AleVia
COMMUNICATION STRATÉGIQUE
& REPRÉSENTATION D'INTÉRÊTS

LES DONNÉES DE SANTÉ
UNE MINE D'OR À HAUT POTENTIEL STRATÉGIQUE

Nicole Tortello Duban

Dans un contexte de numérisation croissante du secteur de la santé, la qualité et la protection des données médicales s'imposent comme des défis cruciaux. Ces informations, particulièrement sensibles, offrent des opportunités considérables pour la recherche et pour l'amélioration des soins, tout en soulevant des questions complexes en matière de fiabilité, de confidentialité et de sécurité.

LE CADRE RÉGLEMENTAIRE EN VIGUEUR

En France, le cadre réglementaire pour la protection des données de santé est particulièrement robuste. Il s'appuie sur plusieurs piliers législatifs, notamment sur la loi Informatique et Libertés de 1978, pionnière en Europe, et sur la loi Kouchner de 2002 qui traite spécifiquement des données médicales.

Plus récemment, le Règlement Général sur la Protection des Données (RGPD) européen, entré en vigueur en 2018, complète ce dispositif qui vise à garantir la confidentialité des informations médicales tout en permettant leur utilisation à des fins de recherche et d'amélioration des soins.

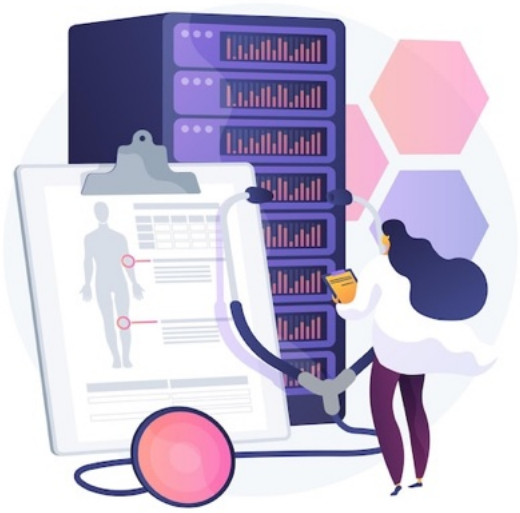
À l'international, la situation est plus contrastée. Aux États-Unis par exemple, le cadre réglementaire est plus fragmenté. Il s'appuie principalement sur la loi HIPAA (Health Insurance Portability and Accountability Act) qui ne couvre pas tous les acteurs du secteur de la santé. La couverture santé y est également plus hétérogène, ce qui impacte la gestion et la protection des données de ce secteur d'activité. Ces différences se retrouvent dans la façon d'approcher l'ouverture des données de santé et de leur commercialisation.

UNE SITUATION PARTICULIÈREMENT FAVORABLE EN FRANCE

Dans ce paysage réglementaire, la France se distingue par une situation particulièrement favorable en matière de données de santé. Le Système National des Données de Santé (SNDS), l'une des plus grandes bases de données de santé au monde, couvre presque toute la population française,

tandis que le Health Data Hub (voir ci-après), créé en 2019, facilite le partage et le croisement de ces données pour promouvoir la recherche.

Notre pays bénéficie ainsi d'un système de santé universel et de bases de données médico-administratives exhaustives, offrant un potentiel exceptionnel pour l'innovation en santé.



Pour utiliser des données de santé dans la recherche, des formalités spécifiques sont requises, notamment la nomination d'un Délégué à la Protection des Données (DPO), la tenue d'un registre des activités de traitement, la réalisation d'une analyse d'impact relative à la protection des données (AIPD), l'information des personnes concernées, et la détermination de la durée de conservation des données. Ces formalités, bien que rigoureuses, s'inscrivent dans une longue tradition française de recherche médicale et épidémiologique, qui a su concilier protection des droits individuels et promotion de l'innovation en santé.

LA QUALITÉ ET LA PROTECTION DES DONNÉES DE SANTÉ S'IMPOSE COMME LE NERF DE LA GUERRE

Souvent qualifiées de "trésor", ces données doivent répondre à des critères stricts d'exactitude, d'exhaustivité et de pertinence pour être utiles et commercialisables. Elles doivent également être parfaitement protégées pour répondre au critère de fiabilité.

