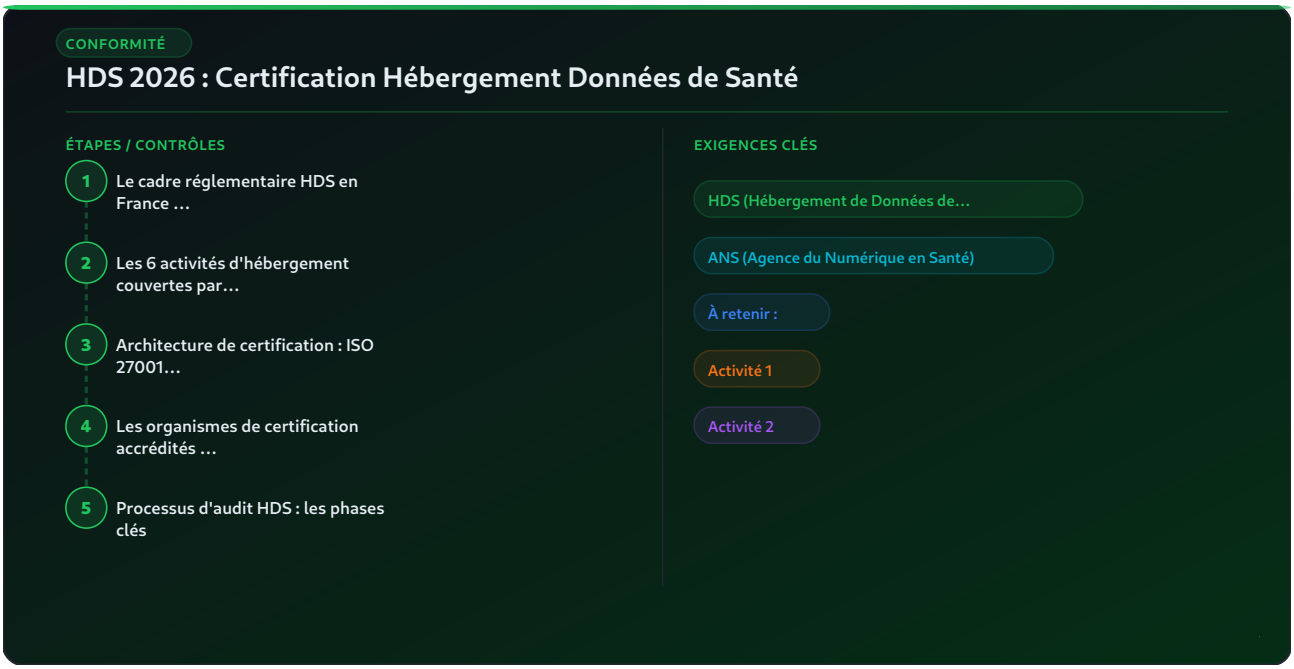
# HDS 2026 : Hébergement Données de Santé — Guide Certification et Conformité

> Certification HDS 2026 : référentiel v2024, 6 activités hébergement, audit LSTI/BSI/BDO, DMP, NIS2 santé et protection données patients en France.

La certification **HDS (Hébergement de Données de Santé)** constitue en 2026 le socle réglementaire incontournable pour tout acteur hébergeant, traitant ou infogérant des données de santé à caractère personnel en France. Réformée en 2024 avec l'entrée en vigueur du nouveau référentiel HDS v2024, cette certification impose des exigences renforcées en matière de sécurité informatique, de continuité d'activité et de gouvernance des données médicales. Dans un contexte où les cyberattaques contre les établissements de santé français ont atteint un niveau critique — le CERT-FR a recensé plus de 70 incidents majeurs en 2025 touchant CHU, EHPAD et cliniques privées —, la certification HDS représente bien plus qu'une obligation légale : c'est un engagement de confiance vis-à-vis des patients et des professionnels de santé. Ce guide complet analyse les 6 activités d'hébergement couvertes, le processus d'audit tripartite (LSTI, BSI Group, BDO), les obligations liées au DMP et à Mon Espace Santé, l'articulation avec NIS2 pour le secteur santé, et les bonnes pratiques pour construire une infrastructure HDS robuste et pérenne face aux menaces cyber croissantes ciblant le secteur médical français.




## Le cadre réglementaire HDS en France : historique et évolution 2024

La certification HDS trouve ses origines dans l'article L.1111-8 du Code de la Santé Publique, qui impose depuis 2011 le recours à des hébergeurs certifiés pour toute externalisation de données de santé. Le référentiel initial de 2018 a été profondément remanié en 2024 pour intégrer les évolutions technologiques (cloud, IA médicale) et renforcer les exigences de sécurité face à la multiplication des incidents.

Le nouveau référentiel HDS v2024, publié par l'**ANS (Agence du Numérique en Santé)** en coordination avec la CNIL et l'ANSSI, restructure les obligations autour de six activités d'hébergement distinctes et introduit des contrôles spécifiques pour l'hébergement cloud souverain.

**À RETENIR**

**À retenir :** Depuis le 1er janvier 2024, tout hébergeur de données de santé doit être certifié HDS v2024. La période de transition pour les certifications HDS v2018 s'est

> achevée le 30 juin 2024. Les nouveaux prestataires doivent obtenir la certification avant toute mise en production.

## Les 6 activités d'hébergement couvertes par la certification HDS

La certification HDS couvre six activités distinctes, chacune pouvant être certifiée indépendamment. Cette approche modulaire permet aux acteurs de ne certifier que les activités réellement exercées.

