médicaments prescrits et achetés, les prescriptions et arrêts de travail, les vaccinations, ainsi que des données temporelles précises telles que la date et parfois même l'heure exacte de la visite médicale ou de l'achat en pharmacie. À ces éléments s'ajoutaient des identifiants professionnels des prescripteurs incluant les numéros RPPS et ADELI, librement consultables en ligne. Le Conseil d'État soulève que « la CNIL relève, sans que ce soit sérieusement contesté, que la société GERS collecte les données des prescripteurs, notamment leurs identifiants ADELI et RPPS, qui permettent de connaître l'identité du professionnel de santé par simple recours à un moteur de recherche publiquement accessible en ligne ». Ce constat illustre la manière dont les infrastructures administratives du système de santé français, avec les répertoires professionnels publics, peuvent constituer des vecteurs de réidentification lorsqu'ils sont croisés avec des données pseudonymisées.

Par ailleurs, le Système National des Données de Santé (ci-après « SNDS »), régi par les articles L.1461-1 et suivants du code de la santé publique, constitue une source externe susceptible d'être croisée avec les données pseudonymisées pour en permettre la réidentification. Le SNDS agrège en effet des données issues de l'assurance maladie obligatoire, des hôpitaux et des causes de décès, couvrant l'ensemble de la population. Ces données destinées à permettre des études épidémiologiques et de santé publique, en font également un outil potentiel de réidentification lorsqu'il est mis en perspective avec des bases de données, comme celles en l'espèce.

Le Conseil d'État identifie, au point 11, la notion de rareté des pathologies. Il énonce que « le risque de réidentification est élevé, notamment lorsque les traitements prescrits sont rares ». Les maladies rares, qui concernent moins de cinq personnes sur dix mille selon la définition européenne consacrée par le règlement n°141/2000, présentent par définition un nombre de

profils compatibles extrêmement réduit dans toute base de données, rendent l'identification quasi-certaine par simple croisement. De même, les traitements orphelins prescrits pour ces pathologies constituent des marqueurs d'identification quasi-univoques. Cette réalité transforme la pseudonymisation en protection illusoire pour ces patients alors que ce sont eux que le droit de la santé a le plus impérieusement vocation à protéger. Enfin, la facilité technique de la réidentification, accomplie au moyen d'un simple tableur d'usage courant, démontre que le seuil du risque insignifiant n'était nullement atteint.

II. LES CONSÉQUENCES JURIDIQUES DE LA QUALIFICATION DE DONNÉES PERSONNELLES SUR LE RÉGIME DES TRAITEMENTS DE SANTÉ

La qualification de données à caractère personnel confirme la gouvernance publique des données de santé dont les exigences ne sauraient être contournées par une pseudonymisation insuffisante (A), et précise l'obligation de privacy by design érigée en critère de licéité à la charge des éditeurs de logiciels médicaux (B).

A. L'exigence confirmée de la gouvernance publique des données de santé

La qualification de données à caractère personnel retenue par le Conseil d'État déclenche l'application d'obligations spécifiques au secteur de la santé. In fine, le droit européen des données personnelles et le droit national de la santé publique s'articulent. Le RGPD, à son article 9, interdit en principe le traitement des données de santé et n'en admet la licéité que dans des cas précis. Parmi ces exceptions figure notamment le consentement explicite de la personne concernée. Or, le Conseil d'État constate qu'« il n'est pas contesté que les données figurant dans les bases "Thin" et "Gers Etudes clients" ont été collectées sans que le consentement des personnes concernées soit recueilli ». Cette absence de consentement exclut le fondement de licéité et oblige à se tourner vers les autres dérogations, notamment celles qui visent respectivement les traitements nécessaires à des fins de santé publique et ceux réalisés à des fins de recherche scientifique ou statistique. Ces dérogations sont toutefois subordonnées à des garanties appropriées que les sociétés du groupe Cegedim n'avaient pas mises en place.

De plus, l'article 66 de la loi n°78-17 du 6 janvier 1978, organise un régime d'autorisation applicable aux traitements de données de santé réalisés sans consentement à des fins d'intérêt public. Cet article exige que de tels traitements soient soit conformes à un référentiel établi par la CNIL en concertation avec la plateforme des données de santé, à savoir le Health Data Hub prévu par l'article L.1462-1 du code de la santé publique, soit préalablement autorisés par la CNIL. L'exigence de concertation avec le Health Data Hub démontre la volonté du législateur de soumettre l'accès secondaire aux données de santé à une gouvernance publique institutionnalisée, fondée sur la confiance et la transparence, en réaction aux pratiques commerciales opaques.