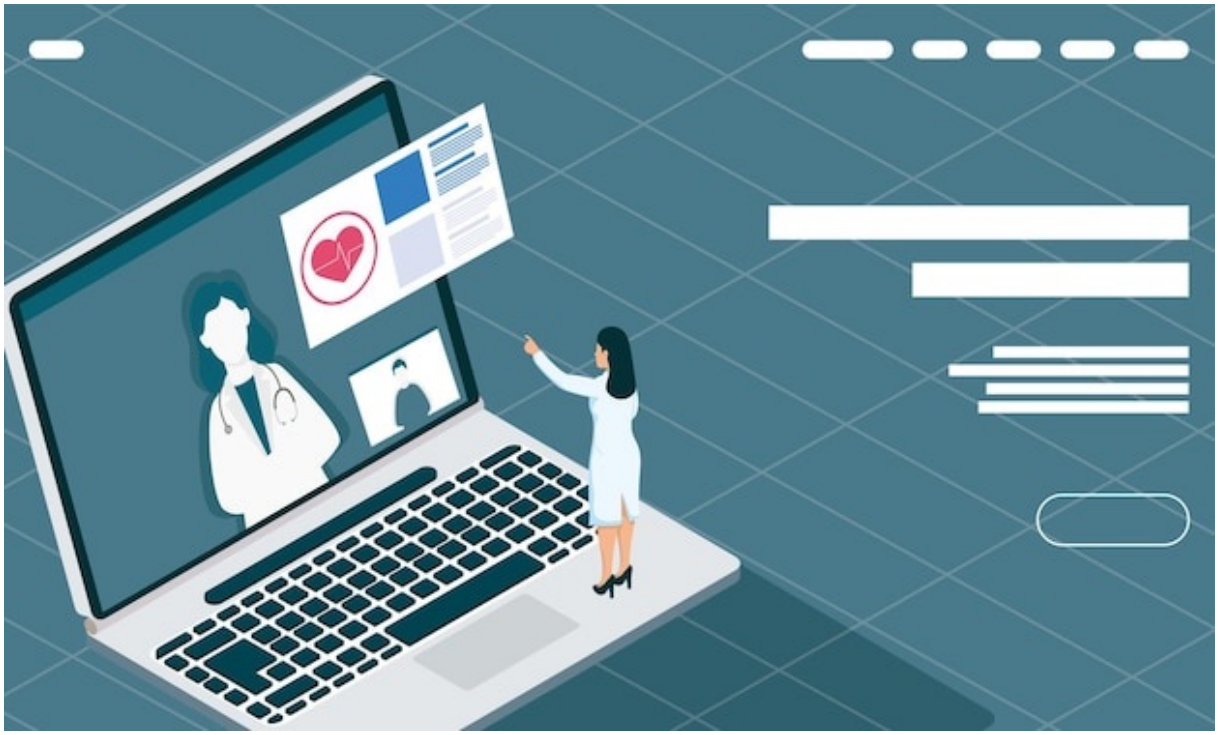
→ **La qualité des données de santé est essentielle pour garantir des soins fiables et efficaces.**

Des données précises et complètes sont nécessaires pour assurer des diagnostics exacts et des traitements appropriés et pour garantir la validité des études cliniques et épidémiologiques. Plus largement, des données fiables permettent une meilleure allocation des ressources dans le système de santé, tant au niveau des établissements qu'à l'échelle nationale. La

définition de politiques publiques bien calibrées dépend donc directement de la qualité des datas.

L'avenir de l'intelligence artificielle dans le secteur de la santé repose également sur la qualité des données. Les algorithmes d'apprentissage automatique nécessitent des données précises pour fournir des résultats pertinents. Des données erronées contribuent à compromettre l'efficacité des outils d'IA.

Pour améliorer la qualité des données, il est fondamental de standardiser les processus de collecte et de traitement. Cela implique la mise en place de normes et de procédures uniformes qui garantissent l'exactitude et la cohérence des informations recueillies. L'utilisation d'outils de vérification automatique contribue à garantir la qualité des données. Le développement de systèmes d'information intégrant des contrôles de cohérence et de qualité des données saisies constitue une approche prometteuse.



