Rapport de l'OFSP du 27 janvier 2026 à l'attention de la CSSS-N pour la séance du 12 février 2026

25.082 Dossier électronique de santé. Loi fédérale

Fiche d'information : bases de l'infrastructure technique

1. Mandat

L'administration a été chargée de répondre aux questions suivantes :
» Quels sont les modèles envisagés en lien avec l'organisation centralisée ou décentralisée de l'infrastructure technique ?
» Comment se structure le lien entre le DES et DigiSanté/l'Espace suisse des données de santé ? Contexte : il est prévu que l'infrastructure technique du DES soit centralisée. Or, dans l'Espace suisse des données de santé (DigiSanté), les données devront être accessibles de manière décentralisée.
» Quels enseignements peut-on tirer en relation avec le projet « Justitia 4.0 » ?

2. Contexte

À l'heure actuelle, les données de santé sont enregistrées de manière décentralisée, sur les très nombreux systèmes des fournisseurs de prestations et des établissements de santé tels que les cabinets, les hôpitaux, les pharmacies ou les laboratoires. Leur conservation sécurisée et conforme à la protection des données relève de la responsabilité propre des fournisseurs de prestations et des établissements de santé.
À l'avenir, les données de santé resteront enregistrées de façon fondamentalement décentralisée, d'autant que l'obligation de documentation individuelle est maintenue pour les fournisseurs de prestations.
L'Espace suisse des données de santé (SwissHDS) a été créé dans le cadre du programme DigiSanté. Il vise à établir des normes uniformes permettant de garantir un échange de données sans rupture de médias afin d'assurer l'interopérabilité des systèmes. De la sorte, les fournisseurs de prestations peuvent échanger des données de santé de manière automatique et efficace (puisqu'alors aucune étape intermédiaire manuelle n'est nécessaire), entre eux ou avec la Confédération.
Les infrastructures de service et les services du SwissHDS sont des composants indispensables pour assurer la gouvernance, l'interopérabilité et la traçabilité. Le dossier électronique de santé (DES) fait partie intégrante du SwissHDS et permet de stocker les données de santé à long terme. En effet, la loi oblige les fournisseurs de prestations à supprimer ces données après un certain temps. Le DES compte parmi les objets à protéger de la Confédération. À ce titre, il est soumis à des mesures de sécurité plus restrictives que celles appliquées aux systèmes d'information usuels des cabinets médicaux et hôpitaux.

3. Conservation des données dans le DES

Le DES est et restera un système d'information secondaire. En d'autres mots, toutes les informations médicales continuent d'être stockées de manière décentralisée dans les systèmes des fournisseurs de prestations. En revanche, le DES enregistre à long terme les données de santé qui seront pertinentes tout au long de la vie des patients. Ainsi, les informations relatives aux vaccins ou aux allergies ne sont pas perdues à l'extinction de l'obligation de conservation ou lors de la fermeture d'un cabinet.
La centralisation du système d'information n'est pas synonyme d'un réservoir unique de données. Il s'agit plutôt de fixer des règles uniformes et des normes communes reposant sur un enregistrement des données chiffré, segmenté conformément aux dernières avancées techniques, et réparti sur plusieurs instances. En outre, la sécurité est renforcée grâce à une isolation technique combinée à des processus cryptographiques et à des restrictions légales.
Une solution décentralisée reposant sur les systèmes primaires avait été étudiée. Il en était cependant ressorti qu'une telle solution n'était pas réalisable à moyen terme, puisqu'elle présupposait que tous les fournisseurs de prestations disposent de systèmes à haute disponibilité répondant aux normes de sécurité et qu'ils soient en mesure de fournir leurs données dans le respect des normes établies, à long terme et en tout temps. Bien que cette

vision figure parmi les objectifs à long terme du SwissHDS, elle ne sera vraisemblablement pas mise en œuvre au niveau national avant 2034. Dans ce contexte, le DES joue un rôle crucial de pont : il anticipe la création des bases nécessaires à une préparation des données structurée, standardisée et sécurisée à la source (systèmes primaires des fournisseurs de prestations). Il agit ainsi comme un catalyseur décisif sur la voie qui mène au SwissHDS. Enfin, le système d'information DES sera, à l'avenir, le seul espace de stockage à long terme des données personnelles de santé.

