Services numériques de santé : il y a urgence à protéger nos données les plus précieuses

Lettre ouverte commune sur les « enjeux de sécurité et de souveraineté » dans le futur référentiel pour l'hébergement de données de santé

Paris, le 7 février 2023

Fin 2022, l'Agence du Numérique en Santé a officiellement lancé la révision du référentiel de certification Hébergeur de Données de Santé (HDS). Cette certification est incontournable pour attester de la capacité d'un opérateur à mettre en place un hébergement protecteur des données de santé à caractère personnel, particulièrement sensibles, et ainsi construire un environnement de confiance autour de la modernisation du système de santé français. **Nous, fournisseurs européens de services d'informatique en nuage (cloud computing),** soutenons pleinement les objectifs affichés par ce projet de révision, et souhaitons aujourd'hui réaffirmer **que l'hébergement des données de santé ne doit être réalisé qu'avec des conditions de sécurité adaptées à leur niveau de criticité. Les données de santé exigent le plus haut niveau de confiance, jusqu'à garantir une immunité aux lois extraterritoriales. Voici trois raisons qui justifient l'évolution de la certification HDS en un vrai référentiel souverain.**

Raison n° 1 : Pour répondre aux impératifs de protection des données de santé.

Les données de santé sont des données hautement sensibles, elles nécessitent des protections à la hauteur des attentes des citoyens. En 2021, 66 % des Français interrogés se disaient prêts à renoncer à un service numérique en cas de manque de transparence vis-à-vis du traitement réservé à leurs données, tel qu'un transfert non consenti[1]. Or, des législations extraterritoriales comme le Foreign Intelligence Surveillance Act ou le CLOUD Act aux États-Unis permettent toujours aux autorités étrangères d'avoir accès aux données sans que les utilisateurs concernés n'aient à en être informés. Une situation qui semble incompatible avec les attentes exprimées en matière de maîtrise et de transparence des données, si l'on estime qu'en 2023, 65 % des patients accèderont aux soins via les services numériques[2]. **Garantir l'absence de transfert de données de santé est un enjeu d'ordre politique, économique, mais aussi sociétal.**

En matière de souveraineté, nous sommes convaincus **qu'aménager le référentiel en s'appuyant sur des exigences en matière de protection vis-à-vis des lois extraeuropéennes** permettrait de répondre aux objectifs de la révision du référentiel. L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) a par exemple défini de tels critères, principalement juridiques, dans sa qualification « SecNumCloud[3] », notamment obligatoire pour les Organisations dites « d'Intérêt Vital » ou les données sensibles des administrations.

Raison n° 2 : Pour aligner la filière et attester le rôle de pionnier de la France.

Aujourd'hui, la France peut compter sur une filière numérique solide et des acteurs présents à chaque étape de sa chaîne de valeur : fournisseurs de services cloud déployés à échelle industrielle,

[1] « Les Français et la souveraineté numérique » Sondage Ifop pour OVHcloud, Janvier 2021

[2] « Redéfinir l'expérience des patients et du personnel : accélérer le développement des plateformes numériques intelligentes dans le secteur de la santé grâce au cloud » Étude IDC pour OVHcloud, Septembre 2021

[3] " Référentiel SecNumCloud v3.2, chapitre 19.6 en tant que critères à utiliser pour évaluer la « sujétion de l'organisation ou de ses éventuels sous-traitants à des législations extra-européennes pouvant entraîner une violation des données de santé à caractère personnel », mentionné à l'exigence 4, l'exigence 10 et dans le chapitre 7.6 relatif à la représentation normalisée des services.

intégrateurs, éditeurs de logiciels spécialisés dans les besoins des établissements de santé, sans compter le vivier de startups qui disposent des moyens et des ambitions pour révolutionner et adapter l'usage des nouvelles technologies appliquées au médical.

Cette filière est parfaitement à même de proposer les services numériques correspondants aux attentes du système santé français et d'innover pour accompagner ses mutations, le tout dans des conditions qui garantissent la protection des données.

L'approche montrerait aussi une nouvelle fois que la France fait de la protection des données de ses citoyens et de l'affirmation de la souveraineté numérique une priorité, en conformité avec le Règlement Général sur la Protection des Données (RGPD). Une stratégie qui renforce son rôle précurseur en matière de protection des données et de valorisation de son industrie.

Raison n° 3 : Pour garantir la robustesse des infrastructures sans concession sur la transparence des services numériques de santé.

En 2021, 63 % des fournisseurs de services de soins de santé européens[4] ont déclaré investir dans des plateformes de collaboration basées sur le cloud, notamment pour améliorer la productivité et l'expérience des employés. Si l'on peut se réjouir des démarches entamées pour la transition numérique du secteur, il est de notre responsabilité d'alerter sur la cybermalveillance qui continue de menacer les établissements publics de santé. Ceux-ci restent, d'après l'ANSSI, la troisième cible privilégiée des rançongiciels en 2022[5], après les entreprises et les collectivités. La protection des systèmes d'information repose sur la complémentarité des moyens mis en œuvre, de l'infrastructure jusqu'aux services. Dans cette équation, produire une architecture réglementaire qui intègre des critères de haute résilience et de réplication contribuerait à mieux anticiper les potentielles menaces.

Appliquer, d'une part, les dimensions juridiques et techniques de la souveraineté à nos systèmes d'information de santé renforcerait leur robustesse physique et cyber, tout en maintenant une véritable transparence technologique vis-à-vis de tous les utilisateurs : patients, établissements de santé et prestataires de services numériques.

Aligner, d'autre, part le référentiel HDS aux critères de souveraineté des données harmoniserait les référentiels et schémas de certification, avec à la clé une meilleure lisibilité des offres pour les utilisateurs de services cloud et une simplification en matière de mise en conformité pour les fournisseurs.

La protection des données de santé est un enjeu collectif, bien au-delà d'intérêts économiques isolés. Faisons le choix de la protection des organisations et des citoyens européens. Alignons-nous sur la souveraineté, la confiance et la transparence.

- Quentin Adam, CEO, **Clever Cloud**
- Arnaud Muller et Jérôme Valet, Co-fondateurs, **Cleyrop**
- Sébastien Lescop et Christophe Lesur, CEO, **Cloud Temple**
- Olivier Vallet, CEO, **Docaposte**
- Denis Planat, Directeur Général, **Free Pro**
- Alain Garnier, CEO, **Jamespot**

---

[4] « Redéfinir l'expérience des patients et du personnel : accélérer le développement des plateformes numériques intelligentes dans le secteur de la santé grâce au cloud » Étude IDC pour OVHcloud, Septembre 2021

[5] https://www.ssi.gouv.fr/actualite/un-niveau-eleve-de-cybermenaces-en-2022/

- Murielle Bochaton, Directrice du développement, **Nameshield**
- Bertrand Servary, fondateur et CEO, **NetExplorer**
- Stanislas De Rémur, CEO et Xavier Filiu, CISO, **Oodrive**
- Thomas Baignères, CEO, **Olvid**
- Philippe Miltin, CEO et David Chassan, Directeur Stratégie, **Outscale**
- Michel Paulin, CEO et Emmanuel Meyrieux, Responsable sécurité clients, **OVHcloud**
- Paul Benoit, Président co-fondateur et Clément Pellegrini, CTO co-fondateur**, Qarnot**
- Arnaud de Bermingham, Président, **Scaleway**
- Éléna Poincet, CEO et co-fondatrice, **Tehtris**
- Anne-Sophie Taillandier, Directrice de **TeraLab**, **IMT**
- Renaud Ghia, Président et Sébastien Jeanjean, Directeur Général, **Tixeo**