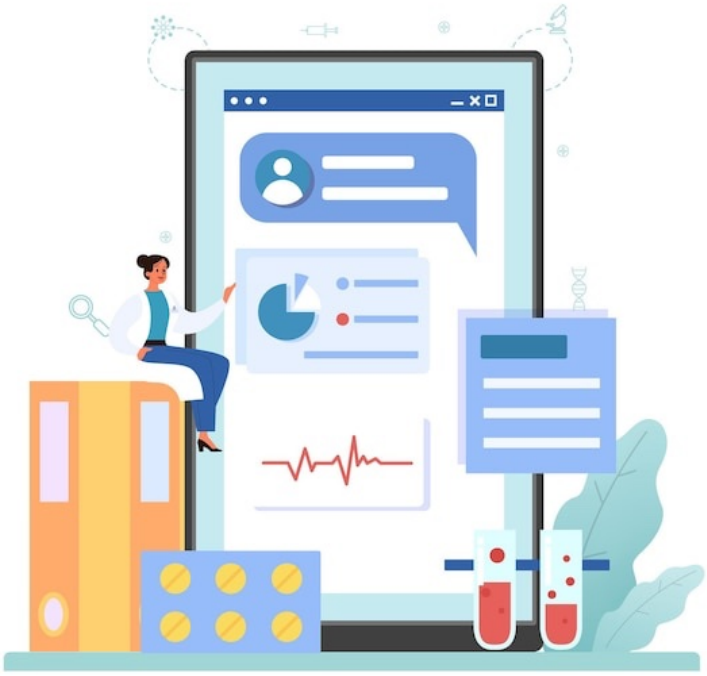
Il convient donc que la formation des professionnels de santé souligne l'importance de la qualité des données de santé pour améliorer la fiabilité des informations. À cet égard, un point d'actualité mérite attention : le Conseil constitutionnel, saisi le 12 juin dernier par le Conseil d'État d'une question prioritaire de constitutionnalité du Conseil national de l'ordre des médecins (Cnom), a validé l'accès des professionnels ne relevant pas de la

catégorie des professionnels de santé au « dossier médical partagé » dans sa décision publiée au Journal officiel du 13 septembre[1].

En complément, l'implication des patients dans la gestion de leurs données doit également permettre d'identifier d'éventuelles erreurs.

→ La sécurité des données est cruciale pour transformer notre système de santé

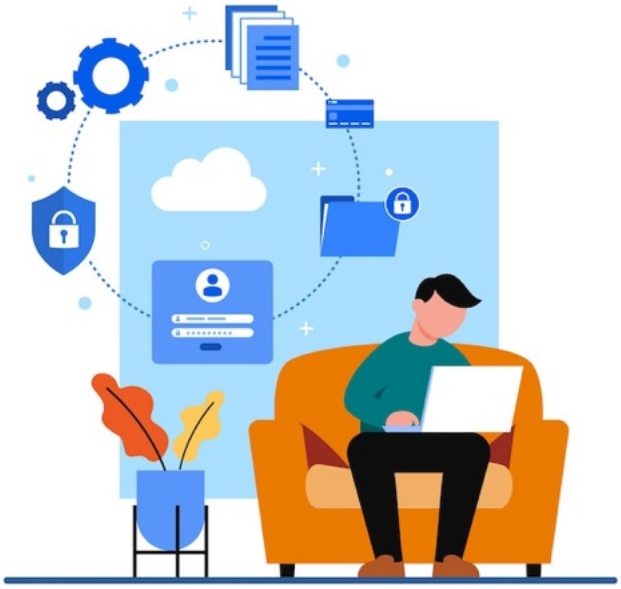
L'accès non autorisé aux données de santé est un problème sérieux qui peut survenir dans diverses circonstances. Sur le plan technique, les systèmes informatiques obsolètes ou mal sécurisés constituent souvent une porte d'entrée pour les intrusions. L'absence de chiffrement des données et les failles de sécurité dans les logiciels utilisés aggravent cette vulnérabilité. Les erreurs humaines jouent également un rôle significatif. Une mauvaise gestion des mots de passe, le partage inapproprié d'informations confidentielles peuvent conduire à des brèches de sécurité. Enfin, des problèmes organisationnels peuvent faciliter les accès non autorisés.



[1] Le fait que tout professionnel participant à la prise en charge d'une personne puisse accéder, sous réserve du consentement de la personne préalablement informée, au dossier médical partagé (DMP) de celle-ci et l'alimenter est "conforme à la Constitution ». De même que l'alimentation de son DMP par ce même professionnel après une simple information de la personne prise en charge.

LES CONSÉQUENCES DE CES ACCÈS NON AUTORISÉS SONT MULTIPLES ET SOUVENT GRAVES.

- Pour les patients, la première conséquence est la violation de leur vie privée. Par ailleurs, ils sont exposés à des risques d'usurpation d'identité médicale et de chantage fondé sur des informations médicales sensibles. Dans certains cas, la divulgation de ces informations médicales les concernant conduit à des discriminations dans l'emploi ou en matière d'assurance.



