École de Guerre Economique

[Année]

L'enjeu stratégique des données de santé françaises

Décembre 2024.

EGE École de Guerre Economique

Table des matières

Partie 1 : L'importance des données de santé au XXIème siècle

A. Santé et données : définition et acteurs

1. La santé, source d'une multitude de données

La quantité de données

Selon une étude de la banque Banque Royale du Canada (BRC)[i], principale banque en termes de capitalisation au Canada, spécialisée dans les études sur la confidentialité des données ; ces données génèrent environ 30 % de toutes les données mondiales.

À titre de comparaison, un seul établissement comme le Grand Hôpital de Charleroi (GHC), stocke aujourd'hui plus de 250 terabits (TB) de données (1 TB = 1 000 gigabits). Il est à noter que ce poids des données de santé a été multiplié par 15 en 7 ans (2013-2020 (voir infographie)), et que ce chiffre ne va cesser de croître, tant les images, et analyses gagnent en précision, mais aussi en poids de traitement. Les recherches de la BRC soulignent d'ailleurs que le poids des données de santé croît à un degré plus rapide que celles d'autres domaines. Elles croissent 6 % plus rapidement que les données manufacturières, 10 % plus vite que les données des services financiers ou encore 11 % plus rapidement que les données médias et divertissement.

Des données très diversifiées et peu définies

Au-delà de leur quantité, ces données sont extrêmement diversifiées. Le premier point fondamental dans l'étude des données de santé et de leur partage est donc de comprendre ce que ces dernières englobent.

En dehors du cadre réglementaire, les données de santé ne sont pas ou peu définies aujourd'hui. Dans la définition sémantique de ces dernières, la CNIL est l'organisme de référence. Elle définit les données de santé comme : « Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, 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. »[ii].

Cette définition de la CNIL est elle-même issue du Règlement Général sur la Protection des Données (RGPD), dans son article 4-15. Cette réglementation précise par ailleurs que ces données s'inscrivent dans trois cadres temporels : le présent, le passé, et le futur.

Il apparaît dès lors que la définition des données de santé est très large, et très peu spécifique. Or, il est primordial avant de pouvoir partager les données de santé, d'être capable de les identifier. Bien que ces données soient très diverses et variées, il semble possible de les classer en neuf catégories qui rassemblent la quasi-totalité de celles-ci (voir tableau).

La définition, le cadrage ainsi que la détection de l'ensemble de ces données de santé est un enjeu majeur, car l'un des freins fondamentaux dans le partage de ces données reste la diversité et la non-identification de ces dernières.

TABLEAU DES PRINCIPALES FAMILLES DE DONNÉES IDENTIFIÉES (NON-EXHAUSTIF)

Type de données	Définition	Exemples
Données administratives	Ces données sont utilisées pour identifier les patients et gérer les aspects administratifs du système de santé.	• Prise de rendez-vous • Remboursements • Numéro de sécurité sociale
Données comportementales	Ces données correspondent aux informations qui décrivent les habitudes, attitudes et comportements d'un individu en lien avec sa santé.	• Exercice quotidien • Nourriture • Tabagisme
Données génétiques et biométriques	Les données génétiques concernent l'information présente dans l'ADN d'un individu. Les données biométriques sont les caractéristiques physiques ou biologiques qui permettent d'identifier une personne ou de mesurer des paramètres de santé.	• Séquençage ADN • Traits du visage
Données mentales	Informations qui concernent l'état psychologique, émotionnel et cognitif d'un individu.	• CR psychiatrique • Diagnostique de trouble • Dossier psychiatrique
Données collectées par les objets connectés	Informations liées à la santé ou aux comportements des individus, enregistrées par des objets connectés (technologies portables, capteurs intégrés, applications numériques de santé).	• Taux d'oxygène dans le sang • Cycle du sommeil
Données épidémiologiques de santé publique	Informations collectées dans le cadre de la surveillance, de l'étude et de la compréhension des facteurs qui influencent les épidémies et maladies dans une population.	• Couverture vaccinale • Études sur les facteurs de risque
Données d'études cliniques	Informations collectées et analysées dans le cadre d'enquêtes ou d'études menées par des institutions publiques ou des organismes mandatées pour évaluer l'état de santé d'une population, comprendre les besoins de soins ou orienter les politiques de santé publique.	• Enquêtes nationales de l'INSERM • Etude Institut Pasteur
Données contextuelles et environnementales	Informations sur les conditions extérieures, environnementales ou sociales, qui influencent directement ou indirectement la santé des individus ou des populations.	• Pollution de l'air • Qualité de l'eau potable • Déserts médicaux
Données cliniques	Informations médicales recueillies par le corps médical lors de la prise en charge ou le suivi d'un patient.	• Traitements • Diagnostics • Résultats d'examen

Tableau réalisé par le groupe du QuestIE de l'EGE

L’enjeu économique du partage des données de santé

De plus, identifier les différentes données de santé permet d’estimer leur valeur et donc d’estimer leur possibilité de partage et à quelles conditions (tarifaires, réglementaires, etc).

Selon la Commission européenne, l’usage secondaire des données de santé devrait représenter une valeur en hausse de 70 %, passant d’une valeur de 25 Md€ en 2020 contre 43 Md€ en 2028, dont 7,3 Md€ pour la France.

Le format : principal obstacle à la valorisation des données de santé

Bien que l’enjeu économique soit fort, pour que celui-ci soit effectif, il est nécessaire que, subséquemment à l’identification et à la définition des données de santé ; que leur diversité de formats soit aussi établie et homogénéisée. En effet, malgré l’implémentation de normes telles que la HL7 ou ISO 13606, qui visent à uniformiser les données de santé afin de faciliter leur partage, de nombreux formats existent toujours.

Il est une nouvelle fois difficile de faire un inventaire exhaustif de ces formats, mais trois familles peuvent regrouper une grande partie de ces derniers (voir infographie des données de santé).

Déterminer ces différents formats est un enjeu important dans le partage de ces données, car cette hétérogénéité des formats de données de santé est un second frein au partage de ces dernières. Des données non-homogènes entraînent une augmentation des difficultés à l’interopérabilité de ces données. Cet obstacle à l’interopérabilité est un obstacle à leur partage, ce qui entraîne in fine une utilisation non-efficiente ou tout du moins non-optimale de ces dernières.

Les normes précédemment citées améliorent la situation, mais de nombreux formats de données de santé différenciés continuent à persister.

2. Acteurs traitant des données de santé

Cartographie réalisée par le groupe du QuestIE de l'EGE

Aujourd'hui, l'industrie de la santé est une thématique particulièrement porteuse. Ce marché connait une croissance continue, stimulée à la fois par l'accroissement démographique et le vieillissement de la population mondiale. Selon le cabinet Frost & Sullivan, le volume de données produites chaque année dans ce secteur devrait ainsi être multiplié par dix au cours des cinq prochaines années. Ces données, essentielles au bon fonctionnement du système de santé, sont traitées par une chaîne complexe d'acteurs, chacun ayant des responsabilités distinctes en matière de collecte, de stockage, de partage et d'analyse des données.

Le parcours des données de santé commence bien souvent dans les pharmacies, chez les médecins généralistes et dans les hôpitaux, où elles sont recueillies au

contact direct des patients. Les pharmacies traitent les ordonnances et enregistrent les informations relatives à la délivrance des médicaments grâce à la carte Vitale. Cette carte, en lien avec le système de la Caisse Primaire d'Assurance Maladie (CPAM), permet la transmission immédiate des données nécessaires au remboursement. Les hôpitaux et cliniques, quant à eux, gèrent des bases de données plus complexes, comme les dossiers médicaux partagés (DMP), qui centralisent des informations comme les antécédents, les interventions chirurgicales et les résultats d'examens.

Les institutions publiques vont également jouer un rôle de premier plan dans la gestion et l'exploitation de ces données. La CPAM les collecte pour traiter les remboursements, tandis que la caisse nationale d'assurance maladie (CNAM) les centralise pour réaliser des analyses approfondies sur le fonctionnement du système de santé français. En parallèle, la plateforme Ameli collecte des informations sur les actes médicaux, les traitements et les démarches administratives des assurés, offrant aux patients des procédures simplifiées. Les Agences régionales de santé (ARS) exploitent les données issues des hôpitaux et laboratoires pour surveiller des indicateurs locaux de santé publique, tandis que Santé publique France les mobilise pour évaluer l'état de santé de la population, mener des campagnes de prévention et gérer des crises sanitaires.

Depuis 2019, la Plateforme des Données de Santé (PDS), également connue sous le nom de Health Data Hub, a renforcé l'architecture de gestion des données en France. Cette plateforme met à disposition des bases de données anonymisées aux chercheurs, aux entreprises et aux institutions publiques.

Elle permet ainsi une centralisation et une exploitation à grande échelle des données de santé. Les données sont néanmoins hébergées par Microsoft Azure, une décision qui a fait polémique en raison de la perte de souveraineté, liée notamment au Cloud Act américain,

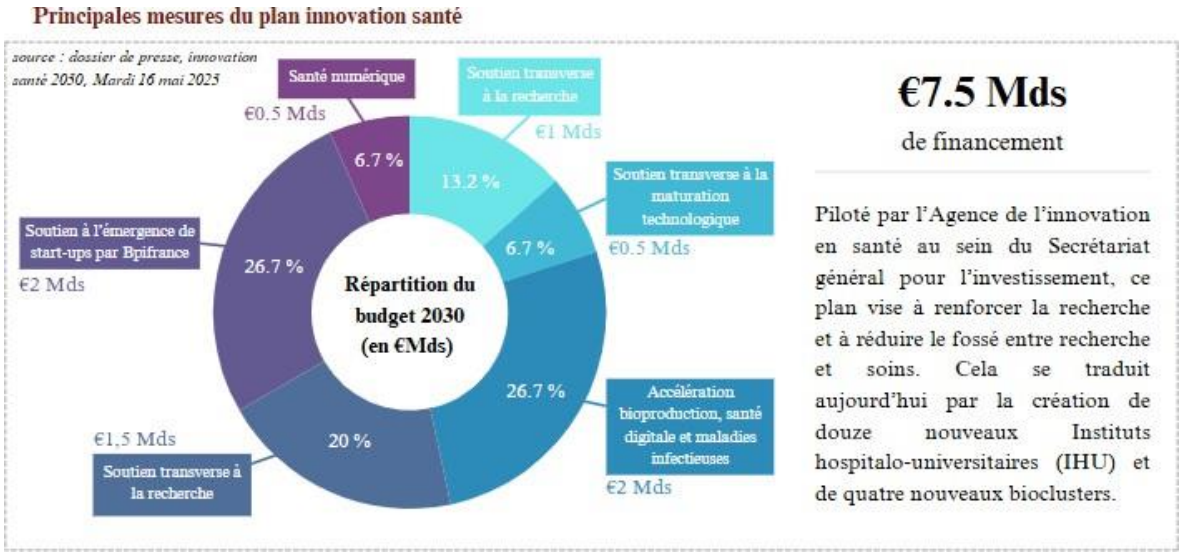
Les laboratoires pharmaceutiques, comme Sanofi et Ipsen, ainsi que les laboratoires d'analyses médicales, tels que Biogroup ou Synlab, jouent également un rôle dans l'utilisation des données de santé. Sanofi et Ipsen, par exemple, s'appuient sur des données issues des essais cliniques pour développer la recherche. Par ailleurs, les laboratoires d'analyses traitent des données biologiques des patients, comme des résultats sanguins ou urinaires, qui sont transmises aux médecins pour guider les soins.

Le numérique a également révolutionné la gestion des données de santé avec la création de plateformes facilitant la prise de rendez-vous ou la consultation en ligne. Des plateformes comme Doctolib ou Qare collectent des informations sur les consultations et les prescriptions. L'ensemble de ces données est ensuite hébergé sur des cloud certifiés HDS. En France, plusieurs acteurs sont certifiés, à l'image d'OVHcloud. Cependant, la certification ne se limite pas aux acteurs nationaux.

Les mutuelles et assurances santé, telles que Groupama, Harmonie Mutuelle et Allianz, participent également au traitement des données en proposant un suivi personnalisé des patients. Selon l'Autorité de contrôle, 96 % des organismes assureurs externalisent des fonctions importantes ou critiques, ce qui leur permet de rationaliser les coûts, mais qui complique la gestion et augmente les risques opérationnels.

Cette cartographie met également en lumière l'apparition d'acteurs étrangers sur le marché français. Les géants technologiques tels que Google Cloud, Microsoft et AWS fournissent des capacités de stockage et de calcul pour les données de santé. Parallèlement, des entreprises comme MyHeritage et TellMeGen, spécialisées dans les tests ADN, collectent des données génétiques, dont une grande partie est envoyée aux États-Unis. Les assureurs étrangers, notamment américains, intègrent eux aussi le marché européen. On assiste donc à une restructuration globale du secteur de la santé de la France, avec des enjeux globaux concernant les données de santé des Français.

3. L'action de France 2030 sur les données de santé



Souveraineté sanitaire : renforcer l'autonomie nationale

La souveraineté dans le domaine de la santé repose sur des initiatives qui permettent à la France de contrôler l'ensemble de la chaîne de valeur, en passant par la recherche jusqu'à l'industrialisation. Le plan prévoit une enveloppe de €1,7 Mds pour la recherche biomédicale, avec une priorité donnée aux bioclusters et aux IHU. Ces infrastructures visent à regrouper les cliniciens, chercheurs, et industriels dans des « pôles d'excellence », favorisant ainsi une recherche intégrée et orientée vers des solutions thérapeutiques locales et indépendantes. Par exemple, le biocluster GenoTher, axé sur les thérapies géniques, a pour mission de rétablir la souveraineté française en matière de production de thérapies avancées en réduisant notamment la dépendance aux infrastructures étrangères.

La souveraineté sanitaire passe également par la modernisation des infrastructures de recherche. À cet effet, €100 M supplémentaires seront investis pour renforcer les infrastructures nationales en biologie et santé. Ces fonds visent à garantir une durabilité optimale des équipements stratégiques tout en s'alignant sur les besoins émergents en matière de santé publique et d'innovation.

Des mesures suffisantes pour positionner la France en leader ?

Les initiatives du plan « France 2030 » pour renforcer la compétitivité et la souveraineté de la France dans le stockage des données de santé sont ambitieuses, mais leur mise en œuvre et leur impact réel soulèvent plusieurs questions. En effet, si la centralisation des données à travers des entrepôts hospitaliers comme ACCES (AP-HP) ou eDOL (CHU de Montpellier) est une avancée significative, notamment en termes d'innovation médicale et de personnalisation des traitements, ces projets, bien qu'interopérables et inclusifs, posent des défis en matière de sécurité des données, notamment vis-à-vis des acteurs technologiques étrangers (comme les fabricants d'équipements) . La souveraineté revendiquée pourrait être compromise si les infrastructures restent dépendantes de solutions matérielles ou logicielles développées à l'étranger.

En somme, si les mesures de France 2030 montrent une vision stratégique pour la santé, les défis liés à la sécurité des données, à la dépendance technologique et à la gouvernance des infrastructures nécessitent une attention constante pour éviter des risques qui pourraient nuire à la souveraineté française.

B. Les mécanismes d'échange et de partage des données de santé

1. Un cas d'utilisation nationale des données de santé : le système national des données de santé (SNDS)

Géré par la Caisse nationale de l'Assurance Maladie (Cnam), le SNDS permet aux utilisateurs d'accéder aux données de santé produites en France selon des modalités adaptées à leur besoin.

Le SNDS pourrait ainsi être considéré comme un modèle français de centralisation et de partage des données de santé, favorisant la mise à disposition de ces dernières, notamment pour stimuler la recherche.

Des modalités d'accès claires et encadrées

Le SNDS est encadré clairement par des conditions d'accessibilité aux données et rattaché au Cnam, un organisme central, qui accompagne les utilisateurs de la plateforme. Cette plateforme encadre ainsi, de manière centralisée, la consultation des données de santé françaises selon 3 besoins clairement identifiés :

- Open data : certaines données agrégées et anonymes sont disponibles pour le grand public
- Accès ponctuel : sur présentation d'un protocole scientifique défini pour travailler sur un projet d'intérêt public, un utilisateur peut demander à consulter les données du SNDS
- Accès permanent : l'Etat, les organismes publics et les organismes chargés d'une mission de service public peuvent consulter les données du SNDS à condition d'être membre d'un organisme habilité et d'avoir fait l'objet d'une habilitation nominative.

En somme, l'accès aux données du SNDS permet différents cas d'usage, maintenant un bon équilibre entre restriction d'accès et ouverture des données.

Une centralisation des multiples données

Le SNDS centralise une grande quantité de données, issues de multiples sources. Ces données proviennent des professionnels de la santé, des hôpitaux, cliniques ou encore laboratoires, et peuvent être utilisées pour produire des analyses privées ou à destination du grand public.

Les données collectées sont de différentes natures, elles concernent des éléments propres aux professionnels de la santé (spécialisation, département du cabinet principal ou secondaire etc.), d'autres propres aux patients (âge, sexe, commune, département de résidence du bénéficiaire) ou encore d'informations issues des infrastructures de soin (hôpitaux, laboratoires, cliniques etc.).

Une incertitude liée à la pseudonymisation des données

Si le SNDS affirme que les données sont systématiquement pseudonymisées et que les données en accès libres sont anonymes, une certaine incertitude demeure à l'égard de ce sujet.

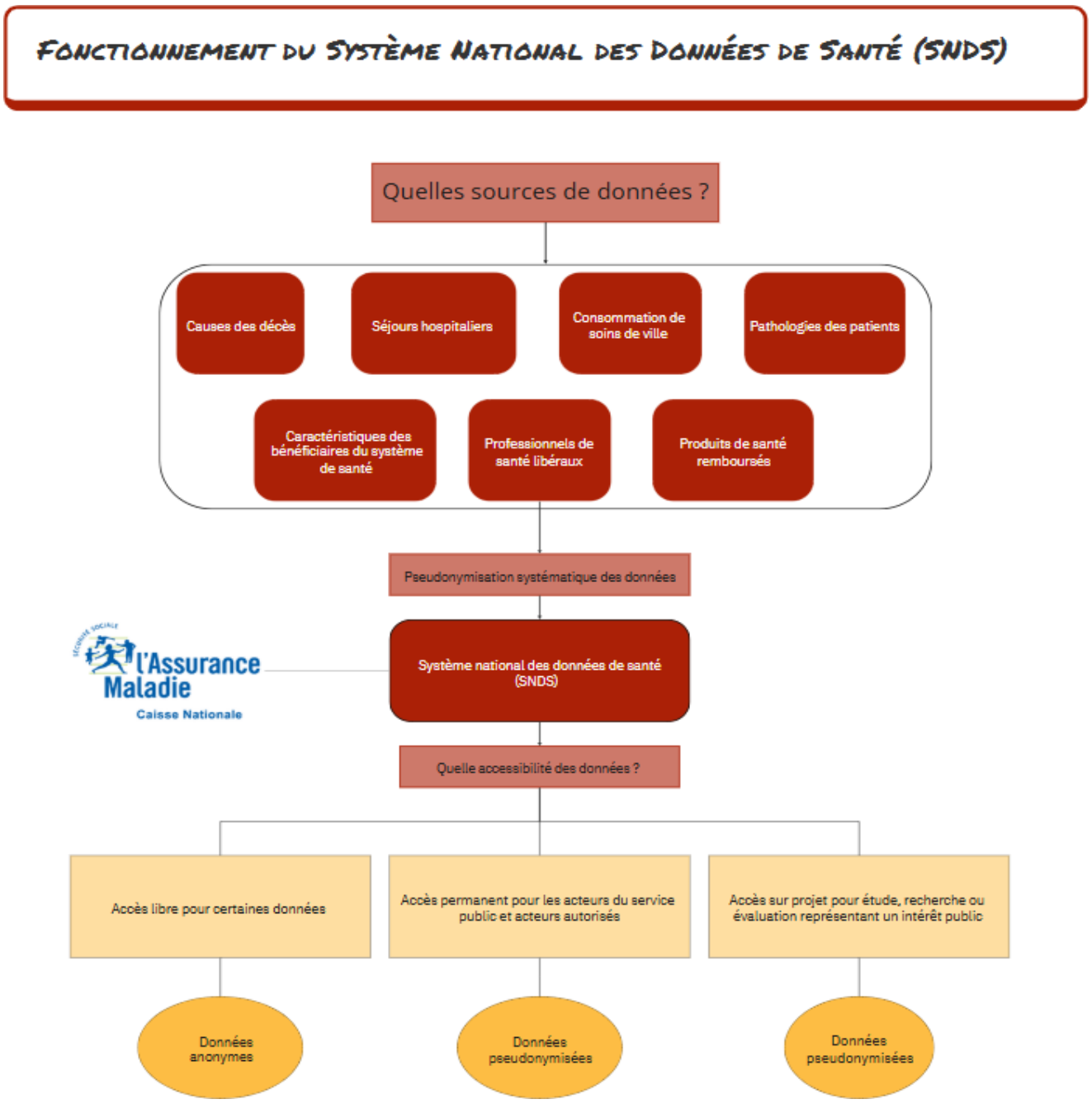
Si l'anonymisation des données permet bien de détacher les données de leur détenteur, elle ne doit pas être confondue avec le principe de pseudonymisation.

La pseudonymisation consiste à attribuer à des données un numéro de rattachement, un identifiant unique ou autre. La donnée, indépendante des autres, ne peut donc donc être rattachée à l'individu concerné. En revanche, la CNIL précise que cette méthode permet à un utilisateur de recouper les données entre elles pour ré-identifier l'individu concernée par les données.

Enfin, la pseudonymisation se distingue également de l'anonymisation par son caractère réversible. Il est donc possible de "dé-pseudonymiser" des données personnelles pour retrouver leur origine.

Ainsi, si le SNDS représente un système clair de centralisation de nombreuses données, il connait une faille en matière d'anonymisation des données. S'il n'existe aucun impératif légal d'anonymiser les données, le RGPD impose des conditions

restrictives pour assurer le respect de la vie privée des individus et pour limiter leur durée de conservation. L'anonymisation n'est qu'une des méthodes qui permettent de répondre aux exigences du RGPD pour exploiter des données personnelles.



2. Transition des données de santé en Europe : Initiatives européennes pour un système de santé interconnecté

La gestion des données de santé actuelle en Europe se présente comme fragmentée, chaque pays disposant de ses propres centres de données nationaux. Actuellement, ces données ne peuvent être partagées entre pays européens seulement si elles sont

envoyées d'un centre de données à un autre, ce qui crée des obstacles en termes d'interopérabilité et de partage transnational de ces informations. Ce manque de fluidité soulève des défis importants pour l'amélioration de la qualité des soins et le développement de politiques de santé cohérentes à l'échelle de l'UE.

La France occupe une place relativement avancée en ce qui concerne le partage de données de santé. En effet, la France lance en 2019 le Health Data Hub, un système de centre de données permettant de croiser les données de santé et de faciliter leur utilisation au niveau national dans des domaines comme la recherche et le développement, tout en respectant la vie privée des usagers du système de santé.

De plus, la France montre l'exemple avec son Health Data Hub et lance cette initiative au niveau européen avec pour objectif la création d'un centre de données de santé européen qui centraliserait l'ensemble des données médicales des citoyens européens et permettrait le transite et l'utilisation de données dans toute l'UE.

Pour répondre à ce besoin, l'Union européenne a lancé le projet *European Health Data Space* (EHDS) en mai 2022. Ce projet, soutenu par un consortium de 21 pays, vise à établir un espace commun pour permettre le partage des données de santé à travers l'Europe. Il met l'accent sur l'exploitation des données secondaire, c'est-à-dire les données de santé avec un autre usage que celui de soigner les patients ; telles que la recherche, l'innovation, ou encore, l'élaboration de politiques publiques. Après deux années de discussions, le projet a été validé par les États membres et le Parlement européen en milieu d'année 2024.

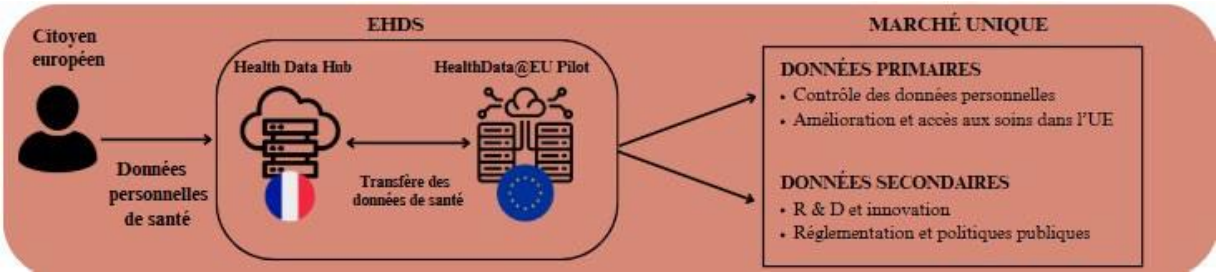
L'un des éléments clé de l'EHDS est la création d'un réseau permettant la centralisation et la circulation des données de santé entre les états membres. Ce besoin a été formalisé à travers l'initiative HealthData@EU Pilot, un projet porté par le programme français *Health Data Hub*. Ce data hub européen servira de base pour la future infrastructure européenne de données de santé. Ce projet bénéficie du co-financement du programme *EU4Health* de la Commission européenne.

L'EHDS prévoit également de placer les citoyens au centre du système de santé, en leur offrant un contrôle total sur leurs données de santé primaires, afin qu'ils puissent bénéficier des meilleurs soins de santé dans tous les pays de l'UE. En parallèle, ce projet ouvre des perspectives pour le développement d'un marché unique des systèmes de dossiers médicaux électroniques.

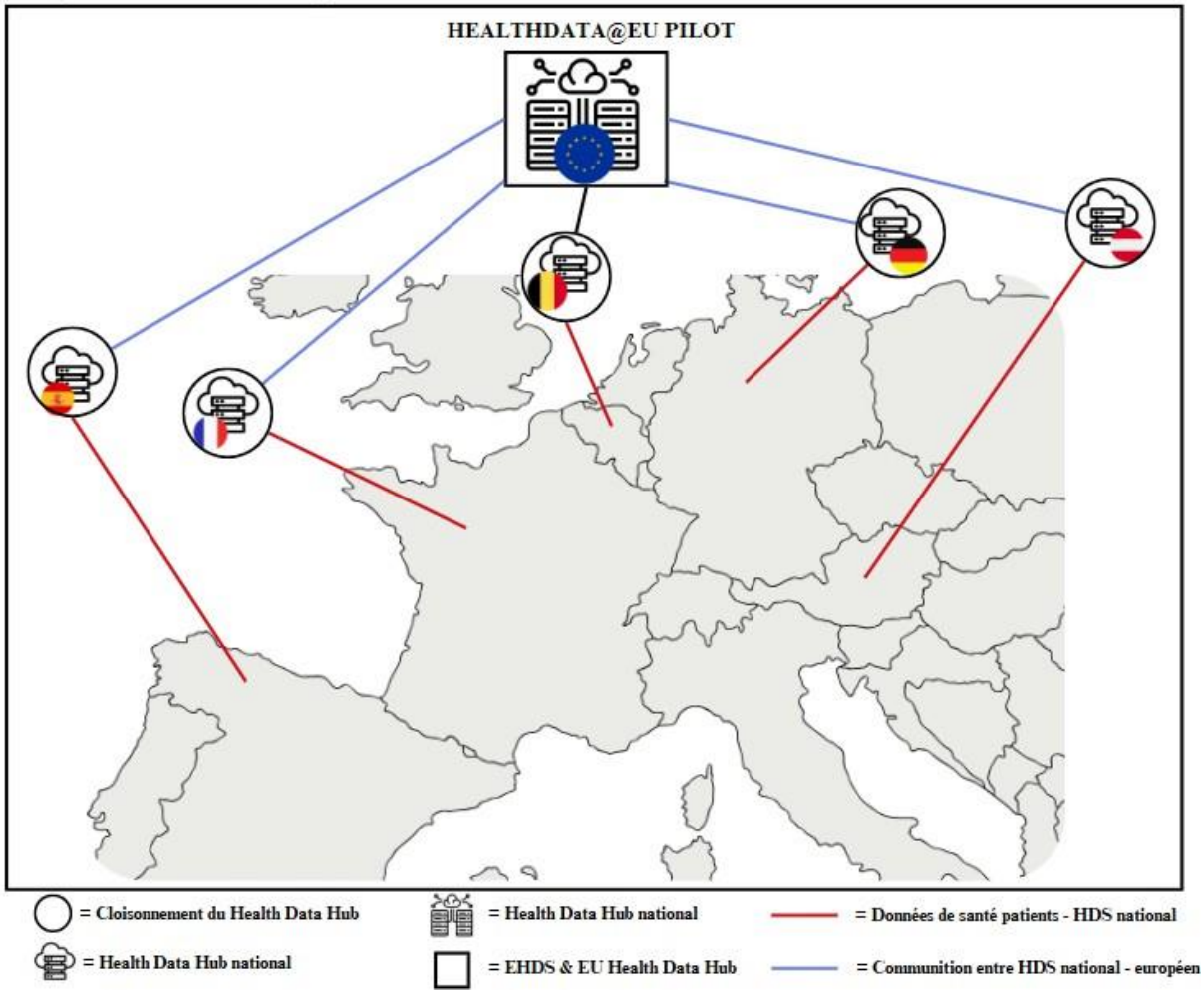
La sécurisation des données de santé est un point clé de cette initiative en raison de leur nature particulièrement sensible et nécessite une protection accrue. L'envergure du projet visant à intégrer l'ensemble des données des patients à l'échelle européenne rend encore plus complexe cette problématique de confidentialité et de sécurité. Cette centralisation permettrait de faciliter l'accès aux données de santé, mais donnerait accès à l'ensemble des données patients en Europe en cas de faille de sécurité.

Pour assurer le succès du projet et la souveraineté des données de santé des citoyens européens, il est essentiel de créer un système fiable et efficace pour la réutilisation de ces données à différentes fins comme l'amélioration des prestations de santé et de

l’accès à ces dernières. Cela permettra de faire évoluer le fonctionnement global du système de soin européen et de faciliter le partage des données avec les décideurs publics européens.



European Health Data Space



Aujourd'hui, les données de santé ne peuvent pas circuler automatiquement entre les pays, étant envoyés de manière indépendante d'un centre de données à un autre. Cette initiative européenne à travers la création d’un espace de données commun marquera une grande avancée pour le système de santé européen. Cependant, son fonctionnement actuel permet malgré tout un cloisonnement de l’information et une plus grande confidentialité des données que ce qui est prévu à l’avenir par le système européen de partage des données de santé (EHDS). La nécessité d’établir une interopérabilité entre les pays européens sur la thématique de la santé est un besoin

auquel il faut pallier.

Face à une problématique majeure de sûreté des données, elle prévoit un financement du HealthData@EU Pilot à hauteur de 37 millions d'euros sous forme de subventions, allouées aux États membres pour la mise en place des infrastructures nécessaires au bon fonctionnement de l'EHDS. Parallèlement, d'autres projets de l'UE, tels que l'action commune *Xt-EHR* et le projet d'exploitation des infrastructures déjà existantes permettront de soutenir et d'accélérer la mise en œuvre de l'espace commun, mais aussi d'en garantir une utilisation durable. Cependant, malgré un besoin de plus en plus urgent, l'UE n'indique aucune date prévisionnelle de mise en place de ce système.

3. Le cas occitan : un cas transposable à la France ?

Le partage des données médicales en Occitanie :

La région Occitanie cherche à développer son système de partage de données patient durant le parcours de celui-ci entre les différents services médicaux. De ce fait, l'objectif de la région est de suivre les orientations politiques françaises sur la création du « carnet de santé numérique ».

La France cherche à moderniser et unifier le système de santé numérique. La plateforme de santé « Mon espace Santé » mise en place en 2022 a pour but de permettre à la fois aux patients, ainsi qu'aux professionnels d'avoir accès à un Dossier Médical Partagé (DMP) tout en garantissant une sécurité de la donnée médicale. Ceci a pour but d'élargir la souveraineté numérique médicale en assurant un développement français d'une solution numérique médicale utile et aux patients, et aux professionnels de santé.

C'est dans ce contexte, que la région Occitanie a déployé différents processus permettant de former et de rendre pratique le partage des données entre professionnels de santé, structures médicales et patients.

Lors d'une conférence organisée le 29 février 2024 par l'Agence du Numérique en Santé Occitanie, des professionnels de santé ont développé et décrit le processus de nouveaux logiciels permettant un partage de données médicales sécurisé. Ce partage assure à la fois un suivi médical clair et contrôlé, tout en garantissant aux patients une sécurité.

Les différentes étapes de partage de la donnée dans un accompagnement patient type :

Occitanie E-santé, est une structure régionale qui permet à ces acteurs d'intégrer des outils numériques garantissant une transmission des données entre les acteurs. De ce fait, aussi bien médecins généralistes et spécialistes, hôpitaux et radiologues bénéficient d'un accès à différents logiciels se répondant entre eux.

Etape 1 Prise de Rendez-vous à travers le logiciel SAS :

Lorsqu'un patient prend rendez-vous vous chez un médecin à travers la plateforme en ligne SAS, l'information est automatiquement partagée à son médecin traitant.

Cet outil permet également de transmettre les informations telles que le compte rendu établi par le médecin régulateur.

Étape 2 Utilisation de logiciels LGB et LGC :

Si des analyses, traitements ou autres consultations sont recommandées ou prescrites, les acteurs suivants :

- laboratoire d'analyse médicale (LGC hellodoc)
- cabinet médical (LGB Dedalus)
- expert médical (médecin spécialisé) (LGC Medimust)

ont accès au dossier patient et peuvent le compléter. Ainsi, des nouvelles données peuvent être générées et partagées.

Étape 3 Transmission des données à l'hôpital :

L'hôpital a accès à partir du logiciel LGB à toutes les données précédemment enregistrées par les professionnels de santé et le patient en plus même. Selon l'Agence du Numérique en Santé Occitanie, ce processus permet une prise en charge plus efficiente pour l'hôpital (disposant de tout le passif médical du patient) et pour le patient directement accompagné.

Étape 4 RIS, DPI, Une hospitalisation encadrée :

A partir des solutions RI pastel, DPI et RIS One Manager les différents services de l'hôpital se transmettent les données de patients.