⚡ **Retour terrain**

Lors d'un accompagnement ISO 27001 pour un hébergeur de données de santé, l'audit de certification a identifié un écart sur le contrôle A.12.4 (journalisation) : les logs d'accès administrateur n'étaient pas centralisés et certains étaient stockés localement sur les serveurs eux-mêmes — effaçables par un admin compromis. La correction a pris 3 semaines ; l'audit de certification avait été planifié 2 semaines après. Leçon : toujours faire un pre-audit interne complet 6 semaines avant la date officielle.

| Activité | Description | Exemples d'acteurs | Spécificités HDS v2024 |
|---|---|---|---|
| **Activité 1** | Mise à disposition et maintien en condition opérationnelle des sites physiques | Datacenters, colocation | Exigences Tier III+, PUE ≤ 1.6, résilience N+1 |
| **Activité 2** | Mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle | IaaS, bare metal | Chiffrement au repos AES-256, TPM 2.0 obligatoire |
| **Activité 3** | Mise à disposition et maintien en condition opérationnelle des plateformes d'hébergement | PaaS, containers | Isolation multi-tenant renforcée, scanning continu |
| **Activité 4** | Mise à disposition et maintien en condition opérationnelle d'infrastructures virtuelles | Cloud IaaS virtualisé | Hyperviseurs certifiés, ségrégation VLAN obligatoire |
| **Activité 5** | Administration et exploitation du système d'information | MSP, infogérance SI | Journalisation 12 mois, SIEM dédié santé |
| **Activité 6** | Sauvegarde externalisée des données de santé | Backup as a Service | Réplication géographique FR obligatoire, test restauration trimestriel |

## Architecture de certification : ISO 27001 comme socle HDS

La certification HDS repose sur un socle **ISO 27001** obligatoire. L'hébergeur doit préalablement obtenir la certification ISO 27001 sur le périmètre concerné avant de pouvoir postuler à la certification HDS. Cette approche en deux couches garantit un niveau de maturité minimal en management de la sécurité de l'information.

Le référentiel HDS v2024 ajoute au-dessus de l'ISO 27001 des *contrôles spécifiques santé* couvrant notamment : la gestion des habilitations pour les données médicales, les procédures de notification de violations au DPO et à la CNIL, les exigences de localisation des données (France ou UE), et les mesures de protection renforcées pour les données génomiques et psychiatriques.

## Les organismes de certification accrédités : LSTI, BSI Group, BDO

Trois organismes sont actuellement accrédités par le COFRAC pour délivrer la certification HDS en France : **LSTI (Laboratoire de la Sécurité des Technologies de l'Information)**, **BSI Group France**, et **BDO France**. Chaque organisme dispose de ses propres auditeurs certifiés HDS et de méthodologies d'audit légèrement différentes.

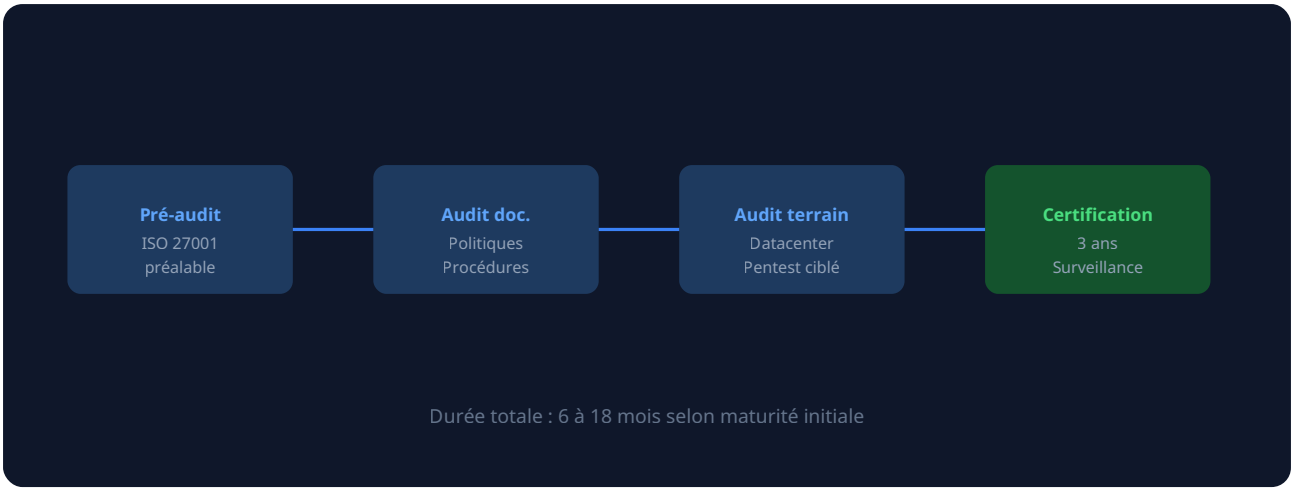
## Processus d'audit HDS : les phases clés

L'audit de certification HDS se déroule en plusieurs phases obligatoires, typiquement sur 6 à 18 mois selon la maturité initiale de l'organisation.

**Phase 1 — Audit documentaire :** L'organisme certificateur examine la politique de sécurité, les procédures opérationnelles, les contrats avec les sous-traitants, et la cartographie des flux de données de santé. Cette phase dure généralement 2 à 4 semaines.

**Phase 2 — Audit terrain :** Les auditeurs visitent physiquement le(s) datacenter(s), inspectent les configurations techniques (pare-feux, chiffrement, contrôle d'accès physique), et réalisent des tests de pénétration ciblés sur les interfaces critiques.

**Phase 3 — Revue des non-conformités :** Les écarts identifiés sont classés en non-conformités majeures (bloquantes) et mineures. Les NC majeures doivent être corrigées avant la délivrance du certificat ; les NC mineures font l'objet d'un plan d'action.




## Obligations DMP et Mon Espace Santé : exigences spécifiques

Les hébergeurs participant à l'écosystème du **Dossier Médical Partagé (DMP)** et de la plateforme **Mon Espace Santé** sont soumis à des exigences supplémentaires définies par l'ANS. Ces acteurs doivent notamment respecter les spécifications techniques d'interopérabilité HL7 FHIR R4, assurer la compatibilité avec les APIs de la plateforme nationale, et garantir une disponibilité de 99,9% pour les services critiques.