- Les établissements de santé s'exposent à des sanctions financières importantes, notamment dans le cadre du RGPD. Les coûts liés à la gestion de la crise et à la notification des personnes concernées sont également considérables. De plus, l'atteinte à la réputation d'un établissement de santé est susceptible d'entraîner une perte de patients. Sur le plan juridique et réglementaire, l'établissement risque des poursuites judiciaires de la part des patients affectés.

- À l'échelle de notre système de santé, les conséquences sont décuplées. Une attaque majeure perturbe le fonctionnement des services de santé et peut mettre en danger la vie de certains patients. Par ailleurs, les violations de données conduisent à une réticence accrue à partager des données, ce qui freine de facto les avancées médicales potentielles. Enfin, la perte de confiance dans les systèmes de santé numériques risque de ralentir l'adoption de ces technologies numériques, pourtant prometteuses.

Aujourd'hui, la cybersécurité des données de santé représente un défi majeur et croissant. Les établissements de santé sont devenus des cibles privilégiées des cybercriminels, attirés par la valeur des données médicales sur le marché noir. Ces criminels utilisent des techniques de phishing visant

spécifiquement le personnel médical. Les ransomwares[2] sont de plus en plus fréquents, tout comme l'exploitation de failles zero-day[3]. Face à ces menaces, les autorités de santé et les agences de cybersécurité - dont l'Agence nationale de la sécurité des systèmes d'information (ANSSI) - collaborent pour renforcer la résilience de notre système de santé.

→ Les questions éthiques méritent la plus vive attention

L'anonymisation et la pseudonymisation, qui visent à protéger la vie privée des patients tout en permettant l'utilisation des données pour la recherche et l'amélioration des soins, soulèvent des questions complexes sur l'équilibre entre confidentialité et utilité des données.[4]

Le risque de ré-identification, malgré l'anonymisation, constitue un vrai sujet d'inquiétude, en particulier pour les maladies rares. La notion de consentement éclairé est également remise en question par l'utilisation secondaire des données, nécessitant de nouvelles approches comme le consentement dynamique. La garantie d'équité et de non-discrimination passe par la sécurisation des données anonymisées ou pseudonymisées contre les piratages. En complément, les patients doivent pouvoir garder un contrôle sur leurs informations et être informés de leur utilisation, ce qui pose des défis techniques et organisationnels. Pour répondre à ces défis, de nouvelles approches techniques comme le chiffrement homomorphe[5] sont à l'étude. L'émergence de technologies

[2] Logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.
[3] Dans le domaine de la sécurité informatique, une faille / vulnérabilité zero-day — également orthographiée 0-day — ou faille / vulnérabilité du jour zéro est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive.
[4] Le 5 septembre 2024, la CNIL a indiqué avoir sanctionné Cegedim Santé. L'éditeur de logiciels de gestion des cabinets médicaux a été condamné à payer une amende de 800 000 euros. Cegedim utilisait des données de santé uniquement pseudonymisées et « très nombreuses sur les personnes concernées » – année de naissance, sexe, allergies, antécédents médicaux, prescriptions, résultats d'analyses, etc. Ces données étaient reliées à un identifiant unique. Des éléments suffisants pour permettre de réidentifier « par des moyens raisonnables » les individus, estime la Cnil. Ces données sont issues d'un panel de médecins clients adhérents à l'« observatoire » de Cegedim Santé. Elles étaient ensuite utilisées par des clients de la société pour « produire des études et des statistiques ». Pour que ce traitement soit régulier, il aurait fallu que l'éditeur déclare à la Cnil sa conformité à ses référentiels ou obtienne son autorisation.
[5] https://www.cnil.fr/fr/definition/chiffrement-homomorphe

telles que la blockchain[6] soulève aussi des interrogations sur leur potentiel pour sécuriser et tracer les échanges de données de santé.

Le recours à l'intelligence artificielle renforce la nécessité de garantir les droits fondamentaux des patients. En effet, les biais potentiels des algorithmes d'IA posent des problèmes d'équité et de discrimination dans les décisions médicales. La centralisation et l'interconnexion des informations augmentent les risques de piratage à grande échelle. La transparence et l'explicabilité des systèmes d'IA sont déterminantes pour maintenir responsabilité médicale et la confiance des patients. Enfin, la commercialisation des données de santé, bien que réglementée, soulève des questions éthiques sur l'exploitation d'informations sensibles.

C'est pourquoi, il convient de disposer d'un cadre éthique et juridique robuste, impliquant l'ensemble des parties prenantes. Il faut aussi des mécanismes de gouvernance adaptés. À cet égard, le Sénat a initié en 2022 une mission d'information pour évaluer la mise en œuvre des dispositions relatives aux données de santé portées par les lois « santé » de 2016 et 2019. Cette mission, conduite par un groupe de travail transpartisan présidé par la présidente de la commission des affaires sociales, Catherine Deroche, a produit le Rapport d'information n° 873 (2022-2023) du 12 juillet 2023.

