Paris, le 11 juillet 2018

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DSSIS DÉLÉGATION À LA STRATÉGIE DES SYSTÈMES D'INFORMATION DE SANTÉ

MINISTÈRE DES SOLIDARITES ET DE LA SANTÉ

Explicitation du champ d'application du cadre juridique de l'hébergement de données de santé par le ministère chargé de la Santé, représenté par la Délégation à la stratégie des systèmes d'information de santé

Question 1 : Quel est l'objectif du régime juridique de l'hébergement de données de santé fixé à l'article L.1111-8 du code de la santé publique ?

L'article L.1111-8 du code de la santé publique[1] relatif à l'hébergement de données de santé a pour objectif d'organiser et d'encadrer la conservation et la restitution des données de santé à caractère personnel recueillies à l'occasion d'activité de prévention, de diagnostic, de soin ou de suivi social et médico-social, dans des conditions propres à garantir leur confidentialité et leur sécurité.

Par cet encadrement, le législateur souhaite garantir la confiance dans les tiers auxquels des structures et des professionnels des secteurs sanitaire, social et médico-social confient les données de santé qu'ils produisent ou recueillent, notamment en mesurant l'impact de l'activité du prestataire sur la protection des données, au travers des critères de sécurité à l'état de l'art « disponibilité, intégrité, confidentialité et auditabilité (DICA) » notamment visés par l'ANSSI et les normes ISO.

Cette confiance dans les tiers agissant pour le compte de ces acteurs sanitaires et sociaux et médico-sociaux est donnée au travers de l'obligation d'être agréés et/ou certifiés « HDS ».

Question 2 : Quel est le champ d'application de la législation sur l'hébergement de données de santé à caractère personnel ?

Le ministère chargé de la santé apporte les explications suivantes sur le champ d'application de l'hébergement de données de santé à caractère personnel

L'obligation de disposer d'un agrément ou d'un certificat de conformité mentionnée à l'article L.1111-8 du code de la santé publique s'applique à toute entité qui propose un service d'hébergement de données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, **pour le compte** du patient ou

[1] Article créé par la loi n° 2002-303 du 4 mars 2002 relative aux droits des patients et modifié en dernier lieu par l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel

pour le compte des professionnels de santé, des établissements et services de santé et tout autre organisme réalisant des missions de prévention, de soins, de suivi médico-social et social.

Par conséquent, les personnes physiques ou morales tenues de recourir à un hébergeur agréé ou certifié pour l'hébergement de données de santé sont d'une part, les patients qui confient l'hébergement de leurs données de santé à un tiers, et d'autre part les responsables de traitements 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.

A contrario, à titre d'exemple, sont exclues de l'obligation de recourir à un prestataire agréé ou certifié HDS : les organismes d'assurance maladie obligatoire et complémentaire dans le cadre de leur activité de prise en charge des frais de santé, les organismes de recherche dans le domaine de la santé, les fabricants/fournisseurs/distributeurs de dispositifs médicaux en dehors du cas où ils interviennent dans des activités de télésurveillance, les associations qui proposent des activités sportives à des personnes handicapées, etc.

Question 3 : Quelles sont les conditions à remplir pour héberger des données de santé à caractère personnel ?

L'article L.1111-8 du code de la santé en public distingue 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)[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 ;

- **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.**

L'hébergeur doit donc être titulaire de l'autorisation d'hébergement de données de santé correspondant au service qu'il propose.

NB : les agréments pour l'hébergement de données de santé sur support numérique délivrés conformément à l'ancienne procédure d'agrément restent valables pendant toute leur durée de validité (3 ans). Les dispositions du décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé restent applicables aux agréments en cours et aux demandes d'agrément en cours de traitement.

[2] Voir ci-dessous en bas de page la note sur les conditions d'agrément des hébergeurs de données de santé à caractère personnel sur support papier.

Question 4 : Quelles activités entrent dans l'exclusion prévue à l'article R.1111-8-8-I alinéa 4

Rappel - L'article R. 1111-8-8.-I. alinéa 4 dispose : « Toutefois, ne constitue pas une activité d'hébergement au sens de l'article L. 1111-8, le fait de se voir confier des données pour une courte période par les personnes physiques ou morales, à l'origine de la production ou du recueil de ces données, pour effectuer un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données. »

Cette exclusion doit être comprise comme couvrant uniquement les activités citées de manière explicite dans le décret. Elle s'ajoute aux activités ne constituant pas un traitement de données à caractère personnel décrites à l'article 4 de la loi Informatique et Libertés, c'est-à-dire aux « *copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises* ».