

HDS « Hébergement de Données de Santé » **Cadre juridique et réglementaire**

Annexe de la page [Certification HDS « Hébergement de Données de Santé »](#)

La certification HDS est définie dans le [Code de la santé publique, Article L1111-8](#).
Sa mise en application est prévue par le [Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel](#).

Nouvelle procédure de certification des hébergeurs de données personnelles de Santé

Elle nécessite, au niveau technique :

- de mesurer l'impact de l'activité de l'hébergeur de données personnelles de Santé sur la protection des données ;
- de se conformer aux critères de sécurité informatique DICA : Disponibilité, Intégrité, Confidentialité, Auditabilité ;
- de respecter les exigences établies à partir de normes ISO et préconisations de l'ANSSI ;
- de procéder à un audit initial : documentaire et sur site, par un organisme certificateur accrédité auprès du COFRAC ;
- après obtention d'un certificat valable 3 ans, de procéder à un audit de surveillance annuel.

Elle remplace la procédure d'agrément des hébergeurs de données de santé, avec mise en place d'une période de transition. Elle est conforme et complémentaire au RGPD.

Sanctions encourues en cas de manquement :

- 3 ans d'emprisonnement,
- amende (45.000 €, 225.000 € pour personnes morales),
- amende administrative prévue par le RGPD,
- injonction de cesser le traitement de données.

Types de certification HDS :

Le rôle général de l'hébergeur consiste à la mise à disposition et au maintien en condition opérationnelle des infrastructures et également, selon les cas, des systèmes et applications informatiques.

Il existe **2 types de certification**, dont les *périmètres* (et donc les exigences) dépendent du rôle précis de l'hébergeur :

1. Certification HDS en tant qu'hébergeur d'infrastructure physique
 - sites physiques permettant d'héberger l'infrastructure matérielle du système d'information
 - infrastructure matérielle du système d'information
2. Certification HDS en tant qu'hébergeur infogéreur
 - plateforme d'hébergement d'applications du système d'information
 - infrastructure virtuelle du système d'information
 - administration et exploitation du système d'information
 - sauvegarde externalisée des données

Référentiel de la certification HDS

Il comprend les éléments suivants :

- en prérequis, toutes les exigences demandées par la certification ISO 27001 ;
- des exigences liées aux systèmes de gestion de la sécurité des systèmes d'information ;
- des exigences supplémentaires provenant des normes ISO 20000-1 « Système de gestion de la qualité des services », ISO 27017-ISO 27018 « Code de bonnes pratiques pour la protection des informations personnelles identifiables dans l'informatique en nuage public » ;
- des exigences supplémentaires spécifiques au domaine de la Santé ;
- des exigences en lien avec l'information et consentement des patients, leur droit d'opposition.