MINISTÈRE
CHARGÉ DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

Délégation au numérique en santé

Paris, le 16 mai 2024

Communiqué de presse

Publication au Journal Officiel du référentiel de certification HDS : souveraineté des données et améliorations du référentiel

La version révisée du référentiel de certification Hébergeurs de Données de Santé (HDS) a été publiée au Journal Officiel, ce jour.

Les hébergeurs de données de santé déjà certifiés HDS devront obtenir la certification HDS conformément à ce nouveau référentiel HDS dans un délai de 24 mois, soit au plus tard le 16/05/2026.

Les nouveaux candidats à la certification HDS à partir du 16/11/2024 seront évalués par rapport à cette nouvelle version du référentiel HDS.

La nouvelle version du référentiel HDS sera présentée aux acteurs de l'écosystème par la Délégation au Numérique en Santé et l'Agence du Numérique en Santé lors d'une conférence organisée à SantExpo l**e mercredi 22 mai à 16h00**, en présence de représentants de l'écosystème et du Député Philippe Latombe (inscription).

La certification des hébergeurs de données de santé permet de garantir la sécurité de l'hébergement des données de santé. En vigueur depuis novembre 2017, c'est un des premiers piliers de la régulation du numérique en santé en France. Tout l'enjeu est de **certifier que les hébergeurs de données de santé mettent en œuvre des systèmes de gestion de la sécurité des systèmes d'information à l'état de l'art** des normes internationales.

C'est un acquis majeur pour la confiance des patients et des professionnels.

A ce jour, 302 acteurs ont été certifiés. Neuf organismes sont accrédités par le comité français d'accréditation (COFRAC) pour procéder à ces certifications.

Suite aux différents retours des acteurs du secteur et cinq ans après la mise en œuvre de cette certification, la Délégation du Numérique en Santé et l'Agence du Numérique en Santé ont lancé **une démarche de révision du référentiel de certification HDS début 2022**.

Cette démarche a associé la Commission nationale de l'informatique et des libertés (CNIL), le Haut Fonctionnaire de Défense et de Sécurité du ministère de la santé (HFDS), ainsi que les fédérations d'industriels de l'écosystème et les organismes certificateurs. Cette nouvelle

version du référentiel a fait l'objet d'une concertation publique fin 2022. L'ANS a reçu plus de 250 contributions qui ont été analysées et traitées début 2023. A l'issue de plusieurs échanges avec la CNIL, celle-ci a rendu un avis favorable au projet de référentiel de certification révisé le 13 juillet 2023.

Ensuite, le projet d'arrêté approuvant la version révisée des deux référentiels a été notifié à la Commission européenne le 7 décembre 2023 pour une période de 3 mois pendant laquelle aucun commentaire n'a été reçu par la Commission.

Le travail autour du référentiel s'est notamment nourri des différents débats qui ont eu lieu dans le cadre du projet de loi visant à sécuriser et à réguler l'espace numérique. La récente adoption de l'article 32 du projet de loi visant à sécuriser et à réguler l'espace numérique (SREN), qui modifie les dispositions relatives à l'hébergement des données de santé, conforte les orientations du référentiel en leur donnant une accroche législative.

En tenant compte des contributions des acteurs, cette nouvelle version du référentiel de certification HDS permet de :

- **Renforcer de manière progressive la souveraineté des données** avec de nouvelles exigences pour renforcer les garanties en termes de protection (voir focus ci-après) ;
- **Clarifier le périmètre des types d'activité d'hébergement** - notamment l'activité dite "5" concernant l'administration et l'exploitation, qui faisait l'objet d'interrogations, et sur laquelle un consensus général a été trouvé – et **renforcer la transparence des hébergeurs sur les types d'activités sur lesquelles ils sont certifié**s ;
- **Préciser l'articulation entre les exigences de la certification HDS et celles de la certification SecNumCloud** proposée par l'ANSSI.
- **Intégrer dans le référentiel de certification HDS certaines évolutions de la norme ISO 27001.**

Focus sur l'ajout d'exigences relatives à la souveraineté des données

La version révisée du référentiel HDS prévoit quatre exigences nouvelles relatives à la souveraineté des données (exigences 28 à 31) :

- **L'hébergement physique des données de santé doit être réalisé exclusivement sur le territoire d'un pays situé au sein de l'Espace Economique Européen** – EEE - (Union Européenne – UE avec la Norvège, l'Islande et le Liechtenstein), ce qui n'était pas une exigence requise jusqu'alors dans HDS. Sans être suffisante pour garantir totalement l'immunité extra-territoriale, cette exigence de localisation apporte néanmoins des garanties importantes en termes de protection des données. Elle permet de renforcer la confiance des patients et professionnels dans le numérique en santé et contribue à l'émergence d'un écosystème d'acteurs européens.

- En cas d'accès distant aux données depuis un pays tiers à l'UE, par l'hébergeur ou l'un de ses sous-traitants, ou en cas de soumission de ces derniers à une législation extra-européenne n'assurant pas un niveau de protection adéquat au sens de l'article 45 du RGPD (voir la carte de la CNIL), alors l'**hébergeur doit en informer ses clients dans le contrat et lui préciser les risques associés**, ainsi que les mesures techniques et juridiques mises en œuvre pour les limiter. Cette transparence est essentielle dans la relation qui lie l'hébergeur au client, responsable du traitement des données.

- L'obligation pour l'hébergeur de rendre public, sur son site internet, **une cartographie des éventuels transferts des données qu'il héberge vers un pays n'appartenant pas à l'EEE**. Cette transparence est essentielle pour les citoyens, les acteurs de santé et l'ensemble de la société civile.

Il est à noter que le référentiel révisé ne prévoit pas, à date, un alignement sur les exigences en termes d'immunité extraterritoriale proposées par le référentiel SecNumCloud V3.2 (notamment celles du paragraphe 19.6). Ce point sera notamment réévalué à la lumière des discussions sur les futurs référentiels européens (European Cybersecurity Certification Scheme for Cloud services - EUCS) et au plus tard en 2027. La prochaine révision de référentiel suivra également l'évolution de la maturité des acteurs du marché.

Corollaire du référentiel HDS, le référentiel d'accréditation, rédigé en collaboration avec le COFRAC, décrit le processus d'accréditation des organismes de certification. Il intègre notamment les retours d'expériences des auditeurs qui ont été recueillis lors d'ateliers dédiés.

Les principales évolutions, concernent les mises à jour en lien avec l'évolution de la norme ISO 27001, l'harmonisation des points en miroir du référentiel HDS (définition, références normatives, chapitre…) et la mise à jour des durées des audits.

Les organismes certificateurs ont ainsi un délai de six mois pour adapter leur procédure de certification au nouveau référentiel HDS.

À propos de la Délégation au numérique en santé : La Délégation au numérique en santé (DNS) assure le pilotage de la feuille de route du numérique en santé et de l'ensemble des chantiers de transformation du numérique en santé avec ses partenaires. La DNS est directement rattachée à la ministre du travail, de la santé et des solidarités. Elle assure un pilotage resserré de l'Agence du Numérique en Santé.

Contact presse : Marion Février // 06 08 77 61 02 // marion.fevrier@sante.gouv.fr