L'article 66, §1 de la LIL pose par ailleurs une autre condition. A ce titre, les traitements ne peuvent être mis en œuvre « qu'en considération de la finalité d'intérêt public qu'ils présentent ». Cette exigence signifie que la valorisation commerciale privée de données de santé, fût-ce à destination de clients publics, n'est admissible que si elle s'inscrit dans une finalité d'intérêt public réelle, identifiée et documentée. Les sociétés du groupe Cegedim, qui commercialisaient des études statistiques auprès d'acteurs privés de l'industrie pharmaceutique, n'avaient ni justifié d'une telle finalité ni sollicité l'autorisation correspondante, commettant ainsi un manquement.

Cette solution doit enfin être mise en perspective avec l'Espace Européen des Données de Santé dont le règlement

européen organise à l'échelle de l'Union le cadre d'accès secondaire aux données de santé à des fins de recherche et d'innovation. L'EHDS consacre une logique similaire à celle de l'article 66 de la LIL. L'accès secondaire aux données de santé est admis sous le contrôle d'autorités publiques désignées et dans le respect de garanties strictes pour les patients. L'arrêt du Conseil d'État s'inscrit ainsi dans un mouvement européen cohérent de régulation publique de l'économie de la donnée de santé entendant mettre fin aux pratiques d'extraction commerciale non encadrée que le groupe Cegedim illustrait.

B. La précision de la notion de privacy by design : l'obligation structurelle pesant sur l'éditeur de logiciels médicaux

Dans son arrêt du 13 février 2026, le manquement reproché à la société Cegedim Santé ne porte pas sur le contenu des données collectées. Il est question de l'**architecture technique** du logiciel médical Crossway dont la conception permettait à la société d'accéder à des données auxquelles elle n'était pas habilitée. Les articles L.162-4-3 et R.162-1-10 du code de la sécurité sociale organisent, au bénéfice des médecins, un téléservice dit HRi permettant, avec l'accord du patient, la consultation des données issues des procédures de remboursement de l'assurance maladie. Ce droit de consultation est strictement personnel. Il appartient au médecin dans le cadre de la relation de soin et ne saurait être délégué ni exploité commercialement par un tiers. Or, le logiciel Crossway était conçu de telle sorte que la consultation des données HRi par le médecin entraînait automatiquement leur téléchargement dans le dossier patient informatisé, sans que le médecin puisse techniquement consulter sans télécharger, permettant ainsi à Cegedim Santé de collecter l'ensemble de ces données. L'article R.1111-8-6 du code de la santé publique, cité par le Conseil d'État, encadre les conditions d'hébergement et de traitement des données de santé à caractère personnel, et sa violation vient compléter le tableau des manquements retenus.

Le Conseil d'État valide la qualification retenue par la CNIL. Cette configuration est un manquement à l'article 5, §1, a) du RGPD, qui impose que les données soient traitées « de manière licite, loyale et transparente ». En effet, les données HRi avaient été collectées en méconnaissance des dispositions du code de la sécurité sociale réservant leur accès aux seuls médecins, ce qui suffisait à caractériser l'illicéité du traitement. Mais au-delà, la conception technique d'un logiciel peut constituer la source d'une illicéité structurelle du traitement indépendamment de toute intention frauduleuse.

Ce principe engage directement celui de privacy by design prévu par l'article 25 du RGPD qui impose au responsable de traitement d'intégrer la protection des données dès la conception de ses outils. Dans le secteur médical, un logiciel de gestion médicale traitant quotidiennement les données sensibles de millions de patients, doit respecter les restrictions d'accès aux données provenant des systèmes d'information. Un éditeur qui, conçoit ses produits sans s'assurer que leur fonctionnement normal ne permet pas de collecter des données en dehors du périmètre légalement autorisé, manque à son obligation dont le respect conditionne la licéité même de son activité. Les éditeurs de logiciels médicaux doivent procéder à des audits de conformité de leurs architectures techniques, non seulement au regard du RGPD, mais également au regard du droit national afin de s'assurer que leurs produits n'offrent pas une voie de contournement des restrictions légales d'accès aux données de santé. Le privacy by design devient un critère concret et exigible de licéité.

