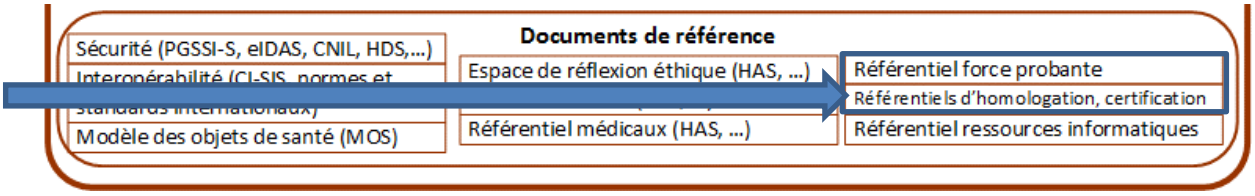
4.2. Sécurité : Certification hébergement des données de santé (HDS)



L'activité d'hébergement de données de santé consiste à **héberger les données de santé à caractère personnel pour le compte de personnes physiques ou morales qui sont à l'origine de la production ou du recueil de ces données** (article R1111-8-8 et R1111-9 du code de santé publique).

Les personnes physiques ou morales concernées par l'hébergement de données de santé sont donc d'une part, les patients qui confient l'hébergement de leurs données de santé à un tiers, et d'autre part **les responsables des traitements**[1] de données de santé à caractère personnel **ayant pour finalité la prévention, la prise en charge sanitaire (soins et diagnostic) ou la prise en charge sociale et médico-sociale de personnes.**

Au regard de la sensibilité particulière des données de santé**, il convient de s'assurer que l'hébergeur de ces données dispose des caractéristiques nécessaires et suffisantes pour en garantir la sécurité** et notamment la confidentialité. Le contrôle qu'il convient d'exercer à ce titre doit se situer pleinement dans l'esprit du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

DOCTRINE

❶ L'Etat encadre l'hébergement des données de santé à caractère personnel afin de garantir un niveau de sécurité homogène et suffisant pour leur conservation et leurs restitutions.

Cet encadrement consiste à s'assurer que :

- **Tout responsable de traitement garantit**, pour ses traitements de données de santé à caractère personnel, **un niveau de sécurité adapté**. Il met en œuvre pour cela des mesures techniques et organisationnelles appropriées afin d'être en mesure de démontrer que le traitement est effectué conformément au RGPD.
- **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, **est agréée ou certifiée** selon les procédures définies par décret :
  - L'hébergement de données de santé sur support papier, qui doit être réalisé par un hébergeur agréé par le ministre de la culture[2] ;

[1] Au sens de la loi n° 78-17 du 6 janvier 1978

[2] Décret 2011-246 du 4 mars 2011

- 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[3].

La procédure de certification, définie par le décret n° 2018-137 du 26 février 2018, permet aux prestataires répondant d'être titulaires d'un certificat de conformité, obligatoire à l'hébergement des données de santé sur support numérique.

Elle repose, à date, sur deux référentiels :

- Le **référentiel de certification**, fixant les conditions requises à l'obtention d'un certificat nécessaire à l'hébergement de données de santé. Deux types de certificats peuvent être délivrés (**certificat « hébergeur d'infrastructure physique » et certificat « hébergeur infogéreur »**),
- Le **référentiel d'accréditation**, fixant les conditions requises à l'obtention d'une accréditation nécessaire aux organismes certificateurs.

Pour ce qui concerne les établissements de santé (des champs sanitaire et médico-sociaux) **un palier de sécurité dit « hébergement de données de santé » est défini dans le cadre du dispositif de certification SI** (cf. paragraphe 4.3, ci-après) et doit être atteint selon un calendrier défini. L'établissement de santé peut garantir ce palier de sécurité en recourant à un hébergeur de données de santé agréé ou certifié ou en assurant lui-même la conformité requise.

❷ L'Etat engage une réflexion sur l'extension du dispositif encadrant l'hébergement des données de santé pour garantir la confiance sur l'ensemble de la chaîne de traitement

L'Etat mène, en concertation avec toutes les parties-prenantes, les extensions nécessaires à la procédure pour **sécuriser l'hébergement des données de santé sur l'ensemble de la chaîne de traitement**. Il s'agit notamment d'étendre le dispositif actuel aux secteurs social et médico-social.

La réflexion portera sur les modalités d'encadrement de l'hébergement des données de santé lorsqu'il est réalisé par les propres moyens des acteurs dont la mission réside dans la prise en charge des usagers ou dans leur suivi social et médico-social est étudiée. Ces derniers pourront démontrer le respect de cette obligation soit en recourant à un hébergeur certifié soit en mettant eux-mêmes en œuvre les moyens permettant de répondre aux exigences de sécurité portées par le dispositif étendu.

Autres sujets identifiés pour l'amélioration continue du dispositif de certification :

- Préciser **l'encadrement de « l'activité d'administration et d'exploitation des SI de santé »** telle qu'elle est actuellement définie dans le référentiel HDS. Ces travaux sont d'ores et déjà initiés.
- Prendre en compte la répartition des responsabilités à l'aune du RGPD (Règlement Général sur la Protection des Données) et la notion de responsabilité de traitement conjointe.

[3] Décret 2018-137 du 26 février 2018 (voir aussi : https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante)

- Préciser le champ d'application du dispositif en fonction des données de santé concernées (recherche, remboursement, mutuelles, réflexion sur l'origine des données de santé utilisées dans un contexte médical - par exemple données produites par un objet connecté).

❸ L'Etat fixe la gouvernance

La gouvernance HDS s'inscrit dans la gouvernance globale du numérique en santé qui sera définie début 2020.

SYNTHESE DES ACTIONS CLES

Le tableau ci-après présente une vue synthétique des actions et les échéances associées.

Action	Jalon
Préciser l'encadrement de « l'activité d'administration et d'exploitation des SI de santé» telle qu'elle est actuellement définie dans le référentiel HDS. Ces travaux sont d'ores et déjà initiés et devront aboutir pour décembre 2019.	GT : T4 2019 Mise en concertation publique : Janvier 2020
Prendre en compte les apports du Règlement Général sur la Protection des Données (RGPD), notamment la notion de responsabilité conjointe, les nouveaux droits des personnes, etc.)	GT à constituer dans le respect des règles du référentiel de gouvernance HDS Objectif – lancement des travaux : T12020
Détermination d'une trajectoire pour atteindre la cible d'amener les acteurs au niveau HDS (sous objectif Articulation entre procédure de certification labellisation SIH / sous-objectif par catégories d'acteurs)	A définir.
Préciser le champ d'application du dispositif en fonction des données de santé concernées (recherche, remboursement, mutuelles, réflexion sur l'origine des données de santé utilisées dans un contexte médical (par exemple données produites par un objet connecté)	GT à constituer dans le respect des règles du référentiel de gouvernance HDS Objectif – lancement des travaux : novembre 2019

POUR EN SAVOIR PLUS

Publication des référentiels sur le site esante.gouv.fr : https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante

- Référentiel de certification et référentiel d'accréditation :
- Procédure de certification opéré par un organisme certificateur accrédité par le COFRAC (Comité Français d'Accréditation) (ou équivalent au niveau européen).