La *politique de sécurité des systèmes d'information de santé (PGSSI-S)* publiée par l'ANS constitue le référentiel de sécurité applicable à ces intégrations. Elle couvre notamment la gestion des identifiants nationaux de santé (INS), la traçabilité des accès aux dossiers patients, et les modalités de consentement patient.

## DPIA santé : analyse d'impact obligatoire pour les données médicales

Conformément à l'article 35 du RGPD, le traitement de données de santé à grande échelle nécessite obligatoirement une **Analyse d'Impact relative à la Protection des Données (DPIA)**.

Pour les hébergeurs HDS, cette DPIA présente des spécificités importantes liées à la sensibilité extrême des données médicales.

Les éléments clés d'une DPIA santé conforme incluent : la cartographie précise des flux de données de santé (incluant les transmissions aux professionnels de santé, aux caisses d'assurance maladie et aux établissements), l'évaluation des risques spécifiques (ré-identification de patients à partir de données pseudonymisées, accès non autorisé aux antécédents médicaux), et les mesures techniques et organisationnelles mises en œuvre.

La CNIL a publié en 2024 des **lignes directrices spécifiques** pour les DPIA dans le secteur santé, recommandant notamment le recours à des techniques de *differential privacy* pour les analyses statistiques et l'application systématique du principe de minimisation des données.

## Cyberattaques contre les hôpitaux français : bilan CERT-FR 2025

Le secteur de la santé est devenu la cible prioritaire des groupes ransomware et des acteurs étatiques. Le **CERT-FR** a documenté en 2025 plus de 70 incidents cyber majeurs affectant des structures de santé françaises, dont :

**CHU de Rennes** (février 2025) : chiffrement de 80% des serveurs, paralysie partielle des urgences pendant 6 jours

**Réseau de cliniques privées** (avril 2025) : exfiltration de 2,3 millions de dossiers patients, rançon de 8 millions d'euros

**GHT Île-de-France** (juillet 2025) : compromission de la chaîne d'approvisionnement via un prestataire non-HDS

Ces incidents illustrent l'importance critique de la certification HDS non seulement pour les hébergeurs principaux, mais aussi pour l'ensemble de la chaîne de sous-traitance. Le nouveau référentiel HDS v2024 impose désormais des exigences de sécurité aux sous-traitants des hébergeurs certifiés.

## Articulation HDS et NIS2 pour le secteur santé

La transposition de la directive **NIS2** en droit français (loi du 15 avril 2024) a considérablement renforcé les obligations des acteurs du secteur santé. Les établissements de santé, hébergeurs HDS et fournisseurs de solutions e-santé sont désormais classifiés comme **Entités Essentielles (EE)** au sens de NIS2.

Cette classification EE implique des obligations additionnelles par rapport à la seule certification HDS : notification des incidents à l'ANSSI dans les 24h, mise en œuvre d'une gouvernance cybersécurité au niveau du Conseil d'Administration, et réalisation d'audits de sécurité réguliers par des prestataires qualifiés PASSI.

L'articulation HDS/NIS2 crée une synergie bénéfique : les contrôles HDS satisfont une partie significative des exigences NIS2, notamment en matière de gestion des incidents, de continuité d'activité et de sécurité de la chaîne d'approvisionnement. Il convient toutefois d'identifier les gaps spécifiques à NIS2 et de les combler par des mesures complémentaires.

## Chiffrement et protection des données de santé : exigences techniques HDS v2024

Le référentiel HDS v2024 détaille précisément les exigences cryptographiques applicables aux données de santé :

**Chiffrement en transit :** TLS 1.3 minimum pour toutes les transmissions de données de santé. Les protocoles TLS 1.0 et 1.1 sont explicitement interdits. Les certificats doivent être émis par des autorités de certification reconnues, avec une durée de validité maximale de 398 jours conformément aux recommandations des navigateurs.

**Chiffrement au repos :** AES-256 obligatoire pour le stockage de toutes les données de santé, avec gestion des clés par HSM (*Hardware Security Module*) certifié FIPS 140-2 Level 3 minimum. Les clés de chiffrement doivent être stockées séparément des données chiffrées.

**Gestion des sauvegardes :** Les sauvegardes de données de santé doivent être chiffrées avec des clés distinctes des données de production. La restauration doit être testée trimestriellement avec documentation des résultats. Les sauvegardes doivent être conservées pendant une durée minimale de 10 ans pour les données médicales (conformément au Code de la Santé Publique).

## Gestion des identités et contrôle d'accès en environnement HDS

La gestion des accès aux données de santé requiert des mécanismes robustes allant au-delà des pratiques standard. Le référentiel HDS v2024 impose notamment :

**MFA systématique :** L'authentification multi-facteurs est obligatoire pour tout accès aux systèmes hébergeant des données de santé, y compris pour les administrateurs techniques. Les solutions MFA basées sur SMS sont déconseillées au profit d'applications TOTP ou de clés matérielles FIDO2.

**Principe du moindre privilège :** Chaque compte doit disposer uniquement des droits nécessaires à sa fonction. Les comptes d'administration doivent être distincts des comptes nominatifs et soumis à une revue trimestrielle des droits. Les accès aux données de santé doivent être journalisés avec horodatage, identifiant de l'utilisateur et nature de l'accès.

**PAM (Privileged Access Management) :** Les accès privilégiés aux serveurs hébergeant des données de santé doivent transiter par une solution PAM avec enregistrement des sessions. Les mots de passe d'administration doivent être gérés par un coffre-fort de mots de passe avec rotation automatique.

## Plans de continuité et reprise d'activité : exigences HDS pour le secteur santé

La continuité des systèmes d'information de santé est un enjeu vital. Le référentiel HDS v2024 impose des objectifs de continuité stricts :

Le **RTO (Recovery Time Objective)** pour les systèmes critiques de santé (bloc opératoire, urgences, réanimation) doit être inférieur à 4 heures. Le **RPO (Recovery Point Objective)** ne peut excéder 15 minutes pour les données de production médicale, imposant des solutions de réplication synchrone ou quasi-synchrone.