Étape 5 L'espace Santé, la finalité de la donnée :

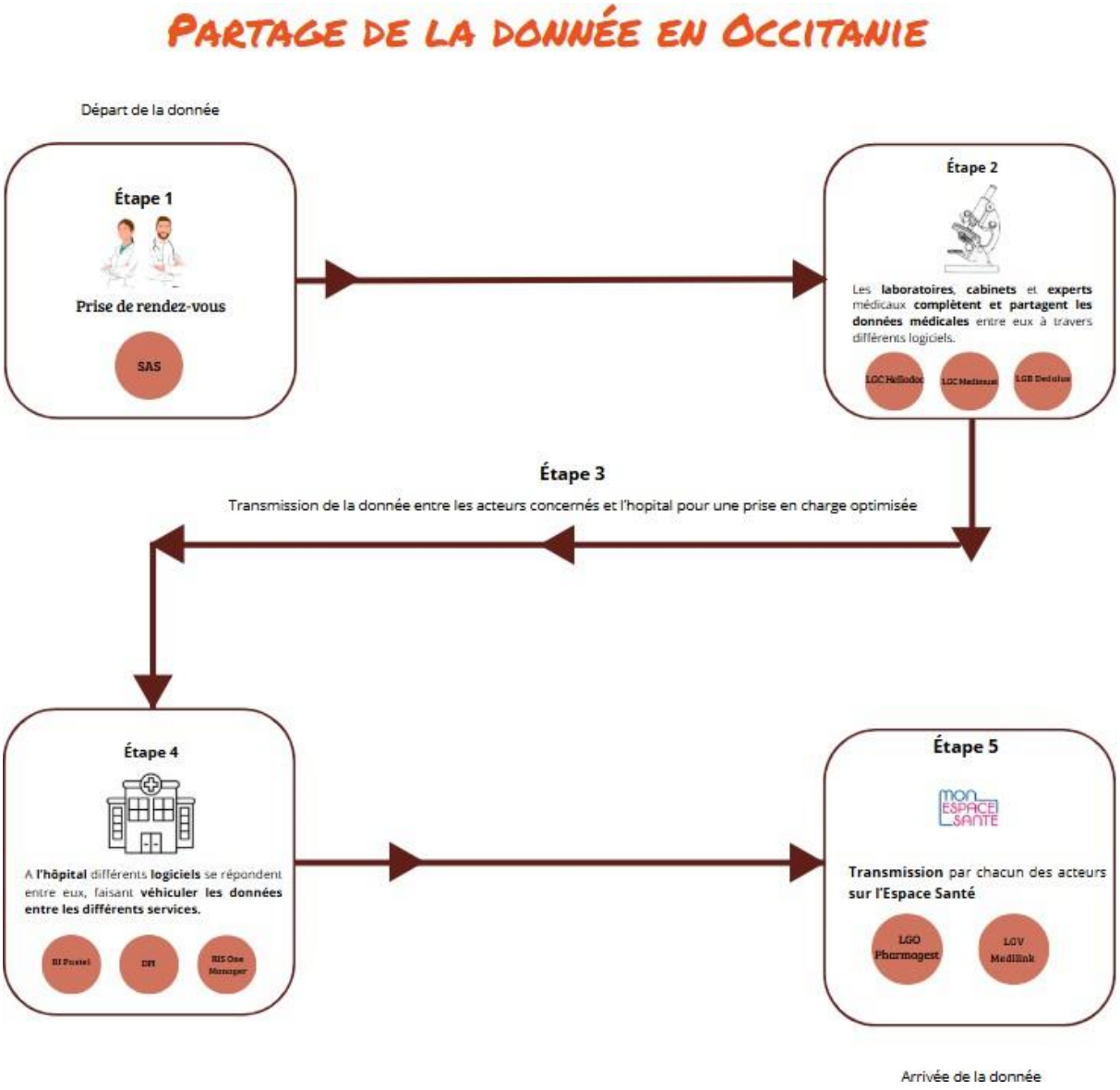
L'hôpital à partir des logiciels intégrés LGO et LGC actualise le dossier patient. Le pharmacien (via LGO Pharmagest) et le médecin traitant (via LGC Medilink) ont accès à toutes les informations médicales liées au parcours du patient entre les différents services.

Ces logiciels automatisent également l'application étatique Mon Espace Santé, de façon que le patient visualise tout son parcours.

Les avantages et inconvénients de ce système :

Le système occitan est le système le plus développé en France permettant une transmission des données entre tous les acteurs concernés. La région s'axe sur une modernisation et centralisation des données médicales avec des solutions françaises. L'interopérabilité des outils assure une efficacité accrue du système de santé de la région tout en garantissant un soutien à la souveraineté française.

Ces logiciels ne sont pas des solutions étatiques et leurs données médicales sont stockées à titre privé. De plus, cette interopérabilité est difficile à mettre en œuvre et peut générer des risques cyber importants. Tous les professionnels de santé, ou même patients ne sont pas formés et ce fonctionnement, qui laisse sous-entendre une dépendance technologique importante.



Les données de santé représentent un levier majeur pour les Etats dans leur stratégie de recherche médicale. La France et l'Union européenne ont très bien compris l'enjeu autour de ces données et ont mis en place de nombreux projets pour faciliter leur transfert et leur exploitation. Cependant, dans la mise en place de ces projets un problème se pose, les pays membres de l'Union européenne dépendent des infrastructures d'hébergement de données d'acteurs américains.

Partie 2 : Le positionnement stratégique de l'Occident sur les données de santé

A. Etat des lieux des solutions d'hébergement des données de santé en France

1. La certification HDS : un gage de sécurité des données de santé accessible aux entreprises françaises et internationales

La certification HDS[iii] est devenue un passage obligatoire pour toutes les entreprises qui hébergent ou exploitent des données de santé à caractère personnel. Cette exigence a été mise en place par la CNIL dans un contexte où le secteur de la santé connaît une digitalisation rapide. Avec l'essor des solutions cloud et la multiplication des données sensibles, il était crucial de renforcer la sécurité autour de leur hébergement.

Face à cette obligation, on observe une véritable inflation des entreprises certifiées. Beaucoup de prestataires, qu'ils soient français ou internationaux, se sont précipités pour obtenir cette certification afin de rester compétitifs sur le marché et conformes aux exigences réglementaires. L'objectif est simple : garantir la protection des données de santé, considérées comme des données sensibles par le RGPD (source : CNIL RGPD[iv]). Cela permet de rassurer les patients et les professionnels de santé sur la sécurité des informations stockées.

La certification HDS est attribuée par des organismes accrédités par le COFRAC (Comité Français d'Accréditation). Ces organismes sont chargés d'évaluer la conformité des entreprises via deux audits successifs :

Le premier est un audit ISO 27001, ce dernier valide la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO 27001. Il couvre tous les aspects essentiels liés à la cybersécurité, comme la gestion des risques, la protection des données et la réponse aux incidents (source : ISO 27001[v]).

Le second est un audit spécifique HDS, celui-ci va plus loin en imposant des critères spécifiques à l'hébergement de données de santé. On y retrouve des exigences précises sur la gestion des accès, la traçabilité des actions effectuées sur les données et le respect strict des obligations légales.

Ces deux audits garantissent que les prestataires certifiés sont capables de sécuriser les données tout au long de leur cycle de vie, depuis leur stockage jusqu'à leur sauvegarde ou d'archivage.

Il existe deux principales certifications HDS. Elles dépendent de l'activité de l'entreprise et de son rôle dans l'hébergement des données de santé : la certification « Hébergeur d'infrastructure physique » et la certification « Hébergeur infogéreur ».

La certification « Hébergeur d'infrastructure physique »

Cette certification concerne les entreprises qui fournissent l'infrastructure matérielle nécessaire à l'hébergement des données de santé. Les prestataires certifiés dans cette catégorie sont responsables de plusieurs aspects importants :

Mise à disposition et maintient en bon état l'infrastructure matérielle utilisée pour le traitement des données de santé.

- Gestion et entretien des sites physiques qui hébergent cette infrastructure, garantissant ainsi la sécurité physique des données à chaque étape de leur cycle de vie.
- Ce type de certification s'adresse principalement aux entreprises qui exploitent des datacenters ou des infrastructures physiques dédiées à l'hébergement des données sensibles de santé.

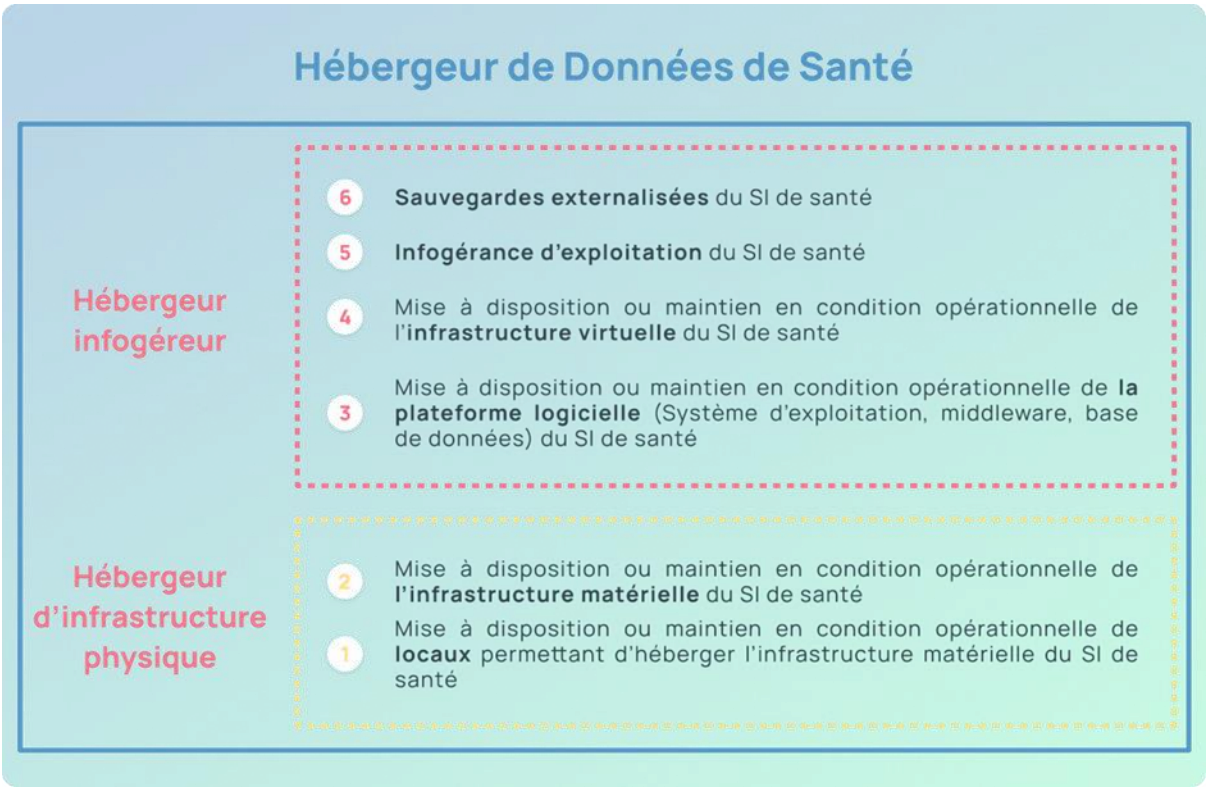
La certification « Hébergeur infogéreur »

Au-delà de l'hébergement physique des données, la certification « Hébergeur infogéreur » est destinée aux prestataires responsables de la gestion et de l'exploitation des systèmes d'information liés aux données de santé. Leur rôle comprend quatre points :

La mise à disposition et le maintien en bon état de l'infrastructure virtuelle (cloud) utilisée pour traiter les données de santé ;

- La gestion de la plateforme d'hébergement des applications liées aux systèmes d'information de santé ;
- L'administration et l'exploitation du système d'information, en assurant la disponibilité, l'intégrité et la sécurité des données de santé ;
- La mise en place de solutions de sauvegarde externalisée pour protéger les données de santé contre toute perte accidentelle ou malveillante.
- Les prestataires certifiés « Hébergeurs infogéreurs » prennent donc en charge la gestion complète de l'environnement informatique permettant de traiter et stocker les données de santé, en mettant particulièrement l'accent sur l'aspect virtuel et la gestion des applications[vi].

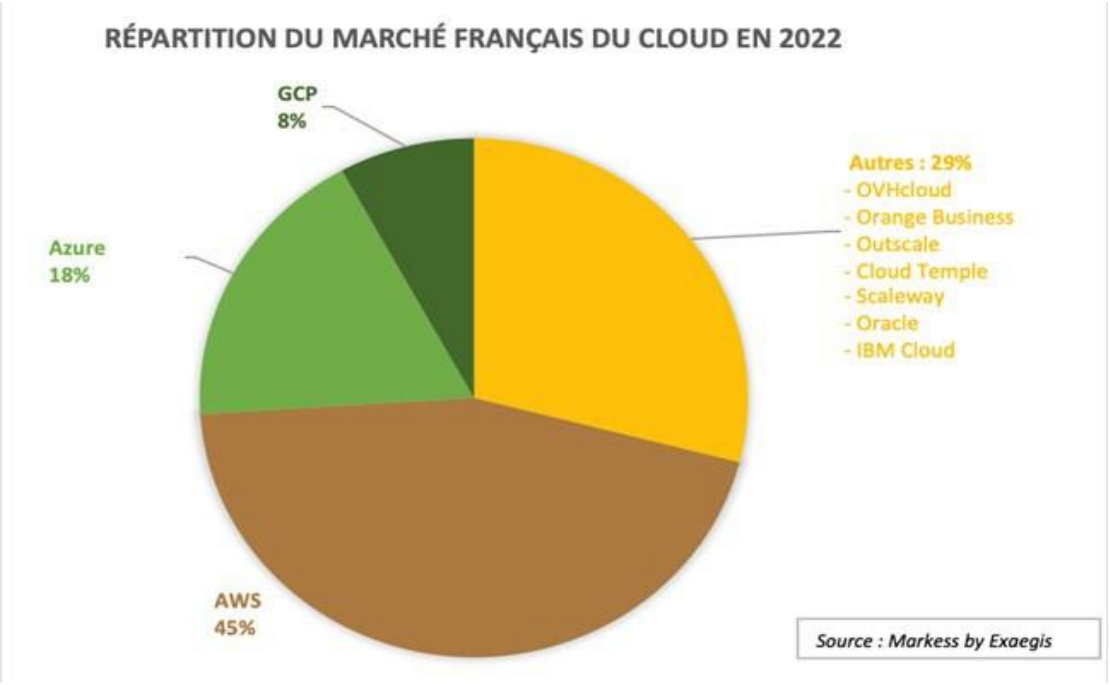
Tableau récapitulatif des niveaux de certification de l'HDS[vii]



Source : Arkhn Blog | La certification HDS [viii]

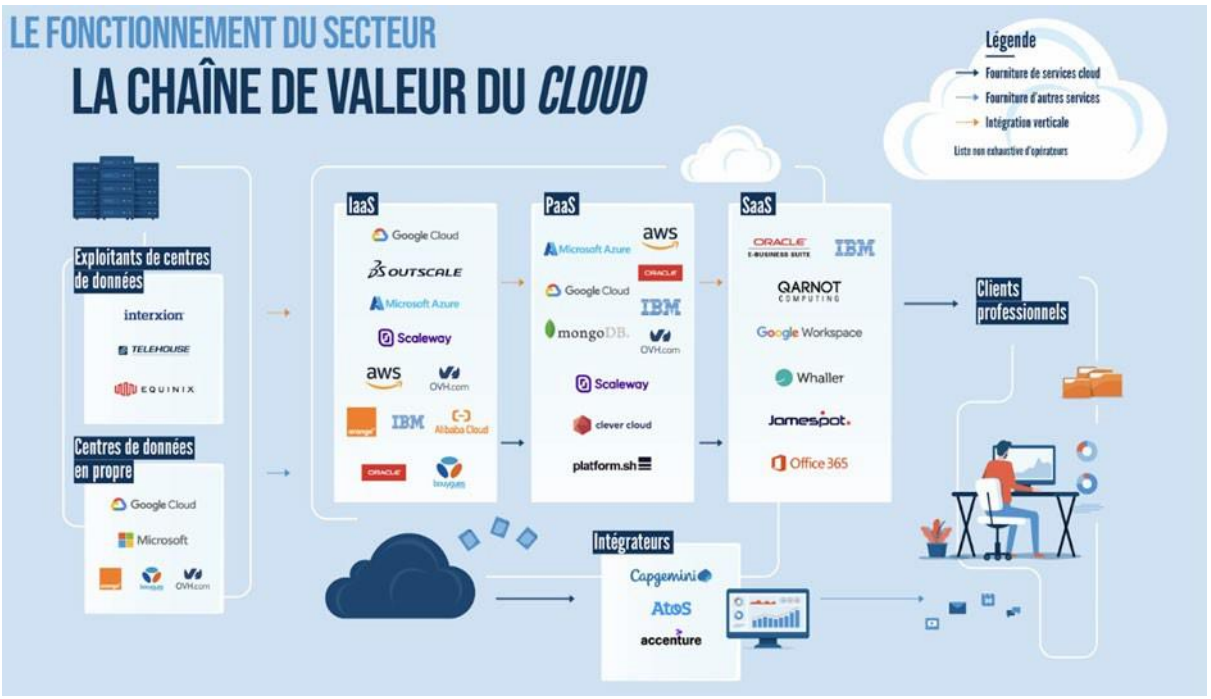
Depuis que la CNIL a imposé la certification HDS, le nombre d'entreprises engagées dans la démarche a considérablement augmenté. Cette dynamique peut être expliquée par plusieurs facteurs. Tout d'abord, il y a un besoin croissant de solutions numériques sécurisées pour les hôpitaux, cliniques et professionnels de santé. En parallèle, la protection de la souveraineté et de la confidentialité des données sensibles face aux cybermenaces est devenue une priorité absolue. L'urgence pour les prestataires, notamment les acteurs du cloud, de se conformer aux nouvelles exigences réglementaires a également joué un rôle clé. Enfin, certains acteurs historiques, tels que les Centres Hospitaliers Universitaires (CHU) ou des hôpitaux privés, ont pris les devants en collaborant avec des hébergeurs certifiés pour sécuriser leurs infrastructures numériques.

Agence du Numérique en Santé. (s. d.-c). Liste des hébergeurs certifiés[ix]



Les essentiels de l'informatique en nuage PDF[x]

Bien que la majorité des Hébergeurs de Données de Santé en France soient de petits acteurs français (77% des acteurs certifiés), cette majorité ne reflète pas la réalité du marché global du cloud en France. En effet, les solutions Saas (Software as a Service) certifiées HDS sont principalement développées par de petites entreprises françaises proposant des solutions innovantes pour les acteurs du secteur. Toutefois, ces solutions reposent majoritairement sur des plateformes PaaS (Platform as a Service) développées par Azure ou AWS et sont hébergées sur des infrastructures IaaS (Infrastructure as a Service) appartenant aux géants américains. Cette tendance est confirmée par la surreprésentation des hyperscalers (AWS, Azure et GCP) dans le marché français du Cloud (71%). En outre, la probabilité qu'un acteur américain soit représenté dans la chaîne de valeur du cloud est hautement probable mais quasiment indispensable[xi].



Source: Autorité de la concurrence[xii]

Si cette dépendance peut sembler moins marquée pour les données critiques comme celles de santé, elle n'en reste pas moins importante. L'exemple du Health Data Hub en est révélateur, malgré son rôle essentiel dans la souveraineté numérique française, il repose sur l'infrastructure technologique du géant américain Microsoft Azure[xiii].

2. Infogérance : une chaîne dominée par les géants américains

Le cloud computing, modèle de fourniture de services informatiques via Internet[xiv], permet aux utilisateurs finaux d'accéder à des ressources informatiques (serveurs, stockage, bases de données, logiciels, etc.) sans avoir à investir dans une infrastructure physique coûteuse. Si des outils tels que Microsoft 365 ou Google Drive ont séduit les acteurs économiques, ces applications ou logiciels représentent la partie visible du Cloud Computing. Structuré en trois couches complémentaires[xv], le cloud compunting offre des niveaux variés de contrôle et de responsabilité dans la gestion des ressources et des données.

L'IaaS (Infrastructure as a Service)

L'IaaS constitue le socle du cloud computing en fournissant des ressources essentielles telles que serveurs, stockage et réseaux, disponibles à la location pour héberger des systèmes d'exploitation et des logiciels. Dans le secteur de la santé, des acteurs certifiés HDS, comme Scaleway, filiale à 94 % du groupe Iliad, garantissent la conformité aux niveaux 1 (sécurité physique) et 2 (sécurité logique)[xvi], assurant ainsi la fiabilité et la sécurité de leurs datacenters. Avec ses quatre sites en France[xvii],

Scaleway propose des infrastructures physiques adaptées aux besoins des entreprises, tout en leur laissant la responsabilité de la gestion de leurs données. Ce modèle s'inscrit dans une chaîne de valeur où l'IaaS forme la base, enrichie par des solutions PaaS et SaaS qui viennent compléter l'offre pour répondre aux besoins des entreprises. Les principaux fournisseurs IaaS, tels que Amazone Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, IBM Cloud et Oracle Cloud[xviii] Infrastructure, proposent des ressources virtualisées à la demande, offrant ainsi une infrastructure flexible, évolutive et sans gestion physique pour les utilisateurs.

Le PaaS (Platform as a Service)

Le PaaS s'appuie sur l'IaaS pour proposer une plateforme prête à l'emploi, idéale pour développer et déployer des applications sans gérer l'infrastructure sous-jacente.[xix] Ce modèle fournit des environnements d'exécution, bases de données et API, tout en automatisant les tâches de maintenance. Pour les données de santé, les PaaS certifiées HDS couvrent les niveaux 2 (sécurité logique), 3 (gestion des données personnelles), et 4 (gestion des opérations), garantissant le chiffrement des données, leur traçabilité, ainsi que des mécanismes de continuité d'activité. Des acteurs comme Outscale, filiale de Dassault Systèmes, offrent des solutions conformes aux normes HDS[xx], tout en partageant avec les utilisateurs la responsabilité de la sécurité des données. Le PaaS simplifie ainsi le développement et s'intègre avec l'IaaS et le SaaS pour répondre aux besoins des entreprises. Les solutions PaaS les plus connues, telles que Microsoft Azure App Services, Google App Engine, AWS Elastic Beanstalk ou Heroku, offrent aux développeurs des environnements clés en main pour concevoir, tester et déployer des applications rapidement, sans gérer l'infrastructure sous-jacente.

Le SaaS (Software as a Service)

Le SaaS propose des logiciels prêts à l'emploi, accessibles via le cloud sans installation ni maintenance locale[xxi]. Ce modèle permet aux entreprises de se concentrer sur l'usage des applications, tandis que le fournisseur gère l'infrastructure et les plateformes sous-jacentes.

Dans le secteur de la santé, des solutions SaaS comme Doctolib[xxii] pour la gestion des rendez-vous médicaux ou Enovacom[xxiii] se distinguent grâce à leurs certifications HDS à tous les niveaux. Ces certifications garantissent la sécurité des données (chiffrement, contrôle d'accès), leur traçabilité et leur portabilité en cas de changement de prestataire.

Le SaaS, en tant que couche applicative du cloud, est directement accessible aux utilisateurs finaux, facilitant ainsi la productivité et la collaboration. Malgré l'émergence de solutions françaises prometteuses, Microsoft 365 et Google Workspace dominent le marché des suites bureautiques et collaboratives avec des outils intégrés tels que Word, Excel, Gmail ou Google Docs. Pour la communication d'équipe, Slack et Zoom s'imposent par leur simplicité et leur efficacité, tandis que dans le domaine de la

gestion de la relation client, Salesforce et HubSpot restent des références incontournables.

La maîtrise des trois couches du cloud compunting : un levier stratégique des hyperscalers

Les trois couches du cloud computing (IaaS, PaaS, SaaS), proposées par divers acteurs français et internationaux, permettent de répondre aux besoins variés des entreprises. Cependant, certains acteurs, notamment les hyperscalers américains, à l'instar d'AWS, GCP et Microsoft Azure, ont adopté une stratégie intégrée visant à contrôler l'ensemble de la chaîne[xxiv]. En maîtrisant les trois niveaux, ces géants offrent des solutions globales et centralisées, attractives pour les utilisateurs grâce à leur efficacité et leur agilité, tout en permettant aux entreprises de décentraliser un hébergement des données consommateur en énergie.

Pour les acteurs de la santé en France, utiliser une offre cloud intégrée couvrant les trois couches (IaaS, PaaS, SaaS) présentent des avantages stratégiques et opérationnels majeurs. L'intégration facilitée par une gestion centralisée constitue un argument simple mais efficace : elle simplifie le déploiement des services, réduit la complexité technique et libère les équipes pour se concentrer sur des projets à forte valeur ajoutée. Les utilisateurs finaux, face au choix d'un cloud computing, demeurent aussi sensibles à l'accès aux technologies développées par les hyperscalers, comme l'intelligence artificielle et l'analyse de données massive.

Cette stratégie favorise une transition massive vers le « tout Cloud », tout en permettant aux hyperscalers de centraliser de vastes bases de données. Ces données massives, alimentées par leurs produits dérivés, telles que les montres connectées ou les smartphones, et exploitées dans leurs modèles d'intelligence artificielle, leur confèrent un avantage compétitif et renforcent leur domination sur le marché mondial de l'infogérance.

Une montée en puissance à travers les trois couches

Historiquement, les géants du cloud computing ont débuté avec des offres SaaS, avant de miser dans l'IaaS et le PaaS pour contrôler l'ensemble des couches du cloud computing. Cette diversification renforce leur rôle de leader et élimine progressivement la concurrence en orientant les utilisateurs vers leur propre écosystème intégré.

Microsoft Azure : Initialement centré sur des outils SaaS comme Microsoft 365 et Dynamics 365, Azure a développé des services IaaS tels que Virtual Machines et Blob Storage, certifiés HDS, pour un hébergement sécurisé des données sensibles. En PaaS, des solutions comme App Service permettent de développer et déployer des applications tout en répondant aux normes de sécurité.

- **Google Cloud Platform (GCP)** : Né comme un moteur de recherche, Google s'est transformé en acteur majeur du cloud computing. À partir de solutions SaaS comme Google Workspace, GCP a élargi son offre à l'IaaS avec Compute Engine et Cloud Storage, puis au PaaS avec des outils tels que BigQuery pour

l'analyse de données et Cloud Healthcare API pour l'interopérabilité des données médicales.

En se positionnant sur les trois couches du cloud computing, des hyperscalers ont su convaincre les décideurs publics, à l'instar de Microsoft Azure pour le Health Data Hub. Le domaine des données de santé, dont la sécurité et la maîtrise est hautement stratégique, suscite l'intérêt de nombreux candidats se présentant comme des alternatives.

Les alternatives françaises dans l'écosystème cloud

Bien que dominées par les géants américains, des offres complètes sont également proposées par des acteurs français comme OVHcloud, qui couvre les trois couches du cloud[xxv] avec des services certifiés à tous les niveaux HDS. OVHcloud propose des infrastructures (IaaS), des plateformes (PaaS) et des solutions tierces (SaaS), adaptées aux données de santé. En outre, OVHcloud possède également la certification SecNumCloud de l'ANSSI[xxvi] qui certifie la souveraineté des données. Par ailleurs, de nombreuses alternatives françaises, qu'elles soient cloud ou non, sont candidates pour participer à l'écosystème stratégique de l'hébergement des données en France. Ces alternatives, offrant différents services de cloud computing, se présentent souvent comme des solutions complémentaires dans l'écosystème cloud.

En effet, des plateformes SaaS telles que Microsoft 365 ou Google Workspace restent les références incontournables en entreprise et donc complète l'offre des solutions françaises par manque d'alternatives holistiques crédibles. Cet écueil rend pour l'heure difficile l'acquisition d'un écosystème cloud et souverain et intégré.

Dans cette optique, cinq solutions d'hébergement françaises et cinq solutions étrangères ont été identifiées comme des acteurs potentiels pour contribuer à cet écosystème, répondant aux besoins stratégiques et réglementaires du secteur.

3. Hébergement des données de santé : comparaison des solutions françaises et internationales

Critères / Entreprises	OVHcloud	DOCAPOSTE	Atos	Scaleway	enovacom	aws	Azure	Google Cloud	EQUINIX	ORACLE HEALTH SCIENCES
Niveaux de certification HDS	[1-2-3-4-5-6]	[1-2-3-4-5-6]	[1-2-3-4-5-6]	[1-2]	[1-2-3-4-5-6]	[1-2-3-4-5-6]	[1-2-3-4-5-6]	[1-2-3-4-5-6]	[1-2]	[1-2-3-4-5-6]
Couches du cloud computing	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, PaaS	SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS	IaaS, PaaS, SaaS
Datacenters en France (propriétaire)	16 (16)	4 (4)	15 (5)	4 (4)	INC	4 (0)	3 (0)	2 (0)	11 (11)	2 (0)
Indépendance stratégique	Très forte (France)	Très forte (France)	Forte (France, UE)	Forte (France)	Forte (France)	Faible (Cloud Act, USA)	Faible (Cloud Act, USA)	Faible (Cloud Act, USA)	Partielle (Data centers FR)	Faible (Cloud Act, USA)
Sécurité des données	HDS, ISO 27001, SECNUMCLOUD, SOC 2	HDS, ISO 27001	HDS, ISO 27001	HDS, ISO 27001	HDS, ISO 27001	HDS, ISO 27001, SOC 2	HDS, ISO 27001, SOC 2	HDS, ISO 27001, SOC 2	HDS, ISO 27001, SOC 2	HDS, ISO 27001, SOC 2
Partenariats	Partenaires locaux, AP-HP	Partenariats hôpitaux	Collaboration académiques	PME, start-ups françaises	Acteurs santé publique	Partenariats start-ups e-santé	Écosystème Microsoft Global	Start-ups IA, recherche	Hôpitaux et entreprises	Agences et organisations
Innovation	Cloud souverain	Cloud santé	IA, HPC, blockchain	Durabilité et accessibilité	Santé et interopérabilité	IA, Machine learning, Internet of Things	Hybridité, IA, analytics	IA, Big Data, HPC	Connectivité globale	Bases de données autonomes, hybridité
Résilience	Très bonne	Bonne	Excellente / ISO 22301	Bonne	Bonne	Excellente / ISO 22301	Excellente / ISO 22301	Excellente / ISO 22301	Très bonne / ISO 22301	Très bonne
Points Forts	Souveraineté	Expertise santé publique	Innovation technologique	Solutions cloud souverain	Spécialisation e-santé	Capacité d'innovation	Intégration avec l'écosystème Microsoft	Analyse de données et IA puissante	Neutralité data centers	Bases de données sécurisées

Source : tableau basé sur des données open source et réalisé par le groupe 20

L'analyse des solutions pour l'hébergement des données de santé en France permet de dégager des tendances entre les acteurs français (OVHcloud, Docaposte, Atos, Scaleway, Enovacom) et les acteurs étrangers (AWS, Azure, Google Cloud, Equinix, Oracle).

D'une part, les entreprises françaises, caractérisées par leur souveraineté numérique et leur conformité stricte aux exigences, notamment grâce à la certification HDS, possèdent des datacenters locaux, garantissant leur indépendance stratégique vis-à-vis des régulations étrangères. OVHcloud, leader incontesté avec 16 datacenters en France[xxvii] et une certification SecNumCloud, compose avec Docaposte[xxviii] et Atos[xxix] qui présentent des offres complètes couvrant les trois couches du cloud (IaaS, PaaS, SaaS). Scaleway et Enovacom, davantage spécialisées, proposent des solutions ciblées, respectivement en IaaS/PaaS et en SaaS.

À l'inverse, les acteurs étrangers comme AWS, Azure, Google Cloud et Oracle dominent le marché mondial grâce à des offres technologiques sans équivalent couvrant IaaS, PaaS et SaaS. Leur capacité d'innovation et leur écosystème global en font des acteurs incontournables pour des besoins de grande envergure. Néanmoins, de par leur origine américaine, leur exposition au Cloud Act soulève des inquiétudes quant à la sécurité et la souveraineté des données, susceptibles de quitter le territoire

français et européen. En matière de datacenters, ces acteurs disposent d'un nombre de sites inférieur à celui des solutions françaises mais restent dans la course grâce à la location de datacenters grands et performants [xxx].

Les solutions françaises offrent des garanties solides en matière de souveraineté, de localisation des données et de conformité réglementaire, ce qui les rend particulièrement adaptées aux besoins du secteur de la santé. Les solutions étrangères, bien qu'avancées technologiquement, présentent un manque d'indépendance stratégique questionnant l'intérêt de leur adoption dans les environnements où la protection des données est primordiale.

Si des solutions françaises à l'image du choix d'Atos pour la création de "Mon Espace Santé"[xxxi] en collaboration avec la Caisse Nationale d'Assurance Maladie (CNAM) sont sélectionnées, cela ne fait pas de ces acteurs des choix évidents pour autant. Malgré des initiatives à l'image de Numspot[xxxii] (Docaposte, Dassault Systèmes et Bouygues Telecom) destinées à faciliter l'accès et le partage des données de santé des patients, les décideurs publics ont à disposition des options distinctes et parfois complémentaires. Face à ces solutions d'hébergement de données, quels vont être les choix stratégiques des autorités pour inaugurer un cloud souverain garantissant la sécurité de nos données de santé ?

4. Étude de cas : le Health Data Hub, un exemple de renoncement stratégique

Créé en 2019, le Health Data Hub (HDH), ou Plateforme des données de santé (PDS), vise à centraliser et structurer les données de santé issues de multiples sources, notamment le Système national des données de santé (SNDS), regroupant Assurance Maladie, hôpitaux, Programme de médicalisation de systèmes d'informations, les registres spécifiques (maladies rares, cancers), les résultats de laboratoires d'analyses médicales, ainsi que les données issues de la recherche clinique. Ces données variées visent à soutenir la recherche de nouveaux remèdes, l'innovation et orienter les politiques publiques tout en respectant la confidentialité afin de favoriser l'innovation et le développement du monde de la santé. Cependant, ce projet, pensé comme un pilier pour moderniser le secteur de la santé en France, est rapidement devenu un sujet de controverse, en raison de choix stratégiques et techniques soulevant des questions de souveraineté et de gouvernance des données sensibles.

La Plateforme des données de santé s'inscrit donc dans une dynamique ambitieuse : valoriser le patrimoine de données de santé françaises, considérées parmi les plus riches et exhaustives au monde[xxxiii]. Ses missions, définies par l'article L.1462-1 du Code de la santé publique, sont variées et prévoient entre autres de :

Rassembler et organiser les données : Les données issues notamment du Système National des Données de Santé (SNDS), comme les résumés de passages aux urgences, sont centralisées et structurées.

- Faciliter l'accès à la recherche : Le HDH permet de mettre ces données à disposition des chercheurs et des porteurs de projets tout en respectant les droits des patients.
- Standardisation et innovation : En accompagnant des projets de recherche et en participant à l'élaboration de normes, le HDH contribue à promouvoir l'utilisation des données de santé dans des cadres innovants et sécurisés.
- Si les objectifs semblent clairs, certaines finalités précises, comme l'anticipation des maladies ou l'orientation des politiques de santé publique, ne sont pas toujours explicitées dans les communications officielles, ce qui nourrit des interrogations. En effet, les conditions d'accès aux données médicales ont été assouplies par le ministère de la Santé : plus besoin de justifier de travaux de recherche, d'étude et d'évaluation, il suffit désormais d'invoquer l'intérêt public.

Dès sa conception, le Health Data Hub s'est retrouvé au cœur de controverses successives, notamment en raison du choix d'héberger ses données sur la plateforme Microsoft Azure. Ce choix stratégique a été largement critiqué pour son manque de cohérence avec les objectifs affichés de souveraineté numérique et de protection des données sensibles en France, et les exigences fixées au départ par l'ANSSI et la CNIL vis-à-vis des hébergeurs de données Français désireux de faire partie du projet. L'attribution de ce contrat, réalisée par l'intermédiaire de l'Union des Groupements d'Achats Publics (UGAP), s'est déroulée sans appel d'offre au niveau français, ce qui a limité la concurrence, et pose des questions de légitimité du choix du fournisseur. À l'époque, UGAP avait approché les entreprises susceptibles d'être intéressées par le projet, en leur présentant un cahier des charges à géométrie variable, comprenant certaines obligations afin de répondre à un éventuel appel d'offres. Or, des entreprises françaises comme OVHcloud, Scaleway ou encore Atos qui étaient candidates, ne disposaient pas de la certification HDS, un prérequis incontournable, contrairement à Azure. Autre critère, détenir une certification SecNumCloud complète, dont aucune entreprise ne disposait. Un appel d'offre public inexistant, qui aurait permis d'explorer des alternatives européennes, voire françaises, capables de répondre aux besoins en garantissant une conformité totale avec le RGPD. Bien qu'en parallèle, Microsoft Azure ne remplissait pas non plus certains critères de cybersécurité comme la certification SecNumCloud, délivrée par l'ANSSI.

