La protection des données de santé avance à grands pas : ne nous arrêtons pas en si bon chemin !

Lettre ouverte commune sur les enjeux stratégiques de sécurité et de souveraineté numériques liés au nouveau référentiel pour l'hébergement des données de santé

Confiance et sécurité : c'est le moins que puissent attendre les citoyens en ce qui concerne des données aussi sensibles que leurs consultations médicales, leurs résultats d'analyses ou leurs comptes-rendus d'opérations… En ce sens, **le référentiel révisé de certification des Hébergeurs de Données de Santé (HDS), qui permet de garantir la sécurité de l'hébergement de données de santé, apporte des garanties importantes**. Nous, fournisseurs européens de services cloud, soutenons depuis le début les objectifs affichés par le projet de révision lancé en 2022 par la Délégation au Numérique en Santé et l'Agence du Numérique en Santé.

C'est tout le sens de notre première lettre commune publiée en février 2023 pour réaffirmer l'importance de **garantir la protection des données de santé hébergées, selon une double exigence de sécurité et de souveraineté numériques** face aux lois extraterritoriales. C'est tout le sens également des travaux du futur Comité Stratégique de Filière « Solutions numériques de confiance », qui vise à accompagner le développement de services protecteurs qui répondent aux attentes des utilisateurs.

Si **nous soutenons le nouveau référentiel HDS**, nous réaffirmons également notre appel à **aller encore plus loin dans la protection des données de santé** lors du nouveau projet de révision du référentiel prévu en 2027. **Anatomie en trois points d'une avancée inédite qu'il reste à amplifier pour sécuriser durablement la transformation numérique de la santé**.

Point 1 : ***Un référentiel plus transparent et exigeant en matière de souveraineté***

Protéger les données de santé, dans un secteur de plus en plus connecté, c'est lutter contre des accès non autorisés, qu'ils proviennent des cybercriminels ou d'États tiers. Aujourd'hui encore, ce type d'accès compromet la maîtrise que les utilisateurs sont en droit d'exiger sur l'utilisation et le traitement de ces données particulièrement sensibles. L'exemple le plus saisissant est sans doute le *Foreign Intelligence Surveillance Act*, cette loi controversée que le gouvernement américain vient de prolonger de deux ans et qui permet aux services de renseignement outre-Atlantique d'avoir accès aux données d'utilisateurs non-américains sans que ces derniers en soient informés.

Dans ce contexte préoccupant, s'entrechoquent des enjeux non seulement numériques mais aussi politiques, économiques, sociétaux et éthiques. **Le nouveau référentiel HDS formalise un certain nombre d'avancées en matière de maîtrise et de transparence des données de santé.** L'ajout d'une nouvelle section, composée de quatre exigences

relatives à la souveraineté des données est un premier pare-feu que nous appelions de nos vœux. En imposant notamment l'hébergement physique exclusif des données de santé au sein de l'Espace Économique Européen et des exigences strictes de transparence, cette section a un double mérite : améliorer la protection de ces données tout en renforçant le niveau d'information des utilisateurs, en particulier sur les risques de transfert de leurs données en dehors de l'Union européenne.

Point 2 : ***L'industrie française du numérique prête et engagée à protéger les données de santé européennes***

Ces nouvelles avancées du référentiel HDS doivent permettre aux utilisateurs de **prendre conscience de l'enjeu d'une protection renforcée de leurs données de santé**, et de s'en saisir, au moment même où la filière numérique française se structure pour mieux répondre à leurs attentes.

Le coup d'envoi officiel des travaux du **Comité Stratégique de Filière « Solutions numériques de confiance »** le 15 mai dernier marque en ce sens un jalon important. Une étape d'autant plus notable qu'elle prend racine dans un pays, la France, précurseur en matière de protection des données et de valorisation de son industrie. Ce Comité illustre l'engagement collectif de la filière à proposer des services numériques innovants et adaptés au besoin de confiance des utilisateurs. Avec la montée en puissance de cette filière, c'est **l'autonomie numérique et technologique de la France et de l'Europe qui est en jeu**. Les acteurs français sont d'ores et déjà prêts et **conformes aux plus hautes exigences de sécurité.**

Point 3 : ***La future version du référentiel devra être plus ambitieuse pour garantir la confiance***

Le rapport Marchand-Arvier publié en janvier 2024 souligne que le potentiel de notre patrimoine de données de santé reste largement sous-exploité, freiné par des processus longs et complexes et surtout un manque de coopération et de confiance au sein de l'écosystème.
C'est pourquoi, nous reconnaissons que l'évolution du référentiel HDS est **un premier pas certes positif mais qui doit en précéder d'autres** : la prochaine révision du référentiel, déjà prévue pour 2027, devra garantir une véritable souveraineté des données de santé, en exigeant une immunité aux lois extraterritoriales. Ce niveau de protection doit dépasser la seule exigence de localisation des données, **insuffisante pour protéger les données contre tout accès par des Etats tiers**. Il convient donc de s'aligner avec les critères du chapitre 19.6 du référentiel « SecNumCloud 3.2 » de l'Agence Nationale de Sécurité des Systèmes d'Information pour assurer une réelle maîtrise des données et rétablir la confiance au sein de l'écosystème. Cette évolution s'inscrit par ailleurs dans la dynamique impulsée par la loi "sécuriser et réguler l'espace numérique" qui va imposer l'hébergement de certaines données du secteur public sur des services cloud qui garantissent les plus hauts critères de sécurité et de protection des données.

Dans un contexte géopolitique incertain, et au regard de la valeur inestimable des données de santé, nous défendons un **modèle de société résolument européen et éthique, dans l'intérêt des organisations et des citoyens**. Nous, industriels européens du cloud, appelons à un numérique en santé qui simplifie, innove et protège.