DES DÉFIS ÉCONOMIQUES MAJEURS ET DES DÉFIS DE SOUVERAINETÉ

Les données de santé sont devenues une ressource stratégique de premier ordre pour transformer le secteur de la santé, tant au niveau national qu'international. Leur exploitation présente des avantages économiques colossaux pour les États et, de manière plus large, pour l'ensemble des acteurs désireux de créer de nouveaux services et produits, d'améliorer la couverture sanitaire globale, d'encourager des comportements plus responsables en matière de santé grâce à des politiques incitatives…

Il faut toutefois garder à l'esprit l'importance de se préserver des ingérences étrangères, qu'elles émanent d'États hostiles ou d'acteurs privés puissants, tels que les GAFAM qui s'organisent depuis plusieurs années pour collecter massivement des données de santé[7].

[6] https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application
[7] Voir : "Le bilan des initiatives des GAFAM dans la santé en 2022" publié par *Mind Health*

La certification HDS (Hébergeur de Données de Santé) n'exclut pas totalement les risques d'ingérences étatiques pour plusieurs raisons :

1/ Bien que la certification HDS impose des normes de sécurité élevées, elle ne garantit pas la localisation exclusive des données en France ou dans l'Union Eur opéenne. Des hébergeurs étrangers, notamment américains tels que Microsoft et Amazon, peuvent obtenir cette certification.

2/ Les grands fournisseurs de cloud américains, même certifiés HDS, restent soumis aux lois de leur pays d'origine. Ces lois, dont le Cloud Act, peuvent permettre aux autorités américaines d'accéder à des données stockées à l'étranger.

3/ La récente décision d'adéquation accordée aux États-Unis par la Commission européenne complique la situation. Cette décision considère que les États-Unis offrent un niveau de protection des données équivalent à celui de l'UE, ce qui exempte les hébergeurs américains de certaines exigences supplémentaires du nouveau référentiel HDS.

4/ La certification HDS se concentre principalement sur les aspects techniques de la sécurité des données. Elle ne traite pas spécifiquement des risques liés aux ingérences étatiques étrangères.

5/ Bien que la certification HDS offre des garanties en matière de protection des données, elle ne couvre pas tous les aspects du RGPD. Elle ne peut donc pas, à elle seule, garantir une protection totale contre les ingérences étatiques.

En bref, malgré les améliorations apportées par le nouveau référentiel HDS, la certification reste insuffisante pour éliminer complétement les risques d'ingérences étatiques, notamment en raison des enjeux géopolitiques et juridiques complexes liés à l'hébergement des données de santé.

Cette fragilité intrinsèque des données fait planer un risque en matière de souveraineté sanitaire, ainsi que la crise sanitaire de la covid-19 nous l'a récemment rappelé.

Au plan mondial, les données de santé peuvent potentiellement être utilisées comme un levier stratégique[8] pour accroître l'influence des États qui misent sur la recherche, sur la cybercriminalité et/ou sur la « guerre informationnelle »[9] !

[8] Pour en savoir plus : https://www.udemy.com/course/pourquoi-les-donnees-numeriques-sont-elles-geopolitiques/

[9] Dans un rapport publié cet été 2024, le Sénat propose de faire de VIGINUM une réelle agence d'État dotée de moyens aussi bien financiers qu'humains. Rattaché au secrétariat général de la Défense et de la Sécurité nationale, ce service technique et opérationnel de l'État chargé de la vigilance et de protection contre les ingérences numériques étrangères a été créé le 13 juillet 2021. Il déjoue au quotidien des opérations numériques de déstabilisation orchestrée depuis la Russie, la Chine, la Turquie – candidate à l'entrée dans l'UE – et l'Azerbaïdjan, pays dont l'Union européenne a choisi de devenir dépendante pour son approvisionnement en gaz. Ce rapport identifie une « guerre des narratifs » au cœur de cette lutte d'influence. Selon le commandant Olivier Martin, la France est en « état de guerre ». Elle affronte une guerre hybride qu'elle s'est donnée les moyens de mener.

Toutefois, tous les pays partagent l'ambition de renforcer les capacités humaines et de vieillir en bonne santé, d'où la multiplication exponentielle d'applications et autres outils numériques qui optimisent l'hygiène de vie des patients, facilitent la pratique de la télémédecine et permettent aux individus de mieux gérer leur santé de façon autonome[10]. Pour les « pays du sud », l'e-santé constitue également un puissant enjeu de développement.

