L'ECLAIRAGE DU MARDI

par

COMETH CO CONSULTING

Certification HDS (Hébergement Données Santé) — Mardi 9 février 2021

La certification relative à l'Hébergement de Données Santé, dite HDS, est l'obligation d'avoir une évaluation de conformité par un organisme certificateur pour, d'après l'article L. 1111-8 du code de la santé publique, *« 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 »*. Au 1er février 2021, 135 hébergeurs sont certifiés.

A noter : les organismes d'assurance maladie obligatoire et complémentaire, dans le cadre de leur activité de prise en charge des frais de santé, sont exclus de l'obligation de recourir à un prestataire certifié HDS (ils manipulent des données de santé mais ils n'en sont pas à l'origine).

Pourquoi une certification ?

Depuis le 1er avril 2018, l'agrément Hébergeur de données de santé délivré par l'ASIP Santé (Agence des Systèmes d'Information Partagés de santé) a été remplacé par une **obligation règlementaire[1] d'obtenir une certification HDS**, par un organisme certificateur indépendant. Les agréments pour l'hébergement de données sur support numérique délivrés avant le 31 mars 2018 ou à la suite de demandes déposées avant cette date, restent valables jusqu'à leur terme.

En fonction de l'activité de l'hébergeur, **deux types de certificats sont possibles : « Hébergeur d'infrastructure physique » et « Hébergeur Infogéreur ».**

- La certification hébergeurs d'infrastructures physiques couvre notamment :
  - La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
  - La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.

[1] Cette obligation est encadrée par les textes suivants :

- L'ordonnance du 12 janvier 2017, prise en application de la loi de modernisation du système de santé du 26 janvier 2016,
- Le décret 2018-137 du 26 février 2018 qui définit la procédure de certification,
- L'arrêté du 29 juin 2018 portant approbation des référentiels d'accréditation et de certification qui permettent l'ouverture du schéma d'accréditation HDS,
- Explicitation du 16 mai 2019 par le ministère chargé de la Santé sur le champ d'application du cadre juridique de l'hébergement de données de santé.

- La certification hébergeurs infogéreurs couvre notamment :
    - La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
    - La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information.

Si l'hébergeur s'inscrit dans les deux types d'activité, l'hébergeur doit obtenir les deux certifications.

Quelle est la procédure de certification à suivre ?

Le **référentiel de certification** HDS est disponible sur le site de l'ASIP. Il **repose sur des normes internationales certifiantes ainsi que sur des exigences complémentaires** :

Normes internationales	Prise en compte HDS	Exigences complémentaires HDS
NF ISO/CEI 27001 : 2013 Exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information.	100% de la norme	Des exigences complémentaires notamment sur : • Rôles et responsabilités • Conformité aux référentiels opposables de la PGSSI-S • Rapports d'audit • Liste des contacts clients • Régionalisation
NF ISO/CEI 20000-1 : 2012 Exigences destinées à établir, implémenter, maintenir et améliorer continuellement un système de management des services (SMS).	2 chapitres relatifs à la continuité de service et à la capacité	
NF ISO/CEI 27018:2014 Contrôles et orientations relatifs à la protection des données à caractère personnel dans l'informatique en nuages.	25 exigences (environ 80% de la norme)	

La procédure de certification repose sur une évaluation de conformité au référentiel de certification.

L'hébergeur choisit un **organisme certificateur qui doit être accrédité** par le COFRAC (Comité Français d'Accréditation) ou équivalent au niveau européen.

L'organisme procède alors à un **audit en deux étapes** pour évaluer la conformité de l'hébergeur aux exigences du référentiel de certification :

- 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.

L'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles non-conformités et faire auditer ses corrections. Passé ce délai et sans action de l'hébergeur, toute la procédure d'audit sur site sera de nouveau réalisée. Le **certificat est délivré pour une durée de trois ans**, par l'organisme certificateur **et chaque année, un audit de surveillance** est effectué.

Quels sont les risques d'une absence de certification ?

Il n'existe pas de sanction spécifique pour les personnes confiant des données de santé à caractère personnel à un tiers non agréé. Cela constituerait en revanche :

- Une violation des obligations de sécurité imposées par l'article 34 de la loi Informatique et libertés à tout responsable de traitement, sanctionnée par 5 ans d'emprisonnement et 500.000 € d'amende ou 2.500.000 € pour les personnes morales.
- Une violation du secret professionnel punie d'un an d'emprisonnement et 15.000 € d'amende ou 75.000 € pour les personnes morales.

Rendez-vous prochainement pour un nouvel éclairage…
et n'hésitez pas à nous contacter pour vos besoins d'accompagnement.

COMETH Consulting – 17 rue Charles Laffitte 92200 Neuilly sur Seine
www.cometh-consulting.com / contact@cometh-consulting.com / Tél : 01 40 54 83 81