Les tests de PCA/PRA doivent être réalisés annuellement en conditions réelles, avec participation des équipes métier santé (médecins, infirmiers, directeurs des soins). Les résultats doivent être documentés et les non-conformités corrigées dans un délai de 90 jours.

## Sous-traitance et chaîne d'approvisionnement : nouvelles obligations HDS v2024

L'une des évolutions majeures du référentiel HDS v2024 concerne la gestion de la chaîne d'approvisionnement. Les hébergeurs certifiés HDS sont désormais responsables de leurs sous-traitants intervenant sur le périmètre HDS.

Concrètement, tout sous-traitant accédant aux données de santé ou aux systèmes les hébergeant doit soit être lui-même certifié HDS (pour les activités d'hébergement), soit démontrer un niveau de sécurité équivalent via un audit spécifique réalisé par l'hébergeur HDS.

Cette obligation s'étend aux prestataires de maintenance (interventions physiques dans les datacenters), aux éditeurs de logiciels ayant accès à des données de production, et aux fournisseurs de solutions de cybersécurité intervenant sur le périmètre HDS.

## Surveillance continue et audit de surveillance HDS

La certification HDS est valide 3 ans, mais elle est assortie d'**audits de surveillance annuels** permettant de vérifier le maintien des conditions de certification. Ces audits, moins étendus que l'audit initial, se concentrent sur les points critiques et les évolutions de l'infrastructure.

Entre les audits formels, les hébergeurs HDS doivent maintenir un programme de **surveillance continue** incluant : monitoring 24/7 des systèmes critiques, gestion proactive des vulnérabilités (délai de patch critique ≤ 72h), tests d'intrusion semestriels, et revues régulières des journaux d'accès.

Les hébergeurs HDS sont également tenus de notifier leur organisme de certification en cas d'incident de sécurité significatif, de modification majeure de l'infrastructure, ou de changement de périmètre des activités certifiées. Le non-respect de cette obligation peut entraîner la suspension de la certification.

## Cloud souverain et HDS : compatibilité SecNumCloud

La question de l'hébergement cloud pour les données de santé cristallise un débat stratégique important. Si la certification HDS ne requiert pas explicitement SecNumCloud, les données de santé les plus sensibles (dossiers psychiatriques, données génomiques, données relatives à des mineurs) sont soumises à des recommandations de souveraineté renforcées.

L'ANS recommande pour les systèmes nationaux (DMP, Mon Espace Santé) le recours à des prestataires disposant à la fois de la certification HDS et de la qualification SecNumCloud ou de l'agrément EUCS niveau élevé. Cette double exigence limite de facto le marché aux acteurs français : OVHcloud HDS, Outscale/Dassault Systèmes, et Bleu (projet France Telecom/ Microsoft).

## Intelligence artificielle en santé : nouvelles exigences HDS pour les modèles IA

L'essor de l'IA médicale (aide au diagnostic, prédiction des risques, optimisation des parcours de soins) soulève de nouvelles questions pour les hébergeurs HDS. Le référentiel v2024 aborde explicitement ce sujet en introduisant des exigences spécifiques pour l'entraînement et le déploiement de modèles d'IA en environnement HDS.

Les données de santé utilisées pour l'entraînement de modèles d'IA doivent avoir fait l'objet d'une **pseudonymisation conforme** aux recommandations du CESP (Centre d'Épidémiologie sur les Causes médicales de Décès) et de la CNIL. L'utilisation de données de santé réelles pour l'entraînement sans pseudonymisation préalable constitue une violation grave du RGPD.

Les modèles d'IA déployés en production dans un environnement HDS doivent être documentés (documentation technique, biais connus, performances sur des populations diverses) et faire l'objet d'une validation clinique avant déploiement. L'Article 22 du RGPD relatif aux décisions automatisées s'applique pleinement aux dispositifs d'aide à la décision médicale.

## Coûts et ROI de la certification HDS : analyse financière

Obtenir et maintenir la certification HDS représente un investissement significatif, mais dont le retour sur investissement est démontrable. Les coûts typiques pour une PME spécialisée en hébergement santé comprennent :

**Coûts d'obtention (année 1) :** Audit ISO 27001 (15 000 à 30 000 €), mise en conformité technique (50 000 à 200 000 € selon l'écart initial), audit HDS initial (25 000 à 60 000 €), formation des équipes (10 000 à 25 000 €). Total : 100 000 à 315 000 € pour un périmètre médium.

**Coûts de maintien annuels :** Audit de surveillance (8 000 à 15 000 €), programme de tests d'intrusion (15 000 à 30 000 €), outils de monitoring et SIEM (20 000 à 50 000 €/an), ressources humaines dédiées (0,5 à 2 ETP RSSI/compliance). Total : 60 000 à 150 000 €/an.

En contrepartie, la certification HDS ouvre l'accès à un marché estimé à 4,2 milliards d'euros en France (hébergement et infogérance santé) avec des marges significativement supérieures au marché généraliste.

## Cas pratique : migration vers HDS d'un SIH hospitalier

La migration du Système d'Information Hospitalier (SIH) d'un CHU régional vers un hébergement certifié HDS illustre la complexité de ces projets. Le projet type comprend plusieurs phases critiques :

**Phase de cadrage (3-6 mois) :** Cartographie exhaustive des données de santé (DPI, PACS, biologie, pharmacie), identification des criticités métier, choix du ou des hébergeurs HDS, et rédaction des appels d'offres intégrant les exigences HDS.

**Phase de migration technique (6-18 mois) :** Déploiement de l'infrastructure cible, migration progressive des applications avec validation fonctionnelle, mise en place du chiffrement et des solutions de supervision, et tests de performance sous charge réelle.