CE, 10ème-9ème chambres réunies, 13 février 2026, n° 498628,
ECLI:FR:CECHR:2026:498628.20260213.

Commentaire sous l'arrêt du Conseil d'État, *Association Les Licornes célestes et autres c. CNIL*, 20 mars 2026 (n°s 503159 et 504171)

par Chaimae HBA

Étudiante en Master 1 Droit du numérique IA, École de droit de Toulouse, Université Toulouse Capitole

La France porte à travers son Système national des données de santé *(SNDS)* la base médico-administrative la plus complète d'Europe, dont l'exploitation à des fins de recherche soulève d'inévitables questions quant au choix de l'hébergeur et à la protection des données des patients face aux législations extraterritoriales, au premier rang desquelles le CLOUD Act américain[365]. C'est dans ce contexte que le Conseil d'État, par une décision du 20 mars 2026, a été appelé à se prononcer sur la légalité de l'autorisation délivrée par la Commission nationale de l'informatique et des libertés *(CNIL)* à l'Agence européenne des médicaments (EMA) pour traiter des données de santé de dix millions de Français, hébergées par la filiale irlandaise de Microsoft, dans le cadre du projet européen DARWIN EU[366].

En l'espèce, l'Agence européenne des médicaments coordonne le réseau DARWIN EU, infrastructure européenne destinée à exploiter des données de santé réelles pour étudier l'emploi, la sécurité et l'efficacité des médicaments et des vaccins. Pour mener des études épidémiologiques portant sur l'estimation de l'incidence et de la prévalence de pathologies dans la population générale en France, l'EMA a sollicité l'extraction de données issues du SNDS, confiant cette mission au groupement d'intérêt public « Plateforme des données de santé » *(PDS, ou Health Data Hub)*, agissant en qualité de sous-traitant. Ce dernier a lui-même recours à la société Microsoft Ireland Operations Ltd, filiale de droit irlandais de Microsoft Corporation, groupe soumis au droit américain, pour héberger les données sur des serveurs situés en France. La CNIL a, par délibération du 13 février 2025[367], autorisé ces traitements automatisés pour une durée de trois ans.

Deux requêtes distinctes en annulation pour excès de pouvoir sont enregistrées devant le Conseil d'État. La première est présentée par l'association Les Licornes célestes, accompagnée de personnes physiques et soutenue par une intervention de sociétés françaises de cloud souverain et d'associations du logiciel libre. La seconde émane de l'association Interhop, de l'association Constances, du Syndicat de la médecine générale, de la Fédération Sud Santé Sociaux et de la Ligue des droits de l'homme. Le Conseil d'État les joint pour statuer par une seule décision, conformément au principe d'économie de procédure.

Les requérants soulèvent quatre séries de moyens. En premier lieu, ils invoquent une erreur de droit tirée de l'impossibilité pour le sous-traitant de garantir l'absence de transfert de données vers les États-Unis, en méconnaissance de l'article 28 §3 a) du

[365] CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*), loi fédérale américaine adoptée le 23 mars 2018. Elle permet aux autorités judiciaires américaines d'exiger d'un fournisseur de services cloud établi aux États-Unis la communication de données stockées sur ses serveurs, y compris lorsque ceux-ci se trouvent hors du territoire américain.

[366] DARWIN EU (*Data Analysis and Real-World Interrogation Network – European Union*) : réseau piloté par l'Agence européenne des médicaments (EMA) depuis 2022 visant à exploiter des données de santé réelles pour évaluer l'efficacité et la sécurité des médicaments tout au long de leur cycle de vie.

[367] CNIL, délibération n° 2025-014 du 13 février 2025, publiée au Journal officiel le 11 mars 2025.

RGPD[368] et de l'article R. 1461-1 du code de la santé publique[369]. En deuxième lieu, ils soutiennent que la CNIL a méconnu les articles 44 et 46 du RGPD[370] en autorisant des transferts de données techniques d'usage vers les États-Unis sans vérification suffisante des garanties. En troisième lieu, ils excipent de l'illégalité de la décision d'adéquation UE-États-Unis du 10 juillet 2023[371] *(Data Privacy Framework)*, dont ils demandent le renvoi préjudiciel devant la CJUE au regard des articles 7, 8, 47 et 52 de la Charte des droits fondamentaux. En quatrième et dernier lieu, ils soutiennent que la délibération méconnaît l'article 31 de la loi SREN du 21 mai 2024[372] relatif à l'exigence de certification SecNumCloud pour les administrations recourant à l'informatique en nuage.

