AYI NEDJIMI Consultants

HDS 2026 : Certification Hébergeur de Données de Santé -

Catégorie : Conformité Lecture : 8 min Publié le : 19/01/2026 Auteur : Ayi NEDJIMI

Guide complet HDS 2026 : certification hébergeur données de santé, exigences techniques, processus audit, articulation ISO 27001 et SecNumCloud pour.

01 Contexte Réglementaire HDS

La certification **HDS (Hébergeur de Données de Santé)** constitue une obligation légale française pour tout organisme hébergeant des données de santé à caractère personnel pour le compte de tiers. En 2026, cette certification reste incontournable pour les acteurs du numérique en santé, avec un écosystème qui s'est considérablement développé et des exigences qui continuent d'évoluer. Guide complet HDS 2026 : certification hébergeur données de santé, exigences techniques, processus audit, articulation ISO 27001 et SecNumCloud pour. Le cadre réglementaire européen impose des exigences croissantes aux organisations. Ce guide sur hds 2026 certification sante fournit les clés de compréhension et de mise en conformité. Nous abordons notamment : 01 contexte réglementaire hds, 02 périmètre des données de santé et 03 exigences techniques hds. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Instaurée par l'article L.1111-8 du Code de la santé publique et précisée par le décret du 26 février 2018, la certification HDS vise à garantir un niveau de protection adéquat pour les données les plus sensibles des citoyens : leurs informations de santé.

Pourquoi HDS est essentiel
Les données de santé sont parmi les plus sensibles au sens du RGPD (Article 9). Leur compromission peut avoir des conséquences graves : atteinte à la vie privée, discrimination, usurpation d'identité médicale, ou risques pour la santé des patients si des données sont altérées.

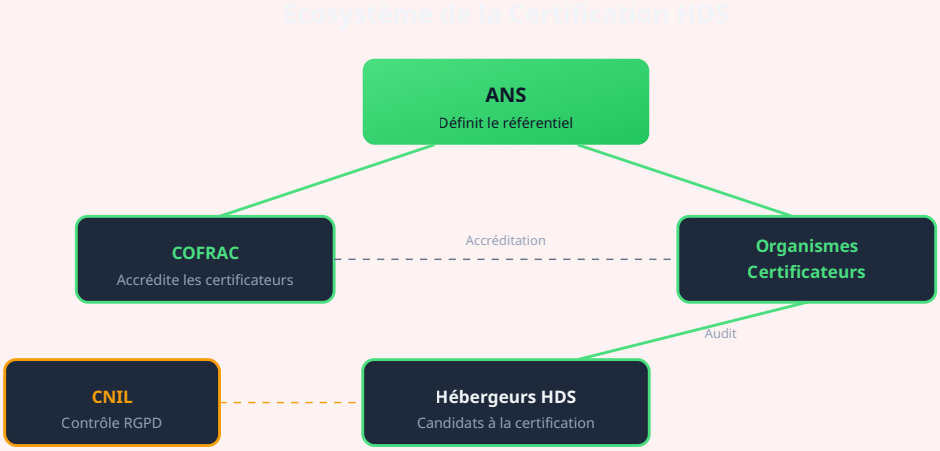
Évolution du cadre réglementaire

Le cadre HDS a connu plusieurs évolutions significatives :

- **2006** : Création de l'agrément ASIP Santé
- **2018** : Passage à la certification HDS (décret du 26/02/2018)
- **2019** : Entrée en vigueur effective de la certification
- **2024** : Révision du référentiel avec renforcement des exigences
- **2026** : Intégration accrue avec les exigences européennes (NIS 2, EHDS)

Les acteurs institutionnels

L'ANS (Agence du Numérique en Santé), anciennement ASIP Santé, définit le référentiel et supervise le dispositif. Les **organismes certificateurs accrédités** par le COFRAC réalisent les audits de certification. La **CNIL** reste l'autorité de contrôle pour les aspects protection des données personnelles.



Les acteurs institutionnels de la certification HDS

Notre avis d'expert
Le RGPD a profondément transformé la gestion des données personnelles en Europe. Au-delà des amendes, c'est la confiance des clients et partenaires qui est en jeu. Nos accompagnements montrent que la mise en conformité RGPD révèle systématiquement des failles de sécurité préexistantes.

