# La certification pour l'hébergement de données de santé à caractère personnel (HDS)

## EN BREF

- La **nouvelle procédure de certification** pour l'hébergement de données de santé à caractère personnel sur support numérique va remplacer l'actuelle procédure d'agrément courant 2018.
- Elle prévoit d'encadrer l'activité d'hébergement de données de santé par une **évaluation de conformité à un référentiel de certification**, délivrée par un organisme de certification accrédité par le COFRAC.
- Le décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel définit la nouvelle procédure de certification. La publication des référentiels d'accréditation et de certification au Journal Officiel de la République française est la dernière étape qui entraînera l'ouverture du guichet de la procédure de certification.

## Le cadre juridique de l'hébergement de données de santé à caractère personnel

Les modalités d'hébergement de données de santé à caractère personnel sont encadrées par l'article L.1111-8 du code de la santé publique :

- toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet ;
- l'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime.

Cet article distingue explicitement trois grandes catégories de services d'hébergement de données de santé :

1. **l'hébergement de données de santé sur support papier**, qui doit être réalisé par un hébergeur agréé par le ministre de la culture (procédure déjà existante – cf. décret 2011-246) ;
2. **l'hébergement de données de santé sur support numérique dans le cadre d'un service d'archivage électronique**, qui doit être réalisé par un hébergeur agréé par le ministre de la culture dans des conditions qui seront définies par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et des conseils des ordres des professions de santé ;
3. **l'hébergement de données de santé sur support numérique (hors cas d'un service d'archivage électronique)** qui doit être réalisé par un hébergeur certifié dans des conditions définies par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et des conseils des ordres des professions de santé.

Pour cette troisième catégorie, la certification remplace l'agrément délivré par le ministère des Solidarités et de la Santé dans les conditions définies par le décret n°2006-6 du 4 janvier 2006.

La procédure de certification relative à l'hébergement de données de santé sur support numérique est définie par le décret n° 2018-137 du 26 février 2018 qui sera lui-même précisé par un référentiel d'accréditation et un référentiel de certification en cours de publication. Des projets de référentiel ont été publiés en novembre 2017 sur **http://esante.gouv.fr/**.

# La certification

## Deux certificats

Deux types de certificats seront délivrés aux hébergeurs pour deux métiers d'hébergement distincts :

1. **un certificat « hébergeur d'infrastructure physique »** pour les activités de mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle ;

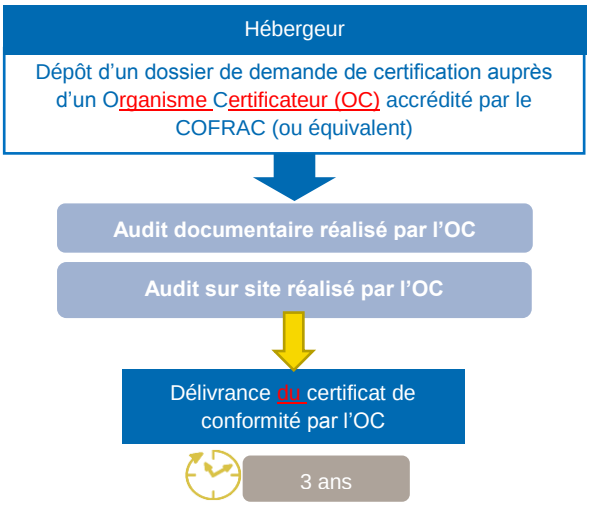
2. **un certificat « hébergeur infogéreur » pour les activités de mise à disposition d'infrastructure virtuelle**, de mise à disposition de plateforme logicielle, d'infogérance et de sauvegarde externalisée.

## Référentiel de certification

Le **référentiel de certification s'appuie sur des normes internationales** :

- la norme **ISO 27001** « système de gestion de la sécurité des systèmes d'information » ;
- des exigences de la norme **ISO 20000-1** « système de gestion de la qualité des services » ;
- des exigences de protection de données à caractère personnel pour lesquelles une conformité à la norme **ISO 27018** confère une présomption de conformité ;
- **et des exigences spécifiques** à l'hébergement de données de santé.

## Procédure de certification




La procédure de certification se fonde sur le processus standard de type système de management décrit dans la norme ISO 17021 :

- L'hébergeur choisit un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen).
- Le cas échéant, l'organisme certificateur vérifie l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000-1 déjà obtenues par l'hébergeur.
- Un **audit en deux étapes conformes aux normes** en vigueur est alors effectué :

**Etape 1**

**audit documentaire**
L'organisme certificateur réalise une revue documentaire du système d'information du candidat afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification ;

**Etape 2**

**audit sur site**
Les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation. L'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles non-conformités et faire auditer les corrections par l'organisme certificateur. Passé ce délai et sans action de l'hébergeur, l'audit sur site devra être recommencé.

**Le certificat est délivré pour une durée de trois ans, par l'organisme certificateur**, lorsqu'aucune non-conformité n'est constatée.
Un **audit de surveillance annuel est effectué** par l'organisme certificateur.

# Phase transitoire

Les agréments délivrés avant l'entrée en vigueur de la procédure de certification produisent leur effet jusqu'à leur terme.
Lorsque l'agrément arrive à échéance avant le 31 mars 2019, la durée de l'agrément est prolongée pour une durée de six mois afin de permettre à l'hébergeur d'effectuer les démarches de certification nécessaires à la poursuite de son activité d'hébergement de données de santé.
Les demandes d'agrément et de renouvellement d'agrément déposées avant le 31 mars 2018 sont instruites selon la procédure d'agrément pour l'hébergement de données de santé sur support électronique (décret n°2006-6).

**Pour plus d'information sur HDS**, connectez-vous sur esante.gouv.fr > Rubrique Services > Hébergement des données de santé