Dès lors, le nœud du litige était de déterminer si l'autorisation délivrée par la CNIL permettant à l'EMA de traiter des données de santé du SNDS hébergées par la filiale irlandaise d'une société soumise au droit américain est légale au regard des exigences du RGPD relatives aux garanties du sous-traitant et à l'encadrement des transferts de données vers des pays tiers, eu égard notamment au risque d'accès extraterritorial fondé sur le CLOUD Act américain.

Le Conseil d'État rejette les requêtes. Il juge, d'une part, que la délibération attaquée n'a pour objet que d'autoriser un traitement de données hébergé sur le territoire français et n'autorise aucun transfert vers les États-Unis, rendant inopérante l'exception d'illégalité de la décision d'adéquation. Il juge, d'autre part, que les données techniques d'usage susceptibles d'être accessibles depuis les États-Unis ne constituent pas des données de santé et sont encadrées par des clauses contractuelles types conformes au RGPD. Il retient enfin que les garanties techniques et organisationnelles déployées *(pseudonymisation, limitation de la durée de conservation, contrôle des risques de réidentification, certification HDS[373])* sont suffisantes au regard des articles 28 et 32 du RGPD[374], et que l'article 31 de la loi SREN était inapplicable en l'absence de décret d'application à la date de la délibération.

Cette décision traduit d'abord une approche pragmatique de l'encadrement du risque extraterritorial par la validation des garanties techniques et juridiques entourant l'hébergement nuage (I), mais révèle dans le même temps les limites structurelles d'une souveraineté numérique sanitaire encore inachevée, à l'heure où le droit européen de l'e-santé s'affirme avec l'EHDS (II).

I. LA VALIDATION PRAGMATIQUE DU RISQUE EXTRATERRITORIAL : UNE CONCILIATION ENTRE IMPÉRATIFS DE RECHERCHE ET

[368] RGPD, art. 28 §3 a) : le sous-traitant « ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ».

[369] Article R. 1461-1 du code de la santé publique : interdit les transferts de données de santé issues du SNDS en dehors du territoire de l'Union européenne.

[370] RGPD, art. 45 : décision d'adéquation adoptée par la Commission européenne ; art. 46 : garanties appropriées en l'absence de décision d'adéquation.

[371] Décision d'exécution n° 2023/1795/UE de la Commission du 10 juillet 2023 constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE-États-Unis (*Data Privacy Framework*), *JOUE* n° L 231 du 20 juillet 2023.

[372] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (SREN), art. 31 : obligation pour les administrations gérant des données sensibles de recourir à des prestataires titulaires de la qualification SecNumCloud délivrée par l'ANSSI.

[373] Article L. 1111-8 du Code de la santé publique : certification « hébergeur de données de santé » (HDS), délivrée après audit régulier par un organisme accrédité par le COFRAC.

[374] RGPD, art. 32 : obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées, comprenant notamment la pseudonymisation, le chiffrement, et la garantie de la disponibilité et de la résilience des systèmes.

PROTECTION DES DONNÉES

La décision du Conseil d'État s'inscrit dans une longue série de contentieux liés à l'hébergement du Health Data Hub par Microsoft. Elle témoigne d'une méthode de contrôle fondée sur la pondération concrète des risques plutôt que sur une approche absolutiste de la souveraineté numérique. Le juge administratif valide la délibération de la CNIL en distinguant soigneusement, d'une part, l'absence de transfert de données de santé vers les États-Unis (**A**) et, d'autre part, la suffisance des garanties techniques et contractuelles entourant les rares transferts de données non médicales (**B**).

A. L'absence de transfert de données de santé : une délimitation stricte de l'objet de l'autorisation

Le Conseil d'État pose en premier lieu un constat déterminant, qui dessine le périmètre du contrôle juridictionnel. La délibération du 13 février 2025 [375] a pour seul objet d'autoriser un traitement de données de santé hébergées sur des serveurs situés en France. Elle *« n'a pas pour objet et ne saurait avoir pour effet »* d'autoriser un transfert de données vers les États-Unis. Cette qualification est décisive, car elle neutralise l'ensemble des moyens construits sur l'hypothèse d'un tel transfert, qu'il s'agisse de l'exception d'illégalité de la décision d'adéquation UE-États-Unis *(Data Privacy Framework)* ou de la violation de l'article R. 1461-1 du code de la santé publique[376] qui prohibe les transferts de données du SNDS hors de l'Union européenne.