02 Périmètre des Données de Santé

La certification HDS s'applique à l'hébergement des **données de santé à caractère personnel** recueillies dans le cadre d'activités de prévention, diagnostic, soins ou suivi social et médico-social. Comprendre précisément ce périmètre est essentiel pour déterminer si une organisation est soumise à l'obligation.

Définition des données de santé

Selon le RGPD et la réglementation française, les données de santé incluent :

- **Données médicales directes** : diagnostics, traitements, résultats d'examens, comptes-rendus médicaux
- **Données médico-administratives** : séjours hospitaliers, actes médicaux codifiés, remboursements
- **Données biologiques** : résultats d'analyses, données génétiques
- **Données d'imagerie médicale** : radiographies, scanners, IRM
- **Données de dispositifs médicaux** : données collectées par les DM connectés

Attention aux données dérivées
Certaines données peuvent devenir des données de santé par croisement ou inférence. Par exemple, des données de bien-être (sommeil, activité physique) peuvent devenir des données de santé si elles sont utilisées dans un contexte médical ou permettent de déduire un état de santé. Pour approfondir, consultez ISO 27001:2022 - Guide Complet de Certification et Mise e....

Activités d'hébergement concernées

Le référentiel HDS définit **6 activités** d'hébergement pouvant faire l'objet de certification :

Activité	Description	Exemples
1. Mise à disposition de locaux	Hébergement physique	Datacenters, salles serveurs
2. Infrastructure matérielle	Fourniture de serveurs physiques	Serveurs dédiés, baies
3. Infrastructure virtuelle	Machines virtuelles, cloud IaaS	VMs, conteneurs
4. Plateforme logicielle	Environnement d'exécution (PaaS)	Bases de données, middleware
5. Infogérance	Administration et exploitation	Supervision, maintenance
6. Sauvegarde externalisée	Stockage des sauvegardes	Backup as a Service

Qui doit être certifié ?

L'obligation de certification s'applique à tout organisme qui héberge des données de santé **pour le compte de tiers**. Cela inclut :

- Les hébergeurs cloud proposant des services aux acteurs de santé
- Les éditeurs de logiciels SaaS santé

- Les prestataires d'infogérance pour établissements de santé
- Les sous-traitants manipulant des données de santé

Exception : Un établissement de santé hébergeant ses propres données n'a pas besoin d'être certifié HDS. En revanche, il doit utiliser un hébergeur certifié s'il externalise cet hébergement.

Êtes-vous certain que votre traitement des données personnelles est conforme au RGPD ?

03 Exigences Techniques HDS

Le référentiel HDS s'appuie sur la norme **ISO 27001** comme socle, complété par des exigences spécifiques au secteur de la santé. Cette approche garantit un niveau de sécurité cohérent avec les standards internationaux tout en répondant aux particularités des données de santé. Les recommandations de CNIL constituent une reference essentielle.

Socle ISO 27001

La certification ISO 27001 est un **prérequis** à la certification HDS. L'hébergeur doit démontrer la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) couvrant : Les recommandations de ENISA constituent une reference essentielle.

- Politique de sécurité de l'information
- Organisation de la sécurité
- Gestion des actifs
- Sécurité des ressources humaines
- Sécurité physique et environnementale
- Gestion des opérations et communications
- Contrôle d'accès
- Acquisition, développement et maintenance des SI
- Gestion des incidents de sécurité
- Continuité d'activité
- Conformité

Exigences spécifiques HDS

Au-delà d'ISO 27001, le référentiel HDS impose des exigences additionnelles :

Protection renforcée des données

- Chiffrement des données au repos et en transit
- Séparation stricte des environnements
- Pseudonymisation des données de test
- Contrôle d'accès basé sur les rôles (RBAC)