LES ACTEURS CLÉS

→ La CNIL

La Commission Nationale de l'Informatique et des Libertés (CNIL) joue un rôle central dans ce dispositif. Elle définit ce qu'est une donnée de santé, assure la promotion de bonnes pratiques pour garantir la qualité des données de santé, établit le cadre légal pour leur utilisation et accompagne les acteurs du secteur dans la mise en conformité de leurs pratiques.

Récemment, la CNIL a renforcé son action dans le domaine de la santé[11].

En février 2024, elle a rappelé les mesures de sécurité et de confidentialité nécessaires pour l'accès au dossier patient informatisé (DPI), mettant en demeure plusieurs établissements de santé de prendre les mesures adéquates.

En mars 2024, elle a appelé à la vigilance concernant les tests génétiques vendus en kit sur Internet, soulignant les risques liés à leur utilisation. Ces actions démontrent l'attention particulière portée aux nouvelles technologies dans le domaine de la santé.

En avril 2024, dans sa dernière mise à jour du guide de sécurité des données personnelles, la CNIL a intégré des recommandations spécifiques au secteur de la santé. Ces nouvelles directives abordent les défis liés à l'utilisation des technologies émergentes telles que le cloud, les applications mobiles et l'intelligence artificielle dans le domaine médical. Elles offrent des conseils pratiques pour assurer une protection optimale de ces données particulièrement sensibles.

Le 21 juin 2024, dans le cadre du règlement européen sur la gouvernance des données (DGA), la CNIL a été désignée autorité compétente en matière d'altruisme des données. Cette nouvelle responsabilité renforce son rôle dans la régulation de l'utilisation des données de santé à des fins d'intérêt général, notamment pour la recherche médicale et l'amélioration des politiques de santé publique. Ces initiatives témoignent de l'engagement continu de la CNIL dans la protection des données de santé. Elles illustrent sa capacité à s'adapter aux évolutions technologiques du secteur médical et soulignent son rôle croissant dans la gouvernance des données de santé, tant au niveau national qu'européen. Cette

[10] Parmi d'autres, l'université de la e-santé de Castres-Mazamet, constitue un laboratoire d'idées pour faire du numérique un levier au service des systèmes de santé et de ses usagers.
[11] https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-pds

version offre une présentation plus concise et percutante des informations, tout en mettant l'accent sur l'importance et les implications de chaque initiative de la CNIL dans le domaine des données de santé.

Le 24 juin 2024, la CNIL, en partenariat avec le Centre d'accès sécurisé aux données (CASD), a publié un guide pratique sur les procédures d'appariement avec le Système National des Données de Santé (SNDS). Ce document vise à faciliter l'exploitation sécurisée des données de santé dans la recherche, tout en garantissant le respect scrupuleux de la confidentialité des informations personnelles.

Le 27 août 2024, l'autorité a publié des questionnaires de suivi à l'intention des multinationales ayant mis en place des règles d'entreprise contraignantes (BCR, en anglais). Ces règles formant un outil, issu du RGPD, permettent de transférer des données personnelles hors de l'UE au sein d'un même groupe. Les questionnaires servent à vérifier le niveau de conformité des multinationales aux exigences de ces règles, adoptées après l'approbation de la CNIL. En mai, cette dernière avait mis en ligne un outil d'auto-évaluation à destination des entreprises souhaitant mettre en place des BCR. La CNIL incite ainsi à ouvrir l'œil sur les transferts de données personnelles hors de l'UE.

La CNIL est également une autorité de contrôle : elle réalise des contrôles réguliers et peut imposer des sanctions en cas de non-respect des règles, assurant ainsi une vigilance constante sur la protection de ces données sensibles.

Dans le domaine de la santé, la CNIL a récemment prononcé plusieurs sanctions.

En mars 2024, la CNIL a infligé à Doctissimo une amende de 380 000 euros pour plusieurs manquements, notamment :

- le non-respect de l'obligation de recueillir le consentement des personnes pour collecter leurs données de santé (via des tests en ligne)
- des durées de conservation excessives des données
- des manquements concernant l'utilisation des cookies

La CNIL a également sanctionné plusieurs médecins généralistes pour des manquements à la sécurité des données de santé, notamment :

- l'utilisation de mots de passe trop simples
- l'absence de chiffrement des données
- le manque de sauvegardes sécurisées

Dans le secteur de la santé, les sanctions prononcées concernent :

- un défaut de sécurité des données (mot de passe insuffisamment robuste, stockage des mots de passe en clair, absence de politique d'habilitation)
- un non-respect des droits des personnes (exercice du droit d'accès à un dossier médical)
- un traitement illicite de données sensibles (diffusion d'une vidéo promotionnelle comportant des données de santé sans le consentement des patients).