**Phase de qualification (3-6 mois) :** Tests d'intrusion, validation des PCA/PRA, formation des équipes hospitalières, et accompagnement lors de l'audit de certification de l'hébergeur.

## Responsabilités juridiques et pénales en cas de violation HDS

Le non-respect des obligations HDS expose les acteurs à des sanctions significatives, à la fois réglementaires et pénales :

**Sanctions CNIL :** La violation de données de santé peut entraîner des amendes RGPD allant jusqu'à 4% du chiffre d'affaires mondial ou 20 millions d'euros. La CNIL a prononcé en 2024-2025 plusieurs sanctions à 7 chiffres contre des acteurs de la santé numérique, dont une amende de 1,5 million d'euros contre un hébergeur n'ayant pas notifié une violation dans les 72h.

**Sanctions pénales :** L'article 226-22 du Code pénal sanctionne la divulgation non autorisée de données de santé de 5 ans d'emprisonnement et 300 000 € d'amende. Les dirigeants d'hébergeurs peuvent être personnellement mis en cause en cas de défaillance grave dans la protection des données.

**Responsabilité contractuelle :** Les contrats d'hébergement HDS prévoient généralement des clauses de SLA avec pénalités financières en cas de non-respect des engagements de disponibilité et de sécurité. La perte de certification HDS peut entraîner la résiliation immédiate des contrats et le rapatriement d'urgence des données.

## DevSecOps et sécurité applicative en environnement HDS

Les hébergeurs HDS qui développent ou hébergent des applications médicales doivent intégrer la sécurité dès la conception (*Security by Design*). Les pratiques DevSecOps deviennent incontournables dans ce contexte :

L'analyse statique du code (SAST) et l'analyse dynamique (DAST) doivent être intégrées dans les pipelines CI/CD. Les vulnérabilités critiques (CVSS ≥ 9.0) détectées avant la mise en production doivent être corrigées sans exception. Les outils comme SonarQube, OWASP ZAP, et Checkmarx sont couramment utilisés dans les environnements HDS.

La gestion des dépendances logicielles (Software Composition Analysis ou SCA) est particulièrement critique en environnement médical : les bibliothèques open source utilisées doivent être inventoriées dans un SBOM (*Software Bill of Materials*), et les mises à jour de sécurité doivent être appliquées dans des délais stricts.

## Monitoring et gestion des incidents de sécurité en environnement HDS

La détection et la réponse aux incidents de sécurité dans un environnement HDS présentent des spécificités importantes. Le référentiel HDS v2024 impose des délais de notification contraignants :

Toute violation de données de santé doit être notifiée à la **CNIL** dans les 72 heures suivant sa détection (Article 33 RGPD). Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, ces dernières doivent également être notifiées

(Article 34 RGPD). Pour les Entités Essentielles au sens NIS2, une notification additionnelle à l'ANSSI est requise dans les 24 heures.

La mise en place d'un **SOC dédié santé** ou d'une astreinte de sécurité 24/7 est fortement recommandée pour les hébergeurs HDS de taille significative. Les équipes de réponse aux incidents doivent être formées aux spécificités du secteur santé, notamment en termes de continuité des soins et de gestion de crise.

## Perspectives d'évolution : HDS et eIDAS 2.0, EUCS, AI Act

Le paysage réglementaire entourant l'hébergement des données de santé continue d'évoluer. Plusieurs textes européens auront un impact significatif sur les hébergeurs HDS dans les prochaines années :

**EUCS (European Union Cybersecurity Scheme for Cloud Services) :** Le schéma européen de certification cloud, attendu pour 2025-2026, créera un cadre commun pour l'ensemble de l'UE. Le niveau "High" d'EUCS devrait être compatible avec les exigences HDS françaises.

**EHDS (European Health Data Space) :** Ce règlement européen, adopté en 2024, crée un espace européen de données de santé permettant le partage transfrontalier de données médicales à des fins de soins et de recherche. Les hébergeurs HDS devront s'adapter aux nouvelles exigences d'interopérabilité et de portabilité.

**AI Act :** Les dispositifs médicaux intégrant de l'IA sont classifiés en catégories à risque élevé par le règlement IA européen. Les hébergeurs fournissant une infrastructure pour ces dispositifs devront démontrer la traçabilité des données d'entraînement et la robustesse des modèles.

# FAQ — Questions fréquentes sur la certification HDS

## Quelle est la différence entre la certification HDS et l'agrément CNIL pour les recherches en santé ?

La certification HDS concerne l'hébergement de données de santé dans le cadre des soins. L'autorisation CNIL (ou avis du CESP via le portail MR) s'applique aux traitements de données de santé à des fins de recherche, d'étude ou d'évaluation. Un même hébergeur peut être certifié HDS pour l'hébergement clinique et traiter séparément des données de recherche sous autorisation CNIL. Ces deux cadres sont complémentaires et non substituables.

## Un hébergeur cloud américain (AWS, Azure, GCP) peut-il être certifié HDS ?

Oui, AWS, Microsoft Azure et Google Cloud Platform sont certifiés HDS pour leurs régions françaises. Cependant, la certification HDS ne résout pas les questions de droit applicable en cas de requête judiciaire américaine (Cloud Act de 2018). Pour les données de santé les plus sensibles, l'ANS recommande des prestataires ne relevant pas du droit américain. La question de la localisation des données et du droit applicable doit être évaluée indépendamment de la certification HDS.

## Comment se préparer efficacement à un audit HDS v2024 ?

La préparation optimale à un audit HDS v2024 comprend : (1) Réaliser un audit à blanc avec un cabinet spécialisé 6 mois avant l'audit officiel ; (2) Documenter exhaustivement toutes les procédures opérationnelles de sécurité ; (3) Réaliser et documenter un test de PCA/PRA complet ; (4) Vérifier la conformité de tous les contrats de sous-traitance ; (5) Former l'ensemble du personnel technique aux procédures HDS. Les organismes certificateurs publient des grilles d'autoévaluation disponibles sur leurs sites respectifs.