À ce sujet, madame Stéphanie Combes déclarait :
"Si nous avions publié un marché public, Microsoft y aurait répondu et Microsoft l'aurait remporté"
– Stéphanie Combes, février 2021 (audition par la mission Latombe)

On peut imaginer que les données de la SNDS étaient déjà stockées sur un cloud Azure et que le choix du HDH de choisir Microsoft n'est qu'une continuité basée sur des facilitations techniques. Or, comme le précise une modératrice de la SNDS lors d'une FAQ sur leur site[xxxiv] : "La base principale du SNDS/base principale est actuellement hébergée par la CNAM, en France, sur ses propres serveurs. À terme,

le HDH recevra une copie de la base principale du SNDS/base principale et héberge aussi le catalogue du SNDS/base principale." Cet état de fait perd tout l'intérêt de stocker sur ses propres serveurs les données de la SNDS puisqu'au final, une copie des données sera transférée sur le cloud Azure de Microsoft. Ce paradoxe a suscité de vives critiques[xxxv], alimentant le sentiment que des décisions clés avaient été prises sans une réelle prise en compte des enjeux stratégiques à long terme. Le collectif « SantéNathon » et la CNIL, avaient par ailleurs déposé des requêtes pour contester ces méthodes, et s'inquiétaient des potentielles atteintes aux règles de commande publique et de souveraineté numérique. Ce type de situation alimente les suspicions de collusion ou de conflits d'intérêts. À tel point qu'en 2021, l'association ANTICOR a saisi le PNF, pour diligenter une enquête, toujours en cours, qui a donné lieu à une perquisition au siège du HDH[xxxvi].

Un autre aspect central des critiques réside dans les implications juridiques du choix de Microsoft Azure. En tant qu'entreprise américaine, Microsoft est soumise au Cloud Act de 2018, qui permet aux autorités des États-Unis d'exiger l'accès à des données détenues par des entreprises américaines, quel que soit l'emplacement géographique des serveurs. Cette réalité juridique signifie que, malgré l'hébergement physique des données dans des centres situés aux Pays-Ba[xxxvii]s, les autorités américaines pourraient potentiellement accéder à ces données, créant un risque significatif pour la confidentialité et la souveraineté des informations médicales françaises. Ces données, qui englobent des informations particulièrement sensibles sur la santé des citoyens, sont au cœur de nombreuses recherches scientifiques et projets stratégiques. Les risques d'exploitation à des fins non prévues, telles que l'entraînement d'algorithmes commerciaux ou des usages par des tiers non autorisés, ajoutent un poids supplémentaire à cette inquiétude.

Face à ces critiques, le gouvernement français, par l'intermédiaire de responsables comme Olivier Véran et Cédric O, avait annoncé en 2020 son intention de migrer les données vers une infrastructure européenne d'ici à deux ans. Toutefois, en 2023, cet engagement n'avait toujours pas été respecté. La CNIL a finalement autorisé une prolongation du contrat avec Microsoft, dans le cadre du projet EMC2, justifiant cette décision par des raisons pratiques, notamment la complexité et le coût élevé d'une migration rapide des infrastructures. Le projet européen EMC2, visant à interconnecter plusieurs plateformes similaires au Health Data Hub (HDH) à l'échelle de l'Europe a encore été attribué à Azure by Microsoft. Cette décision, validée par la CNIL le 31 janvier 2024, reflète une situation où les ambitions de souveraineté numérique européenne se heurtent à des contraintes techniques mais aussi politiques.

Malgré les engagements politiques antérieurs de migrer vers des solutions européennes, la CNIL a accordé une autorisation limitée à trois ans (au lieu des dix ans initialement prévus), invoquant l'absence de prestataires européens capables de répondre aux exigences techniques nécessaires pour le projet EMC2. Parmi ces exigences figuraient des niveaux élevés de sécurité et de performance, ainsi que des certifications comme SecNumCloud, délivrée par l'ANSSI. Or, aucune des solutions

évaluées, y compris celles de Microsoft Azur (la certification SecNumCloud étant exclusivement réservée aux acteurs européens et n'étant pas détenue à plus de 39% par une maison mère hors UE), ne répondait intégralement à ces critères dans les délais impartis.

Une mission d'expertise, mise en place par la CNIL, avait pour objectif d'approcher les prestataires européens potentiels. Cependant, cette mission a révélé que les migrations vers une autre infrastructure cloud prendraient non seulement du temps, mais impliquent également des coûts et des risques opérationnels importants, ce qui a renforcé la position de Microsoft comme fournisseur incontournable dans l'immédiat. Cette dépendance stratégique est également le résultat d'un contexte où les certifications nécessaires prennent des années à obtenir, freinant la montée en puissance des alternatives européennes.

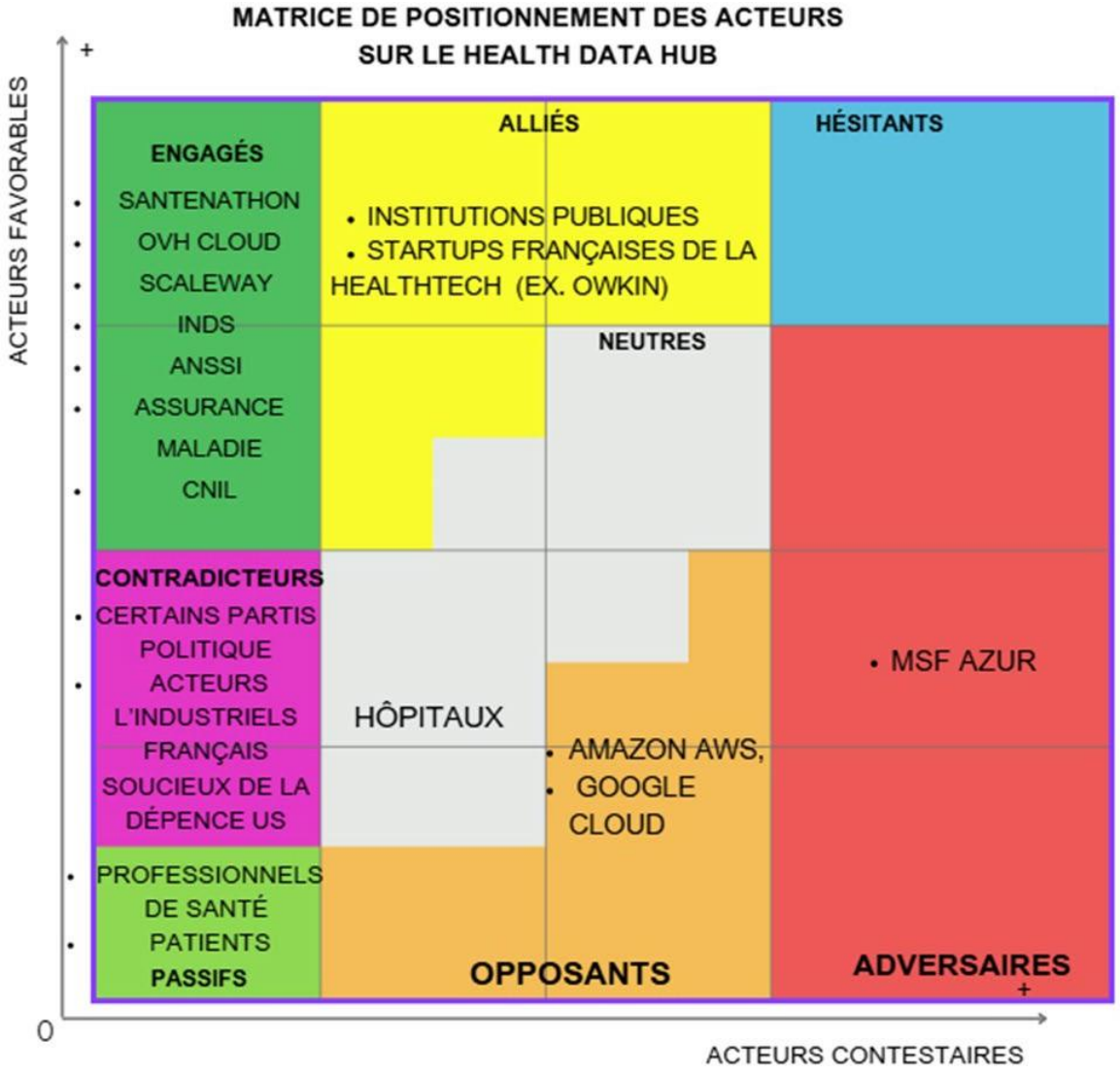
Bien que Microsoft dispose de datacenters en Europe, notamment en Irlande[xxxviii] et en France[xxxix], le fait que la société soit soumise à la législation américaine expose les données, et cette fois européen et non plus Français uniquement, à des risques juridiques et stratégiques réels. Cette situation est perçue comme un compromis sur la souveraineté des données, en contradiction avec les objectifs affichés du projet EMC2.

De plus, certaines critiques, notamment celles exprimées par le PDG d'OVHcloud dans le cadre d'un article de presse, suggèrent que le cahier des charges a été modifié de manière répétée, ajoutant de nouvelles exigences à mesure que les prestataires européens proposaient des solutions capables de répondre aux critères. "En bout de course, Le cahier des charges, est passé de 165 exigences et critères, à 262; ainsi que de 200 cas d'usages, à 466 cas à la fin.[xl]". Ces modifications ont nourri un sentiment de favoritisme envers Microsoft et un manque de transparence dans le processus de sélection. Cette situation reflète non seulement une dépendance technologique aux acteurs non européens, mais aussi un manque d'anticipation et de volonté politique dans la mise en œuvre de solutions alternatives à l'échelle nationale ou continentale.

Le choix de Microsoft Azure a mis la lumière sur des questions d'éventuels conflits d'intérêts. La commission d'enquête sénatoriale sur l'influence des cabinets de conseil, présidée par Arnaud Bazin[xli], a pointé du doigt le rôle de Capgemini, une société de conseil française partenaire de Microsoft[xlii] depuis au moins 2018, dans la recommandation de cette solution d'hébergement faite à l'État en 2019. D'autant plus qu'on peut voir sur le site de microsoft[xliii] que Capgemini est considéré comme un "partenaire premium". Autre fait marquant, Jean-Marc Aubert, principal architecte du Health Data Hub, à travailler de 2013 à 2017 pour IQVIA[xliv], un géant américain du traitement des données médicales, avant sa nomination à la Direction de la Recherche, des Études, de l'Évaluation et des Statistiques (DREES[xlv]). Une semaine seulement après le lancement du Health Data Hub, Jean-Marc Aubert est retourné chez IQVIA pour devenir président de l'entreprise en France[xlvi]. Cette transition a alimenté les soupçons sur les liens étroits entre certains décideurs publics et les

grandes entreprises privées, en particulier dans un contexte où la possession de données de hautes valeurs représente un avantage stratégique conséquent.

En conclusion, le choix de Microsoft Azure pour héberger les données du Health Data Hub soulève des questions cruciales sur la capacité de la France et de l'Europe à garantir leur autonomie technologique et leur souveraineté numérique. Ce cas met en lumière l'urgence de développer des alternatives souveraines, tout en renforçant les mécanismes de transparence et d'éthique dans les décisions qui touchent à des infrastructures critiques comme celles des données de santé.



Source : tableau basé sur des données open source et réalisé par le groupe 20

La matrice de positionnement des acteurs sur le Health Data Hub présente une analyse des différents acteurs en fonction de leur engagement et de leur position par rapport à la souveraineté numérique et la gestion des données de santé en France. L'analyse est axée sur la position des acteurs vis-à-vis de la situation actuelle, c'est-à-dire de la domination de Microsoft Azure à chaque appel d'offre publique, engendrant une problématique de souveraineté.

Les acteurs engagés, comme OVH Cloud, Scaleway, et l'ANSSI, soutiennent activement le projet en raison de l'importance de la souveraineté numérique et de leur implication dans le cloud souverain. Ils sont pour un traitement ainsi qu'un hébergement des données de santé en France, par un hébergeur français. Ils estiment être victimes d'injustice quant au choix de Azure Microsoft.

Les acteurs alliés, tels que certaines startups françaises de la HealthTech, notons OWKIN, qui est bien impliqué dans des projets liés au Health Data Hub. Spécialisée dans l'intelligence artificielle (IA) appliquée à la recherche médicale, elle a été sélectionnée dans plusieurs initiatives impliquant le HDH, notamment pour des projets visant à accélérer les découvertes en médecine grâce à l'utilisation de données de santé. D'autre part, nous avons les institutions publiques qui sont favorables également, mais n'ont pas un engagement aussi fort. Ils nécessitent des incitations supplémentaires (formations, financements…) pour renforcer leur soutien et leur adhésion complète au projet.

Les acteurs neutres incluent les hôpitaux, qui bénéficient indirectement du Health Data Hub sans avoir une position stratégique clairement définie, ou encore les Hôpitaux qui ont leur propres serveurs et modes de stockage de leurs données.

Côté acteurs contradicteurs, certains partis politiques comme le PCF, LR et le PS entre autres ; ainsi que certains industriels français, cherchent à influencer la situation actuelle du HDH et semblent être opposé au projet « dans l'état actuel des choses » pour le faire correspondre à leurs préoccupations liées à la domination des acteurs étrangers, notamment américains, dans le secteur du cloud. Ils agissent activement, et expriment leurs inquiétudes auprès des commissions d'enquête en faveur d'une migration vers une solution d'hébergement des données en France par un hébergeur français.

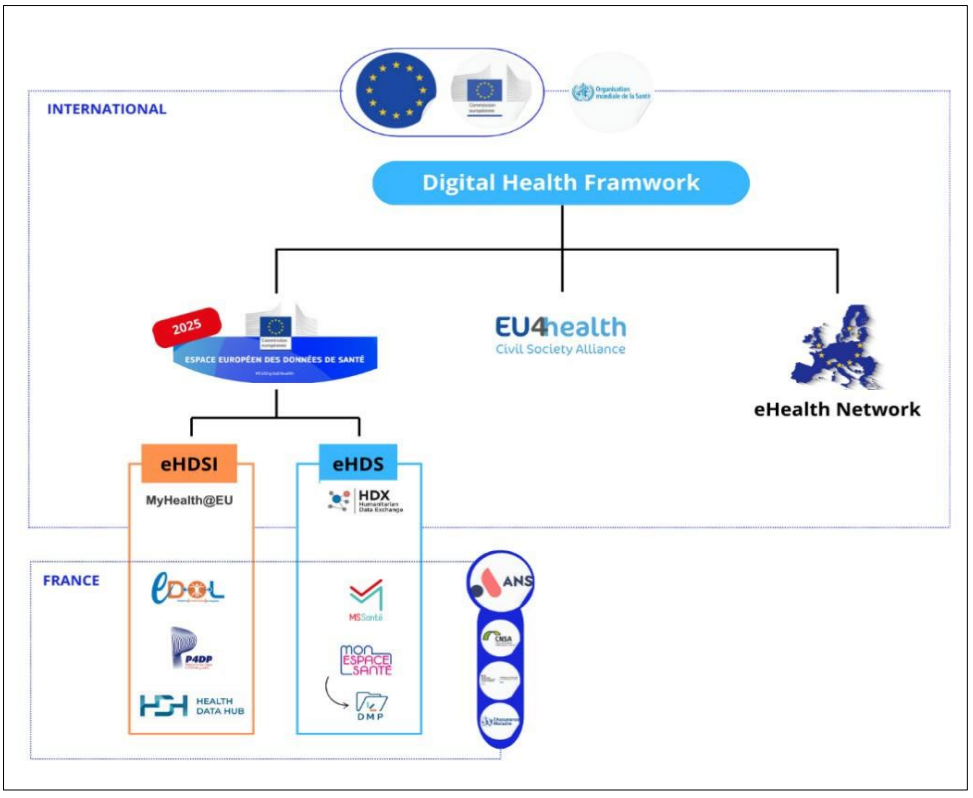
Enfin, les acteurs opposants, comme Amazon AWS et Google Cloud, sont en désaccord avec certaines obligations de cahier de charge, tels que le Secnumcloud (impossible de l'obtenir si l'entreprise est détenue collectivement à plus de 39% par une entreprise basée hors UE), ou encore le fait que Microsoft puisse avoir le contrat sans même remplir ces conditions et sans appel d'offre.

Microsoft Azure, quant à lui, est vu comme un adversaire, étant à la fois un fournisseur de services cloud pour le Health Data Hub et une menace perçue en raison de sa position dominante et des enjeux liés à la souveraineté. Des inquiétudes existent concernant le fait que les données soient stockées dans les serveurs de Microsoft France, dont la maison mère est basée aux USA, donc par le principe d'extraterritorialité du droit, c'est le droit américain qui prime sur le droit français (Cloud Act…), et les données de 67M de français peuvent se retrouver entre les mains des autorités américaines.

B. L’application/implication des normes actuelles dans le système d’interopérabilité des systèmes de santé européens.

1. État de l’art des systèmes d’informations de santé

La complexité des écosystèmes de santé européens et français témoigne de la sophistication des systèmes d’interopérabilité qui les structurent. Il est essentiel de fournir une vue d'ensemble des projets majeurs d’interopérabilité en cours, afin de mieux comprendre les principaux acteurs et programmes qui soutiennent ces initiatives :



Écosystème des projets de santé européens et français

De nombreux programmes d’interopérabilité de santé européens sont développés depuis 2020 comme l’actuel programme de création d’une plateforme commune d’échanges des données de santé, régie par le programme « Espace Européen des Données de Santé » (EHDS). Cette entreprise européenne encourage le développement d’initiatives nationales portant sur l’interopérabilité des systèmes de santé. Acteur principal dans l’implémentation de ces programmes, l’ANS – superviseur des parties prenantes de la santé en France – semble pleinement y intégrer les exigences développées par les projets européens. En tant que membre influent de l'Union européenne, la France s'inspire largement des initiatives européennes, qui

orientent les politiques nationales en matière de santé et d'interopérabilité. Les projets visent ainsi à optimiser l'efficacité des systèmes de santé et à garantir une meilleure interconnexion des données, tout en répondant aux défis contemporains. Toutefois, chaque projet présente un périmètre spécifique et est déployé à des échelles variées, en fonction de ses enjeux et de ses objectifs.

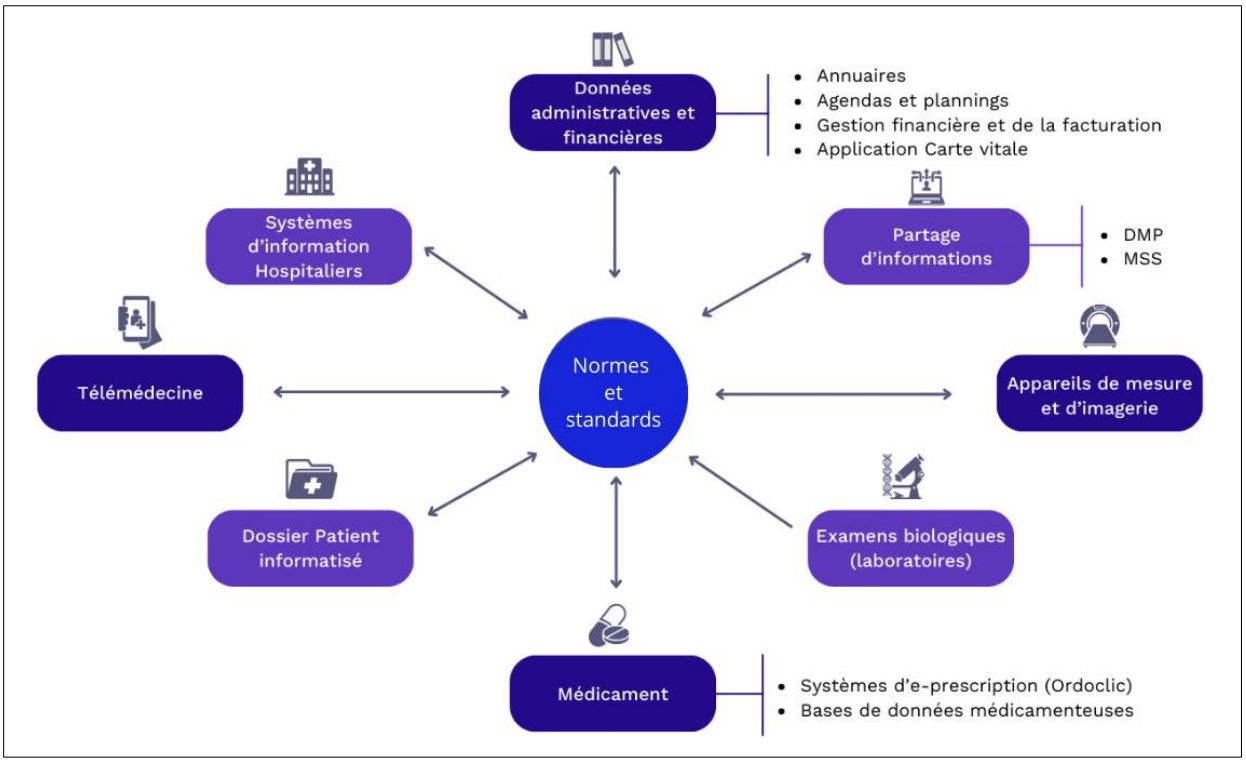
Echelle	Type	Intitulé	Description	Périmètre d'application	Objectifs	Acteurs d'implémentation
Européenne	Health Data Exchange	**EHDS**	Espace Européen des Données de Santé	Partage des données de santé européens	Créer d'un espace numérique des données européen commun dans un domaine.	Commission Européenne/OMS
Européenne	Infrastructure	**eHDSI**	European Health Data Space Initiative	Infrastructure supportant le projet EHDS	Mettre en place des infrastructures techniques et organisationnelles nécessaires pour réaliser l'EHDS.	Union Européenne
Européenne	Projet de financement	**EU4Health**	EU pour la Santé	Financement des projets de santé publique	Financer les projet dans la santé publique et la sécurité sanitaire.	Union Européenne
Européenne	Health Data Exchange	**eHealth Network**	Réseau eSanté	Partage entre les autorités nationales de santé	Connecter les autorités nationales responsables de la santé en ligne.	Union Européenne
Francaise	Plateforme e-santé	**Mon Espace Santé**	Espace numérique de Santé	Plateforme pour professionnels et patients sur la santé numérique	Centraliser les informations médicales personnelles (DMP, ordonnances, résultats d'examens) et offrir un accès sécurisé aux citoyens.	Caisse Nationale de l'Assurance Maladie
Francaise	Outil de gestion des données de santé	**DMP**	Dossier Médicale Partagé	Outil de centralisation des données médicales	Permettre aux professionnels de santé d'accéder au dossier médical complet d'un patient pour améliorer la coordination des soins.	Caisse Nationale de l'Assurance Maladie
Francaise	Plateforme e-santé	**P4DP**	Plateform for Data in Primary Case	Partage entre professionnels des données de santé pour la médecine générale.	Faciliter l'échange de documents médicaux pertinents entre les différents professionnels de santé impliqués dans la prise en charge d'un patient.	Consortium d'acteurs Health Data Hub
Francaise	Messagerie numérique	**MS Santé**	Messagerie Sécurisée de Santé	Messagerie entre professionnels pour s'échanger les données de santé	Partager une messagerie sécurisée pour l'échange de données sensibles entre professionnels de santé.	Agence du Numérique en Santé Ministère de la Santé
Francaise	Entrepot de Données de Santé	**eDOL**	Entrepot de Données de Santé du Languedoc	Outil de collecte et structuration d'informations de santé (niveau régional)	Collecter en une base unique les données patients des établissements du GHT ESt-Hérault Sud Aveyron	CHU de Montpellier
Francaise	Plateforme e-santé	**Health DataHub**	Plateforme de données de santé	Accès des données de santé pour la recherche	Centraliser et faciliter l'accès sécurisé aux données de santé à des fins de recherche et d'innovation en mobilisant les données massives (BigData).	Groupement d'Intérêt Public

Présentation des projets d'interopérabilité européens et français

L'ensemble de ces projets est interconnecté, d'une part grâce à l'implication des différentes parties prenantes, et d'autre part, par l'intégration de normes visant à standardiser les systèmes de santé concernés.

2. La standardisation des systèmes d'interopérabilité par la mise en place de normes

Les normes d'interopérabilité standardisent les échanges et facilitent les interactions entre les acteurs de la santé numérique, tout en assurant la sécurité des données. Elles établissent un cadre technique universel, comme FHIR et HL7 pour les données cliniques ou DICOM pour l'imagerie médicale, permettant ainsi une communication efficace entre hôpitaux, laboratoires et cabinets médicaux tout en réduisant les incompatibilités et ceci même à l'international.



Interopérabilité des données de santé par les normes

Ces normes soutiennent les projets vus précédemment en assurant une interopérabilité immédiate et en limitant les coûts liés à des solutions personnalisées. Elles unifient également les pratiques en facilitant les échanges entre acteurs, adaptées aux spécificités nationales via des référentiels comme le CI-SIS.

Enfin, en alignant leur cadre sur le RGPD, ces normes garantissent la sécurité des informations sensibles par des mécanismes de chiffrement, d'authentification et de traçabilité, avec des infrastructures conformes, comme celles des Hébergeurs de Données de Santé (HDS).

En France et en Europe, il existe différentes normes qui garantissent cette interopérabilité (cf. Annexe 1).

Comparaison des normes et régulations

Comme le montre le benchmark disponible en Annexe 1, FHIR s'impose progressivement comme un standard moderne et flexible pour l'échange de données en temps réel, grâce à sa compatibilité avec des technologies web. En parallèle, la norme HL7 Version 2 reste très utilisée dans les systèmes hospitaliers plus anciens, alors que HL7 Version 3 et CDA apportent une structure rigide pour des documents cliniques complexes. Toutefois, FHIR tend à remplacer ces versions historiques grâce à sa modularité et sa polyvalence.

D'autres standards jouent un rôle clé dans des domaines plus ciblés. DICOM est incontournable dans le domaine de l'imagerie médicale, tandis que SNOMED CT offre une terminologie médicale exhaustive pour assurer une interopérabilité sémantique, même si sa complexité et son coût limitent son adoption. En complément, des

standards comme LOINC, qui, standardisent les résultats de laboratoire, alors que des classifications comme la CIM-10 et sa version modernisée CIM-11 structurent les diagnostics. Par ailleurs, des normes émergentes telles que OMOP-CDM répondent

aux besoins croissants d'analyse des données massives dans la recherche épidémiologique, tandis que des initiatives comme BEACON standardisent les données génomiques pour la médecine de précision. Osiris, spécifique à la France, se concentre, elle sur la gestion des registres médicaux.

Enfin, les normes françaises comme HPRIM et PN13-IS, bien qu'en déclin ou limitées à un usage local, ont contribué à structurer les échanges dans des systèmes historiques et continuent d'interagir avec des standards globaux comme FHIR.

Ces standards collaborent souvent entre eux : par exemple, FHIR et HL7 intègrent des terminologies comme SNOMED CT, LOINC et la CIM-10, tandis que IHE propose des cas d'usage concrets pour faciliter l'intégration entre différents systèmes (PACS, laboratoires, hôpitaux). À travers ces interactions, ils offrent une interopérabilité complète, essentielle à la réussite des projets nationaux tels que Mon Espace Santé ou le Dossier Médical Partagé (DMP), tout en alignant les pratiques françaises sur les standards internationaux.

Focus HL7

Comme l'a démontré le benchmark, FHIR développé par l'organisation HL7 International (HL7 Int.), s'impose aujourd'hui comme une norme globale de référence capable de répondre à une majorité des besoins en matière d'interopérabilité des systèmes de santé. Sa flexibilité, sa modularité et son adaptation aux technologies modernes en font un standard idéal pour l'échange rapide et sécurisé des données de santé dans des environnements hétérogènes.

HL7 International est une organisation basée aux États-Unis, qui conçoit, maintient et publie des normes d'interopérabilité pour faciliter l'échange d'informations de santé à l'échelle mondiale. Son ambition est de garantir que ces standards puissent être exploités et adaptés dans n'importe quel pays, tout en respectant les spécificités locales. Cette vocation mondiale est assurée grâce à des branches affiliées régionales (Europe, Amérique du Nord, Asie, etc.), qui traduisent, adaptent et implémentent ces standards dans leurs contextes nationaux ou continentaux. Les branches affiliées collaborent étroitement avec la maison mère HL7 Int., qui assure le financement et la gouvernance stratégique pour garantir une cohérence globale.

La dernière norme FHIR, qui repose sur la norme ISO 27931 (une référence internationale pour la structuration des messages d'échanges d'informations en santé) s'appuie sur une approche modulaire où chaque ressource (patient, observation, diagnostic, etc.) est indépendante mais interconnectée. Cette conception innovante lui permet de se démarquer des normes historiques comme HL7 V2 et HL7 V3 qui, bien qu'encore largement utilisées, manquent de flexibilité dans les environnements modernes.

Grâce à FHIR, il est désormais possible de faciliter :

- La communication en temps réel entre systèmes de santé (hôpitaux, laboratoires, cabinets médicaux) ;

- L’interopérabilité entre des solutions anciennes et modernes ;
- L’intégration avec des standards complémentaires comme SNOMED CT pour la sémantique, LOINC pour les observations, et DICOM pour les images médicales.

En résumé, FHIR est devenu un standard central en raison de sa capacité à unifier et simplifier les échanges de données dans un système de santé mondialisé et digitalisé, tout en s’intégrant harmonieusement avec les autres normes existantes. Son adoption croissante dans des projets majeurs comme Mon Espace Santé ou le Health Data Hub témoigne de son potentiel à devenir un standard universel.

3. L'existence d'une influence des normes HL7 sur l'interopérabilité des systèmes de santé

La principale force de HL7 réside dans sa capacité à simplifier les échanges et à couvrir l'intégralité des flux d'information des systèmes de santé, tels que la facturation, les prescriptions médicamenteuses, les données patients, etc. Cette fonctionnalité lui confère une légitimité solide pour son adoption dans la majorité des projets européens et français précédemment évoqués. Dès leur mise en place, plusieurs programmes ont adopté le standard HL7, en particulier dans des outils d'interopérabilité déployés en France, comme le Dossier Médical Partagé (DMP), le système MS Santé, ainsi que dans le projet du Health Data Hub, une plateforme nationale visant à centraliser et à sécuriser l'accès aux données de santé.

Dans ce cadre, l'initiative Interop'Santé joue un rôle clé en renforçant l'interopérabilité des systèmes de santé français, et en soutenant l'adoption de normes et de standards comme HL7.

Présentation d'Interop’Santé

Cette association française fédère les 3 organisations de standardisation d’interopérabilité dans le secteur de la santé : HL7 France, IHE et HPRIM. Son rôle est de promouvoir et d’accompagner l’implémentation des normes et standards d’échange afin d’assurer l’interopérabilité des systèmes d’information pour l’ensemble des acteurs du secteur de la santé en France. Créée en 2009, l’association compte aujourd’hui plus de 100 membres, incluant des acteurs de l’industrie des systèmes d’information en santé, des établissements et professionnels de santé, ainsi que des représentants des pouvoirs publics. Grâce à sa présence au sein de l’ensemble de l'écosystème de santé en France, Interop'Santé détient un rôle prépondérant dans la mise en œuvre des normes HL7 et FHIR dans les projets nationaux. Ce leadership se manifeste particulièrement par le partenariat établi en octobre 2020 avec l'ANS qui permet l'accès aux outils d’Interop'Santé pour ses tests d’interopérabilité.

L'une des missions d'Interop'Santé consiste à favoriser l'ouverture aux standards et normes internationaux, en particulier par la “promotion de ces standards”[xlvii] au travers

de formations, d'événements comme à la participation à la Semaine européenne de la E-santé avec l'ANS et de mise en place d'outils. Par cette démarche, Interop'Santé s'engage pleinement dans la promotion de l'adoption de la norme HL7 auprès des acteurs du secteur de la santé. Cette initiative s'inscrirait dans une stratégie d'influence, tant pour Interop'Santé que pour HL7. En effet, HL7, en collaborant avec Interop'Santé, partage cette approche en mettant en avant des axes stratégiques tels que « la promotion de l'implémentation des standards via les affiliés nationales » avec HL7 France, ainsi que « la collaboration avec les experts » et « l'éducation des industriels et des décideurs »[xlviii]. Ces objectifs viseraient donc à étendre l'utilisation des normes dans tout l'écosystème de santé français.

Cette influence se traduit également par une potentielle problématique vis à vis des enjeux de la souveraineté française au sein de HL7 (utilisé par le HDH). En effet, la directrice de HL7 International, Julia Skapik, figure également au sein du comité de HL7 Europe. À cette dernière, s'ajoutent quatre autres ressortissants américains ayant un poste de direction au sein de la branche européenne. L'influence de la maison mère américaine sur sa déclinaison Outre-Atlantique, et donc française, peut ainsi se deviner.

Ainsi, l'interopérabilité des systèmes de santé connait une révolution grâce à l'impulsion de nombreux projets européens et français. La création de normes d'interopérabilité comme HL7, adoptée par la plupart des projets, permet une synergie efficace entre les systèmes de santé européens. Cependant, cette standardisation est sujette à de véritables stratégies d'influences, qui s'étendent à travers l'ensemble de l'écosystème de santé. Cet impact ne parait pas sans conséquence pour la souveraineté européenne voire française.

C. Comparaison des stratégies internationales concurrentes

1. France : Naïveté stratégique ou calcul politique ?

En France, la protection des données de santé repose sur un cadre juridique robuste, articulé autour de lois nationales et de réglementations européennes comme le RGPD. Ce système vise à garantir la sécurité et la confidentialité des données sensibles, tout en permettant leur utilisation à des fins légitimes, notamment la recherche.

Le cadre juridique des données de santé en France évolue dans un environnement complexe, composé d'acteurs, publics et privés, dont les interactions donnent naissance à de nouvelles lois, en constante évolution.

Tout d'abord, l'essentiel des lois existantes en France est actuellement en vigueur à travers :

- Le Code de la Santé Publique (Article L1110-4) : Il consacre le secret médical et impose la confidentialité des données de santé collectées par les professionnels.
- La Loi de Modernisation de notre système de Santé[xlix] : a créé le Système National des Données de Santé (SNDS) pour regrouper et exploiter les données de santé à des fins de recherche, de suivi des politiques publiques et d'amélioration des soins. L'accès est strictement encadré (CNIL, anonymisation) pour garantir la confidentialité et protéger les citoyens.
- La Loi Informatique et Libertés (1978, révisée en 2018)[l] : Elle garantit le droit des individus à la maîtrise de leurs données personnelles. Par exemple, un laboratoire doit obtenir le consentement explicite d'un patient avant d'utiliser ses données pour une recherche clinique.
- Le Décret n° 2016-993[li] : Instaurant le *Health Data Hub* pour centraliser et anonymiser les données de santé en France.
- La Certification HDS (Hébergeurs de Données de Santé) : Imposée aux prestataires pour garantir un haut niveau de sécurité des infrastructures numériques.

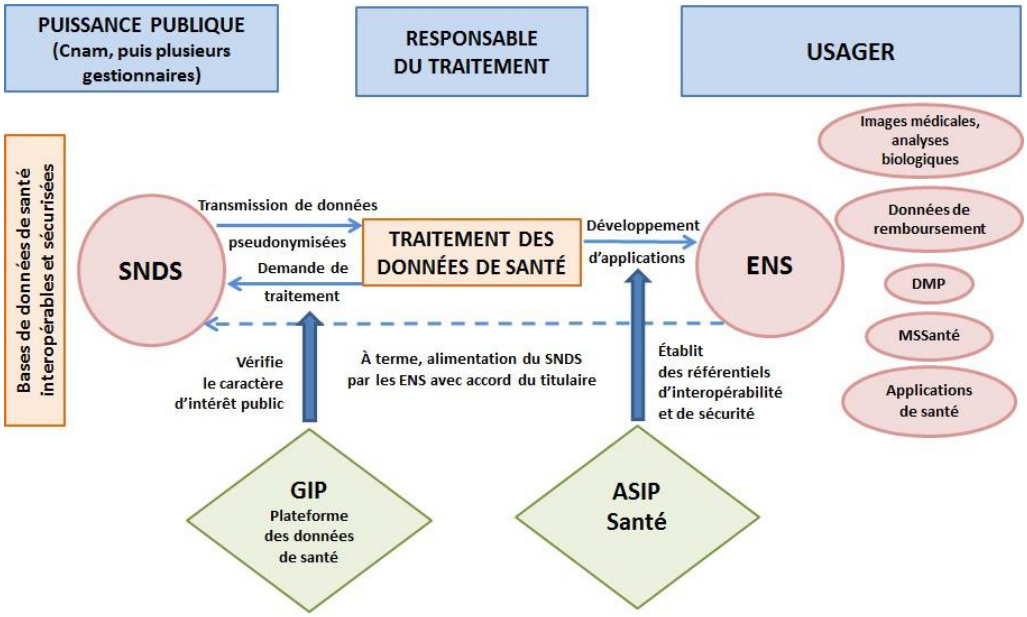
Bien que les acteurs nationaux soient au cœur du dispositif, le RGPD, entré en vigueur le 25 Mai 2018 en France, s'impose comme une norme cadre, renforçant les exigences en matière de consentement et de sécurité.