→ Le Health Data Hub

Créé par la Loi du 24 juillet 2019 relative à l'organisation et la transformation du système de santé, le Health Data Hub est un groupement d'intérêt public (GIP) qui associe 56 parties prenantes, en grande majorité issues de la puissance publique (CNAM, CNRS, Haute Autorité de santé, France Assos Santé…). L'organisme met en œuvre les grandes orientations stratégiques relatives au Système National des Données de Santé (SNDS) fixées par l'État, notamment par le ministère de la Santé. Son financement est majoritairement public.

En tant que plateforme nationale des données de santé, le Health Data Hub a également un rôle essentiel à jouer dans la promotion de standards de qualité pour les données qu'il héberge et partage. En facilitant l'accès aux données tout en garantissant leur sécurité et leur qualité, cette plateforme contribue à l'innovation et à la recherche.

→ Les groupements publics et privés

Outre le Conseil National du Numérique (CNNum), commission publique indépendante « chargée de conduire une réflexion ouverte sur la relation des humains au numérique », de nombreux groupements (Think tanks, associations, syndicats[12], etc.) s'attachent à émettre des recommandations en matière de gestion des données de santé.

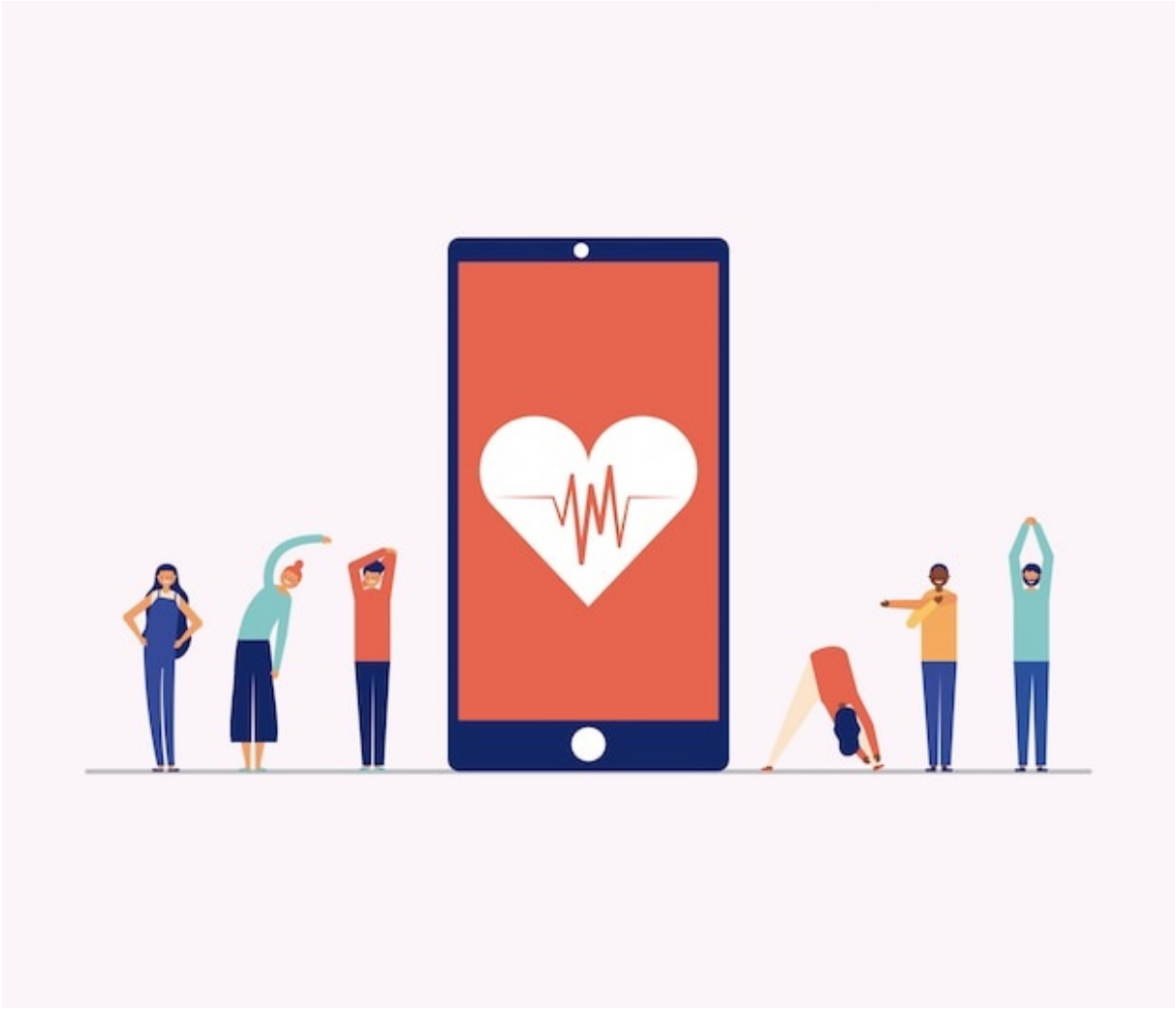
Parmi ces organisations, deux nous semblent mériter une attention particulière, à savoir le Gf2i et l'association Valentin Haüy.