Cette démarche de délimitation stricte de l'objet de l'autorisation est juridiquement rigoureuse. En droit du RGPD, le régime des transferts vers des pays tiers *(articles 44 à 49)* ne s'applique que lorsqu'il y a effectivement communication de données à un destinataire situé hors de l'Union européenne. Dès lors que les données de santé demeurent hébergées sur le territoire français, dans des centres de données localisés en France, les dispositions relatives aux décisions d'adéquation[377] n'ont vocation à s'appliquer ni directement ni par voie d'exception. Le raisonnement du Conseil d'État est ici cohérent avec la lettre du règlement.

On peut néanmoins s'interroger sur la portée réelle de cette délimitation. Comme le Conseil d'État le reconnaît lui-même au considérant 10, le risque d'accès extraterritorial fondé sur les lois américaines, au premier rang desquelles le CLOUD Act, *« ne peut être totalement exclu »*. Cette reconnaissance implicite de l'imperfection structurelle du dispositif est significative. Elle traduit la tension inhérente à la désignation d'un hébergeur soumis à un ordre juridique extraterritorial, tension que le RGPD lui-même identifie à son article 48 sans y apporter de solution universelle. La CNIL avait d'ailleurs expressément reconnu dans sa propre délibération que *« les données stockées par un hébergeur soumis à un droit extra-européen peuvent être exposées à un risque de communication à des puissances étrangères »*. En décidant de valider malgré tout l'autorisation, le juge administratif opère une forme de mise en balance entre l'impératif de protection des données et le

---

[375] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 66 : compétence de la CNIL pour autoriser les traitements de données de santé à des fins de recherche.

[376] CJUE, 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems*, aff. C-311/18 (ECLI:EU:C:2020:559), dit « Schrems II » : invalidation du Privacy Shield, exigence de vérification au cas par cas des garanties offertes par le pays destinataire.

[377] RGPD, art. 48 : « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international […] ».

bénéfice scientifique et public du projet DARWIN EU.

B. La suffisance des garanties entourant les transferts résiduels de données techniques

Le Conseil d'État reconnaît l'existence de transferts de données vers les États-Unis, mais les cantonne à la catégorie des *« données techniques d'usage de la plateforme »* : informations relatives aux connexions des utilisateurs, sans aucune donnée de santé. Pour ces transferts résiduels, il vérifie que les garanties prévues à l'article 46 du RGPD sont respectées, en l'espèce à travers des clauses contractuelles types (CCT). Ce faisant, il applique la méthode de contrôle *in concreto* imposée par l'arrêt *Schrems II* de la CJUE[378] : les clauses contractuelles ne sont pas suffisantes par elles-mêmes, mais doivent être complétées par une appréciation des circonstances concrètes du cas d'espèce.

S'agissant des données de santé à proprement parler, le Conseil d'État examine avec soin les mesures techniques et organisationnelles au regard des articles 28 §1 et 32 du RGPD[379]. Il recense : la pseudonymisation réalisée sous le contrôle de la Caisse nationale d'assurance maladie et de la PDS, la limitation de la durée de conservation des données brutes extraites du SNDS, l'analyse systématique des risques de réidentification lors de chaque export, et le contrôle des traces d'utilisation par la PDS. Il relève également que Microsoft Ireland, bien qu'incapable d'obtenir la qualification SecNumCloud, réservée aux prestataires non soumis à un droit extra-européen, est titulaire de la certification « hébergeur de données de santé » (HDS) prévue par l'article L. 1111-8 du code de la santé publique[380], impliquant un audit régulier par un organisme accrédité.

