HDS et souveraineté : les 10 points à vérifier

Grille de lecture pour évaluer un hébergeur de données de santé

Cette grille rassemble dix questions à poser à un hébergeur de données de santé et l'enjeu de chacune. Elle structure une évaluation, sans fournir de score ni d'avis juridique. Point de départ : la certification HDS atteste la conformité d'un périmètre d'activités d'hébergement aux exigences du référentiel ; elle ne suffit pas à elle seule à écarter l'exposition aux lois extraterritoriales (deux plans distincts que cette lecture sépare).

N°	Critère	La question à poser au fournisseur	Pourquoi c'est décisif
A. Ce que la certification HDS atteste			
1	Certification HDS	Le certificat HDS est-il en cours de validité et délivré par un organisme certificateur accrédité par le COFRAC ou par un organisme européen équivalent ?	Un certificat expiré ou délivré par un organisme non accrédité ne constitue pas une certification HDS valide.
2	Périmètre des 6 activités	La certification couvre-t-elle toutes les activités effectivement réalisées dans le cadre de la prestation, notamment l'administration-exploitation et la sauvegarde ?	Certaines offres ne sont certifiées que sur une partie du périmètre. Une certification partielle peut être suffisante si elle correspond exactement aux activités réalisées par le fournisseur. Les autres activités doivent alors être identifiées et, lorsqu'elles relèvent de l'hébergement HDS, couvertes par un acteur dûment certifié.
B. Ce que la certification HDS ne couvre pas (souveraineté juridique)			
3	Localisation des données	Dans quels pays et datacenters les données de santé et leurs sauvegardes sont-elles réellement stockées, et ce stockage est-il exclusivement situé dans l'Espace économique européen (EEE) ?	Un hébergeur peut stocker les données en France et rester soumis à une loi extra-européenne du fait de sa maison mère.
4	Protection contre les législations extra-européennes	Le fournisseur, les sociétés qui le contrôlent et ses sous-traitants sont-ils exposés à une législation extra-européenne (Cloud Act, FISA) susceptible d'imposer un accès aux données ? Quelles garanties (statut juridique, contrôle capitalistique, localisation et maîtrise des opérations, éventuelle qualification SecNumCloud) limitent ce risque ?	La certification HDS ne supprime pas, à elle seule, le risque d'accès imposé par une autorité étrangère. Le décret n° 2026-209 du 24 mars 2026 renforce le cadre (stockage dans l'EEE, encadrement des transferts, information du client sur les risques et les mesures d'atténuation), mais documente ce risque sans l'écarter. Deux plans distincts se combinent : l'immunité juridique, qui repose sur le statut du prestataire (soumission exclusive au droit européen, contrôle capitalistique, absence de filiale relevant d'un droit tiers) et que peut aussi attester une qualification SecNumCloud ; et l'indépendance technologique vis-à-vis de fournisseurs non européens, que la seule qualification ne garantit pas. Pour les données les plus sensibles, la CNIL recommande un prestataire soumis exclusivement au droit européen et offrant un niveau de protection approprié.

N°	Critère	La question à poser au fournisseur	Pourquoi c'est décisif
5	Localisation des opérations	Depuis quel pays, et par quelles équipes, la plateforme est-elle administrée et exploitée ?	Un accès distant depuis un pays tiers constitue un transfert au sens du RGPD : il doit être juridiquement encadré (décision d'adéquation ou garanties appropriées), et n'est pas en soi synonyme d'exposition effective. Le référentiel HDS impose de documenter les pays concernés, les garanties mises en œuvre, les législations extra-européennes applicables et les risques résiduels, et d'en informer le client dans le contrat.
C. Exploitation, engagement et sortie			
6	Répartition des responsabilités	Quelles obligations restent à la charge du client une fois l'hébergement confié ?	La certification est portée par l'hébergeur et couvre le volet hébergement. Elle ne couvre pas les applications du client ni ses obligations au titre du RGPD.
7	Sauvegarde et reprise d'activité	Comment sont assurées la sauvegarde et la continuité de service (objectifs RPO (objectif de point de reprise) / RTO (objectif de temps de reprise)) ?	La sauvegarde est l'une des activités du référentiel HDS ; elle ne suffit pas à elle seule à garantir la continuité, qui est un sujet distinct. Des objectifs RPO et RTO chiffrés, définis dans le contrat, permettent de mesurer la perte de données acceptable et le délai de restauration visé.
8	Réversibilité	Peut-on récupérer l'intégralité de ses données dans un format exploitable et quitter la plateforme sans dépendance technique ?	Une réversibilité insuffisante crée un verrouillage qui peut augmenter les coûts ou les délais d'une migration et compliquer un changement de fournisseur, par exemple une migration imposée vers une solution souveraine.
9	Transparence	Le fournisseur publie-t-il une cartographie des transferts hors Espace économique européen et documente-t-il ses engagements et mesures de sécurité ?	Le référentiel HDS révisé prévoit déjà la publication et la mise à jour d'une cartographie des transferts hors EEE, des accès distants et des risques d'accès par un État tiers. Cette obligation est également inscrite dans le code de la santé publique par le décret n° 2026-209 du 24 mars 2026, avec une entrée en vigueur différée pour ces dispositions (six mois après la publication au JO). Son absence doit conduire à vérifier la version du référentiel applicable au certificat et à demander au fournisseur comment il satisfait à ses obligations de transparence.
10	Exploitation managée	La plateforme prend-elle en charge chiffrement, isolation, sauvegardes, supervision et mises à jour, ou ces couches restent-elles à configurer par le client ?	Plus le fournisseur limite sa prestation aux couches d'infrastructure, plus le client doit assurer lui-même la configuration, l'exploitation et la surveillance des couches supérieures. Ce partage des responsabilités doit être explicite afin d'éviter les zones non couvertes.

Nota bene

Cette grille est un outil de réflexion destiné à structurer l'évaluation d'un hébergeur de données de santé. Elle ne constitue pas un avis juridique. Les références réglementaires citées sont fournies à titre d'information ; leur application dépend de la nature des données traitées et de la situation propre à chaque organisation. Pour les traitements sensibles, l'appui d'un délégué à la protection des données ou d'un conseil juridique est recommandé.

Sources

- Décret n° 2026-209 du 24 mars 2026 portant modification de dispositions du code de la santé publique relatives à l'hébergement de données de santé (JO du 26 mars 2026). Dispositions sur la localisation du stockage et la cartographie applicables six mois après la publication.
- CNIL - recommandations relatives à l'hébergement des données de santé ; note du 19 juillet 2024 sur les risques d'accès des autorités étrangères aux données sensibles.
- Agence du numérique en santé (ANS) - référentiel de certification des hébergeurs de données de santé (HDS).
- Cour des comptes - recommandation d'alignement du référentiel HDS sur les exigences SecNumCloud.
- Code de la santé publique, articles L. 1111-8, R. 1111-9-1 et R. 1111-11.