En termes d'acteurs publics, le ministère de la Santé pilote les stratégies globales, appuyé par la CNIL, qui veille à la conformité des traitements de données.

Ils sont épaulés par le *Cesrees*, un comité éthique et scientifique dédié, qui s'assure de l'intérêt public dans l'utilisation des données de santé.

L'Espace Numérique de Santé (ENS) et le Système National des Données de Santé (SNDS) travaillent en coordination pour la gestion et le traitement des données de santé.

Le premier se confond avec un carnet de santé numérique et permet d'améliorer la gestion des données. Le second permet une utilisation cohérente et sécurisée de ces dernières pour améliorer la recherche.



Rapport de la Commission des affaires sociales du Sénat, 12 juillet 2023

Le schéma ci-dessus permet d'illustrer les différents rôles et actions des agences et institutions étatiques autour de la gestion de nos données. Il est issu du rapport d'information « *Données de santé : une réforme encore en cours de chargement* » venant de la commission des affaires sociales du Sénat, déposé le 12 juillet 2023[lii].

L'Agence du Numérique en Santé (ANS), quant à elle, développe des infrastructures sécurisées.

Enfin, le *Health Data Hub* est central dans la gestion des données pour la recherche, tandis que les hôpitaux publics assurent le traitement direct des données des patients.

Parmi les entreprises privées, *OVH Cloud*, le plus grand hébergeur Français, se distingue par ses solutions souveraines conformes aux normes HDS.

Doctolib, facilitateur de rendez-vous, gère les données personnelles ainsi que les dossiers médicaux, tandis que Dassault Systèmes propose des outils de modélisation adaptés à la santé, avec notamment l'important rachat de Medidata en 2019.

Les hôpitaux privés de santé, rassemblés dans des grands groupes comme Ramsay Générale Santé, Elsan, Vivalto Santé et Almaviva, traitent les données des patients.

Les assureurs comme AXA et ou ALLIANZ utilisent les données de santé dans un cadre strictement réglementé, notamment pour personnaliser leurs offres ou avoir une meilleure évaluation des risques.

Les laboratoires pharmaceutiques, quant à eux, exploitent ces données pour développer leurs produits ou mener des essais cliniques.

Une partie des collaborations, entre acteurs publics et privés, passent par le *Health Data Hub*.

Ce dernier a été créé afin de centraliser et de mettre à disposition les données de santé pour stimuler la recherche et l'innovation.

Cependant, ces collaborations soulèvent des enjeux de souveraineté numérique et de contrôle des données sensibles.

La stratégie française en matière de cloud computing ambitionne de conjuguer innovation technologique, souveraineté numérique et sécurité des données. Toutefois, face à la montée des cybermenaces et à la prédominance des hyperscalers internationaux, cette approche, bien que présentée comme pragmatique et ambitieuse, soulève des interrogations. Malgré la mise en avant de concepts tels que la doctrine « cloud au centre » ou le cadre du cloud souverain, la réalité témoigne de limites structurelles et d'un déséquilibre persistant en faveur des acteurs étrangers.

La doctrine « cloud au centre », mise à jour en mai 2023, constitue la pierre angulaire de la stratégie française en matière de cloud[liii]. Elle s'adresse principalement aux administrations publiques et aux entreprises manipulant des données critiques ou stratégiques. Elle fixe des règles strictes pour garantir une adoption du cloud dans un cadre sécurisé et souverain.

L'une des exigences fondamentales de cette doctrine est l'utilisation de solutions labellisées SecNumCloud, délivrées par l'ANSSI. Ce label, accessible uniquement aux opérateurs français, garantit que les services cloud respectent des normes élevées en matière de cybersécurité et de protection des données. Les fournisseurs labellisés, comme OVHcloud et Outscale, s'engagent à protéger les données des ingérences étrangères, notamment celles permises par le **Cloud Act américain**[liv] qui autorise l'accès aux données stockées par des entreprises américaines, même hors des États-Unis. Le cas du HDH en est un exemple avec son hébergement sur le Cloud de Microsoft Azure.

Un autre objectif de la doctrine est de moderniser les infrastructures IT de l'administration, afin de favoriser leur migration vers des environnements cloud tout en maintenant un contrôle strict sur les données critiques. À titre d'exemple, certains ministères utilisent des solutions de messagerie sécurisée développées par des acteurs français, garantissant ainsi leur conformité avec les standards SecNumCloud.[lv]

Enfin, la doctrine vise à renforcer la collaboration entre acteurs publics et privés. L'État s'appuie sur des partenaires technologiques locaux pour développer des solutions innovantes tout en minimisant les risques de dépendance envers les géants internationaux. Par exemple, un projet comme NumSpot[lvi], qui réunit Docaposte, Dassault Systèmes et Bouygues Telecom, illustre cet effort de mutualisation des ressources.

Dans un autre domaine d'application de sa stratégie, la France distingue deux types de modèles cloud pour répondre aux défis de souveraineté : le cloud souverain et le cloud de confiance.

Le premier**,** dit "cloud souverain"[lvii] repose sur des infrastructures opérées uniquement par des acteurs nationaux ou européens, indépendants des régulations extraterritoriales. Ce modèle est privilégié pour les données d'une sensibilité particulière, notamment dans les secteurs de la défense, de la santé et des finances publiques. Des entreprises comme Outscale[lviii] (filiale de Dassault Systèmes) sont en première ligne pour répondre à ces besoins spécifiques.

Le cloud dit de "confiance"[lix], quant à lui, autorise des collaborations avec des hyperscalers internationaux, à condition que leurs solutions soient hébergées localement et opérées par des entreprises françaises. Microsoft Azure, en partenariat avec Orange et Capgemini, en est un exemple marquant[lx]. Ce modèle hybride, bien que controversé, permet d'accéder à des technologies avancées tout en respectant les exigences de sécurité nationales.

Les clouds de confiance représentent la solution la plus prometteuse. Allier l'expertise technologique des géants américains avec les garanties de sécurité et de souveraineté exigées par les cadres réglementaires français et européens. Des projets comme S3NS[lxi], développé en partenariat entre Thales et Google[lxii], illustrent bien cette vision. Cette approche permettrait aux entreprises françaises et européennes d'accéder à des technologies avancées tout en respectant des normes de gouvernance et de protection des données imposées localement. En revanche, ce modèle soulève des inquiétudes quant à l'extraterritorialité du droit américain, qui pourrait permettre aux autorités américaines d'exiger l'accès aux données, même lorsqu'elles sont hébergées sur des infrastructures localisées en France. Ainsi, bien que les clouds de confiance offrent une solution pragmatique et prometteuse, ils ne dissipent pas totalement les risques juridiques[lxiii] liés à l'implication d'acteurs américains. Cette double contrainte, entre opportunités technologiques et enjeux de souveraineté, pourrait structurer durablement le marché européen du cloud tout en alimentant un débat sur les alternatives à long terme pour une véritable indépendance numérique.[lxiv]

Côté réglementation, La France s'appuie sur un cadre réglementaire robuste pour garantir une utilisation sécurisée du cloud. Le RGPD s'impose déjà des obligations strictes pour les fournisseurs cloud opérant en Europe. À cela s'ajoute la loi « Sécuriser et réguler l'espace numérique »[lxv], adoptée en 2023, qui fixe des exigences spécifiques pour les opérateurs d'importance vitale (OIV).

Le label SecNumCloud demeure toutefois l'outil central de cette stratégie, bien que critiqué pour sa complexité et son coût, qui peuvent freiner les petites entreprises. En effet, le label présente deux limites sur le plan économique : d'une part, il peut freiner l'innovation puisque les entreprises, une fois le label obtenu, hésitent à modifier leur produit par crainte de le perdre. D'autre part, il n'empêche pas les hypers américains de proposer leurs services en France, en déployant leurs solutions logicielles Paas ou

Saas sur une infrastructure gérée par une entreprise française, ce qui leur permet de capturer une grande partie de la valeur. Néanmoins, le label garantit un haut niveau de conformité et de protection des données.

Enfin, l'hybridité des infrastructures[lxvi] cloud est un choix pragmatique adopté par de nombreuses entreprises françaises. Cette approche[lxvii] permet de combiner les avantages des clouds publics (flexibilité et coût réduit) avec ceux des clouds privés ou souverains (sécurité accrue).

Dans cette optique, deux cas d'études se démarquent : le choix d'EDF, en 2023, de collaborer avec [lxviii]AWS pour héberger certaines de ses données. Ce partenariat vise notamment à utiliser les capacités avancées du cloud public pour la maintenance prédictive de ses centrales nucléaires et d'autres applications non critiques. Toutefois, cette décision a suscité des interrogations quant à la souveraineté numérique et à la sécurité des données sensibles de l'entreprise. Pour pallier ces préoccupations, le groupe EDF s'est également tourné vers des solutions de cloud souverain en collaboration avec des partenaires nationaux comme NXO[lxix]. Ces initiatives garantissent que les données critiques, essentielles à la sécurité énergétique française, restent sous le contrôle de l'État et sont protégées contre des réglementations extraterritoriales telles que le Cloud Act américain. EDF illustre ainsi une stratégie hybride, combinant l'innovation offerte par les hyperscalers et la souveraineté apportée par des solutions locales.

Deuxième cas, celui de la SNCF, qui a migré environ 7 000 serveurs et 250 applications vers AWS[lxx], s'appuyant sur le cloud public pour renforcer l'efficacité de ses opérations numériques. Ce choix vise à améliorer la résilience, la capacité d'innovation et la flexibilité des services informatiques de l'entreprise. Toutefois, consciente des risques liés à une dépendance exclusive à un fournisseur étranger, la SNCF adopte une approche multicloud[lxxi] (ou "fullcloud"). En plus d'utiliser AWS pour des applications courantes, elle prévoit d'intégrer des solutions de cloud souverain dès leur disponibilité. Cette approche garantit la protection des données critiques et répond aux exigences de souveraineté imposées par le cadre réglementaire français et européen. En alliant cloud public et souverain, la SNCF illustre la complexité des défis liés à l'adoption du cloud dans les grandes entreprises.

Cette hybridité reflète aussi une volonté de limiter les dépendances envers les hyperscalers, tout en profitant de leurs innovations technologiques.

La stratégie française en matière de cloud computing est un modèle d'équilibre entre dépendance et souveraineté. En mettant en œuvre des politiques comme le « cloud au centre », en encourageant des collaborations entre acteurs locaux et internationaux, et en renforçant son cadre législatif, la France affirme sa position comme un acteur clé de la gouvernance numérique. Cependant, des défis subsistent, notamment en termes d'innovation et d'investissement dans des technologies compétitives face aux hyperscalers. La réussite de cette stratégie dépendra donc de

la capacité de l’écosystème français à conjuguer indépendance technologique et compétitivité économique.

L’histoire du cloud souverain en France a été marquée par plusieurs échecs retentissants, révélant des erreurs stratégiques et un manque de maturité de l’écosystème numérique. Ces échecs soulignent l'importance de tirer des leçons afin d’éviter de répéter les mêmes erreurs à l'avenir.

En 2009, le gouvernement français initie le projet Andromède, un partenariat public-privé visant à développer un cloud souverain capable de concurrencer les hyperscalers américains comme AWS. Ce projet répond à des préoccupations stratégiques, notamment la montée en puissance du Patriot Act de 2001, qui autorise les autorités américaines à accéder à des données stockées hors des États-Unis. L’ambition était claire : créer un acteur national solide, en collaboration avec Orange, Thales et Dassault Systèmes, soutenu par une enveloppe publique de 150 millions d’euros, gérée par la Caisse des Dépôts et Consignations.

Cependant, des désaccords entre les industriels ont rapidement freiné le projet. Incapables de s’entendre, les partenaires se sont divisés, conduisant l’État à investir 75 millions d’euros dans deux projets concurrents : Cloudwatt, lancé par Orange et Thales, et Numergy, soutenu par SFR et Bull (en remplacement de Dassault Systèmes). Cette fragmentation a affaibli la stratégie initiale, sapant l’objectif de créer un acteur unique capable de rivaliser avec les géants américains.

Entre 2011 et 2015, la création de ces deux entités concurrentes a aggravé les problèmes structurels du projet. Le marché français du cloud manquait de maturité, les offres proposées se limitaient à de simples services d’hébergement, sans véritable différenciation ni cas d’usage adaptés. Par ailleurs, l’investissement s’est concentré sur des solutions logicielles, sans développement d’infrastructures physiques robustes, essentielles pour rivaliser avec AWS ou Microsoft Azure.

Les entreprises françaises n'ont pas adopté massivement ces solutions, en raison d’un manque de directives claires de l’État pour favoriser leur usage, notamment au sein des administrations publiques et des collectivités territoriales. En parallèle, les géants américains poursuivaient leur avancée technologique et commerciale, rendant toute concurrence encore plus difficile.

En 2013, c’est autour des révélations d’Edward Snowden sur la surveillance massive opérée par les États-Unis de mettre sous le feu des projecteurs les risques de dépendance aux services cloud américains. Pourtant, cet événement n’a pas permis de relancer les initiatives françaises. L’incapacité à répondre rapidement aux attentes d’un marché exigeant et l’absence d’une vision stratégique unifiée ont continué à freiner le développement des solutions nationales.

L’adoption du Cloud Act par les États-Unis en 2018 a fragilisé la confiance des acteurs économiques envers les hyperscalers américains, susceptibles d’accéder aux données stockées sur leurs infrastructures, où qu'elles se trouvent dans le monde. Cet

événement, qui a eu un effet toutefois limité sur les parts de marché des hyperscalers, aurait pu représenter une opportunité pour les acteurs français de proposer une alternative souveraine. Cependant, les retards accumulés et la fragmentation du marché ont empêché la France de capitaliser sur cette occasion.

Cette liste des échecs marquant de la politique française sur la question du cloud-computing, en particulier l'échec du projet Andromède et de ses dérivés ont eu des conséquences profondes : premièrement, un affaiblissement de l'acteur national OVHcloud, qui a dû faire face à une concurrence accrue au sein même du marché français. Suivie logiquement par une incapacité à créer des économies d'échelle suffisantes pour rivaliser avec les hyperscalers américains. Et pour finir, un retour sur investissement quasi nul, laissant les deux entités, Cloudwatt et Numergy, sans moyens financiers pour se développer face à leurs concurrents. Le résultat du projet a été que les deux entités ont été rachetées Cloudwatt par Orange en 2015, et Numergy par SFR en 2016, marquant la fin de "l'aventure Andromède".

L'échec de ce programme a mis en lumière des carences en termes de stratégie et d'approche. En outre, le constat est clair, il est nécessaire de relancer un programme d'investissement en adoptant une nouvelle stratégie dans les secteurs d'avenir d'ici la fin de la décennie.

Le programme France 2030 incarne une stratégie ambitieuse visant à positionner la France comme un leader mondial dans le domaine de la santé numérique. Cet objectif s'inscrit dans une vision à la fois technologique, économique et sociétale, visant à transformer durablement le système de santé et à renforcer la souveraineté nationale face aux défis globaux. Avec une enveloppe totale de 718,4 millions d'euros consacrée à la santé numérique, les investissements se répartissent entre plusieurs axes stratégiques et mobilisent un éventail d'acteurs publics et privés.

Les axes stratégiques de France 2030 dans la santé numérique sont tout d'abord l'innovation et la recherche. En effet, l'un des piliers de France 2030 est le soutien à la recherche et au développement dans le domaine des technologies de santé. Une enveloppe de 60 millions d'euros a été attribuée au Programme et Équipements Prioritaires de Recherche (PEPR)[lxxii] « Santé numérique », co-piloté par l'INSERM [Lxxiii] et l'INRIA[lxxiv]. Ce programme vise à développer des technologies de rupture, telles que l'intelligence artificielle appliquée au diagnostic et au traitement des maladies. En complément, 20 millions d'euros[lxxv] par an sont dédiés à l'évaluation clinique des dispositifs médicaux basés sur le numérique, favorisant ainsi leur accès au marché. Ces initiatives illustrent une approche centrée sur l'amélioration des solutions existantes tout en stimulant la création de nouvelles technologies.

Le deuxième axe intègre la formation et les compétences afin de répondre aux besoins en compétences dans un secteur en mutation rapide. Avec 81 millions d'euros alloués à la formation spécifique des acteurs de la filière et 48,4 millions supplémentaires pour la formation générale aux usages du numérique en santé[lxxvi], l'objectif est de former 100 000 apprenants par an. Cette initiative est essentielle pour garantir que les

innovations technologiques soient utilisées efficacement par les professionnels de santé et les patients.

Le troisième pilier se concentre sur les infrastructures et les territoires afin de favoriser le développement et le test des innovations en conditions réelles, France 2030 prévoit la création de 30 tiers-lieux d'expérimentation d'ici 2025, avec un budget total de 63 millions d'euros[lxxvii]. Ces infrastructures permettront aux entreprises et chercheurs de collaborer dans un cadre adapté à la mise en application de leurs solutions. De plus, la modernisation des infrastructures de santé, en particulier dans les territoires, est un autre volet important. Des fonds mobilisés par des acteurs tels que la Banque des Territoires[lxxviii] sont orientés vers des projets régionaux améliorant l'accès aux soins, notamment dans les zones sous-dotées en services médicaux.

France 2030 repose sur une mobilisation coordonnée de plusieurs acteurs, chacun apportant des contributions spécifiques pour garantir l'atteinte des objectifs fixés. Par exemple : Bpifrance[lxxix] : En tant que banque publique d'investissement, elle gère des appels à projets pour l'évaluation clinique des dispositifs médicaux. Elle soutient également les entreprises dans le financement de leurs projets de R&D. Aussi, La Banque des Territoires[lxxx] faisant partie de la Caisse des Dépôts, elle soutient des projets locaux innovants, notamment via des investissements dans les infrastructures et les initiatives territoriales. D'autres institutions comme la Région Île-de-France, par exemple, finance des associations et projets locaux via des subventions spécifiques et des appels à projets comme « Santé Numérique et Innovation », favorisant l'adoption de technologies numériques dans les établissements de santé et les territoires. Enfin, le Health Data Hub[lxxxi] sert de plateforme nationale facilitant l'accès aux données de santé pour les porteurs de projets, favorisant ainsi la recherche et le développement.

Malgré les ambitions affichées et les ressources mobilisées, le succès de France 2030 dans le domaine de la santé numérique repose sur 3 conditions. La première est la nécessité d'une simplification administrative. Les lourdeurs administratives et les délais réglementaires pourraient freiner l'émergence rapide des innovations. La deuxième est la coordination des acteurs. En effet, une meilleure synergie entre les différents acteurs, établissements de santé, industriels, régions et organismes de recherche est cruciale pour maximiser l'impact des investissements. La troisième est son rapport à la coopération internationale. Bien que la souveraineté technologique soit un objectif important, la France doit éviter une approche trop isolationniste qui pourrait limiter ses partenariats stratégiques. Elle doit aussi user de toute son influence pour peser dans l'adoption de standards internationaux afin d'avantager ses solutions.

2. Etats-Unis : innovation technologique ou instrument de domination ?

Le modèle américain se distingue nettement du modèle européen en confiant à l'initiative privée la responsabilité d'organiser le partage des données selon une approche libérale, à des fins commerciales, technologiques ou scientifiques.

Aux États-Unis, deux réglementations principales sont directement liées aux données de santé :

- Le *HIPAA (Health Insurance Portability and Accountability Act)* : Adoptée en 1996, cette loi protège les données de santé des patients tout en autorisant leur utilisation dans les soins médicaux[lxxxii]. Elle repose sur deux règles principales : la *Privacy Rule*, qui régule l'usage et la divulgation des informations de santé, et la *Security Rule*, qui impose des mesures pour sécuriser les données électroniques. Le non-respect de ces règles peut entraîner des amendes substantielles et des sanctions pénales.
- Le *HITECH Act (Health Information Technology for Economic and Clinical Health Act)* : Adoptée en 2009, cette loi encourage l'adoption des dossiers de santé électroniques (DSE) et renforce la sécurité des données, notamment en imposant des amendes en cas de violations de la confidentialité[lxxxiii]. Elle oblige aussi les prestataires de santé à adopter des mesures de sécurité plus strictes pour éviter les piratages et les fuites de données.

Il existe également des réglementations qui, bien qu'indirectement liées, concernent les données de santé :

- Le *CLOUD Act* : Adoptée en 2018, cette loi permet aux autorités américaines d'accéder aux données stockées par des entreprises américaines, même si elles se trouvent à l'étranger. Cela inclut les données de santé, ce qui soulève des questions de souveraineté et de confidentialité à l'échelle internationale.
- Le *FISA (Foreign Intelligence Surveillance Act)* : Depuis 1978, cette loi autorise les agences de renseignement américaines à surveiller les communications de personnes étrangères, y compris celles contenant des données de santé échangées électroniquement. Elle suscite des préoccupations, notamment en Europe. Concrètement, sa section 702 permet aux agences américaines de renseignement de collecter, utiliser et partager des données personnelles étrangères stockées sur des serveurs gérés par des fournisseurs de services cloud domiciliés aux États-Unis.

Aux États-Unis, plusieurs acteurs publics jouent un rôle clé dans la gestion des données de santé. Le *Department of Health and Human Services* (*HHS*), par exemple, supervise les initiatives fédérales en matière de santé publique. Il est également responsable de la mise en œuvre du *HIPAA*, qui protège la confidentialité des informations de santé personnelles.

D'autres organismes, comme les *Centers for Disease Control and Prevention* (*CDC*), utilisent ces données pour surveiller les maladies et promouvoir la santé publique. De son côté, la *Food and Drug Administration (FDA)* collecte et analyse des données relatives aux médicaments, dispositifs médicaux et produits alimentaires, afin de garantir leur sécurité et leur efficacité.

Dans le secteur privé, les entreprises occupent une place centrale dans la gestion des données de santé.

Les *GAMAM* figurent en tête, avec des initiatives comme *Google Health*, qui collecte des données via des appareils connectés, ou les outils d'*Apple (HealthKit, ResearchKit, CareKit)*, qui permettent aux utilisateurs de suivre leur santé et de participer à des recherches. *Amazon*, via *AWS Cloud*, et *Microsoft* avec *Microsoft Cloud for Healthcare*, offrent des solutions pour gérer, analyser et partager ces données.

D'autres entreprises davantage spécialisées, comme *Cerner et Epic Systems*, se concentrent sur les logiciels de gestion des dossiers de santé électroniques tandis que les assureurs (*UnitedHealth Group, Anthem*) exploitent des données détaillées pour optimiser leurs services. Enfin, les laboratoires pharmaceutiques (*Pfizer*, *Johnson & Johnson*…) utilisent des bases de données pour développer des traitements ciblés et identifier des patients spécifiques.

En 2010, le gouvernement Américain a lancé la stratégie "Cloud First"[lxxxiv], qui exigeait des agences qu'elles évaluent les options de cloud computing avant de faire de nouveaux investissements. Cette politique visait à accélérer l'adoption du cloud par le gouvernement afin de tirer parti des avantages de l'infrastructure partagée et des économies d'échelle. Elle a été lancée pour remédier aux inefficacités du gouvernement fédéral en matière de technologies de l'information, caractérisées par une faible utilisation des actifs, une demande fragmentée de ressources, des systèmes redondants et de longs délais d'approvisionnement. Parallèlement à cela, le gouvernement a lancé la Federal Data Center Consolidation Initiative (FDCCI) en février 2010, dans le but de consolider l'environnement fragmenté des datacenters du gouvernement fédéral et de fermer au moins 800 datacenters d'ici 2015. Le gouvernement cherchait à réduire ses dépenses en infrastructures de centres de données, qui représentaient environ 30 % des investissements en TI en 2010. Les agences ont été encouragées à utiliser le cloud computing pour compléter les efforts de consolidation des centres de données en déplaçant les charges de travail et les applications vers des infrastructures détenues et exploitées par des tiers. Ainsi, AWS GovCloud (US) lance sa première région Top Secret pour le gouvernement américain en 2014.

En 2019, le gouvernement américain a adopté une nouvelle stratégie appelée "Cloud Smart"[lxxxv]. Cette stratégie succède à "Cloud First" et vise à fournir des directives pratiques pour une mise en œuvre plus réfléchie des technologies basées sur le cloud

tout en tenant compte des réalités pratiques. Elle reconnaît que le terme « cloud » est souvent utilisé de manière générique, mais il est plus précisément appliqué aux solutions qui présentent les cinq caractéristiques essentielles du cloud computing définies par le National Institute of Standards and Technology (NIST) : service à la demande, large accès au réseau, mise en commun des ressources, élasticité rapide et service mesuré. La stratégie encourage les agences à envisager le cloud comme un éventail de solutions offrant de nombreuses capacités et options de gestion afin d'améliorer leur mission et la prestation de services.

Le "Cloud Smart" est axé sur trois piliers principaux : la sécurité, l'approvisionnement et la main-d'œuvre

Sur le volet sécurité, la stratégie met l'accent sur la protection des données à tous les niveaux, en adoptant une approche de défense en profondeur. Cela implique de ne pas seulement se concentrer sur la sécurité du réseau, mais aussi de renforcer la sécurité au niveau des données elles-mêmes. La sécurité doit être une considération primordiale lors de la planification et de l'implémentation de solutions cloud, en assurant la confidentialité, l'intégrité et la disponibilité des informations. La stratégie impose également l'utilisation de programmes comme Le Federal Risk and Authorization Management Program (FedRAMP), et le State Risk and Authorization Management Program (StateRAMP)[lxxxvi]. Ces deux programmes sont des programmes à l'échelle du gouvernement des États-Unis qui fournissent une approche standardisée en matière d'évaluation, d'autorisation et de surveillance continue de la sécurité des produits et services cloud. Dans les cas d'utilisation d'entreprise plus larges, les capacités du FedRAMP et du StateRAMP remplacent souvent celles stipulées dans les programmes de conformité du secteur tels que SOC2 et HIPAA.

Du Point de vue de l'approvisionnement, Il s'agit d'optimiser les pratiques d'achat des agences fédérales pour les solutions cloud. La stratégie Cloud Smart met en avant la gestion des catégories pour rationaliser les achats et éviter les doublons de contrats. Il est également important d'intégrer des exigences de sécurité et de confidentialité dans les processus d'approvisionnement. Les agences doivent définir clairement les rôles et les responsabilités dans les accords de niveau de service (SLA) avec les fournisseurs, et mettre en place des plans de continuité des activités. Un autre point crucial est d'éviter le verrouillage fournisseur en évaluant les dépendances des processus métiers.

De l'autre côté, concernant la main-d'œuvre, la stratégie reconnaît l'importance de l'investissement dans le personnel fédéral pour réussir la transition vers le cloud. Les agences doivent identifier les lacunes en matière de compétences et mettre en œuvre des programmes de requalification. Il est aussi essentiel de recruter et d'embaucher du personnel qualifié dans le domaine du cloud et de la cybersécurité en simplifiant le processus d'embauche. De plus, les agences doivent communiquer clairement avec leurs employés sur les changements à venir, y compris les nouvelles compétences requises et les ajustements possibles de poste.

Ainsi, dans la continuité de cette stratégie le Pentagone a récemment attribué des contrats, baptisée Joint Warfighting Cloud Capability (JWCC), d'une valeur totale de 9 milliards de dollars à quatre géants technologiques américains[lxxxvii] : AWS, Microsoft Azure, GCP et Oracle. Ces contrats, s'étendant jusqu'en 2028, visent à moderniser et sécuriser les infrastructures cloud du Département de la Défense des États-Unis. Les multinationales américaines profitent donc pleinement du “Cloud Smart”.

Les géants américains du numérique, ont su tirer parti de leur position dominante pour imposer une domination écrasante sur le marché mondial du cloud.

Leur approche repose d’abord sur une politique agressive de diminution constante des prix, illustrée par les « crédits cloud gratuits »[lxxxviii] jugés de “dumping déguisé”. Ces crédits cloud peuvent parfois atteindre 200 000 dollars sur deux ans ce qui rend les entreprises captives. Cette guerre des prix, parfois proche de la vente à perte, met en difficulté les concurrents locaux, qui peinent à suivre le rythme en raison de leurs ressources financières limitées. De plus, des pratiques anticoncurrentielles, telles que celles reprochées à Microsoft dans la plainte déposée par le CISPE[lxxxix], augmentent leur force de frappe à l'international.

En effet, la force des GAFAM repose sur leur maîtrise complète de la chaîne de valeur des données. Depuis la collecte des informations grâce à leurs dispositifs matériels comme l’Internet des objets (IoT), les téléphones mobiles et les ordinateurs, jusqu’au stockage, au traitement et à l’analyse. L’innovation joue un rôle central dans leur stratégie. Les GAFAM investissent massivement dans des technologies de pointe comme le calcul post-quantique, qui prépare les infrastructures à la prochaine génération de traitement de données. Ce contrôle, combiné à leurs solutions de cloud dans les catégories IaaS, PaaS et SaaS, leur permet d’offrir des écosystèmes préférentiels aux entreprises du secteur privé de la santé qui cherchent à rester compétitives face à leurs concurrents.

En parallèle, les GAFAM s’appuient sur une politique d’influence considérable pour s’imposer dans les institutions publiques et privées. Microsoft, par exemple, déploie des cycles de conférences tels que Microsoft Envision à travers l’Europe pour convaincre les décideurs. De plus, ces conférences s’accompagnent de diffusion de formations gratuites des solutions cloud[xc] facilitant grandement l’accessibilité aux différents acteurs économiques.

Les GAFAM sont très au fait de la volonté des états de nationaliser leurs infrastructures et de rendre obligatoire leur "cloud souverain", tel que le Brésil ou les Pays-Bas[xci].

La réponse des GAFAM ne s’est pas fait attendre[xcii]. A la suite de l’affaire Snowden, tous, à l'exception d'Amazon, ont signé une lettre ouverte à Barack Obama et aux parlementaires américains[xciii], pour leur demander de montrer l'exemple en matière de surveillance de communications électroniques. Mais à travers cette lettre au gouvernement américain ce sont tous les pays du monde auxquels les GAFAM se sont adressées. Elles ont listé cinq principes décrivant la libre circulation des données numérique et contre la surveillance des communications :

- Limiter la possibilité pour le Gouvernement de collecter des informations sur les utilisateurs (codifier des limitations dans la loi, et s'interdire toute collecte massive et non ciblée sur des utilisateurs prédéterminés).

- Supervision et responsabilisation (assurer l'indépendance des tribunaux qui accordent les autorisations de collecte, prévoir des procédures contradictoires, rendre publics les jugements importants…).

- Transparence sur les demandes étatiques (autoriser les entreprises à communiquer sur le nombre et la nature des demandes de communication de données, faire que les Gouvernements publient d'eux-mêmes des informations…).

- Respecter la libre circulation des informations (ne pas imposer de frontières au cloud).

- Éviter les conflits entre gouvernements (régler les conflits de juridiction par des accords internationaux).

L'objectif de ces grands principes serait d'interdire aux gouvernements d'imposer le stockage local des données, permettant ainsi leur libre circulation à travers les frontières, même si elles sont sensibles (médicales, financières, diplomatiques). Cette règle empêcherait l'Europe, dépendante des technologies des GAFAM, d'exiger que les données européennes soient hébergées localement, tandis que les États-Unis pourraient imposer aux entreprises américaines de stocker les données nationales sur leur territoire.

Aux États-Unis, les données de santé ne sont pas centralisées dans une base unique. Elles sont réparties entre différents acteurs, notamment les entreprises spécialisées dans les Dossiers Médicaux Électroniques (EHR), telles qu'Epic Systems, Cerner, et Allscripts. Ces entreprises, qui dominent le marché des EHR, jouent un rôle central dans la gestion des données des hôpitaux et des cliniques. Epic Systems, par exemple, gère les données de plus de 305 millions de patients[xciv]. Cependant, l'absence de standardisation entre ces différents systèmes crée des problèmes d'interopérabilité. Ainsi, en 2016, le 21st Century Cures Act, signé par le président Obama[xcv], a imposé aux systèmes de Dossier Médical Électronique (EHR) de fournir des API accessibles aux patients pour maintenir leur certification fédérale. En 2020, les Centers for Medicare & Medicaid Services (CMS**)** ont exigé que les prestataires et assureurs recevant des fonds fédéraux améliorent l'interopérabilité en facilitant l'accès aux informations de santé via des API sécurisées. Ces politiques renforcent l'échange de données pour offrir une vue globale des soins aux patients, prestataires et payeurs, tout en soutenant la santé publique.

Pour répondre à la demande croissante en stockage sécurisé et en traitement des données, ces entreprises EHR collaborent avec des fournisseurs de services cloud tels qu'AWS, Microsoft Azure, et GCP. Ces géants technologiques, qui disposaient déjà d'infrastructures avancées, ont adapté leurs services pour répondre aux exigences spécifiques des données de santé. AWS HealthLake[xcvi], par exemple,

permet non seulement de stocker des données, mais aussi de les analyser et de les rendre interopérables. Le rôle du gouvernement fédéral a été déterminant pour soutenir cette transition. Le HITECH Act de 2009 a injecté plus de 25 milliards de dollars[xcvii] pour encourager l'adoption des EHR. Avant l'adoption de cette loi, seulement 10 % des hôpitaux américains utilisaient des systèmes EHR certifiés ; ce chiffre a atteint 96 % en 2017 [xcviii]grâce aux incitations financières offertes par le programme. Ce financement a permis aux prestataires de santé de moderniser leurs infrastructures numériques via le programme Meaningful Use, qui exigeait non seulement la numérisation des dossiers, mais aussi leur interopérabilité et ainsi augmenter la part de marché des multinationales américaines.

3. La position allemande au sein du cadre juridique de l'UE : entre ambition de souveraineté et dépendance stratégique ?

Au sein de l'Union Européenne, plusieurs réglementations et législations ont pour but d'organiser la gestion des données de santé:

- Le règlement sur l'Espace Européen des Données de Santé (EHDS) crée un cadre d'échange sécurisé des données de santé au sein de l'UE.
- La directive sur les droits des patients en matière de soins de santé transfrontaliers simplifie l'accès des citoyens européens aux soins dans les pays de l'UE[xcix].
- Le règlement sur les dispositifs médicaux met en place la gestion des dispositifs médicaux, notamment ceux générant des données de santé.

Viennent s'ajouter d'autres règlements et législations qui traitent de manière plus globale la gestion de tout type de données, avec parfois une spécification pour les données de santé.

- Le *Data Act*, adopté en 2023, régule l'accès, l'utilisation et le partage des données pour bâtir une économie numérique équitable, tout en empêchant la monopolisation des données par les grandes entreprises. Venant en appui au *Data Governance Act* et au RGPD, il met l'accent sur la souveraineté des utilisateurs, la protection de leurs droits et l'accès aux données en cas de besoins publics exceptionnels.
- La Directive relative à la sécurité des réseaux et de l'information (*NIS Directive* 2016/1148) a pour but de renforcer la cybersécurité au sein de l'UE. Cette directive classe les données de santé comme sensibles, obligeant les opérateurs de services de santé à mettre en place des mesures de sécurité informatique importantes. Si un incident est déclaré, une notification publique est obligatoire.