## Quels sont les délais réels pour obtenir la certification HDS v2024 ?

Le délai moyen pour un acteur partant de zéro (sans ISO 27001 préexistante) est de 18 à 24 mois. Pour un acteur déjà certifié ISO 27001 avec une maturité sécurité correcte, le délai se réduit à 9 à

15 mois. Les principaux facteurs allongeant les délais sont : les non-conformités majeures identifiées lors de l'audit documentaire, les difficultés de mise en conformité technique des datacenters, et la disponibilité des auditeurs des organismes accrédités.

### HDS est-il obligatoire pour les applications mobiles de santé (mHealth) ?

La certification HDS s'applique à l'hébergeur des données de santé, pas nécessairement à l'éditeur de l'application. Si une application mobile de santé stocke des données de santé à caractère personnel sur des serveurs externes, l'hébergeur de ces serveurs doit être certifié HDS. L'éditeur de l'application est responsable du choix d'un hébergeur certifié et doit vérifier que les activités HDS concernées sont bien couvertes par la certification. Les applications stockant des données exclusivement sur le terminal de l'utilisateur (sans serveur externe) ne sont pas concernées par HDS.

## Bonnes pratiques pour maintenir la certification HDS dans la durée

La certification HDS n'est pas un état figé mais un processus continu d'amélioration. Les organisations qui maintiennent leur certification dans la durée partagent plusieurs caractéristiques communes :

Elles ont nommé un **Responsable de la Certification HDS** (distinct du RSSI) chargé de piloter le programme de conformité HDS, de préparer les audits de surveillance, et d'assurer la veille réglementaire. Cette personne est l'interlocuteur privilégié de l'organisme de certification.

Elles maintiennent un **tableau de bord HDS** actualisé mensuellement, incluant : état des contrôles HDS, résultats des derniers tests (PCA, intrusion, restauration), indicateurs de sécurité (délais de patch, taux de MFA), et suivi des actions correctives. Ce tableau de bord est présenté à la Direction générale trimestriellement.

## Ressources et référentiels HDS : où trouver la documentation officielle

Les hébergeurs souhaitant s'engager dans une démarche HDS peuvent s'appuyer sur plusieurs ressources officielles de référence. L'**ANS (Agence du Numérique en Santé)** publie l'ensemble des référentiels HDS, les guides méthodologiques et les FAQ sur son portail esante.gouv.fr. La **CNIL** dispose d'une section dédiée aux données de santé avec des recommandations pratiques pour les DPO et les RSSI du secteur santé. L'**ANSSI** publie des guides spécifiques à la sécurité des systèmes d'information de santé, notamment le guide "Sécurité numérique pour les établissements de santé".

Pour une veille active sur les évolutions réglementaires HDS/NIS2/RGPD santé, l'abonnement aux publications du CERT-FR et de l'ENISA (European Union Agency for Cybersecurity) est indispensable. Les retours d'expérience documentés par le CIOS (Club des Informaticiens et Opérateurs de Santé) constituent également une ressource précieuse pour les praticiens.

Les liens vers la directive NIS2, la certification SecNumCloud, le cadre ISO 27001, et la réglementation DORA permettent d'appréhender l'écosystème réglementaire complet dans lequel s'inscrit la certification HDS. Les acteurs du cloud peuvent également consulter notre analyse sur l'architecture cloud sécurisée. En savoir plus : ANS — Certification HDS et CNIL — Données de santé.

## Interopérabilité et standards techniques HDS : HL7 FHIR, SNOMED CT, IHE

Les hébergeurs HDS opérant dans l'écosystème e-santé français doivent maîtriser les standards d'interopérabilité qui structurent les échanges de données médicales. Le référentiel national d'interopérabilité (RNI) publié par l'ANS définit les standards obligatoires pour les systèmes communiquant avec les services nationaux de santé.

**HL7 FHIR R4** est désormais le standard de référence pour les échanges de données de santé en France. Tous les systèmes se connectant au DMP, à Mon Espace Santé, ou à l'espace numérique de santé (ENS) doivent implémenter les API FHIR conformément aux profils nationaux définis par l'ANS. Les hébergeurs HDS doivent garantir que leur infrastructure supporte les volumes de

transactions FHIR attendus avec les niveaux de performance requis (latence < 200ms pour 95e centile).

**SNOMED CT** (Systematized Nomenclature of Medicine — Clinical Terms) est le référentiel de terminologie clinique adopté en France pour la codification des diagnostics, des actes et des médicaments dans les échanges électroniques. Les bases de données médicales hébergées en environnement HDS doivent supporter les mises à jour régulières de SNOMED CT sans interruption de service.

Les profils **IHE (Integrating the Healthcare Enterprise)** définissent les workflows d'intégration entre systèmes hospitaliers. Des profils comme XDS (Cross-Enterprise Document Sharing), PIX (Patient Identifier Cross-Referencing), et PDQ (Patient Demographics Query) sont essentiels pour l'interopérabilité des SIH hébergés en environnement HDS.

## Gestion des vulnérabilités en environnement HDS : priorités et délais

La gestion des vulnérabilités dans un environnement HDS obéit à des règles plus strictes que dans un environnement standard, compte tenu de la criticité des données hébergées et de l'impact potentiel des incidents sur la sécurité des patients.

Le référentiel HDS v2024 impose un processus de gestion des vulnérabilités formalisé avec des délais de remédiation différenciés selon la criticité : les vulnérabilités de score **CVSS ≥ 9.0** (critiques) doivent être corrigées dans les 72 heures. Les vulnérabilités CVSS 7.0-8.9 (élevées) disposent d'un délai de 7 jours. Les vulnérabilités moyennes (CVSS 4.0-6.9) doivent être traitées dans les 30 jours. Les vulnérabilités de faible criticité font l'objet d'un plan de traitement trimestriel.

