version du 2 avril 2019

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 ».

[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

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

Sur qui pèse l'obligation d'être certifié ?

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

- 1/portant sur des **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**.
- 2/**pour le compte** du patient ou **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 **à l'origine de ces données** .

Ces conditions sont cumulatives.

Il peut s'agir de toute personne (physique ou morale), qu'elle relève du droit public ou du droit privé. A cet égard, l'éventuelle situation de quasi régie définie à l'article 17 de l'ordonnance n°2015-899 du 23 juillet 2015 relative aux marchés publics avancée par certaines entités, qui permet aux acheteurs publics d'attribuer un marché public sans publicité ni mise en concurrence à un opérateur avec lequel il entretient des relations particulières, mais n'est pas de nature à remettre en cause l'analyse relative à l'application des textes sur l'hébergement de données de santé.

**Exemples :**

Tout professionnel manipulant des données de santé à caractère personnel telles que définies par l'article 4-15 du règlement européen relatif à la protection des données personnelles[2] n'est pas systématiquement tenu de faire application de la législation relative à l'hébergement.

Sont concernés tout professionnel de santé, tout établissement et service de santé et tout autre organisme réalisant des missions de prévention, de soins, de suivi médico-social et social ( personnes physiques ou morales) qui produisent les données susmentionnées dans le cadre de **leurs activités de prévention, de diagnostic, de soins ou de suivi social et médico-social**.

Toute personne relevant de l'une de ces catégories doit apprécier au cas par cas si ces données de santé dont il entend confier l'hébergement à un tiers proviennent de son activité **de prévention, de diagnostic, de soins ou de suivi social et médico-social**. La prévention inclut les actes réalisés par les services de santé au travail.

En outre, tout projet de système d'information (SI) portant sur l'exploitation des données susmentionnées nécessite de s'interroger au cas par cas sur l'application de la législation relative à

[2] 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)

l'hébergement des données de santé.  Le responsable du système d'information doit veiller à son respect dès que l'une des fonctionnalités du SI concerne même pour une partie seulement des données de santé répondant aux critères ci-dessus.

Par exemple, un établissement de santé exploitant à des fins de recherche une base de données de santé mise en œuvre dans le cadre de la prise en charge sanitaire des patients est tenu de recourir à un hébergeur certifié HDS en cas d'externalisation de l'hébergement de la dite base.

A contrario, sont exclus 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 ; ces organismes manipulent des données de santé mais ils n'en sont pas à l'origine ;

- les organismes de recherche dans le domaine de la santé lorsque leurs bases de données ne sont pas initialement constituées à des fins de prévention, de diagnostic, de soins ou de suivi social et médico-social ;

- les associations qui proposent des activités sportives à des personnes handicapées. Ces associations manipulent des données de santé mais elles n'en sont pas à l'origine.

## 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)[3] ;

- 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.

[3] 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* ».

**Question 5 : Quels sont les acteurs qui doivent être certifiés au titre de l'activité 5 (administration et exploitation du système d'information de santé) ?**

Cette activité, relative à l'application métier, a conduit de nombreux acteurs (éditeurs de logiciels, fabricants de dispositifs médicaux, etc.) à s'interroger sur la nécessité d'être certifiés. Conscient que cette activité est effectivement à la limite de ce qu'on qualifie normalement d'hébergement, mais que cette activité est néanmoins importante dans la chaîne de sécurité des données de santé à caractère personnel, le ministère chargé de la Santé va engager des travaux pour étudier l'opportunité et les modalités d'encadrement de l'activité d'administration et d'exploitation d'applications. Ces travaux pourront déboucher sur la mise en place d'un dispositif spécifique pour la gestion des applications. Une modification du décret HDS est en tout état de cause prévue pour retirer l' « activité 5 administration et exploitation».

La réflexion sera conduite dans une approche globale du sujet de sécurité et de qualité des applications, du point de vue de la confidentialité des données de santé à caractère personnel comme de celui du bon fonctionnement des applications.