

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.



Tout savoir sur la certification HDS

Résumé

- > La certification HDS (Hébergement de Données de Santé) est une **exigence réglementaire** pour les **organisations hébergeant et exploitant des données de santé**.
- > Elle concerne les établissements de santé, les pharmacies, les laboratoires d'analyse médicale, les organismes d'assurance, les éditeurs de logiciels et les prestataires informatiques qui traitent des données de santé. Elle distingue deux catégories d'activités : **les hébergeurs d'infrastructure physique** et **les hébergeurs gérant des systèmes d'information**.
- > Ses objectifs : assurer **la sécurité des données de santé, protéger la vie privée des patients, garantir la qualité des services d'hébergement des données** et fournir un **cadre de confiance** pour les acteurs du secteur de la santé.

Une obligation pour les organisations traitant des données de santé

La certification HDS (Hébergement de Données de Santé) garantit la qualité, la sécurité et la fiabilité des services d'hébergement et de gestion des données de santé à caractère personnel. Elle est délivrée par des organismes indépendants accrédités par le Comité Français d'Accréditation (COFRAC) et obligatoire pour toute organisation publique ou privée traitant des données de santé :

- > Les établissements de santé (hôpitaux, cliniques, etc.)
- > Les pharmacies et laboratoires d'analyse médicale
- > Les organismes d'assurance et les mutuelles de santé
- > Les éditeurs de logiciels et les prestataires informatiques qui traitent et stockent des données de santé
- > Les associations œuvrant dans le domaine de la santé



Principes et objectifs de la certification HDS



La certification HDS est basée sur la norme internationale de sécurité des systèmes d'information ISO 27001 et comporte des exigences supplémentaires liées au domaine de la santé et à la protection des données personnelles (ISO 27018), en conformité avec le Règlement Général sur la Protection des Données (RGPD).

Elle poursuit ainsi plusieurs objectifs :

- > Assurer la sécurité des données de santé à caractère personnel
- > Protéger la vie privée des patients et le secret médical
- > Garantir la qualité et la fiabilité des services d'hébergement et de gestion des données de santé
- > Fournir un cadre de confiance pour les structures et les professionnels du secteur de la santé qui confient leurs données de santé à des tiers

Les activités soumises à la certification HDS

> Les hébergeurs d'infrastructure physique

Ces hébergeurs sont responsables de la mise à disposition et du maintien en condition opérationnelle :

- > Des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé
- > De l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé



> **Les hébergeurs gérant des systèmes d'information**

Ces hébergeurs sont en charge de la mise à disposition et du maintien en condition opérationnelle :

- > De l'infrastructure virtuelle du système d'information de santé
- > De la plateforme d'hébergement d'applications du système d'information
- > De l'administration et l'exploitation du système d'information contenant les données de santé
- > De la sauvegarde externalisée des données de santé

La complémentarité entre la certification HDS et le RGPD



La certification HDS et le RGPD sont complémentaires dans leur objectif de renforcer la protection des données personnelles de santé. L'obtention d'une certification HDS facilite donc la mise en conformité des responsables de traitement et des sous-traitants avec les exigences du RGPD.

La certification HDS est essentielle pour garantir la sécurité et la confidentialité des données de santé à caractère personnel et les organisations de santé concernées par celles-ci doivent se conformer à la norme ISO 27001 et à des exigences spécifiques pour l'obtenir. Il est donc crucial qu'elles mettent en place les mesures adéquates pour protéger les données de santé des utilisateurs en respectant toutes les exigences évaluées.



NumSpot est spécialisé dans la fourniture de services de cloud performants et sécurisés pour les agences gouvernementales et le secteur privé, notamment dans le domaine des services de santé, banque et assurance.

Si vous souhaitez explorer les avantages d'un cloud souverain pour votre organisation, nous vous encourageons à **nous contacter** pour en savoir plus sur la façon dont nous pouvons vous accompagner dans votre transition. Grâce à nos experts et à notre expérience, nous pouvons vous aider à tirer pleinement parti des avantages d'un cloud souverain pour vos besoins.



À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les réglementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous

 @NumSpot
 @NumSpotCloud