Ce raisonnement appelle plusieurs observations critiques. En premier lieu, le juge administratif n'entre pas dans une analyse comparative entre la certification HDS et la qualification SecNumCloud, dont les exigences en matière d'immunité face aux législations extraterritoriales sont pourtant d'une nature différente. La doctrine cloud de l'État[381], confirmée par la circulaire du Premier ministre du 5 février 2026, impose précisément le recours à la qualification SecNumCloud pour les systèmes traitant des données particulièrement sensibles, afin de les *« immuniser contre toute demande d'autorité publique d'États tiers »*. Or le Conseil d'État semble accepter que la certification HDS puisse, en l'espèce et à titre temporaire, se substituer à cette exigence de souveraineté, sans expliciter les raisons juridiques de cette équivalence fonctionnelle. En second lieu, la durée limitée de trois ans de l'autorisation délivrée, sur laquelle le juge insiste, constitue moins une garantie juridique qu'un outil de gestion du risque dans le temps.

Si la décision valide le dispositif mis en place, elle révèle dans le même temps les insuffisances d'un cadre juridique qui peine à concilier les ambitions de la politique européenne des données de santé avec les

---

[378] Circulaire du Premier ministre du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État, complétée par la circulaire du 5 février 2026 : exigence de solutions qualifiées SecNumCloud pour les données sensibles et les systèmes critiques.

[379] CNIL, délibération précitée, point sur la recommandation : « La CNIL ne peut qu'inciter à nouveau le Gouvernement et la Plateforme des données de santé à travailler activement à la mise en place d'une solution souveraine permettant aux organismes d'avoir accès rapidement aux données du SNDS à des fins de recherche scientifique ».

[380] Annonce du gouvernement du 7 février 2026 : la ministre de la Santé Stéphanie Rist a annoncé la migration du Health Data Hub vers un hébergeur qualifié SecNumCloud, avec appel d'offres lancé le 6 mars 2026 ; attribution prévue fin mars 2026.

[381] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 5 mars 2025 relatif à l'espace européen des données de santé (EHDS), JOUE n° L 96 du 5/04/2025 : vise à garantir aux citoyens l'accès à leurs données de santé électroniques dans toute l'Union et à encadrer l'usage secondaire de ces données pour la recherche et l'innovation.

réalités du marché du cloud. C'est cette tension structurelle qu'il convient d'examiner à présent.

II. LES LIMITES STRUCTURELLES D'UNE SOUVERAINETÉ NUMÉRIQUE SANITAIRE INACHEVÉE : L'APPEL À UNE GOUVERNANCE COHÉRENTE DES DONNÉES DE SANTÉ EUROPÉENNES

La décision du Conseil d'État du 20 mars 2026 s'inscrit dans un contexte de transition normative accélérée. Elle intervient alors que la question de l'hébergement souverain du Health Data Hub demeure en suspens depuis la création de la plateforme en 2019, et que le règlement européen sur l'espace européen des données de santé *(EHDS)* vient d'entrer en vigueur. Elle met en lumière tant l'inapplication provisoire de la loi SREN, révélatrice des difficultés de mise en œuvre du principe de souveraineté numérique (A), que la nécessité d'une articulation cohérente entre les ambitions de l'EHDS et les conditions concrètes d'hébergement des données de santé (B).

A. L'inapplication de la loi SREN : les difficultés de la souveraineté numérique comme impératif juridique

Le quatrième moyen soulevé par les requérants était tiré de la méconnaissance de l'article 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique. Cet article fixe les conditions dans lesquelles les administrations peuvent recourir à des services d'informatique en nuage fournis par des prestataires privés pour des systèmes ou applications informatiques. Il impose, pour les données sensibles, le recours à des offres titulaires de la qualification SecNumCloud de l'ANSSI. Le décret d'application, que la loi prévoyait dans un délai de six mois à compter de sa promulgation, n'avait pas été adopté à la date de la délibération du 13 février 2025. Le Conseil d'État en déduit que les dispositions de cet article n'étaient *« pas invocables »* à l'encontre de la délibération contestée.

Ce raisonnement est formellement correct : un texte législatif qui subordonne lui-même son entrée en vigueur à la publication d'un décret d'application ne peut être opposé aux actes pris avant cette publication. Mais il révèle une situation paradoxale. La loi SREN traduit une volonté politique claire d'ériger la souveraineté numérique en exigence juridique contraignante pour les administrations gérant des données sensibles. Le dépassement du délai de six mois prévus par le législateur pour la publication du décret d'application constitue une carence réglementaire qui a pour effet de priver la loi d'effectivité, précisément dans un contexte où les enjeux de souveraineté étaient au cœur du litige. La CNIL avait elle-même, dans sa délibération, formulé une recommandation explicite en faveur d'un hébergeur souverain, soulignant implicitement l'inadéquation du dispositif existant.