4. Chiffrement

Le DES ne proposera pas un chiffrement de bout en bout systématique basé sur des clés contrôlées uniquement par les patients. En effet, un tel dispositif requerrait un niveau de compétence numérique et de responsabilité qui ne peut être raisonnablement exigé de l'ensemble de la population. Dès lors, la compatibilité au quotidien du DES n'aurait plus été assurée, et ce alors qu'un accès facile, fiable et conforme au droit est pourtant une condition décisive permettant de garantir une véritable autodétermination en matière d'information. Pour cette raison, l'architecture du DES repose sur un chiffrement renforcé des dossiers, mais n'intègre délibérément pas une gestion des clés relevant exclusivement des patients. En parallèle, le cadre technique et la législation garantissent que ni les opérateurs ni les autorités ne puissent accéder au contenu des données de santé.

5. Sécurité et protection des données

Dans le cadre de la nouvelle loi, les données sensibles de santé restent soumises à des exigences en matière de sécurité élevées. L'architecture moderne du DES sera développée dans le respect des principes *zero trust*, *security by design* et *security by default*. Elle sera en outre conforme aux exigences strictes de la loi sur la sécurité de l'information (LSI), de la loi fédérale sur la protection des données (LPD) et de la loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA). Soumises au droit suisse, les données seront exclusivement conservées en Suisse. En outre, un centre de sécurité des opérations, une surveillance continue des systèmes de sécurité et un programme « bug bounty » structuré offriront une protection supplémentaire. De plus, il faudra absolument disposer de journaux d'accès exhaustifs et inaltérables que les patients puissent consulter en tout temps pour vérifier ex post tous les accès demandés. Enfin, la détection d'anomalies et la détection des abus permettront d'identifier les modèles suspects et de déclencher automatiquement un avertissement.

6. Comparaison avec le projet Justita 4.0

L'OFSP mène des échanges avec l'équipe de projet de Justitia 4.0. Il convient toutefois de noter qu'à y regarder de plus près, les deux systèmes – le DES et Justitia 4.0 – ne sont comparables que dans une mesure limitée. En effet, la plateforme Justitia a pour objectif le transfert sécurisé de documents, c'est-à-dire la transmission de documents d'un service à un autre. Actuellement, elle ne fait pas usage d'un chiffrement de bout en bout. De son côté, le DES est un projet beaucoup plus complexe, dans le cadre duquel des données particulièrement sensibles sont enregistrées à long terme tout en devant rester accessibles à un large éventail d'acteurs, de manière contrôlée et restreinte en fonction de la situation. L'enjeu n'est donc pas la transmission de documents, mais la conservation à long terme de données et le contrôle d'accès granulaire pendant de longues périodes, et ce même en cas d'urgence. Ces différences ont une influence considérable sur l'architecture et les stratégies de sécurité de chacun des systèmes.

7. Conclusion et travaux connexes

Il faut des normes exigeantes en matière de sécurité des données afin de faciliter la mise en œuvre de la protection des données et de créer la base de confiance nécessaire à l'acceptation et au succès du DES. Pour ce faire, l'OFSP examine plusieurs options. Pour l'heure, celle retenue consiste en un modèle de sécurité en plusieurs couches proposant un chiffrement renforcé et des contrôles d'accès clairs. L'examen porte également sur la possibilité d'intégrer l'infrastructure de confiance relative à l'identité électronique (e-ID) ou le SwissGovernementCloud. Un comité spécialisé externe clarifie actuellement la forme exacte que prendront les mesures de protection cryptographique, qui seront mises en œuvre en étroite collaboration avec les services spécialisés internes et des experts en sécurité externes. Ensemble, ils s'efforcent de trouver le meilleur équilibre entre la sécurité, la convivialité et l'économicité.
Les détails techniques seront précisés par voie d'ordonnance. De la sorte, il sera possible de s'assurer que les dispositions légales puissent être adaptées en continu et correspondent ainsi à l'état actuel de la technique. Les milieux intéressés sont impliqués dans différents organes et auront l'occasion de prendre position lors de la procédure de consultation relative au droit d'exécution.