La *gestion des correctifs (patch management)* en environnement HDS doit être soigneusement planifiée pour éviter les interruptions de service impactant les soins. Les fenêtres de maintenance doivent être définies en concertation avec les établissements de santé clients, et un plan de rollback doit être disponible pour chaque opération de patching critique.

Les hébergeurs HDS doivent s'abonner aux bulletins de sécurité des principaux éditeurs de logiciels présents dans leur écosystème (Microsoft, Oracle, Philips, Sectra, Dedalus, etc.) et aux

alertes du CERT-FR. La veille CVE doit être automatisée via des outils de scanning de vulnérabilités (Qualys, Tenable, Rapid7) configurés pour couvrir l'intégralité du périmètre HDS.

## Contrôles de sécurité physique : exigences HDS pour les datacenters santé

La sécurité physique constitue un pilier fondamental de la certification HDS. Les datacenters hébergeant des données de santé doivent satisfaire des exigences physiques rigoureuses documentées dans le référentiel HDS v2024 :

**Contrôle d'accès physique :** L'accès aux locaux hébergeant des serveurs de santé doit être limité aux personnes habilitées, avec traçabilité de tous les accès (badges électroniques, logs d'entrée/sortie). Les interventions physiques par des tiers (maintenance, livraisons) doivent être accompagnées et documentées. Les zones hébergeant des données de santé doivent être segmentées physiquement des zones communes.

**Surveillance vidéo :** Les accès aux salles serveurs doivent être surveillés par des caméras de vidéosurveillance avec enregistrement 30 jours minimum. Les images peuvent constituer des preuves en cas d'incident de sécurité ou de vol de matériel. La conservation des images doit respecter les obligations RGPD (information des personnes, limitation des durées de conservation).

**Alimentation électrique :** Les datacenters certifiés HDS doivent disposer d'une alimentation redondante avec onduleurs (UPS) et groupes électrogènes garantissant une autonomie minimale de 72 heures sans alimentation principale. Les tests réguliers de basculement sur groupe électrogène doivent être documentés.

**Climatisation et environnement :** Les systèmes de climatisation doivent être redondants (N+1 minimum) avec monitoring continu de la température et de l'humidité. Des alertes automatiques doivent être configurées pour détecter tout écart par rapport aux plages de fonctionnement optimales (18-27°C, 40-60% humidité).

## Télémédecine et objets connectés médicaux : enjeux HDS spécifiques

L'essor de la télémédecine et des dispositifs médicaux connectés (IoMT — Internet of Medical Things) crée de nouveaux défis pour les hébergeurs HDS. Ces dispositifs génèrent des volumes croissants de données de santé en temps réel, avec des contraintes de latence et de disponibilité spécifiques.

Les moniteurs cardiaques connectés, les glucomètres communicants, les pompes à insuline intelligentes et les systèmes de télésuivi post-opératoire transmettent des données de santé en continu. L'infrastructure HDS hébergeant ces données doit être dimensionnée pour absorber les pics de charge (événements calendaires, épidémies saisonnières) sans dégradation de service.

La sécurité des *dispositifs médicaux connectés (DM logiciels)* est encadrée par le règlement européen MDR (Medical Device Regulation) 2017/745, qui impose des exigences de cybersécurité pour les DM de classe IIa et supérieure. Les hébergeurs HDS accueillant des plateformes de télémédecine doivent s'assurer que les DM hébergés sont conformes au MDR et que les mises à jour de firmware/software sont gérées de manière sécurisée.

L'espace numérique de santé (ENS) et la plateforme Ma Santé 2022+ créent de nouveaux usages de partage de données entre professionnels de santé et patients. Les hébergeurs HDS doivent adapter leurs architectures pour supporter ces flux bidirectionnels tout en maintenant l'intégrité et la confidentialité des données partagées.

## Gestion des incidents cyber dans les hôpitaux : retours d'expérience et leçons apprises

Les incidents de cybersécurité ayant frappé les hôpitaux français ces dernières années fournissent des enseignements précieux pour la conception des architectures HDS résilientes. L'analyse post-incident des attaques contre le CHU de Rouen (2019), l'AP-HP (2021), le CH de Corbeil-Essonnes (2022), et les incidents récents de 2025 révèle des patterns communs exploités par les attaquants.

La **compromission initiale** s'effectue dans la grande majorité des cas via des emails de phishing ciblés (spear phishing), l'exploitation de VPN non patchés (particulièrement Pulse Secure, Citrix et FortiGate), ou la compromission de prestataires tiers (supply chain attack). Les hébergeurs HDS doivent renforcer la sécurité de ces vecteurs d'entrée prioritairement.

La **latéralisation dans le réseau** profite généralement d'une segmentation réseau insuffisante entre les réseaux administratifs et les réseaux médicaux, de mots de passe d'administration partagés ou peu complexes, et d'absences de MFA sur les accès aux systèmes critiques. La mise en œuvre d'une architecture Zero Trust est particulièrement pertinente pour prévenir cette phase.

Le **chiffrement ransomware** final est souvent déclenché après plusieurs semaines de présence discrète de l'attaquant dans le réseau (dwell time moyen : 45 jours dans les hôpitaux français en 2025). Cette phase de persistance est exploitée pour exfiltrer les données avant chiffrement, créant une double extorsion (rançon pour déchiffrement + rançon pour non-divulgation).

## Formation et sensibilisation du personnel médical à la cybersécurité

La dimension humaine reste le maillon faible de la sécurité en milieu hospitalier. Les professionnels de santé, formés prioritairement pour prodiguer des soins, n'ont pas toujours la culture cybersécurité nécessaire pour identifier les tentatives d'hameçonnage ou respecter les procédures de sécurité.