Cette tension entre l'impératif normatif et l'impossibilité pratique immédiate illustre l'un des problèmes récurrents de la souveraineté numérique française : l'absence d'équivalent souverain opérationnel pour des besoins aussi spécifiques que ceux du Health Data Hub. La CNIL avait expressément noté l'impossibilité de trouver une solution souveraine *« susceptible de répondre à ses besoins tout en protégeant les données du SNDS contre les accès des autorités publiques d'État tiers »*. C'est cette réalité économique et technique qui a conduit à l'autorisation provisoire sous conditions. Ce n'est qu'en février 2026 que le gouvernement a officiellement décidé de migrer le Health Data Hub vers un hébergeur qualifié SecNumCloud, avec un appel d'offres lancé le 6 mars 2026,

signalant que la décision du Conseil d'État n'épuise pas la question mais la reporte au plan politique.

B. L'avenir de la gouvernance des données de santé : vers une exigence renforcée de souveraineté dans l'espace européen des données de santé (EEDS)

La décision commentée s'inscrit dans un contexte normatif européen en pleine mutation. Le règlement sur l'espace européen des données de santé du 11 février 2025 constitue l'aboutissement d'un projet qui trouve son origine dans la directive 2011/24/UE relative aux soins transfrontaliers, laquelle avait créé le réseau e-santé, posé les jalons de l'interopérabilité des systèmes et amorcé la coopération entre la Commission et les représentants des Etats membres au sein de ce réseau en matière d'e-prescriptions. Le règlement franchit une étape qualitative en imposant des règles communes pour l'utilisation primaire et secondaire des données de santé électroniques à l'échelle de l'Union, avec des obligations de mise à disposition pesant sur les détenteurs de données, et la création de deux infrastructures transfrontalières d'échange *(MyHealth@EU pour les données primaires et HealthData@EU pour les données secondaires).*

Or, ce nouvel espace européen, qui sera mis en oeuvre progressivement soulève des questions de gouvernance directement en lien avec l'affaire DARWIN EU. Le règlement prévoit en effet la désignation, dans chaque État membre, d'un organisme responsable de l'accès aux données de santé *(« HDAB » ou « ORAD »),* chargé notamment de maintenir un environnement de traitement sécurisé. Il impose des règles strictes quant aux finalités de l'usage secondaire des données et aux garanties protégeant les droits des personnes concernées, incluant un droit de refus *(opt out).* En revanche, le règlement ne tranche pas expressément la question de l'hébergeur : il se contente d'exiger un *« environnement de traitement sécurisé »*, laissant aux États membres une marge d'appréciation sur les modalités techniques. Cette lacune risque de reproduire, à l'échelle européenne, les difficultés observées en France avec le Health Data Hub sauf à développer une solution souveraine au niveau européen.

Le projet DARWIN EU[382] lui-même illustre les tensions que l'EHDS sera appelé à résoudre. Une double base juridique a été retenue pour le règlement EHDS, fondé sur les articles 114 et 16 du TFUE. L'article 114 TFUE, relatif au marché intérieur, habilite l'Union à adopter des mesures d'harmonisation des législations nationales ayant pour objet l'établissement et le fonctionnement du marché intérieur tandis que l'article 16 du TFUE constitue, quant à lui, le fondement du droit fondamental à la protection des données à caractère personnel : il dispose que « *toute personne a droit à la protection des données à caractère personnel la concernant* » et habilite le Parlement européen et le Conseil à fixer les règles relatives à ce droit, c'est-à-dire le cadre même du RGPD. L'article 16 TFUE fonde matériellement les dispositions de l'EHDS relatives aux droits des patients sur leurs données. Il est à noter que l'article 168§ 4 c) TFUE relatif aux normes de qualité et de sécurité des dispositifs médicaux n'a pas été retenu comme base juridique de l'EHDS, choix critiqué par une partie de la doctrine eu égard à la dimension qualité des soins du règlement. Le projet DARWIN.EU[383] soulève simultanément des enjeux de marché intérieur des données et des enjeux de protection des données personnelles de santé. Or, ni l'un ni l'autre de ces fondements ne règle la question de la protection des données face aux législations extraterritoriales, qui relève du RGPD et des choix d'hébergement opérés par les États membres et les institutions européennes.