Le Groupement Français de l'Industrie de l'Information (Gf2i) se distingue par le profil particulier de ses adhérents, représentants d'organismes publics (dont le ministère de l'Intérieur) et d'entreprises privées (du consultant individuel à Total Énergies). À mi-chemin entre le Think & Do Tank et le

[12] Notamment le Syntec numérique (devenu Numeum) dont la commission santé est très active.

représentant d'intérêts, le Gf2i analyse chaque actualité nationale, européenne ou internationale dans ses complexités techniques, réglementaires et économiques dans le but de nourrir la réflexion des professionnels et d'éclairer nos politiques publiques. Ses positions sont systématiquement issues d'un consensus guidé par l'intérêt général, ce qui mérite d'être souligné tant le processus de cette association s'avère exigeant.

L'association Valentin Haüy accompagne quant à elle les personnes malvoyantes et aveugles en militant de longue date pour l'accessibilité numérique. Son président, Sylvain Nivard, lui-même aveugle, entend permettre aux personnes en situation de handicap de travailler, de se soigner et, plus globalement, d'accéder aux mêmes droits que les personnes dites valides dans une société numérisée. Son plaidoyer pour l'accessibilité numérique[13] a permis d'alerter le gouvernement en amont de la transposition de la directive européenne d'accessibilité des biens et services. Une étape clé a ainsi été franchie à cette occasion. Malheureusement, l'accessibilité numérique dans le secteur de la santé reste une trajectoire non-financée.



[13] Plaidoyer conçu et défendu auprès des responsables publics avec le concours d'AleVia Conseil.

→ L'AFNOR

L'Association française de normalisation s'intéresse également au numérique en santé. Le 9 juillet 2024, elle a annoncé la création de sa commission « Numérique en santé ». Cette commission abordera des sujets comme l'interopérabilité des systèmes et dispositifs en santé numérique personnalisée, la gestion de l'information dans le domaine de l'e-santé, les bonnes pratiques concernant la gestion des dossiers patients informatisés ou encore, les exigences de cybersécurité des dispositifs médicaux. Les garanties humaines de l'intelligence artificielle en santé et le e-consentement font aussi partie des aspects qu'elle couvrira.

EN CONCLUSION

L'innovation dans le traitement des données de santé ouvre d'extraordinaires perspectives pour la recherche, le diagnostic et la « médecine 5 P » (personnalisée, préventive, pertinente, prédictive, participative). Cette dernière permet d'identifier des facteurs de risque, des prédispositions à certaines maladies et de détecter précocement des problèmes de santé publique, en impliquant le patient. L'exploitation massive de données, notamment génomiques, permet de développer des approches plus efficientes, ouvrant la voie à des interventions anticipées et ciblées.

L'avenir de notre système de santé repose cependant sur notre capacité à garantir non seulement la fiabilité et la pertinence des données de santé, mais aussi leur protection. La qualité des données est ainsi un enjeu transversal qui impacte tous les aspects du système de santé, de la prise en charge individuelle des patients à la recherche médicale et à l'élaboration des politiques de santé publique. Pour exploiter pleinement le potentiel des données de santé, il est impératif d'adopter une approche collaborative impliquant tous les acteurs du secteur, des professionnels de santé aux patients, en passant par les autorités réglementaires et les développeurs de technologies de santé.

Au plan opérationnel, une veille politique, réglementaire et technologique s'avère cruciale pour anticiper les risques et les opportunités à saisir. C'est à cette condition que nous pourrons tirer parti des promesses de la révolution numérique dans le domaine de la santé.