Réforme de l'accréditation et de la certification pour l'hébergement des données de santé Commentaire: Arrêté du 26 avril 2024 modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel

Margo Bernelin

▶ **To cite this version:**

Margo Bernelin. Réforme de l'accréditation et de la certification pour l'hébergement des données de santé Commentaire: Arrêté du 26 avril 2024 modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel. 2024. hal-04859278

HAL Id: hal-04859278
https://hal.science/hal-04859278v1

Preprint submitted on 30 Dec 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - ShareAlike 4.0 International License

Réforme de l'accréditation et de la certification pour l'hébergement des données de santé

Commentaire: Arrêté du 26 avril 2024 modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel

Auteur : Margo BERNELIN

Le dernier régime relatif à la certification des hébergeurs de données de santé avait été adopté en 2018. Ces hébergeurs ont une tâche clef : stocker des données personnelles sensibles, les données de santé, pour le compte d'un tiers. Mais en six ans, les enjeux techniques et juridiques ont évolué conduisant, en 2024, à réformer les référentiels relatifs à l'accréditation des organismes de certification des hébergeurs de données de santé mais aussi celui relatif à la certification de ces hébergeurs.

Le référentiel d'accréditation HDS

Le premier référentiel pose les règles applicables aux organismes auditant et certifiant les hébergeurs de données de santé. Ces organismes doivent en effet être accrédités pour pouvoir certifier les hébergeurs. À cet égard, Le document rappelle en tout premier lieu les règles dédiées et en particulier liste les normes ISO de référence avant même de rappeler le cadre fixé par le code de la santé publique.

Les organismes en cause sont accrédités en France par le COFRAC, lequel devra suivre la procédure détaillée dans ce nouveau référentiel. Les exigences posées tiennent à la compétence technique du personnel des organismes sollicitant l'accréditation ou son renouvellement, à la confidentialité s'imposant à eux si l'audit impose l'accès à des données de santé (conclusion d'un accord de confidentialité) mais aussi à leur obligation de communiquer avec l'autorité compétente toute suspension ou retrait d'une certification HDS et détaille les procédures en cause.

Le référentiel de certification HDS

Le référentiel de sécurité relatif à la certification des hébergeurs de données de santé est celui retient le plus l'attention. En effet, outre le fait qu'il met à jour le précédent référentiel quant aux normes applicables en matière de sécurité de l'information (exigences par exemple quant à la gestion des risques), qu'il vient détailler les clauses contractuelles encadrant la relation entre l'hébergeur et ses clients (sur le traitement des incidents, le

recours à la sous-traitance, l'accès aux données entre autres, la transparence sur le stockage des données), il revient sur la question épineuse des transferts et de l'accès aux données hors UE.

Le document rappelle ainsi les conditions d'attributions élémentaires de la certification d'un hébergeur à savoir notamment la mise en œuvre d'un « Système de Management de la Sécurité de l'Information (SMSI) certifié selon la norme ISO 27001 », la conclusion de contrats entre l'hébergeur et ses clients respectant les exigences du référentiel et le respect des « exigences relatives à la souveraineté ». Ces dernières sont définies par le chapitre 7 du référentiel et visent à ne pas interdire tout recourt vers un prestataire américain, nationalité largement représentée lorsqu'il s'agit de numérique en santé.

Ce chapitre 7 et son exigence 28 précisent que les données de santé doivent être exclusivement stockées « au sein de l'Espace Économique Européen (EEE) » et que l'hébergeur doit communiquer à ses clients la localisation du stockage. Si le stockage ou la nationalité de l'hébergeur implique un accès distant aux données depuis/par un État tiers de l'EEE alors l'hébergeur doit se fonder soit sur une décision d'adéquation (comme le *Privacy Framework* pour les États -Unis) soit sur une des garanties de l'article 46 du RGPD afin de protéger les données. L'hébergeur doit également informer ses clients sur ce point et notamment sur les garanties mises en place pour garantir la protection des données.

Si l'hébergeur, ou un de ses sous-traitants est « soumis à la législation d'un pays tiers n'assurant pas un niveau de protection adéquat » alors il doit en informer ses clients et nommer la législation en cause, les risques d'accès non autorisés aux données et les mesures prises pour les limiter. Ainsi, le référentiel n'impose donc pas la qualification SecNumCloud qui interdit tout accès non autorisé par un état tiers aux données mais organise en pratique le recours à des prestataires hors EEE en misant sur la transparence à ce sujet.

Entrée en vigueur

L'article 3 de l'arrêté précise que les référentiels entreront en vigueur six mois à compter de la publication de ce dernier, soit en novembre prochain pour les demandes de certification ou leur renouvellement. Cela va donc imposer un travail important pour les candidats au renouvellement qui devront se saisir de ces nouveaux référentiels. Ainsi, avec le jeu des renouvellements de certification, au plus tard en mai 2026, tous les hébergeurs de données de santé devront satisfaire ce nouveau référentiel (Communiqué de Presse, Ministère du travail, de la santé et des solidarités, 16 mai 2024).