- Le règlement européen sur l'IA encadre le développement, la marchandisation et l'utilisation des systèmes d'IA sur les secteurs à risques (Santé, Sécurité, Droits Fondamentaux…).
- Le règlement général sur la protection des données fournit un cadre harmonisé pour la protection des données personnelles. Dans ce règlement, les données de santé sont classifiées comme des données sensibles et sont traitées de façon rigoureuse.
- Le règlement sur la gouvernance des données *(Data Governance Act)*, en vigueur depuis septembre 2023, encadre le partage, l'utilisation et la gestion des données dans l'UE, notamment en facilitant leur réutilisation et en créant un cadre de confiance pour les intermédiaires. Il complète le RGPD en renforçant la gouvernance des données, tout en encourageant le partage volontaire et la coopération dans des secteurs clés comme la santé.
- Le règlement sur les services numériques *(Digital Services Act)*, adopté en 2022, modernise les règles des plateformes en ligne pour créer un environnement numérique sûr, transparent et équitable, tout en protégeant les droits fondamentaux. Il impose des obligations de modération des contenus, de transparence et de protection contre les contenus illicites, complétant ainsi le *Digital Market Act*.

Le principal acteur concernant la régulation des données de santé est la Commission Européenne, responsable de la stratégie de l'UE en matière de santé et du programme *EU4Health*[c], dont l'objectif est de renforcer les systèmes de santé et de données de santé sur un plan européen.

Le Parlement Européen, autre acteur majeur, est l'organe législatif de l'Union Européenne.

Son rôle est de proposer différents textes pouvant émaner d'acteurs privés ou bien d'organisations engagées, comme le *European Patients' Forum* (EPF), qui a pour principale mission la défense des intérêts des patients au niveau européen.

Au sein de ce conglomérat d'acteurs, il faut aussi souligner le travail de fond des lobbys auprès des institutions de l'UE. Dans ce domaine on peut citer :

- L'organisation professionnelle de santé (ordre des médecins, ordre des pharmaciens…).
- *Health Data Governance Initiative* (*HDGI*), est un groupe de travail qui vise à promouvoir une gouvernance solide et transparente des données de santé au niveau européen.

- *European Medical Information and Communications Systems Society* (*EMICSS*) : une organisation qui défend les intérêts des entreprises de santé et des systèmes d'information en matière de protection des données de santé.

Enfin il est important de souligner le travail de l'Agence Européenne pour la Cybersécurité (ENISA).

Cette dernière fournit des recommandations pour renforcer la cybersécurité dans la gestion des données de santé.

Au milieu de ce cadre légale, l'Allemagne se positionne comme un acteur majeur dans le domaine de l'e-santé en Europe, avec une approche qui privilégie la souveraineté numérique. À l'inverse de la situation française où le Health Data Hub a été confié à Microsoft Azure, suscitant des débats sur la dépendance aux acteurs étrangers, l'Allemagne affiche une volonté claire de maîtriser l'hébergement et le traitement des données de santé en s'appuyant sur des infrastructures locales.[ci]

Cette démarche repose sur un double enjeu : garantir la sécurité des données sensibles des citoyens et assurer la conformité avec le cadre juridique européen, notamment le RGPD. Toutefois, malgré cette ambition de souveraineté, l'Allemagne reste ouverte à des collaborations avec des acteurs internationaux comme Microsoft et AWS, sous réserve de conditions strictes de régulation. Ces conditions incluent notamment le respect des réglementations européennes en matière de protection des données et de concurrence. Par exemple, AWS a annoncé le lancement de l'AWS European Sovereign Cloud[cii], une nouvelle infrastructure cloud indépendante conçue pour aider les clients des secteurs publics et hautement réglementés à répondre aux exigences strictes de résidence des données et d'autonomie opérationnelle au sein de l'Union européenne (UE). Cette initiative vise à garantir que toutes les métadonnées créées par les clients restent dans l'UE et que seules des personnes résidant dans l'UE contrôlent les opérations et le support de cette infrastructure. Sur le volet concurrentiel, le Bundeskartellamt (Office fédéral allemand des cartels) a déterminé que Microsoft est une entreprise d'importance capitale pour la concurrence sur les marchés[ciii], la soumettant ainsi à un contrôle accru pour éviter toute pratique anticoncurrentielle. Ces mesures illustrent l'engagement de l'Allemagne à collaborer avec des acteurs internationaux tout en veillant à ce que ces partenariats respectent les normes strictes de régulation et de souveraineté numérique établies par l'UE. Ce compromis permet de combiner des solutions locales souveraines avec l'expertise technologique globale nécessaire pour moderniser ses systèmes de santé.

En comparaison avec la France, où la centralisation des données via le Health Data Hub a renforcé la dépendance à des solutions étrangères, le modèle allemand s'appuie davantage sur une régionalisation et une diversification des acteurs impliqués. Cette approche reflète non seulement les spécificités du système fédéral allemand, mais également une volonté politique de favoriser des alternatives locales,

avec des entreprises comme SAP, T-Systems ou STACKIT jouant un rôle central dans la transformation numérique du secteur de la santé.

Ainsi, l'exemple allemand soulève des questions essentielles : comment équilibrer souveraineté numérique et coopération avec des entreprises étrangères pour répondre aux besoins croissants en matière de santé numérique ?

Parmi les principaux acteurs nationaux de l'hébergement de données de santé allemande, nous noterons tout d'abords le Bundesministerium für Gesundheit (BMG), qui est le ministère de la Santé allemand et qui joue un rôle central dans la définition des politiques de santé numérique, notamment en fixant les cadres réglementaires et en supervisant les projets stratégiques nationaux comme l'Elektronische Patientenakte (ePA). Il veille à la cohérence des initiatives et à leur conformité avec les règlements européens.

Par la suite, Gematik, créé en 2005 (GmbH), est chargée de concevoir, développer et déployer les infrastructures numériques de santé. Son rôle s'apparente à celui de l'Agence du Numérique en Santé (ANS) en France, avec un focus particulier sur la gestion des dossiers médicaux électroniques (ePA) et la sécurisation des échanges d'informations entre les acteurs de la santé.

Toutefois, l'Allemagne ne dispose pas d'une plateforme centralisée comme le Health Data Hub français. Les données de santé sont réparties entre plusieurs opérateurs, publics et privés. L'approche décentralisée de l'Allemagne pour la collecte et le traitement des données de santé découle directement de son organisation fédérale et de son héritage historique. Contrairement à la France, où le Health Data Hub centralise les données de santé à l'échelle nationale, l'Allemagne délègue cette responsabilité aux Länder (États fédérés) et favorise des partenariats public-privé pour stimuler l'innovation. Ce choix repose sur plusieurs piliers : la structure politique fédérale, la sensibilité historique à la protection des données, et la volonté d'assurer une souveraineté numérique renforcée.

La structure fédérale allemande, inscrite dans la Loi Fondamentale (*Grundgesetz*), confère une autonomie importante aux 16 Länder dans les domaines de la santé et de l'administration publique. Chaque Land est libre de gérer ses systèmes de santé, y compris la collecte et le traitement des données[civ], conformément au principe de subsidiarité. Ce fonctionnement décentralisé permet une adaptation aux besoins locaux, mais rend difficile la mise en place d'un système centralisé unique comme en France.

Par ailleurs, l'histoire allemande a façonné une culture de la protection des données profondément ancrée dans la société. Les abus commis sous les régimes nazi et est-allemand (Stasi) ont laissé une méfiance durable envers la centralisation des données, perçue comme une menace potentielle pour les libertés individuelles. Un sondage réalisé par Bitkom révèle que 92 % des Allemands considèrent la protection des données comme une priorité majeure[cv]. Cette sensibilité explique pourquoi les

Initiatives de centralisation sont souvent rejetées au profit de solutions locales et régionales.

En complément, l'Allemagne favorise une collaboration étroite entre le secteur public et le secteur privé pour le développement de solutions innovantes dans la gestion des données de santé. Le programme Digital Health Applications (DiGA)[cvi] en est un exemple concret : il permet à des entreprises privées de proposer des applications numériques validées pour les patients. Ces partenariats, souvent contractualisés à l'échelle des Länder, assurent une flexibilité et une innovation accrues tout en maintenant un contrôle régional strict.

Enfin, la question de la souveraineté numérique joue un rôle déterminant dans l'organisation allemande. Contrairement à la France, qui a choisi Microsoft Azure comme hébergeur du Health Data Hub, l'Allemagne privilégie des solutions européennes pour le stockage des données sensibles. Des acteurs comme T-Systems ou SAP sont régulièrement sollicités pour garantir que les données restent sous contrôle européen. Cette stratégie vise à éviter la dépendance vis-à-vis des fournisseurs étrangers et à renforcer la sécurité des données.

En somme, l'approche allemande repose sur une décentralisation institutionnelle[cvii], une sensibilité culturelle forte à la protection des données, et une stratégie proactive en matière de souveraineté numérique. Si cette organisation limite la création d'un système national unique, elle offre une adaptation fine aux réalités locales tout en favorisant l'innovation technologique.

Toutefois, des initiatives existent déjà, comme le Forschungsdatenzentrum Gesundheit (FDZ Gesundheit), centre de données de recherche sur la santé en français, rattaché à l'Institut fédéral des médicaments et des dispositifs médicaux (BfArM), qui a pour objectif de promouvoir la recherche médicale afin d'améliorer les soins prodigués aux citoyens, et permettent d'accéder à des données pseudonymisées pour la recherche scientifique. Cet accès reste encadré par des régulations strictes telles que le Gesundheitsdatenschutzgesetz (GDSG) et le RGPD.

Dans le secteur privé et local, il existe SAP, géant du logiciel allemand, qui propose des solutions innovantes pour la gestion et l'exploitation des données de santé, notamment via son cloud sécurisé SAP Health Data Services. SAP joue un rôle clé dans l'interopérabilité des systèmes de santé et dans la mise en conformité des solutions numériques aux régulations européennes.

Autre acteur majeur, T-Systems Filiale de Deutsche Telekom, spécialisée dans l'hébergement et la gestion des données critiques sur des infrastructures cloud certifiées. Grâce à sa capacité à offrir des solutions locales et conformes aux normes européennes, T-Systems se positionne comme un acteur stratégique dans la protection des données de santé.

Enfin, STACKIT (Schwarz Digits), filiale IT du groupe Schwarz (propriétaire de Lidl et Kaufland), émerge comme un fournisseur de solutions cloud souveraines et

sécurisées. STACKIT collabore avec des acteurs publics pour proposer une alternative locale aux solutions étrangères, renforçant ainsi la souveraineté numérique de l'Allemagne.

Nous noterons toutefois la présence d'opérateurs étrangers, à l'image du colosse Microsoft Azure, qui malgré une volonté affichée de souveraineté numérique, reste présent dans certains projets stratégiques allemand, notamment à travers des partenariats public-privé. La conformité stricte au RGPD et aux normes locales permet à Microsoft Azure de maintenir sa participation dans l'écosystème allemand. AWS intervient également dans l'hébergement des données de santé via des infrastructures dédiées. Toutefois, en raison des réticences politiques et stratégiques vis-à-vis des acteurs non européens, son rôle demeure plus limité qu'aux États-Unis ou en France.

Du côté des infrastructures, l'Elektronische Patientenakte (ePA), dossier de santé électronique centralisé inauguré par l'Allemagne le 1er janvier 2021 sous la supervision de Gematik, l'organisme public responsable de la numérisation du système de santé, est un cas d'école allemand. L'ePA vise à centraliser les données médicales des citoyens allemands, facilitant ainsi l'accès, l'échange et la gestion des informations médicales entre les patients et les professionnels de santé. Son développement s'inscrit dans une volonté d'améliorer l'efficacité des soins, d'augmenter la transparence et d'assurer une interopérabilité optimale entre les systèmes d'information de santé.

L'ePA présente un avantage en termes de contrôle de la donnée : ce sont les patients qui décident si et quelles données du contexte de traitement actuel sont stockées dans l' ePA , ainsi que quelles données doivent être à nouveau supprimées.[cviii]

Les objectifs sont clairs : garantir la sécurité des données, stockage et la gestion des informations se font dans des environnements cloud hautement sécurisés, conformes au RGPD. L'ePA facilite l'interopérabilité, en permettant aux différents prestataires de soins (médecins, hôpitaux, pharmacies) d'accéder aux données nécessaires à travers une plateforme unifiée, réduisant les silos d'information. Et l'amélioration des soins : Les patients peuvent suivre leur parcours de santé, consulter leurs dossiers médicaux et partager facilement leurs données avec les prestataires. Toutefois, malgré les avancées technologiques, l'adoption de l'ePA reste progressive, notamment en raison des préoccupations liées à la sécurité et à la confidentialité des informations médicales sensibles. Il est en phase de test depuis 2021, et sera généralisé pour tous les citoyen et acteurs de la santé à partir du 15 janvier 2025[cix].

Conscient des enjeux liés à la souveraineté numérique et à la dépendance envers les fournisseurs étrangers, l'Allemagne promeut activement des solutions cloud locales et des espaces de données sécurisés. Cette approche vise à protéger les données sensibles, notamment les données de santé, tout en respectant les régulations strictes imposées par le RGPD. Dans cette démarche de Cloud souverain et Data Space, d'autres initiatives intéressantes sont à aborder. Le projet GAIA-X, une infrastructure de cloud européenne, lancé en 2021 suite à une initiative Franco-Allemande, appuyée

par 22 acteurs de divers secteurs économiques (cloud service provider, utilisateurs, recherche et association). Gaia-X est une initiative européenne qui vise à créer une infrastructure de données et de cloud computing interconnectée et souveraine. L'idée principale derrière ce projet est de mettre en place un cadre qui permet aux différents services cloud de travailler ensemble, tout en respectant les valeurs et les réglementations européennes. Concrètement, Gaia-X cherche à construire un écosystème numérique ouvert où les entreprises, les chercheurs et les institutions peuvent collaborer plus facilement. Au lieu de créer une nouvelle plateforme centralisée, le projet se concentre sur la connexion des infrastructures existantes. L'objectif de Gaia-X est de renforcer l'innovation et la compétitivité en Europe dans le domaine du cloud computing, tout en garantissant que les données des utilisateurs restent protégées et sous contrôle Européen. En favorisant un partage sécurisé des données entre différents secteurs.

L'Allemagne participe activement à cette initiative européenne, visant à créer un environnement cloud sécurisé, transparent et interopérable. GAIA-X permet de connecter les solutions de différents fournisseurs tout en garantissant la localisation pour l'UE des données et leur conformité avec les normes européennes. Cela offre une alternative crédible aux solutions des géants technologiques étrangers comme Microsoft Azure et AWS.

En complément de GAIA-X, l'Allemagne développe ses propres *Data Spaces* dédiés aux données de santé. Ces espaces de données facilitent le partage sécurisé des informations entre les acteurs du système de santé (hôpitaux, laboratoires, organismes de recherche) tout en préservant la confidentialité et la souveraineté des données.

Des entreprises allemandes comme STACKIT (filiale du groupe Schwarz), T-Systems (branche IT de Deutsche Telekom) et SAP jouent aussi un rôle clé dans l'hébergement des données de santé. Ces acteurs proposent des solutions conformes aux exigences nationales et européennes, favorisant une infrastructure cloud robuste, locale et souveraine.

En Allemagne, le cadre réglementaire entourant l'e-santé repose sur plusieurs lois et certifications clés visant à garantir la sécurité des données sensibles et à renforcer l'indépendance technologique. Parmi ces dispositifs, le « Gesundheitsdatenschutzgesetz [cx]» (GDSG) et la certification C5[cxi] jouent un rôle central, complétés par des initiatives européennes comme le RGPD et les projets d'harmonisation à l'échelle de l'UE.

Le GDSG, ou loi sur la protection des données de santé, établit des règles strictes pour la gestion des informations médicales. Ce texte impose des standards élevés de stockage, de transfert et de traitement des données sensibles, avec des sanctions sévères en cas de non-conformité. Ces dispositions s'inscrivent dans une volonté de maintenir un contrôle rigoureux sur les données de santé, réduisant ainsi la dépendance aux acteurs non européens. Ce cadre est renforcé par le RGPD, qui

s’applique à l’ensemble de l’Union européenne. Le RGPD, fournissant une base solide pour la protection des données personnelles, est complété par des exigences supplémentaires issues du GDSG, créant un environnement encore plus contraignant pour les acteurs du secteur de la santé.

La certification C5 (« Cloud Computing Compliance Controls Catalogue »), développée par l’Office Fédéral pour la Sécurité des Technologies de l’Information (BSI), constitue une pierre angulaire de la stratégie allemande de cybersécurité. Bien que non obligatoire, cette certification est devenue une référence incontournable pour les fournisseurs de services cloud opérant dans des secteurs sensibles, notamment celui de la santé.

Initialement introduite en 2016 et actualisée pour intégrer les nouvelles menaces, la certification C5 a été conçue pour garantir la transparence et la sécurité dans l’utilisation des services cloud. Les fournisseurs certifiés doivent se conformer à des normes rigoureuses, incluant des exigences en matière de sécurité physique et logique, des mécanismes de gestion des incidents de cybersécurité, et des audits réguliers effectués par des tiers indépendants. Ces audits, conformes aux standards internationaux comme l’ISO/IEC 27001, permettent de vérifier que les pratiques des fournisseurs respectent les exigences définies.

Pour le secteur de la santé, la certification C5 présente plusieurs avantages spécifiques. Elle garantit un haut niveau de confidentialité pour les données médicales sensibles, favorise l’interopérabilité des solutions cloud avec les infrastructures existantes, et renforce la crédibilité des fournisseurs certifiés, ce qui est essentiel pour gagner la confiance des institutions et des patients. Cependant, cette certification comporte également des limites. Son obtention et son maintien nécessitent des investissements financiers et humains conséquents, ce qui peut constituer un frein pour les petites entreprises. De plus, la complexité des exigences techniques peut poser des défis pour certaines organisations, en particulier celles qui ne disposent pas d’une expertise avancée en cybersécurité. Les plus gros opérateurs mondiaux ont tous une attestation C5 comme Microsoft, Google, AWS, OVH, Oracle etc… (liste exhaustive des attestations[cxii])

Dans un contexte européen, la certification C5 pourrait évoluer avec l’introduction du « European Cybersecurity Certification Scheme » (EUCS)[cxiii]. Ce projet vise à harmoniser les normes de cybersécurité à l’échelle de l’Union européenne, offrant ainsi un cadre commun pour les certifications nationales comme le C5 en Allemagne ou l’ENS[cxiv] en Espagne. Si l’EUCS venait à remplacer ou compléter le C5, cela permettrait de réduire les disparités entre les pays membres et de renforcer l’interopérabilité des systèmes. Toutefois, cette transition pourrait nécessiter des ajustements pour intégrer pleinement les spécificités des cadres nationaux dans une certification européenne unifiée.

Enfin, l'Allemagne se distingue par des initiatives nationales complémentaires comme la loi « Digitale-Versorgung-Gesetz[cxv] » (DVG), adoptée en 2019, qui encadre

l'utilisation d'applications numériques de santé (DiGA)[cxvi] et la télémédecine. Ce texte assure une évaluation stricte des solutions numériques avant leur intégration dans le système de santé et impose des règles de sécurité, d'interopérabilité et de protection des données rigoureuses. En parallèle, face à la recrudescence des cyberattaques, notamment sur les infrastructures critiques comme les hôpitaux, le gouvernement allemand renforce ses efforts pour sécuriser le domaine de la santé. Les collaborations entre le BSI[cxvii] et les établissements médicaux visent à prévenir les incidents, grâce à des recommandations techniques et des centres de réponse rapide. Ces mesures, combinées à des investissements dans des solutions cloud souveraines, illustrent la stratégie allemande pour équilibrer souveraineté numérique et sécurité des données dans le secteur de l'e-santé.

En outre, le cadre réglementaire allemand repose sur une combinaison de normes nationales rigoureuses et d'initiatives européennes, visant à créer un environnement sécurisé et souverain pour le développement de l'e-santé. La certification C5, bien qu'elle ait des limites, s'impose comme un pilier de cette stratégie, et son évolution dans le contexte européen pourrait renforcer encore davantage la sécurité et l'interopérabilité des systèmes de santé numérique.

En matière de gouvernance des données de santé, la France et l'Allemagne présentent des modèles contrastés qui reflètent leurs approches respectives en termes de centralisation et de souveraineté numérique. En France, la plateforme centralisée Health Data Hub (HDH) est devenue le point d'entrée principal pour la collecte, le traitement et la valorisation des données de santé. Placée sous la supervision de l'État, cette structure centralisée a pour objectif de faciliter l'accès aux données pour la recherche scientifique et les innovations en matière de santé publique. Toutefois, son partenariat avec Microsoft Azure pour l'hébergement a suscité des critiques concernant la souveraineté numérique, notamment en raison de la dépendance à une infrastructure étrangère soumise à des régulations extraterritoriales telles que le Cloud Act américain.

À l'inverse, l'Allemagne adopte une gouvernance des données de santé plus régionalisée, fidèle à son système fédéral, comme expliqué plus haut. Cette décentralisation se traduit par une multiplicité d'acteurs impliqués dans la gestion des données de santé, rendant l'ensemble moins uniforme, mais plus flexible et adapté aux besoins locaux.

Concernant les acteurs majeurs et le marché des hébergeurs de données, la France a vu émerger des entreprises comme OVHCloud et Scaleway, qui disposent de certifications nationales telles que HDS (Hébergeur de Données de Santé) et SecNumCloud délivrées par l'ANSSI. Ces certifications permettent de garantir un haut niveau de sécurité pour l'hébergement des données sensibles. Toutefois, la prédominance de Microsoft Azure dans le cadre du HDH reste un sujet sensible, reflétant la difficulté à concilier innovation technologique et souveraineté numérique.

En Allemagne, la stratégie privilégie des solutions locales pour réduire la dépendance aux GAFAM. Des entreprises comme STACKIT, filiale du groupe Schwarz, et T-Systems, branche IT de Deutsche Telekom, se positionnent comme des alternatives souveraines pour l'hébergement des données de santé. SAP, acteur historique du logiciel allemand, propose également des solutions conformes aux exigences européennes. Bien que Microsoft et AWS soient présents dans certains projets stratégiques, leur rôle est beaucoup plus limité qu'en France, et les autorités allemandes maintiennent une vigilance accrue pour éviter une externalisation excessive des infrastructures critiques.

En matière de certifications et de standards, la France dispose d'un cadre réglementaire spécifique avec les certifications HDS et SecNumCloud, qui imposent des exigences strictes pour les hébergeurs de données de santé. Ces standards, sous l'égide de l'ANSSI, visent à assurer un niveau de sécurité maximal pour les infrastructures sensibles. En Allemagne, il n'existe pas de certifications équivalentes directement comparables, mais la conformité au RGPD et les exigences nationales en matière de protection des données restent des priorités. Les régulations comme le Gesundheitsdatenschutzgesetz (GDSG) garantissent un haut niveau de sécurité, bien que le cadre soit moins formalisé qu'en France.

Ainsi, si la France et l'Allemagne partagent des objectifs communs en matière de sécurité et de valorisation des données de santé, leurs approches diffèrent largement. La France mise sur une centralisation assumée mais controversée, tandis que l'Allemagne privilégie une décentralisation plus cohérente avec son modèle fédéral, tout en réduisant activement sa dépendance aux acteurs étrangers pour préserver sa souveraineté numérique.

Tableau d'analyse des stratégies des acteurs

Critères / Pays	France	Etats-Unis	Allemagne
Doctrine d'Etats	Cloud au centre (2021)	Cloud First (2012) Cloud Smart (2019)	Digital Healthcare Act (2019)
Standards de sécurité des données de santé	HDS (2018) SecNumCloud (2016) RGPD (2018)	HIPAA (2013) NIST Cybersecurity Framework (2014) SOC 2 (2011) FedRAMP (2019) StateRAMP (2021)	GDSG (1994) DSGVO (RGPD 2018) C5 (2016) RGPD (2018) BfDI (1978)
Interopérabilité et modernisation des données de santé	Health data Hub (2019)	21st Century Cures Act (2016)	l'Elektronische Patientenakte (ePA) (2021)
Investissements publics pour numérique de santé	France 2030 Plan Santé BPI France	HITECH Act (2009) Joint Warfighting Cloud Capability (JWCC)	GEMATIK (2005) DiGA (2019) KHZG (2020)

Source : tableau basé sur des données open source et réalisé par le groupe 20

Matrice SWOT des stratégies des acteurs

Critères / Pays	France	Etats-Unis	Allemagne
• Forces	• Système de certification robustes, • Règlementation claire et exigeante.	• Politiques gouvernementales, • Financements Publiques, domination technologique.	• Un cadre législatif strict pour une protection optimale des données (DSGVO, GDSG), • Acteurs technologiques nationaux puissants (ex. SAP, T-Systems).
• Faiblesses	• Manques de moyens et financements, • Pas de préférence nationale, • Adoption du cloud ralentis par les démarches administratives.	• Complexité réglementaire, • Coûts élevés des infrastructures, • Surveillance et Confidentialité.	• Décentralisation : coordination difficile entre les Länder, • Adoption lente de l'ePA, • Coûts élevés des certifications de sécurité (C5, EUCS).
• Opportunités	• Possibilité d'avoir un hyperscaler souverain, • Evolution vers une diminution de l'impact environnemental.	• Libre circulation des données, • Transition numérique dans les données de santé, • Influence culturelle et éducative.	• Renforcer le leadership européen initiatives open-source souveraines, • Améliorer la coopération entre Länder, • Développer des partenariats public-privé (ex : SAP, Fraunhofer Institute).
• Menaces	• Dépendance des hyperscalers Américains, • Concurrence locale et européenne accrue, • Exploitation des données personnelles de santé en dehors de la règlementation européenne.	• Réglementations restrictives, • Perception négative des pratiques anticoncurrentielles.	• Réticence des citoyens allemands à partager leurs données médicales, • Réglementation stricte pouvant freiner l'innovation, • Concurrence internationale.

Source : tableau fondé sur des données open source et réalisé par le groupe 20 du QuestIE de l'EGE

La prise de hauteur sur les projets européens et français et sur leur organisation est douloureuse à observer. Les acteurs américains (hébergement et norme de transfert de données) ont une place dominante pour les projets actuels et futurs. Les systèmes juridiques de la France et des Etats européens sont strictes mais les gouvernements ont besoin des acteurs américains pour réaliser leur projet. Cette gestion des données de santé par la France et l'Union européenne donnera lieur à plusieurs conséquences pouvant impacter profondément ces sociétés.

Partie 3 : Les impacts de la gestion française et européenne des données de santé

A. La gestion française des données de santé, source de risque pour la stratégie nationale

1. Risques et menaces concernant le secteur public

L'hébergement des données de santé françaises sur des serveurs étrangers, notamment américains comme *Microsoft Azure*, soulève des préoccupations majeures concernant la perte de contrôle des données. En effet, cette situation expose les informations sensibles à des législations étrangères, telles que le *CLOUD Act* et le *Patriot Act*, qui permettent aux autorités américaines d'accéder à ces données, compromettant ainsi leur confidentialité. De plus, les techniques de *lawfare*, ou « guerre par le droit », utilisées par les États-Unis augmentent le risque d'interception des données par leurs services de renseignement. Cette dépendance à des infrastructures cloud non-européennes pose également un dilemme pour l'État français, qui doit naviguer entre l'innovation technologique nécessaire pour la recherche médicale et la protection des données personnelles de ses citoyens.

Les citoyens français, préoccupés par la protection de leurs informations médicales personnelles, pourraient intenter des actions en justice contre l'État français. Leur inquiétude porte sur le fait que leurs données sensibles soient stockées et gérées par des organisations étrangères, hors du territoire national. Cette situation expose donc l'État français à des risques légaux potentiellement conséquents. En effet, les citoyens pourraient arguer que l'État manque à son devoir de protection des données personnelles en permettant leur hébergement à l'étranger, où les lois sur la confidentialité et la sécurité des données peuvent différer des normes françaises.

La gestion des données de santé en France, et les vides ou désavantages juridiques, révèlent une fragilité structurelle où l'état peine à protéger ses individus et ses entreprises. En plus de désavantager les entreprises françaises face aux concurrents, cette situation engendre des risques économiques significatifs, une perte de pertinence des politiques publiques et une érosion de la confiance citoyenne. Les rapports du *Health Data Hub* confirment cette défiance : 77% des Français se sentent mal informés sur l'utilisation de leurs données de santé, et seulement 20% connaissent précisément leurs droits, alimentant une méfiance croissante qui affecte non seulement le système de santé français mais également la perception globale de la gestion des données en Europe[cxviii].

Le principe du « guichet unique » du RGPD consiste à faire appliquer le RGPD par l'autorité de protection des données du pays d'installation de l'entreprise concernée, et non celui où résident les utilisateurs. Ce principe conduit à une véritable perte de souveraineté numérique française. En pratique, toutes les grandes plateformes du numérique ont leur siège social européen à Dublin, ce qui fait de facto de la *Data Protection Commission* (l'équivalent de la CNIL en Irlande) un acteur central. De ce fait, l'Irlande exerce une influence disproportionnée sur la régulation des données en Europe. Cette situation compromet non seulement l'efficacité globale du RGPD, notamment son objectif d'harmonisation, mais affaiblit également la position de la France face à la DPC irlandaise.

Si les réglementations européennes et américaines peuvent poser des problématiques au niveau des acteurs publics, il en va de même au niveau des acteurs du domaine privé, tant au niveau de la compétence que de la compétitivité.

2. Risques et menaces concernant le secteur privé

Face à la législation des données de santé, les acteurs peuvent en tirer profit, ou au contraire les subir.

Comme expliqué ci-dessus, la plupart des plateformes du numérique en Europe ont leur siège social à Dublin ce qui implique une suprématie des acteurs irlandais sur les acteurs français. On sait que l'Irlande dépend grandement des *GAMAM (Google, Apple, Meta, Amazon, Microsoft)* pour sa croissance et son écosystème économique. Il y a donc un risque de soumission pour l'Irlande et donc pour son autorité de protection des données (*Data Protection Commission*), à des pressions extérieures de l'UE (notamment les Etats-Unis). Ce qui contredit le principe de souveraineté des entreprises françaises dans le domaine de la santé, et auprès de la législation irlandaise. Ils sont directement sujets à des risques de conflits d'intérêts, qui deviennent une menace sur la souveraineté et l'intégrité des données françaises et des autres pays de l'Union Européenne.

Les entreprises américaines qui traitent des données européennes se retrouvent dans une position compliquée : en respectant le *CLOUD Act* et en transmettant leurs données au gouvernement américain, elles enfreignent le RGPD. Mais en refusant cette transmission de données, elles transgressent le *CLOUD Act* (elles ne peuvent refuser cette transmission s'il s'agit d'une "*US Person*", citoyen américain ou individu résidant sur le sol américain). Quant aux entreprises européennes, le fait d'utiliser des structures américaines pour stocker ses données de santé (*AWS, Microsoft...)* peut entraîner une demande d'accès aux données de la part des autorités américaines. Cet état de fait entraîne une grave violation au principe de confidentialité du RGPD, ce qui pose également un problème de protection. Cette situation peut possiblement entraîner d'autres conséquences au niveau de la souveraineté des données de santé. Le RGPD impose que les individus aient explicitement donné leur accord pour le traitement de leurs données de santé. Une fois ces données stockées sur des

Infrastructures américaines, l'entreprise européenne peut perdre le contrôle de ses données. Même en respectant elle-même le RGPD, ses prestataires américains restent soumis aux lois américaines. Une entreprise française peut donc également se retrouver entre le marteau et l'enclume quant à sa responsabilité : elle peut se retrouver dans une situation où un choix s'impose entre respecter le RGPD ou le *CLOUD Act*.

Au niveau de la législation française, aucune loi n'oblige les entreprises françaises à stocker leurs données au sein d'un hébergeur de données français. Ce vide juridique ne profite pas aux solutions d'hébergement françaises, qui sont pourtant bien présentes. Pour une entreprise française, le fait d'héberger ses données sur un cloud français, situé en France, réglerait ce problème de souveraineté, ces dernières n'étant communiquées à d'autres gouvernements ou acteurs privés étrangers, à l'exception des investisseurs selon les clauses de partage de données.

L'application des règlements n'est pas la même selon les entreprises. Cette dernière est plus difficile pour les TPE et PME. D'un côté, celles-ci se pensent moins concernées par les encadrements juridiques liés aux données et ont tendance à involontairement transgresser ces cadres légaux. De plus, les règlements ne prévoient pas de principe de proportionnalité quant à la sanction applicable à une entreprise qui ne respecte pas ces mêmes règlements. En somme, une entreprise de grande taille se verra infliger la même amende qu'une TPE/PME. Pourtant, cette amende sera bien plus difficilement payable par la TPE/PME et donc plus handicapante.

La transformation numérique de l'économie et l'importance des données dans les nouveaux modèles d'affaires, notamment des grandes plateformes du numérique, ont fait émerger des questions nouvelles à l'intersection de l'analyse concurrentielle et de la protection des données personnelles (Doctolib, Amélie…) (La CNIL et l'Autorité de la concurrence ont décidé de se saisir ensemble de ces questions et d'approfondir leur coopération).

3. Risques et opportunités liés à l'éthique et à la protection de l'individu

L'utilisation de l'éthique comme fer de lance de la gestion des données de santé des Français constitue un levier majeur de différenciation face aux autres puissances.

Cet avantage spécifique au cadre juridique français, également étendu dans une moindre mesure à l'Union Européenne, met en lumière de nombreux atouts compétitifs pour le domaine de la santé française.

Il pose cependant quelques limites dans le champ de l'innovation.

En France, l'éthique en matière de données de santé représente un choix ambitieux mais coûteux à l'ère du numérique, car elle exige des moyens considérables pour garantir leur protection face aux menaces.

Ce choix sociétal, porté par une volonté de protection des individus, se différencie de celui des autres puissances et entraîne des conséquences distinctes.

Sur le plan éthique, deux visions se distinguent entre le RGPD et le *CLOUD Act* concernant les données de santé.

Les positions des puissances sur les données de santé oscillent entre protection des droits fondamentaux et exploitation économique : en Europe, le RGPD impose un cadre strict pour le traitement des données de santé alors que le *CLOUD Act* américain autorise une utilisation plus large de ces données, à des fins tant publiques que privées.

Sur le court terme, cette approche stricte du règlement européen entraîne des défis significatifs, susceptibles de freiner l'innovation et l'efficacité des établissements de santé.

- La mise en conformité avec le RGPD exige des investissements conséquents de la part des acteurs de la santé. Qu'il s'agisse des hôpitaux, des laboratoires pharmaceutiques ou des start-ups spécialisées, ces acteurs doivent assurer une sécurisation rigoureuse des données, procéder à leur anonymisation, et obtenir des consentements éclairés pour chaque usage.

Un manquement à ces règles peut entraîner des incidents comme *l'Affaire Dedalus* en 2020, où une fuite massive de données de santé a touché plus de 500 000 patients en France. A l'issue du procès, la CNIL a condamné *Dedalus Biologie* à payer une amende de 1,5 million d'euros.

- Ces exigences freinent parfois aussi le développement de projets innovants, notamment dans l'intelligence artificielle, où l'accès à de vastes ensembles de données de santé est crucial pour entraîner des algorithmes performants.

Cette limitation est un frein pour la compétitivité des entreprises européennes, alors que leurs homologues américaines bénéficient elles d'un cadre plus permissif.

Cet environnement juridique leur permet d'exploiter des bases de données gigantesques, souvent issues d'accords avec des établissements hospitaliers ou des assurances santé.

Un exemple frappant de ce décalage compétitif est le développement des technologies d'intelligence artificielle dans le domaine de la santé. Des acteurs américains comme *Google Health* ou *IBM Watson* accèdent à des volumes massifs de données, qu'ils utilisent pour concevoir des outils prédictifs ou des diagnostics assistés par IA. Ces données, souvent obtenues grâce à des partenariats publics-privés, permettent une avancée rapide dans le domaine, mais elles soulèvent des préoccupations majeures quant à la confidentialité des patients.