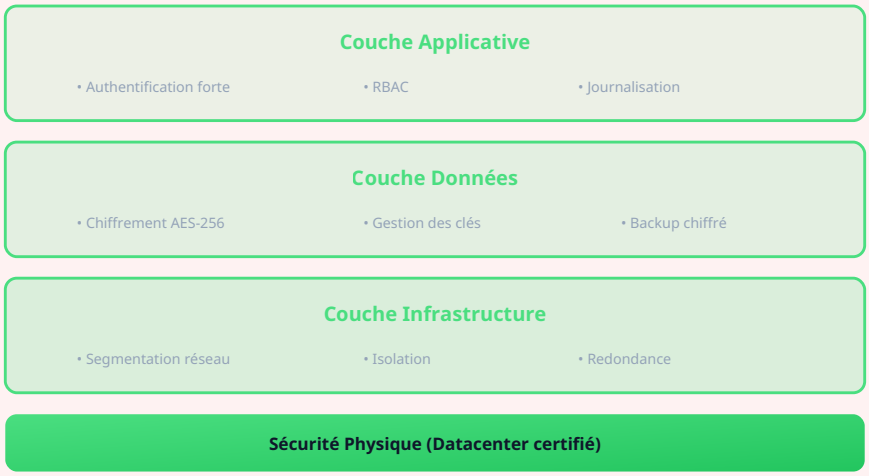
Traçabilité des accès

- Journalisation exhaustive des accès aux données
- Horodatage fiable et inaltérable

- Conservation des logs conforme à la réglementation
- Capacité d'audit et d'investigation

Continuité d'activité santé

- RTO/RPO adaptés à la criticité des données
- Plan de continuité testé régulièrement
- Redondance géographique pour les données critiques
- Procédures de reprise documentées



Architecture de sécurité en couches pour l'hébergement HDS

Cas concret
L'amende de 35 millions d'euros infligée à H&M par l'autorité allemande de protection des données pour surveillance excessive de ses employés a mis en lumière les risques RGPD liés aux pratiques RH. L'entreprise collectait des données de santé, de conviction religieuse et de vie privée lors d'entretiens informels.

04 Processus de Certification

Le processus de certification HDS suit un parcours structuré impliquant plusieurs étapes et acteurs. La durée totale, de la décision initiale à l'obtention du certificat, varie généralement de **12 à 24 mois** selon la maturité de l'organisation.

Phases du parcours

Phase 1 - Évaluation préliminaire : L'organisation évalue son positionnement par rapport aux exigences HDS et ISO 27001. Un gap analysis permet d'identifier les écarts et de planifier les actions de mise en conformité. Pour approfondir, consultez SOC 2 : Guide Complet Conformite pour Organisations.

Phase 2 - Mise en conformité : Déploiement du SMSI, mise en œuvre des mesures techniques et organisationnelles, formalisation de la documentation, sensibilisation des équipes.

Phase 3 - Audit ISO 27001 : Si l'organisation n'est pas encore certifiée ISO 27001, elle doit d'abord obtenir cette certification auprès d'un organisme accrédité. Pour approfondir, consultez SOC 2 Type II : Retour d'Experience Implementation.

Phase 4 - Audit HDS : L'organisme certificateur HDS réalise l'audit complémentaire sur les exigences spécifiques santé. Cet audit peut être combiné avec l'audit ISO 27001.

Phase 5 - Certification : En cas de conformité, le certificat HDS est délivré pour une durée de 3 ans.

Les 5 phases du parcours de certification HDS

Coûts de certification

Poste	Fourchette	Commentaire
Accompagnement conseil	50 000 - 150 000 €	Gap analysis, mise en conformité
Audit ISO 27001	15 000 - 40 000 €	Si non déjà certifié
Audit HDS	10 000 - 25 000 €	Exigences complémentaires
Maintien annuel	15 000 - 30 000 €	Audits de surveillance

05 Audit et Points de Contrôle

L'audit HDS vérifie la conformité aux exigences du référentiel. Les auditeurs examinent tant les aspects documentaires que techniques, incluant des vérifications sur site et des tests de configuration.

Points de contrôle clés

- **Gouvernance** : PSSI santé, comité sécurité, revue de direction
- **Gestion des risques** : Analyse de risques santé, plan de traitement
- **Contrôle d'accès** : Authentification, habilitations, traçabilité
- **Chiffrement** : Données au repos et en transit, gestion des clés
- **Continuité** : PCA/PRA testés, sauvegardes fonctionnelles
- **Incidents** : Procédures de gestion et notification

• **Contrats** : Clauses RGPD et HDS avec les clients

06 Articulation avec ISO 27001

La certification ISO 27001 constitue le fondement du référentiel HDS. Cette articulation permet de capitaliser sur un standard international reconnu tout en ajoutant les spécificités du secteur santé.

