[HDS] Sujet hébergement

L’obtention de la certification HDS est obligatoire pour les entreprises qui hébergent ou manipulent des **données de santé à caractère personnel**.

- **L'infogérant est certifié HDS**, cela signifie qu’il est responsable de l’hébergement et de la sécurité des infrastructures qui stockent les données de santé. Cela couvre les aspects techniques liés à l’hébergement, y compris la sécurité physique, la disponibilité et la confidentialité des infrastructures où sont stockées ces données.
- **L'éditeur de logiciel**: n’ayant pas accès à l’infrastructure elle-même, mais seulement à l’**interface d’administration** du logiciel (pas du serveur ou de l’infrastructure), se situe dans le domaine de la gestion logicielle ou applicative.

Le cadre légal impose la certification HDS à **toute entité qui héberge ou administre directement des données de santé**. Cependant, il est important de distinguer plusieurs niveaux :

1. **L'éditeur ayant accès uniquement à la partie logicielle (application)**, mais pas directement à l’administration du **système d’information** sous-jacent (serveurs, bases de données, réseau, etc.), **n’es pas techniquement considéré comme un "hébergeur"** au sens HDS. L'infogérant, qui gère l’infrastructure, reste celui qui porte cette responsabilité.
2. **Administration du logiciel** : Même si l'éditeur a accès à une interface d’administration applicative, cela ne signifie pas qu'il administres le SI hébergeant les données de santé. Son rôle semble plus s'apparenter à un **traitement des données** plutôt qu’à une administration du système d'information.
3. **L'éditeur manipulant des données,** étant amené à **traiter des données de santé**, même indirectement via l’administration du logiciel, pourrait être considéré comme **sous-traitant** (au sens RGPD). En tant que sous-traitant de données de santé, il doit s’assurer que les accès et le traitement des données sont effectués conformément aux règles RGPD et HDS. Cependant, la certification HDS n’est pas directement requise, sauf si il accèdes ou gères l’infrastructure de manière directe, ce qui n'est pas le cas dans notre cas

N'ayant aucun **rôle direct dans la gestion ou l'administration de l’infrastructure hébergeant les données de santé**, c'est-à-dire responsable de la sécurité, de la maintenance ou de la gestion technique des serveurs, même ayant un rôle dans l'administration applicative alors la certification HDS n'est pas nécessaire.

Notre infogérant étant dument certifié et nous ayant fourni les preuves nécessaires, nous n'avons pas besoin nous même d'être certifié

Quelques informations Complémentaire

https://esante.gouv.fr/produits-services/hds

Quelles utilisations ?
« 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.1111-8 du code de la santé publique, modifié par la loi n° 2016-41 du 26 janvier 2016
Tous les organismes publics ou privés qui hébergent, exploitent le SI de santé, ou réalisent des sauvegardes pour le compte d'un établissement de santé ou d'un tiers de santé doivent être certifiés HDS. à l'exception des services d'archivages informatiques qui ne sont pas concernés par ces obligations. Les établissements de santé qui gèrent leur propre Système d'Information de santé n'ont pas la nécessité d'être certifié HDS.

Le référentiel d'exigences s'applique aux Hébergeurs de données de santé à caractère personnel visés à l'article L.1111-8 du code de la santé publique.

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049571347

Article L1111-8
Version en vigueur depuis le 23 mai 2024

Modifié par LOI n°2024-449 du 21 mai 2024 - art. 32 (V)
I.-Toute personne 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 et 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, réalise cet hébergement dans les conditions prévues au présent article.
L'hébergement, quel qu'en soit le support, papier ou numérique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime.
La prestation d'hébergement de données de santé à caractère personnel fait l'objet d'un contrat.
II.-L'hébergeur de données mentionnées au premier alinéa du I sur support numérique est titulaire d'un certificat de conformité.
Ce certificat est délivré par des organismes de certification accrédités par l'instance française d'accréditation ou l'instance nationale d'accréditation d'un autre Etat membre de l'Union européenne mentionnée à l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie.
Les conditions de délivrance de ce certificat sont fixées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé.