À l'inverse, les entreprises européennes, bien que techniquement compétentes, doivent naviguer dans un cadre juridique qui freine l'accès à ces ressources essentielles, réduisant leur compétitivité sur le plan mondial.

D’un autre côté, sur le long terme, les contraintes imposées par le RGPD sur les données de santé ont également des retombées positives.

- En garantissant une stricte protection de ces informations sensibles, l’Europe renforce la confiance des citoyens envers les institutions et entreprises chargées de leur hébergement et de leur traitement. Ce lien de confiance peut devenir un avantage compétitif, en particulier dans des domaines où la confidentialité est un enjeu central, comme la télémédecine ou les dossiers médicaux partagés. En France, des plateformes comme Doctolib ou l'Assurance Maladie ont largement communiqué sur leur conformité au RGPD, renforçant leur crédibilité et leur adoption par le grand public[13]. Cette vision s’oppose au paradigme des États-Unis, ou la flexibilité du *CLOUD Act* favorise une innovation rapide mais suscite des critiques croissantes concernant l’éthique et la confidentialité. Cette situation peut ternir l’image des entreprises américaines sur des marchés étrangers, notamment en Europe, où la protection des données est une valeur fondamentale.
- Par ailleurs, le RGPD positionne l’Europe comme une référence mondiale en matière d’éthique des données de santé. Cette position permet d’établir un cadre normatif qui inspire d’autres régions du monde. Des pays comme le Japon ou le Brésil ont adopté des législations similaires, ce qui favorise les entreprises européennes lorsqu’elles collaborent avec ces marchés. Cette reconnaissance éthique renforce également les acteurs européens du cloud, comme *OVH ou T-Systems*, qui se démarquent par leur conformité et leur engagement à respecter la souveraineté des données, y compris celles liées à la santé.
- Bien que la réglementation limite parfois l’exploitation des données de santé, elle stimule également l’innovation dans des domaines spécifiques. L’anonymisation avancée, la sécurisation des échanges ou la création de plateformes décentralisées deviennent des priorités pour les entreprises européennes, qui développent des solutions adaptées à ces contraintes.

Des acteurs, comme *Health Data Hub* en France, montrent comment ces efforts peuvent aboutir à des modèles d'exploitation des données de santé respectueux de l'éthique tout en favorisant la recherche.

En définitive, le cadre éthique imposé par le RGPD semble parfois contraignant, il constitue une opportunité stratégique pour les données de santé en Europe. Trouver un équilibre entre la protection des droits des patients et la flexibilité nécessaire à l’innovation représente un enjeu crucial. Ce modèle pourrait positionner l’Europe comme un leader mondial dans une économie des données de santé fondée sur l’éthique et la durabilité.

B. Les atouts et limites de l'interopérabilité au sein des systèmes de santé européens

1. l'interopérabilité : acteurs de la coopération européenne

a. Le prisme européen

Dans le cadre du réseau européen eHealth Network, la norme HL7 joue un rôle central au sein de l'infrastructure MyHealth@EU. Cette norme, conçue pour structurer et échanger des données de santé dans des environnements multi-systèmes, s'avère particulièrement pertinente pour la création du Patient Summary.

Le Patient Summary[cxix] (PS) est un document synthétique contenant les informations médicales essentielles d'un patient. Il vise à garantir la continuité et la qualité des soins, notamment dans un contexte transfrontalier. HL7 fournit un cadre structuré permettant de représenter ces données de manière uniforme. Ce format harmonisé est essentiel pour :

- Éviter les ambiguïtés lors des échanges de données ;
- Garantir une compréhension des informations dans plusieurs pays et langues

Grâce à la flexibilité de HL7, il est possible d'ajouter ou de modifier des éléments dans le Patient Summary tout en préservant la cohérence du format. De plus, ce document repose sur des systèmes de codification standardisés, tels que SNOMED CT, ICD-10, ou LOINC (cf. Annexe 1) pour uniformiser les termes médicaux, intégrés facilement grâce à HL7.

L'échange sécurisé de données à travers des API modernes est une autre contribution clé de HL7. Cela permet aux professionnels de santé d'un pays d'accéder instantanément aux informations médicales pertinentes d'un patient, stockées dans un autre pays.

La norme HL7 est également utilisée dans l'infrastructure HealthData@EU. La base technique de cette dernière, l'European Electronic Health Record exchange Format (EEHRxF), repose sur HL7 pour structurer divers documents cliniques, comme les Patient Summaries, les rapports de laboratoire ou les comptes rendus d'imagerie médicale.

L'interopérabilité des données de santé dans la gestion sanitaire

Les normes d'interopérabilité des données de santé, dont HL7, ont démontré leur utilité dans la gestion des crises sanitaires, même si leur efficacité varie selon les pays et les régions. Elles ont joué un rôle clé, notamment lors de la pandémie de Covid-19, ou encore dans le suivi de patients atteints de maladies graves.

Une initiative est le projet PanCareSurPass[cxx], financé par l'Union européenne. Ce projet vise à améliorer les soins de suivi pour les survivants de cancers pédiatriques

et adolescents en Europe. Son principal outil, le Survivorship Passport, fournit un résumé détaillé des traitements reçus, accompagné de recommandations personnalisées pour les soins futurs. Le projet s'appuie sur la norme HL7 FHIR pour garantir la portabilité des informations contenues dans le Survivorship Passport, facilitant ainsi leur usage dans divers systèmes de santé.

Ce projet illustre comment l'interopérabilité des systèmes de données de santé peut améliorer la qualité de vie des patients, tout en promouvant l'innovation dans les soins de santé transfrontaliers.

Le cadre juridique, RGPD et législations complémentaires :

Le Règlement général sur la protection des données (RGPD), loin de représenter un obstacle, constitue un atout pour l'adoption de HL7 en Europe. En effet, le RGPD offre un cadre juridique clair pour l'utilisation des données de santé tout en respectant les droits des patients.

Les organisations européennes de santé peuvent s'appuyer sur HL7 pour garantir une conformité automatique aux exigences légales, tout en bénéficiant des avantages d'une norme reconnue mondialement. HL7 intègre également les principes de sécurité promus par le RGPD, tels que :

- Le chiffrement des données en transit ;
- Des mécanismes d'authentification robustes ;
- Un contrôle strict des accès.

En renforçant la sécurité et la confiance dans l'échange de données, le RGPD favorise une adoption harmonisée de HL7 à l'échelle européenne. Par ailleurs, son approche unifiée simplifie la gestion des données personnelles dans l'ensemble des pays membres de l'UE, accélérant ainsi l'intégration des standards HL7 au sein des infrastructures de santé européennes.

Le prisme français :

L'interopérabilité s'impose aujourd'hui par son influence comme la pierre angulaire au sein des systèmes de santé en Europe, mais aussi en France. Permettant l'échange de données entres acteurs (établissements de santé, praticiens, laboratoires, patients), l'interopérabilité s'exprime en France par de nombreux projets : GRADe, MSSanté, le DMP/DME ou encore Mon Espace Santé. Ces projets illustrent l'interopérabilité et l'échange de données afin d'améliorer la qualité des soins, d'optimiser les ressources ou encore l'autonomie du patient.

Les initiatives comme GRADe[cxxi] permettent de fournir une base de données unifiée aux professionnels des établissements de santé. Cette base de données couplée à la messagerie sécurisé MSSanté, facilite la communication de manière rapide et sûre entre praticiens. Ceci permet alors une prise en charge optimale du patient.

De manière plus ample, la France mène des initiatives d'interopérabilité telles que les dossiers médicaux partagés (DMP) et électroniques (DME) qui centralisent le passé médical du patient. L'ensemble est alimenté par la Classification Commune des Actes Médicaux (CCAM) qui standardise les procédures facilitant alors la gestion administrative. Cette standardisation des actes permet alors la facilitation de la gestion administrative (gain de temps), permettant de se concentrer pleinement sur le patient. Ces outils, nombreux, certes, nécessitant sûrement une homogénéisation, facilitent l'exercice des praticiens notamment dans le contexte des déserts médicaux où une gestion efficace et coordonnée des ressources est primordiale. L'interopérabilité, par l'accès aux données de santé, permet également l'autonomisation du citoyen.

Ce dernier a alors accès à son dossier et peut consulter ses traitements, ses antécédents... Cet accès permet en outre une meilleure communication entre les praticiens, et ce, même à l'étranger, comme cela a pu être démontré précédemment. Cet espace permet d'échanger en sécurité avec un praticien, permettant de partager les informations ou les dossiers médicaux du patient [cxxii].

En France, c'est la plateforme MonEspaceSanté[cxxiii] qui s'est imposée MonEspaceSanté propose ainsi des services qui peuvent avoir des similitudes avec le DMP / DME ou encore *Sesali*[cxxiv]. Bien que MonEspaceSanté soit réellement tourné vers le patient et son autonomisation, en France et en Europe force est de constater qu'il existe une redondance des systèmes. L'interopérabilité des systèmes de santé, entre l'ensemble des acteurs, est alors certes nécessaire, mais la concentration sur un unique projet français ou européen d'interopérabilité permettrait une efficacité accrue.

Rapidité et fiabilité des diagnostics :

L'interopérabilité a un effet sur l'autonomisation du citoyen, mais permet également une rapidité et fiabilité des diagnostics[cxxv] (avec l'exemple français de l'utilisation du DMP et du DME qui permet aux praticiens de suivre le dossier du patient à « distance » et l'évolution des analyses de laboratoire). Ces dispositifs sont complétés par l'utilisation de l'application *Sesali*. Cette dernière, permet ainsi aux praticiens de santé d'accéder au dossier médical d'un patient de l'Union européenne. Ce programme, proposé par l'Agence du numérique en santé, sous l'égide du ministère de la Santé et en collaboration avec la Commission Européenne s'applique actuellement dans 20 pays européens et respecte le secret médical ainsi que le RGPD. L'influence de l'interopérabilité est considérable pour le citoyen français et européen qui peut (presque) n'importe où en Union européenne, s'il rencontre des difficultés médicales, être traité. Une fois encore, alors que la prise en charge des patients est de plus en plus compliquée en France (en raison des déserts médicaux et la raréfaction des spécialistes), l'interopérabilité représenter une alternative afin de pallier les défaillances du système de santé. Son influence est importante, mais ne constitue pas une solution en elle-même. Aujourd'hui l'interopérabilité permet une continuité des soins lorsque, le patient est obligé de se déplacer pour être diagnostiqué, traité, rétabli. Néanmoins, l'utilisation des DME, et de l'interopérabilité en général nécessite la

capacité de manier les outils informatiques que les différences culturelles et générationnelles fracturent.[cxxvi]

Éviter la redondance des coûts :

L'interopérabilité aurait également des effets sur le coût de la santé. En effet, l'OCDEcxxvii estime qu'entre 20 et 30 % des dépenses de santé sont non "pertinentes". En France, cela représenterait entre 32 et 48 milliards d'euros. Pour exemple, l'utilisation des DME et DMP, permettrait selon les estimations d'éviter les actes inutiles ou redondants grâce au suivi dématérialisée et conduirait à l'économie de 4.6 milliards pour le système de santé.[*cxxviii*]

Ainsi, accentuer l'interopérabilité parce qu'elle accroit la fiabilité des diagnostics permet d'éviter les examens complémentaire (générant ainsi des économies directes, liées au coût des examens, mais aussi indirectes en libérant du temps de consultation). L'exemple pris dans L'importance de l'interopérabilité en santé[*cxxix*] semble pertinent : "*les données d'un patient qui a subi une analyse sanguine la semaine dernière dans un laboratoire peuvent être utilisées aujourd'hui, lors d'un déplacement aux urgences, ce qui permet d'économiser le temps et de réduire les coûts nécessaires pour effectuer davantage de tests (et des tests inutiles) à l'hôpital.*"

Néanmoins, afin de récolter le fruit de l'interopérabilité, il est important de poursuivre l'investissement (actuellement les États membres investissent à hauteur de 12 milliards d'euros pour la santé, comprenant la santé numérique et l'utilisation secondaire des données de santé[cxxx].

Confiance et qualité des données :

L'interopérabilité et l'échange de données de santé influencent considérablement la relation entre le patient et le praticien. La confiance est alors primordiale, le patient doit consentir à l'utilisation de ses données notamment pour une utilisation secondaire comme la recherche scientifique. À cette fin, le respect du RGPD est essentiel.[cxxxi] L'État et le système de santé doivent ainsi fournir des garanties au patient. Pour ce, l'État doit être souverain dans la collecte, le traitement, la sauvegarde des données. Avoir confiance dans le système de santé[cxxxii], et l'interopérabilité, permet également de fournir des données fiables et de qualité (le patient ne cherchera pas à mentir ou tromper s'il a confiance en son médecin et en l'interopérabilité).

Opportunités technologiques et innovatrices :

Enfin, pour garantir la confiance du patient envers l'interopérabilité et le traitement de ses données, il faut lui proposer des solutions souveraines qu'elles soient européennes ou françaises à l'image du système Diane de l'entreprise Bow Médical[cxxxiii], certifié La French Fab[cxxxiv]. Ce système d'interopérabilité, utilisant les fameux protocoles HL7 FHIR afin de proposer aux établissements et aux professionnels de santé des réponses sur l'identification, la localisation, le travail collaboratif, le partage des données. De fait " La plateforme DIANE dédiée aux soins critiques se connecte directement aux systèmes d'information du SIH grâce aux flux

d’interfaçages et aux nombreux drivers développés par notre équipe d’interopérabilité”. L’étude du système français Diane (cf. Annexe 2) permet de relever les éléments remarquables suivants : ce système offre la capacité à maintenir le service d’interopérabilité en cas de panne (bascule vers un serveur localisé et ce en mode déconnecté) mais aussi la mutualisation des bases de données au sein d’un établissement de santé (ce qui permet de réduire le nombre de systèmes informatiques différents entre la chirurgie et la réanimation par exemple).

2. Limites, risques & freins de l’interopérabilité des systèmes de santé

Enjeux de cybersécurité :

Le domaine de la santé fait régulièrement l’objet d’attaque de son environnement cyber en témoigne le nombre significatif des attaques répertoriées, la France se plaçant en 4ème position des pays les plus touchés par les cyber-attaques au second semestre 2023[cxxxv]. Les tentatives de rançongiciel sont particulièrement fréquentes et figurent parmi l’une des principales menaces au même titre que le vol de données (des activités des brokers data notamment).

Cet environnement informatique constamment menacé se voit davantage exposé par l’émergence des applications de santé qui sont particulièrement vulnérables aux tentatives d’intrusion et qui peuvent manquer de résilience face aux attaques[cxxxvi]. A ces fragilités de conception et d’entretien des systèmes s’ajoute une vulnérabilité liée aux standards protocolaires de gestion des données de santé tels que HL7 et FHIR.

Ces deux protocoles présentent ainsi des vulnérabilités notables en matière de sécurité et ses lacunes se répercutent sur les entités utilisant ces normes. HL7, en particulier les versions plus anciennes, manque souvent de fonctionnalités de sécurité robustes. Pour exemple, les messages HL7 sont généralement transmis en texte clair n’offrant aucune sécurité en cas d’interception. FHIR, bien que plus moderne, fait également face à des défis. L'utilisation des API RESTful dans FHIR peut exposer les systèmes à des attaques courantes basées sur le web, telles que l'injection SQL, le cross-site scripting (XSS) et les attaques de type "man-in-the-middle" (MITM). Les deux protocoles peuvent également être vulnérables à des tentatives d’authentification et d’autorisation incorrectes, ce qui permettrait un accès non autorisé aux données sensibles de santé. Afin de corriger ces vulnérabilités, il apparaît primordial d’établir des mesures de sécurité plus strictes, telles que le cryptage et l'authentification sécurisée et mettre en place des audits de sécurité fréquents, afin de protéger les informations des patients et de maintenir l'intégrité et la confidentialité des échanges de données de santé.

Ainsi un système de données est aussi faible que ses standards normatifs d’échanges le sont, et ces derniers présentent des risques d’interception, d’intrusion, de corruption de données et de potentielles absences de chiffrage.

Enjeux législatifs :

Comme vu précédemment, l'interopérabilité des systèmes de santé et leur utilisation secondaire font l'objet de cadrages législatifs nationaux (notamment celui de la CNIL[cxxxvii]) et européens (comme le RGPD) permettant d'assurer des niveaux de protections afin de sécuriser l'anonymat des données et leur utilisation. Néanmoins, les mêmes textes peuvent aussi s'avérer être des freins à leur développement et implémentation opérationnelle. Cette affirmation peut être illustrée par les différentes tentatives de création d'un espace européen de données de santé qui se voient ralentis par les différentes juridictions des pays. Le projet du *European Health Data Space* (EHDS) a notamment été victime de ce frein selon Markus KALLIOLA, directeur dudit projet : " *Lorsque nous parlons de données de santé, les gens pensent souvent que nous essayons de résoudre des problèmes techniques. (...) Lorsque nous avons examiné les articles scientifiques et les entretiens avec les experts, nous avons découvert que la technologie n'était pas le principal problème mais que c'était plutôt les questions juridiques*". Il s'agirait selon lui de s'accorder sur les définitions de base afin de construire par la suite ces projets d'interopérabilité. La définition du terme "utilisation secondaire" est mentionnée comme point de divergence entre État. Établir une base commune de cadrage permettra de définir l'utilisation des données par ces projets : « *Peuvent-elles être utilisées pour l'enseignement, les statistiques, la recherche et l'innovation ? Le secteur privé peut-il utiliser les données pour la recherche scientifique ou est-ce seulement pour le secteur public ?* ».[cxxxviii]

Il convient néanmoins de souligner les liens d'intérêts parfois conflictuels entre les entités de centralisation de données internationales et leur proximité avec certains data brokers (souvent Outre-Atlantique) les revendant aux plus offrants. Il ne serait pas irraisonnable d'affirmer que les régulations restrictives de protection ne siéent pas aux individus essayant de capitaliser dessus.

Enjeux de souveraineté :

L'exemple du data broker américain IQVIA et le rôle de son président France, Jean-Marc AUBERT dans la mise en place du *Health Data Hub* (HDH) français est symptomatique d'une opacité de fonctionnement de gouvernance de ces projets. En effet, Jean-Marc AUBERT était encore un cadre de la société américaine lorsqu'il a été nommé à la tête de la mise en place du *Health Data Hub* et, après avoir achevé le lancement du HDH, il a réintégré IQVIA en tant que président France.

Il est à noter qu'il est à craindre que l'entité américaine profite de l'utilisation des données des Français pour les monnayer aux plus offrants permet d'émettre des suspicions légitimes quant à l'éthique médicale et aux sujets de souverainetés des informations initialement confidentiels des ressortissants français.

Les résultats de l'implémentation du *HDH* sur le paysage français favorisent le travail des data broker car les données sont préalablement lissées et uniformisées grâce à HL7 FHIR. Les data broker sont ainsi libres de les commercer telles quelles sans besoin de reformatage. Une question demeure : comment se fait-il que les data

brokers aient la permission d'avoir accès à de telles bases de données ? La réponse serait liée à l'absence d'obligation de présenter une justification liée à "la recherche, une étude ou une évaluation". Il suffirait en effet d'invoquer "l'intérêt public" pour accéder aux données de santé du Hub. La notion "d'intérêt public" étant juridiquement flou, cette dernière favorise les data brokers pour accéder aux données.[cxxxix]

Le contrôle et consentement :

Comme évoqué dans le cas des data brokers, la question du consentement au recueil des données se pose bien que le RGPD et son article 9[cxl] disposent que la collecte des données de santé est autorisée légalement dans l'Union européenne et ses États membres. Néanmoins, le recueil et l'exploitation des données doivent être anonymes lorsqu'elles sont faites à des fins d'utilisation secondaire[cxli]. La collecte et le traitement des données s'avèrent donc parfois plus complexe que ce que l'aspect juridique nous propose.

Ainsi des problèmes concernant l'anonymisation des données ont été soulevés dans *Cash Investigation* de mai 2021. L'enquête révèle que l'entreprise IQVIA récupérait en 2021 dans différents hôpitaux français (Tours, Besançon, Strasbourg) les données de santé des services d'oncologie. Ces services qui traitent les malades de cancer n'ont pas été choisis par hasard, le traitement des cancers est une industrie pharmaceutique particulièrement lucrative. Comme vu plus haut, IQVIA[cxlii] justifie l'interopérabilité entre établissements de santé et data brokers dans le but d'œuvrer en faveur de « l'intérêt public ». Or avec un chiffre d'affaires prévisionnel d'environ 15.5 milliards de dollars en 2024, il ne serait pas aberrant de supposer que les dividendes versés aux actionnaires soient l'un des sujets prévalant du comité exécutif, au potentiel détriment dudit "intérêt public".

Le principe d'un consentement libre et explicite peut lui aussi être remis en cause. Alors que des millions de données de santé de patients sont récoltés, dans une situation d'urgence et de détresse, ces derniers ne semblent pas avoir conscience que leur accord implique la transmission, l'exploitation et la monétisation de leurs données médicales.

Un autre cas d'étude réside dans la collecte des données liés aux montres de sport connectées. Bien que les CGU - Conditions Générales d'Utilisation - soient acceptées par l'utilisateurs lors de l'installation de la montre et de son application mobile, leur longueur et leur technicité ne permettent pas aux usagers d'en comprendre la portée Et pourtant, leurs données seront vendues et exploitées avec leur consentement. Il serait alors techniquement possible d'identifier un individu via ses données sportives (désanonymisation des données via des recherches en OSINT) ouvrant la voie, dans un monde dystopique, à l'utilisation de ses fréquences cardiaques pour accorder ou non un crédit par une banque.

Il faut donc, au-delà de prôner le consentement, remettre en avant l'aspect, « accessible » et « explicite » des fins de la collecte des données pour protéger efficacement le consommateur.

L’interopérabilité des données pose la question de la localisation de ces dernières, ainsi que de leurs niveaux de protection. Selon Licínio Kustra Mano, charge des systèmes d'information à la Direction générale de la santé et de la sécurité alimentaire à la Commission Européenne. « Il n'existe aucune base de données européenne centralisée qui regrouperait toutes les données des patients […] Les informations restent là où elles ont été collectées et on y accède quand on en a besoin ».

S’il n’existe aucune base de données regroupant toutes les données de patients, l’Internet n’a pas de frontières. Certaines données transitent dans des États étrangers. Selon le principe de territorialité des lois, même si la France assure la confidentialité et l’intégrité des données médicales dans son territoire, elle n’en a pas la capacité quand ces données transitent à l’étranger. Les autres États étrangers membres de l’UE, dans le cadre du RGPD, n’ont pas de position hostile par rapport à la protection des données personnelles.

Cependant, les États-Unis constituent un exemple de risque d’atteinte à la protection des données de santé d’un citoyen français. La législation américaine permet à l’état de disposer des données personnelles sur le fondement de suspicion de terrorisme ou d’espionnage. Cette règle pourrait faire l’objet d’abus.

Aussi, les données de santé sont d’autant plus vulnérables qu’elles peuvent faire l’objet de fuite ou d’attaques en France et à l’étranger. En 2021, le gouvernement américain annonçait que plus de 40 millions de patients avaient vu leurs données médicales compromises. Des technologies qui ne sont pas encore appréhendées par la loi peuvent présenter un risque pour la protection des données, notamment le Cloud (un système permettant de stocker des données sur un serveur distant). Quand des données sont stockées sur le cloud, elles se retrouvent dans des Datacenters qui peuvent être localisés dans des pays étrangers. Se pose alors la question de savoir qui dispose de quel droit sur ces données dans ce cas-là. Les données médicales ne semblent néanmoins pas faire l’objet de stockage massifs dans des Clouds étrangers pour l’instant.

À noter que des progrès sont réalisés en France pour résoudre ce problème : En 2009 le gouvernement français élaborait le projet « Andromède », qui prévoit de stocker sous la forme d’un « Cloud souverain » les données nationales du gouvernement, de son administration et d’autres entreprises.

Face à ces différents risques, la France et l’Union européenne ne peuvent garder cette dynamique. De nombreuses actions sont possibles en s’appuyant sur la force réglementaire de la France et de l’Union européenne. Les acteurs français sont compétents mais ils doivent recevoir le soutien nécessaire à leur développement international.

Partie 4 : Les actions possibles pour renforcer la position de la France sur le marché des données de santé

A. Le positionnement stratégique d'autres pays européen

1. La Suisse, exemple d'une protection solide des données

La Suisse se distingue par sa neutralité numérique et ses standards élevés en matière de protection des données. Elle s'appuie sur des centres de données certifiés et hautement sécurisés pour garantir que les informations restent sur son territoire.

En 2020, la Suisse a adopté la nouvelle Loi fédérale sur la Protection des Données (nLPD), qui vise à mieux protéger les données personnelles, dont les données de santé, et à améliorer leur traitement.

Entrée en vigueur en septembre 2023, la nLPD est le résultat de l'évolution technologique et sociale, notamment l'utilisation accrue d'Internet, des smartphones, des réseaux sociaux, du *Cloud* et de l'Internet des objets (*IoT*).

Certains éléments de la loi permettent à la Suisse de renforcer la protection de ses données de santé, lui permettant d'adopter une position stratégique dans le domaine:

- L'inclusion des données génétiques et biométriques dans la catégorie des données sensibles permet de renforcer la protection de ces informations cruciales dans le domaine de la santé. Bien que la Suisse ne soit pas membre de l'UE, elle adapte régulièrement ses lois pour rester alignée sur le RGPD afin de faciliter les échanges économiques avec l'UE. La Loi fédérale sur la protection des données (nLPD), entrée en vigueur le 1er septembre 2023, reprend ces concepts[cxliii] :
    - PbD : Obligation pour les entreprises d'intégrer la protection des données dès la conception des traitements.
    - PbDf : Les entreprises doivent configurer par défaut leurs systèmes pour limiter les traitements de données au strict minimum nécessaire.
- L'obligation de mener des analyses d'impact en cas de risque élevé pour la personnalité ou les droits fondamentaux s'applique également aux traitements de données de santé, renforçant la protection des individus en Suisse.

Cette obligation s'applique pour toutes les entreprises et organisations qui traitent les données, ainsi que leur sous-traitant.

- L'extension du devoir d'informer lors de la collecte de données personnelles concerne également le secteur de la santé et renforce la transparence de la Suisse dans ce domaine.
- L'obligation de tenir un registre des activités de traitement permet à la Suisse de mieux contrôler et suivre l'utilisation des données de santé.

La Suisse a également adopté une initiative pour la numérisation des données de santé.

Sur la base du volontariat des citoyens, qui choisissent de créer un Dossier Électronique du Patient ou non, le DEP est géré par des plateformes régionales, certifiées par l'État.

Bien que l'idée soit pertinente pour une gestion optimale des données de santé, son adoption reste limitée et concerne encore une faible part de la population.

Également, l'interopérabilité de la donnée de santé Suisse est l'un des défis majeurs en ce qui concerne le secteur : même si la Confédération a introduit des standards techniques communs, les différences cantonales font que les données et les protocoles de communication ne sont pas tout le temps transmissibles de façon simple.

Malgré cela, plusieurs initiatives pour l'innovation et la recherche sont mises en place en Suisse : le *Swiss Personalized Health Network*, un programme cherchant à promouvoir l'utilisation de données de santé anonymisées et pseudonymisées pour la recherche.

D'autres initiatives sont également mises en avant, notamment sur les projets d'intelligence artificielle et d'amélioration des soins.

Outre ces aspects, la Suisse conserve à travers l'OBSAN, un droit de regard sur les santés de manière à promouvoir aussi l'innovation à travers l'analyse et l'utilisation des données de santé.

L'une des difficultés auxquelles la Suisse doit faire face est due à son modèle fédéral complexe, basé sur la décentralisation, n'est pas forcément efficace pour améliorer le système de gestion de données de santé qui demande à développer une interopérabilité importante.

2. L'Estonie, un exemple de souveraineté et de résilience

L'Estonie gère ses données de santé de façon souveraine, notamment en ce qui concerne la numérisation de son système de santé.

95% des données médicales des citoyens estoniens sont accessibles en ligne par leur propriétaire de manière sécurisée[cxliv].

L'Estonie a par ailleurs créé un dossier médical électronique (DME) en 2008, permettant de centraliser les différentes données (examens et résultats, ordonnances, diagnostics, etc...).

Cette centralisation permet un stockage sécurisé de ces données sur une plateforme nationale unique.

Les patients ont accès à leurs données de santé via un portail (e-Patient). Ces données sont également interopérables, car les services publics estoniens (notamment les hôpitaux, cliniques, laboratoires) ont notamment un besoin fort d'accès et d'utilisation optimale de ces données.

La blockchain fait également partie intégrante de la stratégie de protection des données de santé estonienne, assurant à la fois une traçabilité et une transparence importante. Ce système repose sur la carte d'identité numérique estonienne, sécurisée notamment par un cryptage de données.

La signature numérique tient également une place importante dans ce système, permettant d'attester de la véracité de documents et de données.

La prescription peut également être électronique (99% des prescriptions sont électroniques).

Les Estoniens ont un contrôle total de leurs données : ils peuvent consulter une liste des personnes ayant accédé à leurs données, et peuvent également restreindre l'accès à certains professionnels ou même refuser l'accès et l'utilisation.

De plus, l'Estonie utilise la plateforme *X-Road*, la plateforme de transfert de données interopérables, qui permet un routage des données et des accès et empêchent la centralisation des données (les données de santé ne sont pas stockées sur le même support que les données financières)[cxlv].

Enfin, le monde de la recherche profite aussi de ce système souverain: les données de santé sont anonymisées, et les chercheurs doivent être habilités pour y accéder.

L'Estonie est donc un bon exemple de pratique de gestion des données de santé qui s'appuie sur quatre piliers principaux : la numérisation complète et contrôlée, l'utilisation de technologie à sécurité élevée, l'assurance du contrôle permanent par les citoyens de la donnée ainsi que la transparence totale de l'utilisation de la donnée, et enfin l'interopérabilité efficace (mais aussi régulé par des normes de protection de données strictes).

3. Singapour, un exemple de souveraineté à travers l'*Open Source*

Singapour se distingue du modèle français grâce à son utilisation de solutions Open Source garantissant sa souveraineté numérique, notamment en matière de données

de santé. Concrètement, les logiciels ou solutions numériques utilisés ou développés par Singapour sont ouverts : leur code source est librement accessible, modifiable et réutilisable[cxlvi].

Cette volonté s'est traduite par différentes initiatives, dont GovTech (Government Technology Agency), une agence gouvernementale dédiée au développement de solutions numériques pour l'État et les citoyens. GovTech s'appuie activement sur l'Open Source pour concevoir des outils accessibles, transparents et flexibles, qui permettent une plus grande autonomie :

- Cela évite la dépendance aux géants étrangers qui vendent des solutions « clés en main », mais qui en restent les propriétaires.
- Ce modus operandi permet à Singapour de développer en interne ses propres outils, sans dépendre de licences onéreuses ou de prestataires étrangers.

Les technologies Open Source sont également utilisées pour les infrastructures critiques toujours dans le but de réduire la dépendance aux solutions de propriétés étrangères, ce qui permet une meilleure maîtrise et flexibilité. On peut notamment citer :

- Le SingPass, le système d'identification numérique des citoyens, intègre des composants Open Source dans son architecture.
- Le FormSG, un outil Open Source, facilite la création de formulaires numériques pour les services publics.

Nous pouvons citer également le projet Electronic Medical Report (EMR), né en 2018 qui permet d'adresser directement les données au ministère de la Santé Singapourien. Sur la base du volontariat cette stratégie fait plus écho aux institutions publiques tandis que le privé privilégie la fidélisation et incite les patients à rester chez eux, les acteurs du privé n'ont donc que peu d'intérêt à rejoindre ce projet. Cette double démarche leur offre une gestion décentralisée des données et permet d'éviter une attaque dévastatrice pour tous les citoyens.

En misant sur l'Open Source, Singapour a réussi à limiter sa dépendance technologique tout en encourageant l'innovation locale. Un autre point fort de cette méthode réside dans la résilience de ses infrastructures. Bien que cette stratégie est assez situationnelle étant donnée la situation de Singapour, ces pistes peuvent être intéressantes à explorer pour un pays comme la France.

B. Assurer l'indépendance numérique française et réduire les dépendances extérieures

1. Axe défensif : consolider le marché national

L'introduction de la préférence nationale dans les appels d'offres publics pourrait être un levier important pour renforcer la souveraineté numérique de la France. Depuis 2019, l'article L2112-4 du Code de la commande publique permet d'imposer des quotas pour favoriser les fournisseurs français, notamment pour garantir la « sécurité des informations ou des approvisionnements ».

Cela offrirait une réelle opportunité de réduire la dépendance aux hyperscalers Américains et de soutenir le développement des acteurs locaux. En privilégiant des solutions souveraines, la France pourrait non seulement sécuriser ses données sensibles, mais aussi encourager l'émergence et la compétitivité de nouvelles entreprises technologiques françaises.

En effet, en mettant l'accent sur des acteurs locaux dans les appels d'offres, la France créerait un environnement favorable à l'innovation. Les entreprises françaises auraient davantage d'opportunités pour se développer, expérimenter et perfectionner leurs produits, ce qui renforcerait à terme l'écosystème numérique national. De plus, cette démarche favoriserait la création de nouvelles solutions adaptées aux besoins locaux, et offrirait des alternatives aux hyperscalers Américains. Cela aurait également des effets positifs sur l'emploi dans le secteur technologique, en stimulant la formation de talents locaux et en renforçant l'attractivité de la France en tant que hub technologique européen.

Adapter les cahiers des charges des appels d'offres publics en fonction des spécificités et des atouts de nos fleurons nationaux pourrait constituer une stratégie efficace pour renforcer la souveraineté numérique de la santé et du cloud en France. En fixant des exigences précises, telles que l'obtention de certifications françaises par exemple, il devient alors possible de favoriser nos entreprises tout en garantissant un haut niveau de sécurité pour les données sensibles.

Prenons l'exemple du Health Data Hub : en rendant la certification SecNumCloud obligatoire pour la gestion des données de santé, la France aurait pu écarter automatiquement les hyperscalers américains comme Azure, tout en offrant une opportunité unique à des acteurs nationaux tels qu'OVHcloud ou Outscale. Cette démarche aurait pu garantir non seulement une gestion souveraine des données critiques, mais aurait pu valoriser également les investissements réalisés par les entreprises françaises pour répondre à des standards exigeants.

Comme l'a souligné le député Philippe Latombe en 2021 lors d'une réunion du Club numérique et Territoires de Com'Publics autour du rapport[cxlvii] d'information "*Bâtir et promouvoir une souveraineté numérique nationale et européenne"*, « 1 euro de chiffre d'affaires génère sept fois plus de valeur ajoutée que 1 euro de subvention ». Ainsi, en

favorisant nos entreprises via des appels d'offres adaptés, l'État pourrait stimuler plus efficacement l'économie numérique française, tout en consolidant la souveraineté nationale. (Source:Alliancy[cxlviii])

Investir pour créer un fleuron français ou européen souverain sur le modèle d'Airbus. Ce cas illustre parfaitement comment une stratégie européenne coordonnée peut renverser un secteur dominé par les Américains. Face à la domination de Boeing dans les années 60, Airbus a émergé grâce à des investissements publics massifs, des politiques protectionnistes ciblées et une mutualisation des savoir-faire des pays membres de l'UE. En répartissant la production entre les différents États, l'Europe a su créer un acteur compétitif, capable de rivaliser puis surpasser le monopole américain grâce à des innovations comme l'A320 et à des politiques commerciales agressives avec des prix compétitifs et des contrats plus flexibles.

Appliquer ce modèle au numérique pourrait permettre de réduire la dépendance européenne aux GAFAM. Avec des financements publics ciblés, des cahiers des charges favorisant les acteurs locaux, et une meilleure coopération entre les États membres, l'Europe pourrait bâtir un écosystème numérique souverain. Un "Airbus du numérique" qui permettrait à l'Europe de devenir une alternative sérieuse aux GAFAM, en garantissant la souveraineté sur ses données stratégiques et en stimulant l'innovation au sein de son écosystème local.