Ce qu'ISO 27001 apporte

- Cadre méthodologique pour le SMSI
- 114 mesures de l'Annexe A (ISO 27002)
- Approche par les risques
- Amélioration continue (PDCA)
- Reconnaissance internationale

Ce que HDS ajoute

- Exigences renforcées sur les données de santé
- Clauses contractuelles obligatoires
- Traçabilité spécifique santé
- Exigences de localisation des données
- Conformité RGPD renforcée

07 HDS et SecNumCloud

Pour les données de santé les plus sensibles, notamment celles relevant de la doctrine "Cloud au Centre" de l'État, la question de l'articulation entre HDS et SecNumCloud se pose avec acuité.

Complémentarité des certifications

HDS se concentre sur les exigences spécifiques aux données de santé : confidentialité médicale, traçabilité des accès, continuité des soins. Pour approfondir, consultez Cyber Resilience Act 2026 : Guide Anticipation Produits C....

SecNumCloud apporte les garanties de souveraineté et d'immunité aux législations extra-européennes, essentielles pour les données stratégiques.

Recommandation pour les données sensibles
Pour les données de santé de l'État (hôpitaux publics, recherche médicale financée par le public, données du Health Data Hub), la combinaison HDS + SecNumCloud devient la référence. Plusieurs hébergeurs proposent désormais cette double certification.

08 Acteurs Certifiés en 2026

L'écosystème HDS s'est considérablement développé depuis 2019. En 2026, plusieurs dizaines d'hébergeurs sont certifiés, offrant une diversité de services adaptés aux besoins du secteur santé.

Catégories d'acteurs certifiés

- **Hébergeurs cloud généralistes** : OVHcloud, Scaleway, Outscale
- **Acteurs spécialisés santé** : Cegedim, Docaposte, Santeos
- **ESN avec offres HDS** : Atos, Capgemini, Sopra Steria
- **Éditeurs SaaS santé** : Nombreux éditeurs de DPI, télémédecine

09 Cas d'Usage et Bonnes Pratiques

L'application de HDS varie selon les contextes métier. Voici les principaux cas d'usage et les bonnes pratiques associées.

Établissements de santé

Les hôpitaux et cliniques externalisent de plus en plus leur infrastructure IT. Le choix d'un hébergeur HDS est obligatoire pour les données patient. Points d'attention : intégration avec le SI existant, performance pour l'imagerie médicale, support 24/7.

Éditeurs de logiciels santé

Les éditeurs de DPI, LAP, télémédecine doivent être certifiés HDS s'ils hébergent les données de leurs clients. L'alternative est de s'appuyer sur un hébergeur certifié en mode IaaS/PaaS.

Recherche médicale

Les entrepôts de données de santé pour la recherche (type Health Data Hub) nécessitent HDS + considérations de souveraineté. Le pseudonymisation et l'accès contrôlé sont critiques.

10 Évolutions 2026-2028

Le cadre HDS continue d'évoluer pour s'adapter aux transformations du secteur santé et aux nouvelles réglementations européennes.

Tendances réglementaires

- **EHDS (European Health Data Space)** : L'espace européen des données de santé impactera les exigences d'interopérabilité et de portabilité
- **NIS 2** : Le secteur santé étant couvert, renforcement des exigences de cybersécurité

- **AI Act** : Impact sur l'utilisation de l'IA en santé et les données d'entraînement

Évolutions techniques

- **Confidential Computing** : Protection des données en cours de traitement
- **Interopérabilité** : Standards FHIR, HL7 v3
- **Edge Computing santé** : Traitement local pour les DM connectés

Pour approfondir ce sujet, consultez notre outil open-source iso27001-toolkit qui facilite l'accompagnement à la certification ISO 27001.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, déployer des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Sources et références : CNIL · ANSSI

Conclusion

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2026 — Reproduction interdite sans autorisation.