III.-L'hébergeur de données mentionnées au premier alinéa du I est agréé par le ministre chargé de la culture pour la conservation de ces données sur support papier ou sur support numérique dans le cadre d'un service d'archivage électronique.
Les conditions d'agrément sont fixées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé.

L'agrément peut être retiré, dans les conditions prévues par les articles L. 121-1, L. 121-2 et L. 122-1 du code des relations entre le public et l'administration, en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.
IV.-La nature des prestations d'hébergement mentionnées aux II et III du présent article, les rôles et les responsabilités de l'hébergeur et des personnes physiques ou morales pour le compte desquelles les données de santé à caractère personnel sont conservées, les obligations de l'hébergeur en matière de stockage de ces données sur le territoire d'un Etat membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen ainsi que les stipulations devant figurer dans le contrat mentionné au I, y compris concernant les mesures prises face aux risques de transfert de ces données ou d'accès non autorisé à celles-ci par des Etats tiers à l'Union européenne ou à l'Espace économique européen, sont précisés par un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux des ordres des professions de santé.
V.-L'accès aux données ayant fait l'objet d'un hébergement s'effectue selon les modalités fixées dans le contrat dans le respect des articles L. 1110-4 et L. 1111-7.
Les hébergeurs ne peuvent utiliser les données qui leur sont confiées à d'autres fins que l'exécution de la prestation d'hébergement. Lorsqu'il est mis fin à l'hébergement, l'hébergeur restitue les données aux personnes qui les lui ont confiées, sans en garder de copie. Les hébergeurs de données de santé à caractère personnel et les personnes placées sous leur autorité qui ont accès aux données déposées sont astreints au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal.
VI.-Les hébergeurs de données de santé à caractère personnel ou qui proposent cette prestation d'hébergement sont soumis, dans les conditions prévues aux articles L. 1421-2 et L. 1421-3, au contrôle de l'inspection générale des affaires sociales et des agents mentionnés aux articles L. 1421-1 et L. 1435-7, à l'exception des hébergeurs certifiés dans les conditions définies au II. Les agents chargés du contrôle peuvent être assistés par des experts désignés par le ministre chargé de la santé.
VII.-Tout acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du code pénal.

Administration et exploitation du système d’information contenant les données de santé

L’activité d’administration et exploitation du système d’information contenant les données de santé consiste en la maitrise des interventions sur les ressources mises à la disposition du client de l’Hébergeur. Elle comprend l’intégralité des activités annexes suivantes :
- La définition d’un processus d’attribution et de revue annuelle de droits d’accès nominatifs,

justifiés et nécessaires ;
- La sécurisation de la procédure d’accès ;
- La collecte et la conservation des traces des accès effectués et de leurs motifs ;
- La validation préalable des interventions (plan d’intervention, processus d’intervention).

La validation des interventions consiste à s’assurer qu’elles ne dégradent pas la sécurité de l’information hébergée ni pour le client concerné ni pour les autres clients de l’Hébergeur. Cette validation peut être effectuée dans les cas suivants :
- A priori, pour les interventions que le client pourrait effectuer en autonomie ;
- Lors de la demande d’intervention lorsqu’il sollicite l’Hébergeur.

La définition du processus d’attribution, la sécurisation, la collecte, la validation sont intrinsèques et obligatoires aux activités définies au 1 à 4 de l’article R. 1111-9 du code de la santé publique. Si elles sont effectuées uniquement en ce qu’elles sont liées et consubstantielle aux activités 1 à 4, l’Hébergeur n’est pas tenu d’être certifié pour l’activité 5. Il ne sera tenu de l’être que dans le cas où il exerce uniquement l’activité 5.

Révision #6
Créé 27 septembre 2024 08:55:19 par Thibaut
Mis à jour 27 septembre 2024 13:29:43 par Thibaut