CONSTAT	MESURES	MISE EN PRATIQUE
Sur-représentation des GAFAM dans le marché du cloud Français	Introduire la préférence nationale dans les appels d'offres publics	• L'article L2112-4 du Code de la commande publique permet d'imposer des quotas pour favoriser les fournisseurs français
Appels d'offres de projets d'intérêt national remportés par des puissances étrangères	Adapter les cahiers des charges des appels d'offres publics pour favoriser nos acteurs locaux	• Imposer des certifications Françaises comme SecNumCloud • Transmettre en amont les cahier des charges à nos entreprises locales
Aucune entreprise Française ou Européenne n'a la capacité de concurrencer sérieusement les GAFAM	Adopter un stratégie similaire à celle qui a été utilisé avec Airbus pour créer une alternative aux hyperscalers américains	• Investissements publics massifs • Politiques protectionnistes ciblées • Mutualisation des savoir-faire des pays membres de l'UE

Source : tableau fondé sur des données open source et réalisé par le groupe 20 du QuestIE de l'EGE

2. Axe offensif : Stratégie française juridique à développer

Il semble impératif d'empêcher ce qu'on appelle le *lock-in* (verrouillage de fournisseur) de la part des GAFAM dans les solutions d'hébergement des données de santé afin de pouvoir transférer facilement les données vers d'autres fournisseurs. Plusieurs initiatives existent déjà :

Règlement Européen sur le libre transfert des données non personnelles (2018): Ce règlement promeut la libre circulation des données non personnelles dans l'Union européenne et encourage l'élimination des barrières à la portabilité entre fournisseurs cloud. Cependant, il reste non contraignant sur la mise en œuvre technique de l'interopérabilité.

- **Le Code de conduite SWIPO (Switching and Porting)**: Ce code, adopté en 2020, encourage les fournisseurs cloud à faciliter la portabilité des données et des applications. Cependant, il reste volontaire et manque d'impact contraignant.
- **Le label SecNumCloud de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)** impose des critères stricts pour les fournisseurs cloud souhaitant obtenir une certification, y compris des mécanismes facilitant la migration et la portabilité des données.

La recommandation principale serait de transposer l'aide à la mobilité bancaire, instaurée dans de nombreux pays (notamment avec la loi Macron en France), au service cloud. Cette loi aurait pour objectif de permettre aux clients de changer de fournisseur de service cloud, sans obstacles administratifs ou financiers majeurs. Elle pourrait alors s'inspirer des 4 principes fondamentaux inclus dans la loi Macron : la simplification des migrations, des délais de migration réglementés, la gratuité ou la transparence des coûts, et un support client.

L'Union Européenne/France pourrait créer une autorité proactive qui surveillerait les pratiques anticoncurrentielles des GAFAM. Ainsi, L'Union européenne pourrait maintenir la pression sur les GAFAM avec un cadre évolutif d'amendes dissuasives, et inclure des suspensions d'accès au marché public en cas de récidive. Cette approche pourrait s'inspirer des sanctions européennes déjà imposées[cxlix] mais avec une portée renforcée. Ces amendes infligées aux GAFAM pourraient alimenter un fonds destiné à financer l'innovation locale et à soutenir les start-ups et PME européennes. Cela pourrait s'accompagner de crédits d'impôt pour les entreprises sélectionnées pour tenter de combler l'écart technologique.

Lancement d'une offensive médiatique et politique : Actuellement, les citoyens et les entreprises françaises sont insuffisamment informés des risques associés à l'hégémonie des GAFAM, notamment dans le domaine des données de santé. Cette méconnaissance généralisée freine l'adhésion aux initiatives souveraines et perpétue une dépendance excessive aux solutions technologiques étrangères. Pour remédier à cette situation, il est crucial de lancer une campagne de communication massive visant à sensibiliser le grand public et les acteurs économiques aux dangers liés à cette dépendance technologique. Cette campagne devrait non seulement informer sur les

risques pour la sécurité des données, mais aussi valoriser les alternatives nationales et européennes en matière de souveraineté numérique. Pour être efficace, elle devra s'appuyer sur une mobilisation des think tanks, des médias, et des influenceurs qui pourront diffuser ce message à grande échelle. En sensibilisant l'opinion publique, cette campagne exercera une pression sur les décideurs politiques afin qu'ils adoptent des mesures concrètes, soutenant l'indépendance numérique et favorisant la mise en place de solutions technologiques locales et souveraines.

Un autre axe d'amélioration, sur un plan offensif serait d'Encourager une diplomatie numérique offensive. Les initiatives européennes visant à établir une infrastructure numérique souveraine, comme Gaia-X, rencontrent des difficultés à se faire une place face aux standards dominants et aux pressions des géants américains. De plus, les divergences entre les pays européens affaiblissent cette ambition commune, rendant l'Europe vulnérable aux stratégies technologiques extraterritoriales. Pour surmonter ces obstacles, la France doit adopter une diplomatie numérique proactive, visant à harmoniser les politiques de souveraineté numérique au sein de l'Union européenne. Cela implique un soutien renforcé à des projets tels que Gaia-X, tout en adoptant une posture ferme contre l'application extraterritoriale du Cloud Act américain, qui menace la protection des données européennes. En cas de non-conformité des acteurs étrangers aux exigences européennes, des menaces d'exclusion totale devraient être envisagées. Parallèlement, il est essentiel de négocier des garanties solides pour assurer la souveraineté numérique, garantissant ainsi que les données sensibles des citoyens et entreprises européennes restent protégées contre les ingérences extérieures.

CONSTAT	MESURES	MISE EN PRATIQUE
Lock-in des GAFAM	Imposer l'interopérabilité des données	• Inspirer une loi similaire à l'aide à la mobilité bancaire (loi Macron) : simplification des migrations, délais réglementés, gratuité ou transparence des coûts, support client obligatoire
Pratiques anticoncurrentielles des GAFAM	Créer une autorité proactive pour surveiller et sanctionner les pratiques anticoncurrentielles	• Mettre en place un cadre évolutif d'amendes dissuasives, incluant des suspensions d'accès au marché public en cas de récidive. • Utiliser les amendes pour alimenter un fond dédié à l'innovation locale et aux start-ups européennes
Manque d'informations sur les risques de l'hégémonie des GAFAM et de soutiens étatique aux solution souveraine	Lancer une offensive médiatique et politique	Mobiliser les médias, les Think tanks et les relais d'influence pour sensibiliser aux risques et valoriser les solutions souveraines
Les initiatives européennes pour une infrastructure numérique souveraine peinent à s'imposer face aux pressions américaines	Encourager une diplomatie numérique offensive	Renforcer Gaia-X et négocier des garanties pour limiter l'impact des lois extraterritoriales comme le Cloud Act

Tableau fondé sur des données open source et réalisé par le groupe 20 du QuestIE de l'EGE

C. Les stratégies pour renforcer la position française dans les projets européens d'interopérabilité

1. Stratégie de réforme régulatoire : légiférer l'interopérabilité des systèmes de santé

Alors que l'approche européenne a été abordée dans le paragraphe 1. A. faisant un état des lieux des initiatives mises en place, la création d'un espace européen des données dans le secteur de la santé reste l'une des priorités de la Commission Européenne tel qu'expliqué par l'Union Nationale des Professionnels de Santé[cl] : "La création d'un espace européen des données est l'une des priorités de la Commission pour la période 2019-2025, y compris dans le secteur de la santé." Par ailleurs, les formats HL7 et FHIR actuellement utilisés pour la transmission des données entre hôpitaux et systèmes médicaux ne doivent pas obérer la mise au point d'un dispositif plus complet de transmission des données.

À ce titre, une proposition de réglementation sur l'espace européen des données de santé a été formulée en 2022 dans laquelle la Commission européenne indiquait son souhait de développer un format européen d'échange de dossiers de santé électroniques. Ce format, basé sur des normes ouvertes, visait à garantir un accès sécurisé aux données sanitaires des citoyens de l'UE. Cette initiative évoquait sans les nommer des mesures incitatives pour encourager l'adoption du format d'échange européen, notamment l'accès à des financements européens (la Commission européenne avait fait le choix de mobiliser des fonds du programme *Connecting Europe Facility* et d'*Horizon 2020* pour soutenir le développement de ce format).

Mais cette proposition qui manquait encore d'ambition n'a pas été suivie d'effet. Depuis 2022, aucune initiative d'envergure n'a été annoncée. Néanmoins, le recours à l'adoption d'un règlement européen apparaît comme l'outil idoine pour imposer aux États membres un système uniformisé. Celui-ci pourrait s'appuyer sur les différents systèmes nationaux de santé à la condition d'éviter des instabilités dans le système. Il est à noter que le système français mis en place, en raison de son efficacité, pourrait être présenté comme une solution opérationnelle pour les États de l'union non encore dotés de systèmes nationaux.

De cette manière, il semble possible pour la France de constituer et proposer un projet autour de ce qu'elle a mis en place sur son territoire avec l'agence numérique de santé (ANS), point de contact de MaSanté@UE. L'ANS met ainsi en œuvre Sesali.fr (Service Européen de Santé en Ligne) qui permet aux professionnels de santé français d'accéder à la synthèse médicale d'un patient européen de manière sécurisée, structurée et en français.

L’idée alors ne serait pas de créer une structure pan-européenne mais d’imposer à chaque État membre de collaborer afin de permettre à leurs systèmes d’atteindre un niveau d’interopérabilité fluide. Mais une telle harmonisation présente un risque dilatoire dans une union à 27 pays où chaque État a atteint un niveau de digitalisation de l‘information différent. D’autre part, il est à redouter que certain État fasse preuve de résistance dans la mesure où des partis eurosceptiques constituent leur gouvernement ou occupent une place importante sur leur scène politique intérieure. Pourtant il est à considérer qu’une poignée d’État déjà impliquée dans le programme MaSanté@UE (France, Allemagne[cli], Italie[clii], Pays-Bas[cliii]) peut créer une dynamique positive au sein des membres de l’UE.

Cependant, cette solution pourrait nécessiter la création d’un système d’échange intermédiaire voire potentiellement la création d’un organisme de gestion de ce système.

2 Stratégie de la centralisation : création d’une agence du numérique en santé européen

Si une réforme régulatoire apparaît comme la stratégie la plus susceptible d'obtenir l'accord des États membres, elle n'atteindra pas l’objectif d’uniformisation des systèmes et laisserait aux États la liberté de fixer leur propre calendrier. Alors que la création d’un système d’échange intermédiaire géré par un organisme européen pourrait alors être nécessaire pour accompagner cette stratégie, il est intéressant d’envisager une stratégie plus globale autour de la création d’une agence numérique de santé européen investie par le parlement européen d‘une autorité régulatoire.

Si l'objectif principal d’uniformiser les données serait alors nécessairement atteint, la mise en place d’une telle agence présenterait d’autres avantages importants pour les systèmes de santé européens.

Tout d’abord, elle renforcerait la résilience sanitaire. En effet, une telle agence permettrait d’accroître la coordination inter-étatique lors de futures crises sanitaires notamment en opérationnalisant l’échange des données de santé. Elle favoriserait également la détection de nouvelle crise par le croisement des données. Enfin, en l’absence même de crise, cette agence simplifierait le partage des bonnes pratiques entre pays européens.

Ensuite, cette agence stimulerait nécessairement l’innovation et la recherche. Elle pourrait être désignée pour piloter la politique numérique de santé et son développement. Sous son autorité, elle faciliterait également l’accès aux données de la santé pour la recherche médicale, dans le respect de la confidentialité. Enfin, l’uniformisation des données permise par l’agence concourrait à l’émergence de champion européen dans le domaine de la e-santé.

Il est à noter également que cette agence serait génératrice d'économies pour les États membres (en évitant les redondances nationales) et pourrait être financées par des fonds européens.

Cependant cette stratégie n'est pas sans risque. La formation d'un nouvel organisme européen devrait passer par de nombreuses étapes dans son élaboration qui serait de fait pan-européen et qui pourrait voir la vision de la France diluée lors de son approbation par le Parlement européen et de sa mise en œuvre par la Commission européenne. De plus, le processus ne sera certainement pas sans risque de blocage car il est fort probable que les États membres et factions dans un Parlement à tendance eurosceptique pourraient faire barrage à une initiative qui ne manquerait pas d'être interprétée comme une nouvelle imposition de la part d'eurofédéralistes.

Pour conclure, une agence numérique de santé européenne contribuerait à créer un véritable espace européen des données de santé plus efficace et moins coûteux.

3 ; Stratégie de l'innovation : création logiciel européen

Alors que les approches législatives et/ou administratives pourraient paraître expéditives et poser des difficultés politiques, et que l'imposition d'une structure administrative centrale dans une Union européenne fragilisée pourrait rendre le projet non viable, il est intéressant de réfléchir à une approche plus consensuelle. Il s'agirait ainsi d'une approche par l'innovation et l'adoption volontaire de nouvelles technologies contribuant à encourager un ralliement rapide à un nouveau système dont l'objectif final resterait l'intégration des systèmes de transmission de l'information en Europe.

La meilleure solution pourrait être le développement d'un logiciel offrant une solution intégrale permettant la transmission instantanée de données médicales encryptées à l'échelle continentale. Il ne s'agit pas ici de remplacer les formats HL7 ou FHIR mais de les intégrer dans un software unique qui, une fois développé, serait offert aux différents États membres. Le logiciel ne serait pas un simple outil de transmission de données mais devrait offrir une solution interactive intégrale permettant de connecter non seulement les divers soignants et hôpitaux mais aussi les patients. Un tel logiciel devrait être équipé d'un moteur de recherche permettant aux patients de trouver des soignants adaptés à leur besoin, de prendre rendez-vous et d'automatiquement transmettre les informations vitales du patient au soignant.

Doctolib, plateforme utilisée en France, est une bonne démonstration de ce concept. La plateforme permet déjà à un patient de chercher divers soignants selon des critères géographiques, de prendre rendez-vous et de transmettre des informations clé en numérisant des documents médicaux ce qui est préférable à leur transport physique ou à l'envoi par voie numérique non encryptée. Un tel logiciel devrait rencontrer un certain nombre de critères. En tout premier lieu une intégration HL7/FHIR et des modalités de communication intra-européennes entre soignants et patients. En deuxième lieu, une base de données encryptée, une fonctionnalité de messagerie

instantanée, un moteur de recherche permettant la prise de rendez-vous et l'utilisation d'identifiants propres à l'identité nationale des divers citoyens de l'UE. Une fois opérationnalisé., ce système serait une véritable révolution en termes d'intégration médicale au niveau européen.

Pour résumer, le logiciel pourrait :

1. Intégrer les systèmes HL7 et FHIR ;
2. Proposer un système de messagerie entre hôpitaux, cliniques, soignants individuels et patients ;
3. Offrir un moteur de recherche permettant de trouver divers soignants à travers tous les pays connectés ;
4. Intégrer un système de paiement ;
5. Permettre de stocker et transmettre des données médicales encryptées.

Le développement d'un tel logiciel est entièrement possible avec le savoir-faire technique français et pourrait potentiellement être une itération sur un logiciel déjà établis tel que Doctolib, ce qui réduirait les coûts de développement. Le financement pourrait être obtenu sur des fonds européens, afin de donner plus de légitimité au projet, ou avec un partenariat public-privé. Avec un nombre suffisant de participants nationaux, l'impératif de participer à ce nouveau système se dessinerait par lui-même car les bénéfices apportés. On parle donc ici d'une approche strictement volontariste sans aucune coercition. Un système efficace ferait ses preuves et la pression en faveur de son adoption viendrait sans doute des populations mêmes des pays réfractaires qui souhaiteraient sans doute bénéficier des avantages d'une meilleure intégration des technologies et de la médecine.

Les avantages d'un tel système sont nombreux :

1. La centralisation des dossiers médicaux des patients permettrait son accès instantané à tous les soignants connectés au système. *In fine* son adoption permettrait un suivi continu de tous les patients tout au long de leur vie.
2. Permettrait une meilleure mobilité des travailleurs de l'UE qui serait capable de se faire traiter plus facilement partout où le système est en place sans avoir besoin de faire des consultations supplémentaires afin d'établir un dossier médical.
3. Permettrait à certains pays d'Europe dotés d'appareils médicaux moins coûteux de bénéficier de tourisme médical en facilitant la tâche aux patients voulant faire du tourisme médical intra-européen. Les bénéfices économiques seraient un argument très fort en faveur de l'adoption du système.

4. Si le secteur TI de France peut être le *driver* principal de l'adoption de cette technologie, cela se traduira non seulement par des retombées économiques importantes mais le contrôle du logiciel de traitement des données médicales par une ou des firmes françaises se traduirait par une influence accrue de la France et donc, une augmentation de sa puissance.

5. Finalement, une fois que le nombre d'utilisateurs de ce système atteindra une masse critique, on pourra considérer la création d'un standard Européen administré par l'UE pour éventuellement remplacer HL7 qui est un standard privé. Cela se manifesterait par un renforcement de la souveraineté médicale européenne. Il serait aussi possible d'envisager une exportation de ce système à des nations partenaires tel que le Brésil ou le Royaume-Uni.

L'option de l'innovation quoique plus complexe sur le plan technique et comportant plus de risques financiers (puisque l'état français et l'industrie engageraient des coûts de développement important sans garantie de succès) est d'abord politiquement moins problématique : basée sur le consensus et l'adoption volontaire, cette approche sera certainement plus efficace pour séduire les partenaires de tendance eurosceptique. Un bon compromis qui se solderait, *in fine* par une augmentation de la puissance française et de meilleures retombées financières pour les populations françaises et européennes.

Les recommandations ici présentées ont vocation de proposer des projets qui, par diverses voies, ont un objectif unique : harmoniser et fluidifier les échanges de données médicales au niveau européen en premier lieu, et renforcer la puissance française par l'augmentation de son influence. Les avantages mais aussi les frictions voire difficultés à leur mise en place ont été identifiés. Le facteur déterminant permettant l'adoption de ces mesures reste la bonne volonté des instances européennes et nationales. Tout de même, il faut s'assurer de proposer un équilibre entre les intérêts des divers étants membres de l'UE qui permettra en fin *in fine* à tous les participants d'en tirer leur propre compte. De tels projets pourraient être menés par une petite communauté de pays dont la France : Une pionnière dans le domaine. Le projet peut paraître complexe, certes, et aussi ambitieux mais, de le mener à termes permettrait à la France de rayonner au sein de l'UE et d'encore une fois mettre de l'avant l'excellence française ce qui ne manquerait guère de contribuer à la richesse et l'influence de la France au sein de l'UE.

Conclusion

La souveraineté française sur les données médicales des citoyens français est difficile à établir. Le droit français, appuyé par le droit européen peine à s'appliquer face à la domination technologique américaine.

Le gouvernement français a choisi, Microsoft pour le Health Data Hub par manque d'acteurs français compatibles. Ce choix, très controversé et maintenu depuis plusieurs années, favorise la participation d'acteurs américain dans le projet européen de gestion de données médicales. Cette présence d'acteurs étrangers ne se fait pas ressentir que sur les infrastructures mais aussi dans les normes de transfert de données. La norme HL7 s'est imposée sur le continent européen et sur les futurs projets de l'Union européenne.

Sur ces deux aspects techniques, le droit américain peut pleinement s'appliquer, notamment sur la récolte de données. L'argument de l'anonymisation est souvent utilisé par les institutions françaises et européennes mais, avec l'émergence de nouvelles technologies comme l'IA ou le développement d'ordinateurs quantiques, les données pourront être désanonymisées. L'Union européenne et la France ne dispose pas encore de leviers suffisant pour se séparer des sociétés américaines. De plus, l'enchaînement des crises géopolitiques fragilise les économies occidentales et bouscule les financements prévus pour le développement de nouvelles technologies ou de chaînes de production souveraines.

La France doit dès lors prendre l'initiative et recourir à la qualité de son secteur technologique afin d'atteindre une position stable. Considérant le risque de fuite de données non maîtrisé vers les Etats-Unis causé par le Cloud Act par le biais des hyperscalers américains, les entreprises françaises prometteuses ont une carte à jouer. D'années en années, la population française prend conscience de l'importance des données qu'elle produit. L'opinion public peut devenir une force impactante dans la mise en place d'acteurs français sur les marchés.

À l'heure où l'innovation et la recherche sont largement dominées par l'Intelligence artificielle, il devient essentiel de développer et de maîtriser une stratégie cloud souveraine. Ces deux secteurs sont intrinsèquement liés et reposent sur des facteurs communs : des équipes spécialisées, des infrastructures à la pointe de la technologie et une gestion maîtrisée des Big Data. En somme, exceller dans le cloud est non seulement un moyen de faire avancer des technologies comme l'IA, mais aussi un levier pour soutenir leur développement à long terme, étant donné que les leaders sur la chaîne de valeur du cloud computing sont également les leaders dans la chaîne de valeur de l'IA.

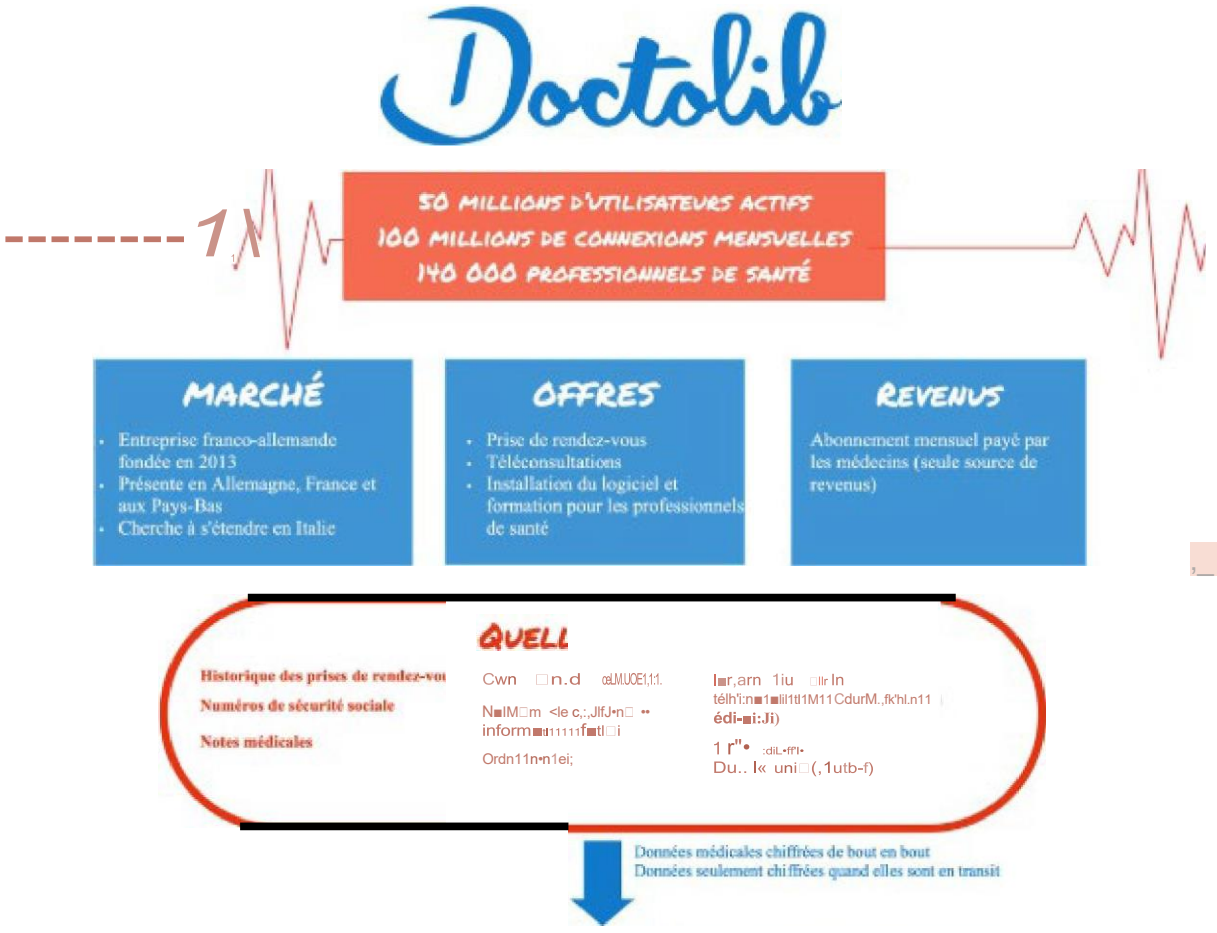
Annexe :

Normes et Standards	Objectifs principaux	Adoption	Forces	Faiblesses	Interactions avec autres normes	Exemples d'utilisation
FHIR	Standardiser l'échange de données de santé en temps réel	Adoption rapide. surtout dans les nouveaux systèmes	Flexible, moderne, compatible avec REST/JSON/XML	Complexité d'intégration initiale	Intègre HL7 V2N3, CDA, SNOMED CT, LOING, DICOM	Portails de santé. applications mobiles. Mon Espace Santé
HL7V2	Échanger des messages textuels entre systèmes	Très utilisé dans les anciens systèmes hospitaliers	Simplicité, large adoption	Obsolète, manque de modularité	Compatible avec CDA, utilise des terminologies (CIM-10)	Systèmes hospitaliers, laboratoires anciens
HL7V3	Structurer les échanges complexes (basésurRIM)	Adoption limitée par manque de silplicité	Structuration robuste	Complexité importante, abandon progressif	Base de CDA, interactions limitées avec HL7V2	□MP en France. projets spécifiques
CDA	Structurer les documents cliniques	□i□a□□; en combinaison	Bonne adaptation pour les dossiers patients	Pas adapté aux flux en temps réel	Utilise HL7 V3, compatible avec FHIR	DMP, rapports médicaux
IHE	Intégrer les normes dans des cas d'usage concrets	Adoption croissante en Europe	Crée des profils pratiques pour workflows spécifiques	Dépend des autres normes	Combine HL7, DICOM, SNOMED CT. FHIR	Échanges hospitaliers, intégration de systèmes PACS
DICOM	Standardiser l'imagerie médicale	Très utilisé dans la radiologie	Universel dans le domaine de l'imagerie	Limité aux données d'imagerie	Compatible avec FHIR et IHE	Radiologie, systèmes PACS
SNOMED CT	Standardiser la terminologie médicale		Exhaustif, supporte l'interopérabilité sémantique	Licence coûteuse, complexité	Intégré à FHIR, HL7, LOINC	
HPRIM	Échanger des doonées simples	Utilisation en déclin	Facile à implémenter dans des systèmes existants	Limité, local à la France	Compatible avec HL7, FHIR	
PN13-IS	Coder les actes pour le système national français	Utilisé dans le secteur public	Simple et adapté au cadre français	Pas de portée internationale	Utilisé avec FHIR pour standardisation	Gestion des actes médicaux en France
INS	Identifier les patients de manière unique		Réduit les erreurs d'identité	Nécessite une adoption complète	Compatible avec FHIR, HL7	Mon Espace Santé, DMP
CIM-10	Classifier les diagnostics		Reconnaissance internationale	Peu détaillé pour certains cas spécifiques	Intégré dans FHIR, HL7	Codage des pathologies
LOINC	Standardiser les tests de laboratoire et observations	Adoption dans les laboratoires	Adapté aux analyses biologiques	Limité à son domaine	Intégré à HL7 el FHIR	Résultats d'analyses, interprétation biologique
CCAM	Coder les actes médicaux en France	Obligatoire en France	Adapté au système français de remboursement	Limité au cadre national	Compatible avec FHIR, INS	Gestion des actes médicaux et facturation en France
OMOP-CDM	Modéliser les doonées cliniques pour l'analyse		Standardisation pour□recherche clinique	Adapté aux big data, mais lourd à implémenter	Complémentaire à SNOMED CT, LOING, CIM-10	Analyse des données de santé, épidémiologie
BEACON	Harmoniser les données génomiques	Adoption émergente	Optimisé pour les données de séquençage génomique	Domaine de niche, adoption lente	Interagit avec FHIR et HL7	Recherches en génétique, médecine de précision
Osiris	□:□anu□□□a□□;□sées des registres	Adoption nationale	Adapté aux registres de maladies	Très spécifique à un usage français	□□:émentaire aux systèmes	Registres des maladies chroniques et rares
CIM-11	Évolution de la CIM-10 avec précision accrue	Déploiement progressif	Structure numérique moderne, meilleure granularité	Transition complexe pour les systèmes existants	Utilisé avec HL7, SNOMED CT, FHIR	Codage des maladies complexes et
ICHI	Classifier les interventions médicales	Adoption croissante	Compatible avec CIM-11, couverture large	Encore en phase d'adoption	Complémentaire à CIM-11 et SNOMEO CT	Codification des interventions chirurgicales et cliniques

Annexe 1 : *Comparatif des normes et des standards appliqués aux systèmes d' interopérabilité de santé*

Annexe 2 : *Schéma de présentation du système d'interopérabilité Diane*

***Annexe 3** : Fiche sur l'acteur Doctolib*



RISQ l:S

Am:uo11Wtb &m(;i fit so1.mi"s à ln lntlo118mttlaluc(Clooo ACT! amori.se les mmriirs RrMJiC8illcas il **D({MeJ DID{** info=tiom

...rn;::kœ 1r 1"" :St"f\ i,:ur,; de-.; t"nlJÇJ1Tis. ['lill ii.1 lt;&(..m 1:11mf«r-n)

'tp'jo1wtfTI111,t" dg,n11c'li pm,;'liMt.•,,; mm,: i:n ZO:'f i;IV 61.,8 rhiz:-vnns Jin1't':, 1,Jrt!!' fi.Jil di= r.:1.1n, d t l :P,on-c-; i: mlst nom , "'i]ec,;111h

1n1ltl111ilill Û\'cau !i.111 c1Li11t'tlll crd

Ab ·mtr de t.bllTremell.lde out bo• . Co.i,rral.ft:tru.'lll aJiirm.l.1lOO!l de Durnlltb. cc-namt> ii,uDl:c, bJc de, utilbattlil>.

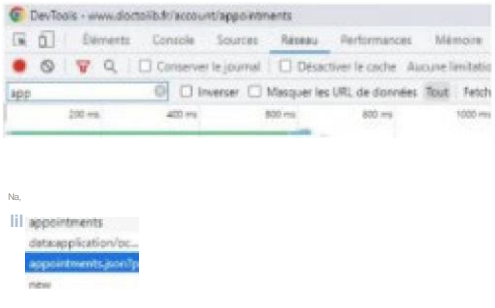
ci:,nime l<""S Tl'nd<".7-S'Of.m<'>1-rn1.11 i: s,o t]'ll' cnifff"ée, d. r-:JIJl n hn11•

AcL:l!♦ll;lhili•ir d d,unnl"t'lii • rn 111specl.:!11 le ,:-.;_de m1m.:e d'i.:.11e ♦-=s,io.. iiiii:-;;1♦♦L1r,•t.a n d♦bogllt'lLT♦11("-1 JH.'"-""irble d ,,.stub-..erl♦♦

u110mwlt m C'OclfLili: 1tid l'.:Sl 1.clC?-i qi.t: a: rcm:lt.:-\'OU.S: paKMl((uIJr. .