[382] V. site officiel.

[383] https://darwin-eu.org/

Cependant, la décision du Conseil d'État valide un état transitoire sans fixer de critères précis permettant de déterminer à partir de quel seuil les garanties techniques ne sauraient plus suppléer l'absence de souveraineté juridique de l'hébergeur. En reconnaissant que le risque d'accès extraterritorial *« ne peut être totalement exclu »* tout en le jugeant acceptable, le juge administratif s'engage sur un terrain d'appréciation casuistique qui, s'il peut se justifier dans un contexte de transition, ne saurait constituer une doctrine durable de gouvernance des données de santé. L'article 48 du RGPD, qui interdit la reconnaissance de toute injonction de transfert d'une juridiction d'un pays tiers non fondée sur un accord international, demeure une protection formelle dont l'effectivité réelle, en cas de demande fondée sur le CLOUD Act, reste incertaine ainsi que le souligne la doctrine.

En définitive, l'arrêt du 20 mars 2026 apporte une réponse juridique solide aux questions de droit positif, mais laisse en suspens les enjeux de politique publique numérique que la construction de l'EHDS et la migration vers un hébergeur souverain devront collectivement résoudre. Il confirme que le droit de la e-santé européen, ce droit *sui generis* en construction, ne peut se passer d'une architecture de gouvernance des données cohérente, associant exigences juridiques, capacités techniques et souveraineté numérique opérationnelle. La récente annonce de la migration de l'hébergement vers Scaleway, une solution française, fait parfaitement suite à cette succession de polémiques et illustre par ailleurs les recompositions actuellement à l'œuvre en matière de souveraineté numérique et d'hébergement des données de santé : la souveraineté est amenée à devenir un enjeu de premier ordre[384].

CE, Section du contentieux, 10ème chambre, 26 mars 2026, n°s 503159-504171, ECLI:FR:CECHS:2026:503159.20260320.

[384] « Le Health Data Hub choisit l'hébergeur français Scaleway", Léo Caravagna et Marion-Jeanne Lefebvre,Tic Pharma, 24/04/2026

Bulletin de
l'EDiHL
European Digital Health Law

LISTE DES CONTRIBUTEURS

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

Franck AZNAR
Diplomé en biotechnologies, biologie moléculaire et cellulaire
Titulaire du DU EDiHL

Sarah BISTER
Avocate au Barreau de Paris
Docteure en Droit public

Claire BORIES
Docteure en Droit public
Chargée de mission à la Direction de la Sécurité sociale (DSS/DACI)

Thomas BOUDON
Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Maïlys CAPELL
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Maddalena DE CARLO
Etudiante en Master 2 Droit international et comparé, École de droit de Toulouse, Université Toulouse Capitole

Sarah DE HEER
Doctorante en Droit public, Université de Lund (Suède)

Marie DESMEULES
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Winnie DONGBOU WAMBA
Doctorant en Droit public, EDT-R-IRDEIC, Université Toulouse Capitole
Juriste en droit de la protection des données de santé MyData-TRUST

Noémie DUBRUEL
Docteure en Droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier, UMR 1295 Inserm équipe BIOETHICS

Laure DUGRAVOT
Étudiante en Master 1 Droit du numérique – parcours IA, École de droit de Toulouse, Université Toulouse Capitole

Lisa FERIOL
Doctorante CIFRE, Ekitia et Équipe BIOETHICS, CERPOP UMR1295 Inserm et Université Toulouse Paul Sabatier

Alizée FERNANDEZ
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Lili-Marie FERRANDO
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Joud GHARZEDDINE
Étudiante en Master 2 Droit des Libertés et titulaire du Master Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Chaimae HBA
Étudiante en Master 1 Droit du numérique IA, École de droit de Toulouse, Université Toulouse Capitole

Clarance JEAN-PIERRE
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Lukas MARA
Étudiant en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Amina MOUSTOIFA
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Philippine NEGRAULT
Étudiante en Master 1 Droit du numérique – parcours IA, École de droit de Toulouse, Université Toulouse Capitole

Mélanie SOUSA BARBEIRO
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Salaheddine ZAHID
Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Bulletin de l'EDiHL

European Digital Health Law

N° 3

3ème année – Bulletin annuel
Juin 2025 – Juin 2026

Cofinancé par l'Union européenne