

3. Sécurité, confiance et souveraineté renforcées pour le partage des données de santé

3.1. Garder la maîtrise des données de santé : une souveraineté nécessaire

La réutilisation des données de santé ne peut se développer sans garanties fortes en matière de sécurité, de maîtrise des infrastructures et de protection contre les accès non autorisés. Le règlement EEDS consacre ainsi le principe selon lequel les données de santé électroniques à caractère personnel utilisées dans le cadre de l'usage secondaire doivent être conservées et traitées au sein de l'Union européenne par les ORAD, les détenteurs de données de santé de confiance et le service d'accès aux données de santé de l'Union. Cette exigence traduit la volonté de renforcer la maîtrise européenne des données de santé et de garantir un haut niveau de protection des personnes concernées.

L'hébergement souverain des données de santé

La souveraineté numérique constitue une priorité du gouvernement. Pour l'usage secondaire, la France retient une trajectoire exigeante : les données de santé à caractère personnel traitées par les ORAD, les détenteurs de données de confiance (DDC) ou les environnements de traitement sécurisés ont vocation à rester hébergées et manipulées dans l'Union européenne, sans mobiliser l'exception prévue par l'art. 87§2 du règlement. Cette orientation s'inscrit dans un cadre national déjà structuré par la loi SREN, la certification HDS, le référentiel de sécurité du SNDS et les référentiels établis par la CNIL.

3.2. Proposer des environnements de traitement sécurisés

Ce que prévoit le règlement EEDS

Le règlement EEDS prévoit à l'art. 73 la mise en place d'environnements de traitement sécurisé (Secure Processing Environment) permettant de travailler sur les données de santé considérées comme sensibles, au premier titre desquelles les données personnelles de santé pseudonymisées ou toute autre donnée protégée (propriété intellectuelle, secret des affaires, etc.). Ces environnements doivent permettre un accès contrôlé aux données, limité aux personnes habilitées et aux finalités autorisées, tout en garantissant la confidentialité, l'intégrité, la traçabilité des opérations et la prévention des extractions non autorisées de données personnelles.

L'ORAD opérateur doit proposer de tels environnements aux utilisateurs. D'autres acteurs peuvent également en proposer et cela fait partie en particulier des critères exigés pour être qualifié de DDC.

Ce qu'il reste à préciser au niveau européen

L'art. 73 fait l'objet d'un acte d'exécution, en cours de discussion au niveau européen. Il s'agit d'un socle de sécurité minimal à adopter pour chaque fournisseur d'environnements sécurisés. Ce référentiel exigeant se base pour partie sur les normes existantes en termes de management de la sécurité de l'information.

Ce que prévoit la mise en œuvre en France

En France, la généralisation des environnements de traitement sécurisés s'inscrit dans la stratégie nationale « intelligence artificielle et données de santé », qui identifie le renforcement des infrastructures souveraines, sécurisées et interopérables comme une condition de réussite de l'utilisation secondaire. Ces environnements ont vocation à soutenir la mise à disposition des données

dans un cadre maîtrisé, en cohérence avec les exigences nationales de sécurité, d'hébergement et de souveraineté. Il existe déjà des référentiels ad hoc au niveau français pour travailler dans des environnements de traitements sécurisés, en local ou à distance : référentiel de sécurité du SNDS ou référentiel des entrepôts de données de santé de la CNIL, qui peuvent eux-mêmes être adossés à d'autres référentiels : HDS, SecNumCloud, PGSSI-S.

Ces référentiels seront adaptés en fonction des exigences qui seront édictées par l'acte d'exécution de l'art. 73 du règlement EEDS. L'objectif est également de les harmoniser pour permettre une lisibilité claire des exigences techniques et organisationnelles au niveau des gestionnaires d'environnements sécurisés.

Ce qu'il reste à préciser au niveau national

Les travaux nationaux préciseront les modalités concrètes de mise en œuvre des environnements de traitement sécurisés : habilitation des utilisateurs, journalisation des opérations, contrôle des accès, gestion des exports de résultats, audit, exploitation, articulation avec les différents parcours d'accès et exigences applicables aux détenteurs de données de confiance. Ces travaux sont conduits dans le cadre du GT CNS n° 3 « *Exigences de sécurité pour l'hébergement et la mise à disposition des données de santé* », co-piloté par la DGRINES et la PDS, dont les ateliers ont porté sur la pseudonymisation, le chiffrement et le cloisonnement, la traçabilité et la gestion des incidents, la sécurité physique et celle des postes d'accès, la gestion des exports de résultats et de l'anonymisation, ainsi que la territorialité et la souveraineté, y compris les transferts hors Union européenne. La stratégie nationale prévoit en complément la clarification de la doctrine relative aux bulles sécurisées et un travail de simplification des référentiels de sécurité applicables : référentiel de sécurité du SNDS, référentiel « entrepôts » de la CNIL, certification HDS et qualification SecNumCloud (objectif 3.1).