&tnlIrL

l r ♦ rDocmLib



Légende : page code source Doctolib où l'on peut voir les informations sur les rendez-vous de la personne

1lfo. IJ. 1 1

Sources

[i] *RBC Capital Markets | Navigating the Changing Face of Healthcare Episode*. (s. d.). https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion

[ii] Qu'est-ce ce qu'une donnée de santé ? (s. d.). CNIL. https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

[iii] Agence du Numérique en Santé. (s. d.-b). *Liste des hébergeurs certifiés*. Agence du Numérique En Santé. https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies

[iv] *Comprendre le RGPD*. (s. d.). CNIL. https://www.cnil.fr/fr/comprendre-le-rgpd

[v] *ISO/IEC 27001 : 2022*. (s. d.). ISO. https://www.iso.org/isoiec-27001-information-security.html

[vi] Feel Agile. (2024, 19 juin). *Comprendre la certification HDS - Feel Agile*. https://feelagile.com/certification-hds/

[vii] *Arkhn Blog | La certification HDS*. (s. d.). https://www.arkhn.com/fr/blog/certification-hds#:~:text=Il%20existe%206%20niveaux%20possibles%20de%20certification%20HDS.&text=Les%20niveaux%201%20et%202,qui%20encadrent%20les%20environnements%20applicatifs

[viii] *Arkhn Blog | La certification HDS*. (s. d.). https://www.arkhn.com/fr/blog/certification-hds#:~:text=Il%20existe%206%20niveaux%20possibles%20de%20certification%20HDS.&text=Les%20niveaux%201%20et%202,qui%20encadrent%20les%20environnements%20applicatifs

[ix] Agence du Numérique en Santé. (s. d.-c). *Liste des hébergeurs certifiés*. Agence du Numérique En Santé. https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies

[xi] *Autorité de la concurrence.* Avis 23-A-08 du 29 juin 2023. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.autoritedelaconcurrence.fr/sites/default/files/2023-06/Presentation-4.pdf

[xii] *Autorité de la concurrence*. Avis 23-A-08 du 29 juin 2023. https://www.autoritedelaconcurrence.fr/sites/default/files/2023-06/Presentation-4.pdf

[xiii] Metraux, P., & Metraux, P. (2023, 2 juillet). *Acteurs du Cloud : quelle concurrence ?* Tout Sur Google. https://www.toutsurgoogle.com/acteurs-du-cloud-quelle-concurrence/

[xiv] Democrite.org . http://democritique.org/IT/Cours_CLOUD_Page07.svg.xhtml

[xv] *Couches de cloud computing*. (s. d.). (C) Copyright 2023. https://docs.oracle.com/fr-fr/iaas/Content/cloud-adoption-framework/cloud-computing-layers.htm

[xvi] (2024, 7 mars). *Scaleway annonce sa certification HDS, pour garantir la sécurité des données de santé*. Scaleway. https://www.scaleway.com/fr/news/scaleway-annonce-sa-certification-hds-pour-garantir-la-securite-des-donnees-de-sante/

[xvii] *Our certifications & security*. Scaleway. https://www.scaleway.com/en/security-and-resilience/

[xviii] BIAL-X. Les meilleurs fournisseurs de services cloud en 2024. https://www.bial-x.com/blog/actualite/fournisseurs-de-services-cloud-2024/?utm_source=chatgpt.com

[xix] *Qu'est-ce qu'un PaaS - Définition PaaS*. (s. d.). Oracle France. https://www.oracle.com/fr/cloud/definition-paas/

[xx] Deun, E., Deun, E., & Deun, E. (2024, 5 mars). *Quel Cloud choisir : IaaS, SaaS, PaaS et pourquoi pas le CIPS ? - OUTSCALE blog*. OUTSCALE Blog. https://blog.outscale.com/iaas-saas-paas-cips-quel-avenir-pour-le-cloud/

[xxi] Ibm. (2024, 30 septembre). SaaS. *IBM*. https://www.ibm.com/fr-fr/topics/saas

[xxii] *Doctolib se lance sur le marché du logiciel de gestion de cabinet médical avec une offre « SaaS »* . (s. d.). Caducee.net. https://www.caducee.net/actualite-medicale/15354/doctolib-se-lance-sur-le-marche-du-logiciel-de-gestion-de-cabinet-medical-avec-une-offre-saas.html

[xxiii] Alice-Prayal. (2024, 24 juin). *Explorez le SaaS en santé : l'innovation qui redonne souffle aux DSI*. Enovacom. https://www.enovacom.com/explorez-le-saas-en-sante-linnovation-qui-redonne-souffle-aux-dsi/

[xxiv] Majed, C. (2024, 16 mai). *La stratégie du cloud français à l'épreuve de l'hégémonie des hyperscalers étrangers*. Blog Economie Numérique. https://blog.economie-numerique.net/2024/02/23/la-strategie-du-cloud-francaise-a-lepreuve-de-lhegemonie-des-hyperscalers-etrangers/

[xxv] *OVHCloud*. (s. d.). OVHcloud. https://www.ovhcloud.com/fr/

[xxvi] *ANSSI SecNumCloud*. (s. d.). OVHcloud. https://www.ovhcloud.com/fr/compliance/secnumcloud/

[xxvii] 2022-10-26-ovhcloud-fy22-results-presentation-vdef

[xxviii] *Cloud souverain et de confiance - Docaposte*. (2024b, février 23). Docaposte. https://www.docaposte.com/linstant-numerique-cloud-souverain

[xxix] Atos SE. (2024, 25 novembre). *Cloud et infrastructure - ATOS*. Advancing What Matters. https://atos.net/fr/services/cloud-et-infrastructure

[xxx] Crochet-Damais, A. (2023, 1 mars). *La carte des data centers des clouds amé ; ricains en France*. https://www.journaldunet.fr/web-tech/guide-de-l-entreprise-digitale/1514137-la-carte-secrete-des-data-centers-des-clouds-providers-americains-en-france/

[xxxi] Igrange. (2022, 23 novembre). *Atos déploie avec succès Mon Espace Santé*. Advancing What Matters. https://atos.net/fr/2022/communiques-de-presse_2022_11_23/atos-deploie-avec-succes-mon-espace-sante

[xxxii] Afp, L. F. A. (2024, 3 avril). L'offre de cloud français Numspot accueillera « à la rentrée » ses premiers clients, dont l'Etat. *Le Figaro*. https://www.lefigaro.fr/flash-eco/l-offre-de-cloud-francais-numspot-accueillera-a-la-rentree-ses-premiers-clients-dont-l-etat-20240403

[xxxiv] *Chez quel hébergeur sont stockées les données du SNDS/base principale ? Dans quel pays ?* (2024, 26 janvier). Communauté D'entraide SNDS. https://entraide.health-data-hub.fr/t/chez-quel-hebergeur-sont-stockees-les-donnees-du-snds-base-principale-dans-quel-pays/1858

[xxxv] Hermann, V. (2024b, février 5). *« Ça va être sanglant » : la CNIL autorise les données de santé chez Microsoft*. Next. https://next.ink/126283/ca-va-etre-sanglant-la-cnil-autorise-les-donnees-de-sante-chez-microsoft/

[xxxvi] Maïlys. (2021, 21 mai). *Health Data Hub : Anticor saisit le PNF. - Anticor*. Anticor. https://www.anticor.org/2021/03/26/health-data-hub-anticor-saisit-le-pnf/

[xxxvii] *Le contrat Health Data Hub et Microsoft bient*t rompu*. (2020, 9 octobre). LeMondeInformatique. https://www.lemondeinformatique.fr/actualites/lire-le-contrat-health-data-hub-et-microsoft-bientot-rompu-80654.html

[xxxviii] Local, M. (2024, 7 juin). *Irlande*. Microsoft Local. https://local.microsoft.com/fr/communities/emea/dublin/

[xxxix] *Microsoft France annonce l'ouverture de quatre data centers en France – News Centre*. (2018, 23 janvier). https://news.microsoft.com/fr-fr/2018/01/23/microsoft-france-annonce-louverture-de-quatre-data-centers-en-france/

[xl] Hermann, V. (2024c, février 5). *« Ça va être sanglant » : la CNIL autorise les données de santé chez Microsoft*. Next. https://next.ink/126283/ca-va-etre-sanglant-la-cnil-autorise-les-donnees-de-sante-chez-microsoft/

[xli] Public Sénat. (2022, 3 février). Cédric O bousculé au Sénat sur le choix de Microsoft pour héberger le Health Data Hub. *Public Sénat*. https://www.publicsenat.fr/actualites/non-classe/cedric-o-bouscule-au-senat-sur-le-choix-de-microsoft-pour-heberger-le-health

[xlii] *Microsoft*. (2019, 6 février). Capgemini France. https://web.archive.org/web/20190322151307/https:/www.capgemini.com/fr-fr/partenaire/microsoft/

[xliv] Cash Investigation - France Télévisions. (2024, 13 décembre). *Nos données personnelles valent de l'or - Cash investigation* [Vidéo]. YouTube. https://www.youtube.com/watch?v=cb3jfxMnZU4

[xlv]https://fr.wikipedia.org/wiki/Direction_de_la_Recherche,_des_%C3%89tudes,_de_l%27%C3%89valuation_et_des_Statistiques

[xlvi] Jean-Marc Aubert est retourné chez IQVIA pour devenir président de l'entreprise en France

[xlvii] **Interop'Santé**. (n.d.). *Interop'Santé - Accueil*. Interop'Santé. Consulté le 19 décembre 2024, à l'adresse https://www.interopsante.org/

[xlviii] **HL7 France**. (n.d.). *HL7 France - Accueil*. HL7 France. Consulté le 19 décembre 2024, à l'adresse https://www.hl7.fr/

[xlix] Légifrance. (s.d.). Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000029589477/

[l] Légifrance. (s.d.). Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

[li] Légifrance. (s.d.). Décret n° 2016-993 du 20 juillet 2016 relatif à la lutte contre les ruptures d'approvisionnement de médicaments. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000032922434

[lii] Sénat. (2023, 12 juillet). Rapport « Données de santé »

[liii] *Cloud au centre : la doctrine de l'État*. (s. d.). numerique.gouv.fr. https://www.numerique.gouv.fr/services/cloud/doctrine/

[liv] Lausson, J. (2018, 30 juillet). Souveraineté numérique : la France précise ses plans dans le cloud. *Numerama*. https://www.numerama.com/politique/392780-souverainete-numerique-la-france-precise-ses-plans-dans-le-cloud.html

[lv] *Secteur public*. Scaleway. https://www.scaleway.com/fr/secteur-public/

[lvi] NumSpot. (2024, 10 décembre). *Accueil - NumSpot*. https://www.numspot.eu/

[lvii] Portail-Ie. (2024, 29 février). *Le cloud français peine à raccrocher les wagons de la souveraineté numérique*. Portail de L'IE. https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2024/le-cloud-francais-peine-a-raccrocher-les-wagons-de-la-souverainete-numerique/

[lviii] OUTSCALE, Elevate Your Experiences. (2024, 17 octobre). *Cloud Souverain - OUTSCALE | Elevate your experiences*. OUTSCALE | Elevate Your Experiences - Experience As A Service. https://fr.outscale.com/cloud-experience/cloud-souverain/

[lix] *Clouds de confiance, une souverainet*[?] *au rabais ?* (2023, 8 septembre). https://www.lemondeinformatique.fr/les-dossiers/sommaire-lire-clouds-de-confiance-une-souverainete-au-rabais-250.html

[lx] *Cloud de confiance : quel avenir pour la micro-fus*[?]*e Bleu ?* (2024, 17 janvier). LeMondeInformatique. https://www.lemondeinformatique.fr/actualites/lire-cloud-de-confiance-quel-avenir-pour-la-micro-fusee-bleu-92696.html

[lxi] *S3NS | Thales x Google Cloud visant le cloud de confiance*. (s. d.). https://www.s3ns.io/?utm_source=chatgpt.com

[lxii] Gavois, S. (2022, 15 décembre). *Thales et Google détaillent le fonctionnement de S3ns sur le « cloud de confiance »* . Next. https://next.ink/1531/thales-et-google-detaillent-fonctionnement-s3ns-sur-cloud-confiance/?utm_source=chatgpt.com

[lxiii] Loukil, R. (2023, 6 avril). Faut-il faire confiance aux clouds franco-américains ? *www.usinenouvelle.com*. https://www.usinenouvelle.com/article/faut-il-faire-confiance-

aux-clouds-franco-americains.N2064757?utm_source=chatgpt.com

[lxiv] De Rémur, S. (2024, 9 juin). « L'Etat français et l'Europe doivent prendre conscience des risques qu'il y a à renoncer à la souveraineté économique sur les données » . *Le Monde.fr*. https://www.lemonde.fr/idees/article/2024/06/09/l-etat-francais-et-l-europe-doivent-prendre-conscience-des-risques-qu-il-y-a-a-renoncer-a-la-souverainete-economique-sur-les-donnees_6238189_3232.html?utm_source=chatgpt.com

[lxv] Assemblée nationale. (s. d.). *Projet de loi visant à sécuriser et réguler l'espace numérique*. Assemblée Nationale. https://www.assemblee-nationale.fr/dyn/16/dossiers/DLR5L16N47884

[lxvi] *Modèles d'usage autour du Cloud hybride*. (s. d.). Hitachi Vantara. https://www.hitachivantara.com/en-us/company/events-and-webinars/mod-les-d-usage-autour-du-cloud-hybride

[lxvii] *Le cloud hybride s'installe progressivement dans les entreprises*. (2020, 5 novembre). LeMondeInformatique. https://www.lemondeinformatique.fr/les-dossiers/lire-le-cloud-hybride-s-installe-progressivement-dans-les-entreprises-1142.html

[lxviii] Loukil, R. (2024, 16 septembre). Les explications du PDG d'EDF sur le choix du cloud d'Amazon. *www.usinenouvelle.com*. https://www.usinenouvelle.com/article/les-explications-du-pdg-d-edf-sur-le-choix-du-cloud-d-amazon.N2208434?utm_source=chatgpt.com

[lxix] Magazine, C. (2024, 5 décembre). *EDF joue la carte du NetDevOps en s'appuyant sur l'expertise de NXO*. Cloud Magazine. https://www.cloudmagazine.fr/edf-joue-la-carte-du-netdevops-en-sappuyant-sur-lexpertise-de-nxo/?utm_source=chatgpt.com

[lxx] Du Digital, L. R. (2021, 11 décembre). *SNCF plébiscite son passage dans le Cloud d'Amazon de 7000 serveurs - La Revue du Digital*. La Revue du Digital. https://www.larevuedudigital.com/sncf-plebiscite-son-passage-dans-le-cloud-damazon/?utm_source=chatgpt.com

[lxxi] Lemaire, B. (2024, 18 juillet). Pourquoi la SNCF a fait le choix du full cloud. *Républik IT le Média*. https://www.republik-it.fr/decideurs-it/gouvernance/pourquoi-la-sncf-a-fait-le-choix-du-full-cloud.html?utm_source=chatgpt.com

[lxxii] *Santé numérique | ANR*. (s. d.). Agence Nationale de la Recherche. https://anr.fr/fr/france-2030/programmes-et-equipements-prioritaires-de-recherche-pepr/sante-numerique/

[lxxiii] Inserm. (s. d.). *Institut national de la santé et de la recherche médicale · Inserm, La science pour la santé*. https://www.inserm.fr/

[lxxiv] *Accueil | Inria*. (s. d.-b). https://www.inria.fr/

[lxxv] , 20 millions d'euros

[lxxvi] *1 an de France 2030 : des résultats concrets et des moyens nouveaux pour la santé numérique | info.gouv.fr*. (s. d.). info.gouv.fr. https://www.info.gouv.fr/actualite/1-an-de-france-2030-des-resultats-concrets-et-des-moyens-nouveaux-pour-la-sante-numerique?utm_source=chatgpt.com

[lxxvii] *Appel à projets tiers lieux d'expérimentation en santé numérique*. (s. d.). Groupe Caisse des Dépôts. https://www.caissedesdepots.fr/actualites/appel-projets-tiers-lieux-dexperimentation-en-sante-numerique

lxivBanque des territoires | Groupe Caisse Des dépôts. (2023, 30 mars). https://www.banquedesterritoires.fr/

[lxxix] *Bpifrance - Servir l'Avenir*. (s. d.). https://www.bpifrance.fr/

[lxxx] *Banque des territoires | Groupe Caisse Des dépôts*. (2023b, mars 30). https://www.banquedesterritoires.fr/

[lxxxi] *Page d'accueil | Health Data Hub*. (s. d.). Health Data Hub. https://www.health-data-hub.fr/

[lxxxii] U.S. Government Publishing Office. (1996). Health Insurance Portability and Accountability Act. https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[lxxxiii] U.S. Government Publishing Office. (2009). Health Information Technology for Economic and Clinical Health Act. https://www.govinfo.gov/content/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf

[lxxxiv] FEDERAL CLOUD COMPUTING STRATEGY Vivek Kundra U.S. Chief Information Officer FEBRUARY 8, 2011

[lxxxv] *Strategy | Federal Cloud Computing Strategy*. (n.d.). https://cloud.cio.gov/strategy/

[lxxxvi] *Qu'est-ce que le FedRAMP ? | Glossaire*. (n.d.). HPE France. https://www.hpe.com/fr/fr/what-is/fedramp.html

[lxxxvii] Echos, L. (2022, December 8). Etats-Unis : le Pentagone signe pour 9 milliards de dollars de contrats dans le cloud. *Les Echos*. https://www.lesechos.fr/tech-medias/hightech/etats-unis-le-pentagone-signe-pour-9-milliards-de-dollars-de-contrats-dans-le-cloud-1887022

[lxxxviii] Piquard, A. (2022, May 17). Les géants américains du cloud accusés de fausser la concurrence. *Le Monde.fr*. https://www.lemonde.fr/economie/article/2022/05/17/les-geants-americains-du-cloud-accuses-de-fausser-la-concurrence_6126468_3234.html

[lxxxix] https://siecledigital.fr/2022/11/09/un-regroupement-dacteurs-du-cloud-attaque-microsoft-devant-la-commission-europeenne/

[xc] *Événements de formation et de certification gratuits | Webinaires en direct et à la demande | AWS*. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/fr/training/events/?get-certified-vilt-courses-cards.sort-by=item.additionalFields.startDateSort&get-certified-vilt-courses-cards.sort-order=asc&awsf.get-certified-vilt-courses-type=*all&awsf.get-certified-vilt-courses-series=*all&awsf.get-certified-vilt-locations=*all&awsf.get-certified-vilt-countries=*all&awsf.get-certified-vilt-languages=*all&awsf.get-certified-vilt-courses-level=*all&awsf.get-certified-vilt-courses-tech-category=*all

[xci] Champeau, G. (2011, September 21). Le cloud computing est aussi un enjeu de souveraineté nationale. *Numerama*. https://www.numerama.com/tech/19888-le-cloud-computing-est-aussi-un-enjeu-de-souverainete-nationale.html

[xcii] Champeau, G. (2013, December 9). Google, Microsoft, Facebook… veulent interdire d'interdire le cloud américain. *Numerama*. https://www.numerama.com/politique/27756-google-microsoft-facebook-veulent-interdire-d-interdire-le-cloud-americain.html

[xciii] Champeau, G. (2013, December 9). Les géants du web US demandent une réforme de la surveillance étatique. *Numerama*. https://www.numerama.com/politique/27755-les-geants-du-web-us-demandent-une-reforme-de-la-surveillance-etatique.html

[xciv] *TICSanté - Articles*. (n.d.). https://www.ticsante.com/story?ID=7150

[xcv] https://www.ibm.com/topics/interoperability-in-healthcare

[xcvi] *Normes FHIR relatives au stockage et à l'interopérabilité des données de santé – AWS HealthLake – Amazon Web Services*. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/fr/healthlake/

[xcvii] Béjean, M., Kletz, F., Moisdon, J., & Sicotte, C. (2016). Informatisation incrémentale ou de rupture ? Le cas du dossier patient hospitalier. *Journal De Gestion Et D Économie Médicales*, *Vol. 33*(7), 445–467. https://doi.org/10.3917/jgem.157.0445

[xcviii] *National Trends in hospital and physician adoption of electronic health Records | HealthIT.gov*. (n.d.). https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records

[xcix] Commission européenne. (s.d.). Présentation des soins de santé transfrontaliers. Public Health. https://health.ec.europa.eu/cross-border-healthcare/overview_fr

[c] EU4Health: *Regulation - 2021/522 - EN - EUR-LEX*. (s. d.). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2021.107.01.0001.01.ENG

[ci] *Les données de santé - Sénat*. (2023, January 1). Sénat. https://www.senat.fr/lc/lc324/lc324.html?utm_source=chatgpt.com#toc11

[cii] *Amazon Web Services to launch AWS European Sovereign Cloud*. (2023, October 25). US Press Center. https://press.aboutamazon.com/2023/10/amazon-web-services-to-launch-aws-european-sovereign-cloud?utm_source=chatgpt.com

[ciii] *Microsoft also subject to extended abuse control pursuant to Section 19a GWB – Bundeskartellamt determines paramount significance across markets*. (n.d.). Bundeskartellamt. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/30_09_2024_Microsoft_19a.html

[civ] https://www.cjfa.eu/REPOSITORY/EDCJFA_3.pdf

[cv] EV, B. (2024, December 18). *Bitkom e. V.* Bitkom E. V. https://www.bitkom.org/

[cvi] *Bundesministerium für Gesundheit (BMG)*. (n.d.). BMG. https://www.bundesgesundheitsministerium.de/

[cvii] *Better policies for better lives*. (n.d.). OECD. https://www.oecd.org/

[cviii] *Elektronische Patientenakte (EPA)*. (n.d.). BMG. https://www.bundesgesundheitsministerium.de/themen/digitalisierung/elektronische-patientenakte/epa-bis-15-01-25.html

[cix] *Digitalgesetze im Bundestag beschlossen*. (n.d.). BMG. https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/bundestag-verabschiedet-digitalgesetze-pm-14-12-23.html

[cx] *Gesundheitsdatennutzungsgesetz (GDNG) | BMG*. (n.d.). BMG. https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/gesundheitsdatennutzungsgesetz.html

[cxi] Briasmitatms. (n.d.). *Catalogue des critères de conformité cloud computing (C5) - Microsoft Compliance*. Microsoft Learn. https://learn.microsoft.com/fr-fr/compliance/regulatory/offering-c5-germany

[cxii] *List of C5 attestations*. (n.d.). https://www.c5-attestations.com/c5-list.html#content4-11

[cxiii] Bodelot, A. (2024, May 9). *EUCS : l'Europe sur le point de renoncer à la protection juridique des données numériques les plus sensibles*. Portail De L'IE. https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2024/eucs-leurope-sur-le-point-de-renoncer-a-la-protection-juridique-des-donnees-numeriques-les-plus-sensibles/

[cxiv] *SNE (Espagne) – Conformité | Google Cloud*. (n.d.). Google Cloud. https://cloud.google.com/security/compliance/ens?hl=fr

[cxv] *Ärzte sollen Apps verschreiben können*. (n.d.). BMG. https://www.bundesgesundheitsministerium.de/digitale-versorgung-gesetz.html

[cxvi] *#DiGA: L'Allemagne peut-elle servir de modèle afin de favoriser l'acceptation internationale des applications de santé numérique ? | INES FRANCE*. (n.d.). https://ines-france.fr/diga-lallemagne-peut-elle-servir-de-modele-afin-de-favoriser-lacceptation-internationale-des-applications-de-sante-numerique/

[cxvii] Contributeurs aux projets Wikimedia. (2023, February 14). *Office fédéral de la sécurité des technologies de l'information*. https://fr.wikipedia.org/wiki/Office_f%C3%A9d%C3%A9ral_de_la_s%C3%A9curit%C3%A9_des_technologies_de_l%27information

[cxviii] *Health Data Hub*. (s.d.). Rapport annuel 2023. https://www.health-data-hub.fr/actualites/le-health-data-hub-publie-son-rapport-annuel-2023

[cxix] **Assurance Maladie**. (n.d.). *Mon espace santé : Le carnet de santé numérique*. Ameli.Consulté le 18 décembre 2024, à l'adresse https://www.ameli.fr/assure/sante/mon-espace-sante/mon-espace-sante-carnet-sante-numerique

[cxx] **PanCareSurPass.** (n.d.-b). *HL7 Europe Team*. Consulté le 18 décembre 2024, à l'adresse https://www.pancaresurpass.eu/team/hl7-europe/.

[cxxi] **G_NIUS.** (n.d.). *Groupement régional d'appui au développement de la e-santé (GRADES)*. G_NIUS. Consulté le 18 décembre 2024, à l'adresse https://gnius.esante.gouv.fr/fr/acteurs/fiches-acteur/groupement-regional-dappui-au-developpement-de-la-e-sante-grades.

[cxxii] **bioMérieux**. (n.d.). *Data interoperability is critical for modern healthcare systems*. bioMérieux. Consulté le 18 décembre 2024, à l'adresse https://www.biomerieux.com/corp/fr/blog/actualites-tendances-diagnostic/data-interoperability-is-critical-for-modern-healthcare-systems.html

[cxxiii] **Commission Nationale de l'Informatique et des Libertés (CNIL)**. (n.d.). *Règlement européen sur la protection des données*. CNIL. Consulté le 17 décembre 2024, à l'adresse https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[cxxiv] **SESALI.** (n.d.). *NCPEHFR - GUI*. SESALI. Consulté le 17 décembre 2024, à l'adresse https://sesali.fr/ncpehfr-gui/index.html.

[cxxv] **InterSystems.** (n.d.). *Données de santé accessibles sur FHIR*. InterSystems. Consulté le 16 Décembre 2024, à l'adresse https://www.intersystems.com/fr/solutions/fhir/.

[cxxvi] **Calmedica.** (2021, 17 février). *L'importance de l'interopérabilité en santé*. Calmedica. Consulté le 17 Décembre 2024, à l'adresse https://www.calmedica.com/interoperabilite-en-sante/.

[cxxvii] AJEF. (2016). *Lutter contre le gaspillage : Synthèse FR*. Association des journalistes économiques et financiers. Consulté le 11 Décembre 2024, à l'adresse https://www.ajef.net/wp-content/uploads/2016/12/Lutter-contre-le-gaspillage_Synth%C3%A8se-FR.pdf.

[cxxviii] Union Française pour une Médecine Libre (UFML). (n.d.). *30 % des actes médicaux ou des dépenses de santé seraient inutiles ?* UFML-Syndicat. Consulté le 14 Décembre 2024, à l'adresse https://www.ufml-syndicat.org/30-actes-medicaux-depenses-de-sante-seraient-inutiles/.

[cxxix] **Calmedica**. (2021, 17 février). *L'importance de l'interopérabilité en santé*. Calmedica. Consulté le 10 Décembre 2024, à l'adresse https://www.calmedica.com/interoperabilite-en-sante/.

[cxxx] **Sénat**. (2023). *Pour un espace européen des données de santé dans l'intérêt des patients*. Sénat. Consulté le 07 Décembre 2024, à l'adresse https://conferenceconsensuslogement.senat.fr/rap/r22-848/r22-848_mono.html.

[cxxxi] ***Ministère de l'Économie.*** *(n.d.). Le règlement général de protection des données (RGPD), mode d'emploi.* Ministère de l'Économie. Consulté le 17 décembre 2024, à l'adresse :https://www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd

[cxxxii] **Chassan**, **D**. (2024, 23 mai). *Renforcer la confiance dans les données de santé pour un meilleur avenir*. OUTSCALE Blog. Consulté le 15 Décembre 2024 à l'adresse https://blog.outscale.com/renforcer-la-confiance-dans-les-donnees-de-sante-pour-un-meilleur-avenir/.

[cxxxiii] **Bow Medical.** (n.d.). *Interopérabilité : l'évolution de l'e-santé*. Consulté le 18 décembre 2024, à l'adresse https://bowmedical.com/interoperabilite-evolution-de-l-e-sante/

[cxxxiv] **La French Fab.** (n.d.). *Qui sommes-nous ?* Consulté le 18 décembre 2024, sur https://www.lafrenchfab.fr/qui-sommes-nous/.

[cxxxv] **Healthcare-ISAC.** (n.d.). *Potential threats to healthcare executives are circulating online*. Healthcare-ISAC. Consulté le 18 décembre 2024, à l'adresse https://health-isac.org/potential-threats-to-healthcare-executives-are-circulating-online/.

[cxxxvi] **Blazeinfosec.** (n.d.). *Cybersecurity risks digital health apps*. Consulté le 18 décembre 2024, à l'adresse https://www.blazeinfosec.com/post/cybersecurity-risks-digital-health-apps/.

[cxxxvii] **CNIL.** (n.d.). *Règlement européen protection des données*. Consulté le 18 décembre 2024, à l'adresse https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article9.

[cxxxviii] **Euractiv.** (2024, 18 décembre). *Les questions juridiques et non les infrastructures freinent dans les données de santé*. Consulté le 18 décembre 2024, à l'adresse https://www.euractiv.fr/section/sante-modes-de-vie/news/les-questions-juridiques-et-non-les-infrastructures-freinent-la-recherche-dans-les-donnees-de-sante/.

[cxxxix] **Cash Investigation.** (2021, 20 mai). *Nos données valent de l'or* [Vidéo]. YouTube. Consulté le 18 décembre 2024,https://www.youtube.com/watch?v=cb3jfxMnZU4.

[cxl] **CNIL**. (n.d.). *Chapitre 2 : Principes relatifs au traitement des données personnelles-Article 9*. CNIL. Consulté le 12 décembre 2024, à l'adresse https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article9.

[cxli] **Brac de La Perrière, M.** (2024, 16 février). *Utilisation secondaire des données de santé, accès aux données de vie réelles, des perspectives !* Fieldfisher. Consulté le 11 Décembre 2024, à l'adresse https://www.fieldfisher.com/fr/insights/utilisation-secondaire-des-donnees-de-sante-acces.

[cxlii] **IQVIA.** (s.d.). *Powering healthcare with connected intelligence*. IQVIA. Consulté le 17 décembre 2024, à l'adresse https://www.iqvia.com/.

[cxliii] Confédération suisse. (s.d.). Nouvelle loi sur la protection des données (nLPD). https://www.kmu.admin.ch/kmu/fr/home/faits-et-tendances/digitalisation/protection-des-donnees/nouvelle-loi-sur-la-protection-des-donnees-nlpd.html

[cxliv] G_NIUS. (s.d.). Le numérique en santé en Estonie. https://gnius.esante.gouv.fr/fr/acteurs/decryptez-la-e-sante-a-linternational/le-numerique-en-sante-en-estonie

[cxlv] Lars, E. (2024, 2 juillet). X-Road. e-Estonia. https://e-estonia.com/solutions/x-road-interoperability-services/x-road/

[cxlvi] Singapore government developer portal : Open-source technologies. (2024, 29 avril). *Singapore Government Developer Portal*. https://www.developer.tech.gov.sg/products/categories/open-source/

[cxlvii] *Rapport d'information*. (n.d.). 15e Législature - Assemblée Nationale. https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information

[cxlviii] Moal, C., & Moal, C. (2021, December 6). Pour mieux comprendre la souveraineté numérique. *Alliancy, Le Mag Numérique Et Business*. https://www.alliancy.fr/mieux-comprendre-souverainete-numerique

[cxlix] Gazzane, H. (2021, November 10). Les 5 plus grosses amendes infligées par l'UE aux Gafam. *Les Echos*. https://www.lesechos.fr/tech-medias/hightech/les-5-plus-grosses-amendes-infligees-par-lue-aux-gafam-1362733

[cl] **Numerikare.** (n.d.). *Un espace européen des données de santé pour 2022*. Consulté le 18 décembre 2024, à l'adresse https://www.numerikare.be/fr/actualites/e-health/un-espace-europeen-des-donnees-de-sante-pour-2022.html

[cli] **Gematik** est le responsable de la stratégie allemande d'interopérabilité utilisant FHIR dans le cadre du dossier patient électronique.

[clii] **Agenzia per l'Italia Digitale** met en œuvre la stratégie italienne d'interopérabilité s'appuyant sur le format FHIR.

[cliii] **Nictiz** développe des profils FHIR adaptés au système néerlandais.

Sources complémentaires :

- **AJEF** (2016). *Lutter contre le gaspillage : Synthèse*. Consulté le 18 décembre 2024, sur https://www.ajef.net/wp-content/uploads/2016/12/Lutter-contre-le-gaspillage_Synth%C3%A8se-FR.pdf
- **About us - EU4Health**. (s. d.). *EU4health*. https://eu4health.eu/about-us/
- **Agence du Numérique en Santé.** (s. d.-c). *MSSanté*. Agence du Numérique En Santé. https://esante.gouv.fr/produits-services/mssante
- **Agence du Numérique en Santé.** (2023, 6 décembre). *Partenariat entre l'Agence du Numérique en Santé et Interop'Santé*. Agence du Numérique En Santé. https://esante.gouv.fr/actualites/partenariat-entre-lagence-du-numerique-en-sante-et-interopsante
- **Beale, S. H. T**. (s. d.). *OpenEHR-Home*. https://openehr.org/
- **BioMérieux.** (n.d.). *Data interoperability is critical for modern healthcare systems*. Consulté le 18 décembre 2024, sur https://www.biomerieux.com/corp/fr/blog/actualites-tendances-diagnostic/data-interoperability-is-critical-for-modern-healthcare-systems.html
- **Blazeinfosec.** (n.d.). *Cybersecurity risks digital health apps*. https://www.blazeinfosec.com/post/cybersecurity-risks-digital-health-apps/
- **Bow Medical.** (n.d.). *Interopérabilité : l'évolution de l'e-santé*. Consulté le 18 décembre 2024, sur https://bowmedical.com/interoperabilite-evolution-de-l-e-sante/
- **Cahen, M**. (n.d.). *La protection des données médicales*. https://www.murielle-cahen.fr/la-protection-des-donnees-medicales/#
- **Calmedica.** (n.d.). *Interopérabilité en santé : enjeux et solutions*. Consulté le 18 décembre 2024, sur https://www.calmedica.com/interoperabilite-en-sante/
- **Cash Investigation** du 20 mai 2021. "Nos données valent de l'or". https://www.youtube.com/watch?v=cb3jfxMnZU4
- **CCNE & CNPEN**. (2023). *Groupement de travail sur les problématiques des données de santé : Avis final du 27 mars 2023*. Consulté le 18 décembre 2024, sur https://www.ccne-ethique.fr/sites/default/files/2023-05/CCNE-CNPEN_GT-PDS_avis_final27032023.pdf
- **CNIL**. (n.d.). *Règlement européen sur la protection des données - Chapitre II : Principes*. Consulté le 18 décembre 2024, sur https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article9
- **Contributeurs aux projets Wikimedia.** (2024b, septembre 29). *Agence du numérique en santé*. https://fr.wikipedia.org/wiki/Agence_du_num%C3%A9rique_en_sant%C3%A9

- **Cyber Risk GmbH.** (s. d.). *The European Health Data Space (EHDS)*. https://www.european-health-data-space.com/
- **Digital Health Uptake.** (n.d.). *Executive Digest: EHDS interoperability and validation*. https://digitalhealthuptake.eu/wp-content/uploads/DHU-Executive-Digest-EHDS-interoperability-4-validation-1.pdf
- **Documentation collaborative du SNDS** | Documentation du SNDS & SNDS OMOP. (s. d.). https://www.documentation-snds.health-data-hub.fr/snds/
- **EDHEALTH & eHDSI**. (s. d.). *Digital Health Interoperability*. Consulté le 18 décembre 2024, sur https://edhealth.org/digital-health-interoperability/
- **EHDS.** (2023, 12 septembre). *The European Health Data Space Regulation: Transforming Healthcare in Europe*. https://ec.europa.eu/health/data_collection/policy/european_health_data_space_en
- **Enea**. (n.d.). *Interoperability: Key to Effective Healthcare Systems*. Consulté le 18 décembre 2024, sur https://www.enea.com/healthcare/interoperability
- **Euronews**. (2022, 1er septembre). *Espace européen des données de santé : quels ressorts technologiques ?* https://fr.euronews.com/sante/2022/09/01/espace-europeen-des-donnees-de-sante-quels-ressorts-technologiques
- **European Commission.** (2023). *eHealth Digital Service Infrastructure (eHDSI)*. Consulté le 18 décembre 2024, sur https://ec.europa.eu/health/ehealth-digital-service-infrastructure
- **European Commission.** (n.d.). *Guidelines on the electronic exchange of health data under the Cross-Border Healthcare Directive: Patient Summary*. https://health.ec.europa.eu/document/download/e020f311-c35b-45ae-ba3d-03212b57fa65_en?filename=ehn_guidelines_patientsummary_en.pdf
- **European Data Protection Board.** (2023). *Guidelines on the Right to Data Portability*. https://edpb.europa.eu/data-portability-guidelines_en
- **French Health Data Hub**. (n.d.). *Mission et objectifs du Health Data Hub*. Consulté le 18 décembre 2024, sur https://health-data-hub.fr/mission
- **Gouv.fr.** (n.d.). *Le numérique au service de la santé*. https://www.gouvernement.fr/le-numerique-au-service-de-la-sante
- **HL7 Europe.** (n.d.). *FHIR Implementation Guide*. https://build.fhir.org/ig/hl7-eu/pcsp/
- **IBM**. (2022). *How Data Interoperability Transforms Healthcare Systems*. Consulté le 18 décembre 2024, sur https://www.ibm.com/industries/healthcare/resources/data-interoperability
- **IEEE.** (n.d.). *Standards for Interoperability in Healthcare*. https://standards.ieee.org/healthcare/interoperability/
- **INSEE**. (2023). *Les données de santé en France : analyse des enjeux économiques et sociaux*. Consulté le 18 décembre 2024, sur https://www.insee.fr/fr/statistiques/sante-donnees/
- Interop'Santé. (n.d.). *La normalisation au service de la santé*. Consulté le 18 décembre 2024, sur https://www.interopsante.org/

- **ISO.** (2023). *Healthcare Data Interoperability Standards*. https://www.iso.org/standards/healthcare-interoperability
- **Microsoft**. (2023). *Achieving Data Interoperability in Digital Health Solutions*. Consulté le 18 décembre 2024, sur https://www.microsoft.com/healthcare/interoperability
- **Open Health Tools.** (2023). *Accelerating Open Source Solutions for Healthcare*. https://www.openhealthtools.org/
- **PanCareSurPass**. (n.d.-b). *HL7 Europe Team*. https://www.pancaresurpass.eu/team/hl7-europe/
- **PanCareSurPass.** (n.d.-a). *Home*. https://www.pancaresurpass.eu/?utm_com
- WHO. (2022). *Global Strategy on Digital Health 2020–2025*. https://www.who.int/publications/global-strategy-digital-health-2020-2025
- **OpenEHR**. (n.d.). *Standards and Tools for Digital Healthcare Systems*. Consulté le 18 décembre 2024, sur https://www.openehr.org/standards
- **Orange Healthcare**. (2024). *Interoperability in Connected Healthcare*. Consulté le 18 décembre 2024, sur https://healthcare.orange.com/interoperability
- **Philips.** (2023). *Driving Interoperability for Improved Patient Outcomes*. Consulté le 18 décembre 2024, sur https://www.philips.com/healthcare/interoperability
- **SAP**. (n.d.). *Enhancing Healthcare Systems through Data Integration*. Consulté le 18 décembre 2024, sur https://www.sap.com/industries/healthcare.html
- **SNDS.** (2024). *Système National des Données de Santé : fonctionnalités et impact*. Consulté le 18 décembre 2024, sur https://www.snds.gouv.fr/
- **Telstra Health.** (n.d.). *The Role of Data Interoperability in Modern Healthcare*. https://www.telstrahealth.com/interoperability
- **Université de Lorraine.** (2023). *L'avenir de l'interopérabilité dans la santé en France*. https://www.univ-lorraine.fr/interop-sante
- **VMware Healthcare**. (n.d.). *Securing Interoperable Health Systems*. Consulté le 18 décembre 2024, sur https://www.vmware.com/solutions/healthcare.html
- **WHO**. (2023). *Interoperability and Standards in Global Health Initiatives*. Consulté le 18 décembre 2024, sur https://www.who.int/interoperability
- **Wolters Kluwer Health**. (2023). *Achieving Interoperability in Digital Medicine*. Consulté le 18 décembre 2024, sur https://www.wolterskluwer.com/interoperability
- **Xerox Healthcare**. (n.d.). *The Future of Interoperable Health Data Systems*. https://www.xerox.com/healthcare/interoperability
- **Zeenea.** (2024). *Data Catalogs for Enhanced Health Data Management*.