Les hébergeurs HDS jouent un rôle de sensibilisation auprès de leurs clients établissements de santé. Des programmes de formation adaptés au personnel médical (format court, exemples concrets, impact sur les soins) ont montré des résultats significatifs dans la réduction des incidents de phishing. La simulation d'attaques de phishing ciblées permet de mesurer le niveau de sensibilisation et d'adapter les programmes de formation.

Les **référents cybersécurité hospitaliers**, promus par le Programme CaRE (Cybersécurité accélération et Résilience des Établissements) lancé par le gouvernement français en 2023, constituent des relais essentiels au sein des établissements. Les hébergeurs HDS ont intérêt à travailler en étroite collaboration avec ces référents pour garantir la cohérence des mesures de sécurité entre l'infrastructure hébergée et les pratiques internes des établissements.

Le **Programme CaRE**, doté de 750 millions d'euros sur la période 2023-2027, finance notamment des diagnostics de cybersécurité, des formations, et des projets d'amélioration de la sécurité des SI hospitaliers. Les hébergeurs HDS peuvent s'inscrire comme partenaires de ce programme pour accompagner leurs clients dans leur montée en maturité cybersécurité.

## Audit de sécurité HDS : méthodologie d'un test d'intrusion en environnement santé

Les tests d'intrusion réalisés dans un environnement HDS présentent des spécificités importantes par rapport aux pentests standard. La criticité des systèmes (les données médicales peuvent impacter directement la sécurité des patients) impose une approche particulièrement rigoureuse et concertée.

La phase de **reconnaissance et cartographie** d'un pentest HDS inclut l'identification des systèmes exposés sur Internet (portails patient, interfaces API FHIR, accès VPN, messageries sécurisées de santé), l'analyse des certificats TLS pour détecter les systèmes sous-domaines oubliés, et l'inventaire des applications médicales (SIH, PACS, LIS, système de pharmacie) et leurs versions.

La phase d'**exploitation contrôlée** cible en priorité les interfaces d'authentification (force brute sur portails patient, énumération de comptes), les APIs REST exposant des données FHIR (autorisation, injection), les interfaces de télémaintenance des équipements biomédicaux, et les interconnexions avec les partenaires (laboratoires, radiologie, médecine de ville).

Le rapport de pentest HDS doit être particulièrement soigné, avec une classification des vulnérabilités selon leur impact sur la confidentialité des données de santé et la disponibilité des soins. Les recommandations de remédiation doivent être priorisées selon ces deux axes et intégrer les contraintes opérationnelles du milieu médical (impossibilité d'interrompre certains services critiques).

Les prestataires réalisant des tests d'intrusion en environnement HDS doivent être qualifiés **PASSI (Prestataire d'Audit de Sécurité des Systèmes d'Information)** par l'ANSSI. Cette qualification garantit la compétence des auditeurs et leur connaissance des référentiels de

sécurité applicables. La liste des prestataires PASSI qualifiés est disponible sur le site de l'ANSSI.

## Archivage électronique des données de santé : durées légales et sécurité

Les données de santé sont soumises à des durées de conservation légales strictes définies par le Code de la Santé Publique. Les hébergeurs HDS doivent concevoir leurs solutions d'archivage en intégrant ces contraintes dès la conception.

Le dossier médical en établissement de santé doit être conservé pendant **20 ans** à compter de la date du dernier séjour ou de la dernière consultation externe pour les adultes. Pour les patients mineurs, la conservation doit être assurée jusqu'aux 28 ans du patient (majorité + 10 ans). Les données relatives à des accidents du travail et maladies professionnelles ont des durées encore plus longues (jusqu'à 50 ans dans certains cas).

Ces durées de conservation imposent aux hébergeurs HDS de planifier leurs architectures d'archivage sur des horizons temporels très longs. Le risque d'obsolescence technologique (formats de fichiers, supports de stockage, systèmes de déchiffrement) doit être anticipé avec des plans de migration réguliers. Les données archivées doivent rester lisibles et intègres pendant toute leur durée de conservation légale, ce qui impose des vérifications périodiques d'intégrité et des migrations de format si nécessaire.

La *valeur probante de l'archivage électronique médical* est encadrée par les référentiels de l'ANS sur la dématérialisation et l'archivage. Un document numérique a la même valeur juridique qu'un document papier s'il satisfait aux exigences d'intégrité, d'authenticité et de lisibilité définies par ces référentiels.

## Ecosystème des fournisseurs HDS certifiés en France : panorama 2026

Le marché de l'hébergement certifié HDS en France comprend en 2026 plus de 80 prestataires certifiés, couvrant des profils très variés : grands acteurs du cloud (OVHcloud, Orange Business, SFR Business), spécialistes de la santé numérique (Maincare, Enovacom, Dedalus Cloud), et hébergeurs régionaux de proximité.

Les **Groupements Hospitaliers de Territoire (GHT)** développent également des capacités d'hébergement mutualisé pour leurs membres. Ces datacenters hospitaliers, portés par les DSI de CHU référents, offrent une alternative publique aux offres privées tout en garantissant la certification HDS. Ils bénéficient d'une confiance naturelle de la part des établissements de santé membres.

La **concentration du marché** s'accélère : les fusions-acquisitions entre hébergeurs santé se multiplient, les acteurs étrangers (AWS, Azure, GCP) gagnent des parts de marché sur les segments les moins sensibles, et les spécialistes régionaux peinent parfois à amortir les coûts de certification sur des périmètres limités. Cette évolution pose des questions de souveraineté que les pouvoirs publics suivent attentivement.

Les opportunités de marché restent importantes : la transformation numérique du secteur ambulatoire (médecins libéraux, pharmacies, laboratoires) génère une demande croissante d'hébergement HDS. La mise en œuvre du carnet de santé électronique, des ordonnances numériques et du compte rendu de biologie électronique ouvre de nouveaux marchés pour les hébergeurs capables d'accompagner les acteurs de ville dans leur transition numérique sécurisée.