ÉVOLUTION DE LA PROCÉDURE D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ

asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

ÉVOLUTION DE LA PROCÉDURE D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ

Un dispositif prévu par la loi

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 social ou médico-social **pour le compte d'un tiers**, doit être agréée 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.

L'évolution de l'article L.1111-8

L'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel a modifié l'article L.1111-8 du code de la santé publique en distinguant explicitement trois grandes catégories de services d'hébergement de données de santé :

- 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) ;
- 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 ;
- **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 (CNIL) et des conseils des ordres des professions de santé.**

La procédure d'agrément

Le décret n° 2006-6 du 4 janvier 2006 définit la procédure d'agrément pour l'hébergement de données de santé à caractère personnel sur support informatique et les exigences à respecter :

- **Le décret fixe le contenu du dossier de demande d'agrément.** Sont ainsi évalués la capacité financière du candidat, le type de prestation proposée, le niveau de sécurité et les conditions du respect des principes de la protection des données personnelles et des droits des personnes ;
- **L'agrément est délivré pour une durée de trois ans** par le ministre chargé de la Santé après avis de la CNIL et du comité d'agrément des hébergeurs (CAH - organe consultatif créé par le décret précité). Si l'hébergeur agréé souhaite poursuivre son activité d'hébergement au-delà de la durée d'agrément de trois ans, il doit effectuer une demande de renouvellement d'agrément qui sera instruite comme la demande initiale.

La liste des hébergeurs agréés est publiée sur le site de l'ASIP Santé (http://www.esante.gouv.fr)

L'évolution de la procédure (Mise en œuvre début 2018)

Le nouveau dispositif pour l'hébergement de données de santé sur support numérique est défini par la DSSIS et l'ASIP Santé et validé par un comité de pilotage qui réunit des représentants institutionnels (Ministère de la Santé, ANSSI, CNIL, Fédérations hospitalières, Ordres, etc.) et des représentants d'industriels (AFHADS, ASINHPA, FEIMA, LESSIS, SNITEM et SYNTEC numérique).

Ce nouveau dispositif est une évaluation de **conformité à un référentiel de certification, délivrée par un organisme certificateur** accrédité par le COFRAC (ou équivalent au niveau européen) et choisi par l'hébergeur.

Deux certificats

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

- Un certificat **« hébergeur d'infrastructure physique »** pour les activités de mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle ;
- 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** « système de gestion de la qualité des services» ;
- Des exigences de la norme **ISO 27018** « protection des données à caractère personnel » ;
- 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 et précisé dans la norme ISO 27006 :

- 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 déjà obtenues par l'hébergeur ;
- Un audit en deux étapes conformes aux normes en vigueur est alors effectué :

  - **Étape 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.

  - **Étape 2 : audit sur site**.

Les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation basé sur les normes ISO 17021 et ISO 27006.

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.

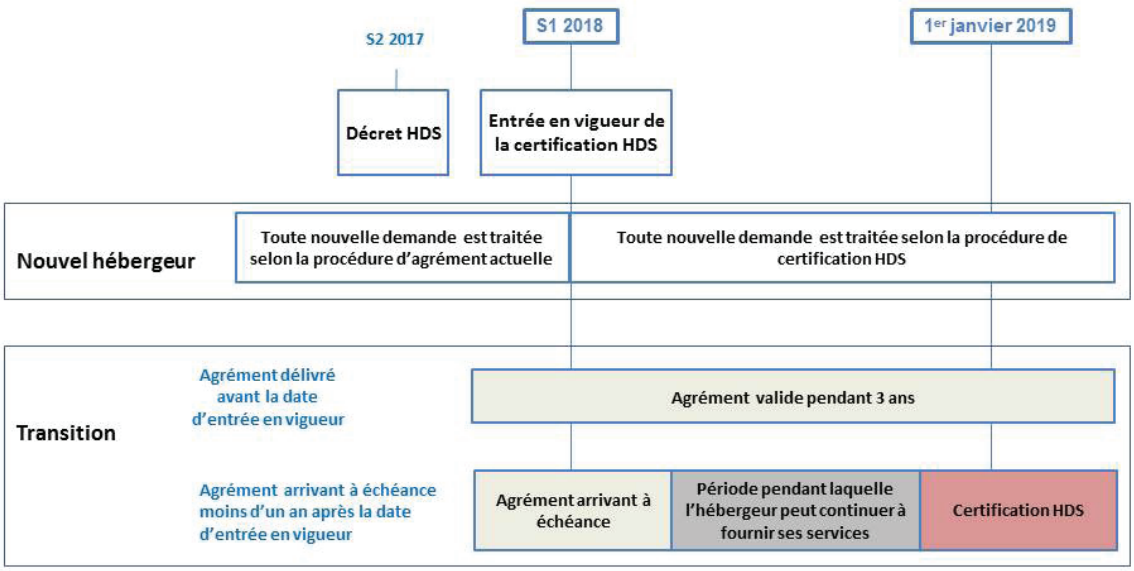
Point de situation (mai 2017)

Le référentiel de certification a été validé par le comité de pilotage. Il sera approuvé par arrêté du ministre chargé de la Santé. Dans l'attente de cette approbation une version provisoire sera publiée sur le site e.sante.gouv.fr en juin 2017.

Le décret qui doit définir la procédure de certification sera publié au JOFR au second semestre 2017. Il définira les modalités de mise en œuvre de la certification et de transition entre la procédure d'agrément et de certification :

- Les agréments délivrés avant l'entrée en vigueur de la procédure de certification produisent leur effet jusqu'à leur terme ;
- Les hébergeurs dont l'agrément arrive à échéance moins de 12 mois après la date d'entrée en vigueur de l'obligation de certification, disposeront d'un délai pour se mettre en conformité avec l'obligation de disposer d'un certificat de conformité technique ;
- Les demandes d'agrément et de renouvellement d'agrément déposées avant la date d'entrée en vigueur de l'obligation de certification sont instruites selon la procédure d'agrément pour l'hébergement de données de santé sur support électronique (décret 2006-6 précité).

Ce futur décret désignera l'ASIP Santé comme l'organisme chargé d'établir et de participer au développement de la procédure de certification.



ASIP Santé
9, rue Georges Pitard - 75015 Paris
T. +33 (0)1 58 45 32 50
Du lundi au vendredi de 8h30 à 18h30 *(hors jours fériés)*