LA CERTIFICATION POUR L'HEBERGEMENT DE DONNEES DE SANTE A CARACTERE PERSONNEL (HDS)

EN BREF

- Les données personnelles de santé sont des données sensibles dont l'accès est encadré par la loi pour protéger les droits des personnes.
- L'hébergement de données de santé à caractère personnel est soumis à une certification prévue par le décret n°2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel.
- La procédure de certification pour l'hébergement de données de santé à caractère personnel sur support numérique est opérationnelle depuis juillet 2018 : elle consiste à procéder à une évaluation de conformité à un référentiel de certification par un organisme de certification accrédité par le COFRAC.

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 ;
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 ;
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.

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 (décret HDS), précisé par l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel.

La certification

Le périmètre

Le décret HDS définit cinq activités d'hébergement soumis à la certification :

1. la mise à disposition et le 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 ;
2. la mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
3. la mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du

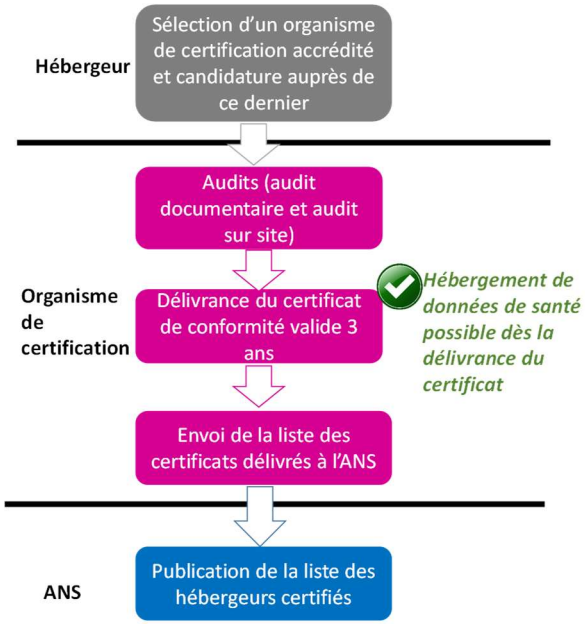
système d'information utilisé pour le traitement des données de santé ;
4. la mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
5. l'administration et l'exploitation du système d'information contenant les données de santé ;
6. la sauvegarde des données de santé.

Le référentiel de certification

Le référentiel de certification s'appuie essentiellement 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 spécifiques.

La procédure de certification



Retrouvez la liste des organismes de certification accrédités et des hébergeurs certifiés sur le site de l'ANS

Organismes de certification

Hébergeurs certifiés

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.

L'hébergeur est autorisé à héberger des données de santé dès la délivrance du certificat par l'organisme de certification.

Tous les mois, les organismes de certification envoient la liste des certificats qu'ils ont délivrés à l'ANS qui publie la liste consolidée.