Supplément au règlement de certification systèmes de management

Hébergeurs de données de santé à caractère personnel sur support numérique

Réf : Q004-1 Version : 2.1_HDSV2 Nombre de pages : 5

Nom du fichier : Q004-1_V2.1_HDSV2_27001_2022.docx

apave LSTI

Sommaire

Suivi des modifications

Date	Version	Rédigé par	Origine de l'évolution et validation
20/04/2018	V1.0	Armelle Trotin	Création du document
19/09/19	V1.1	Eva Tourneur	Ajout des 6 activités au sens du §2 du référentiel d'accréditation. Ajout des obligations si des données de santé à caractère personnel sont accessibles lors de l'audit
17/09/20	V1.2	Eva Tourneur	Correction orthographique
30/07/21	V1.3	Eva Tourneur	Ajout des critères de détermination du temps d'audit
08/02/22	V1.4	Manon Mix	Mise à jour graphique
27/04/23	V1.5	LG	Changement des références normatives ISO/IEC 27001
28/08/24	V2.0	LG	Mise à jour application référentiels HDS V2.0
14/01/25	V2.1	Manon Mix	Mise à jour graphique

1. Objet du document

Ce document décrit les conditions particulières d'évaluation et de certification des hébergeurs de données de santé (HDS). Il supplémente les conditions générales décrites dans le règlement de certification Q004 « règlement de certification système » qui s'appliquent intégralement pour la certification HDS.

Références :

- Articles L. 1111-8 du code de la santé publique relatif à l'hébergement de données de santé
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27/04/2016 (« règlement général sur la protection des données")
- Article R. 1111-8-8 du code de la santé publique relatif à l'activité d'hébergement de données de santé
- Articles R1111-9 à R-1111-11 du code de la santé publique relatifs à l'hébergement des données de santé à caractère personnel sur support numérique soumis à certification.
- Article 2 de l'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
- ISO/IEC 17021-1 « Évaluation de la conformité –Exigences pour les organismes procédant à l'audit et à la certification de systèmes de management – partie 1 exigences »
- ISO/IEC 27001 – Sécurité de l'information, cybersécurité et protection de la vie privée-Systèmes de management de la sécurité de l'information -- Exigences
- Référentiel d'accréditation HDSv2
- Référentiel de certification HDSv2 – Exigences et contrôles

2. Champ d'application

Ce document décrit les exigences qu'un Hébergeur doit satisfaire pour obtenir la certification d'Hébergeur de données de santés. Il s'applique aux Hébergeurs de données de santé à caractère personnel visés à l'article L.1111-8 du code de la santé publique.

La certification HDS s'applique à toute personne physique ou morale qui fournit tout ou partie d'un service d'hébergement de données de santé à caractère personnel et qui a la qualité de sous-traitant au sens de l'article 28 du RGPD.

La certification est délivrée pour six types de portées :

- 1° La mise à disposition et le maintien en condition opérationnelle de sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
- 2° 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 ;
- 3° 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 ;
- 4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
- 5° L'administration et l'exploitation du système d'information contenant les données de santé ;
- 6° La sauvegarde des données de santé.

Un prestataire peut demander à être certifié pour l'une ou toutes les portées.

3. Procédure de certification

3.1. Cas des hébergeurs non certifies iso 27001

Le processus de certification est décrit dans le document Q004. Le référentiel d'évaluation est le référentiel de certification HDS v2 – exigences et contrôles.

3.2. Cas des hébergeurs certifies iso 27001

Dans le cas où l'hébergeur dispose d'une certification de conformité, délivrée par LSTI, à la norme ISO 27001, valide et dont le périmètre inclut celui pour lequel l'hébergeur demande la certification HDS, celui-ci peut demander un audit d'extension pour laquelle seules les exigences spécifiques du référentiel HDS font l'objet d'une évaluation.

3.3. Critères de détermination du temps d'audit

La détermination du temps d'audit d'une certification HDS repose sur le nombre réel d'employés impliqués dans le service d'hébergement de données de santé (Cf. Annexe A du référentiel d'accréditation HDS v2). Le temps d'audit peut ensuite être ajusté en fonction des facteurs suivant :

- La complexité du SMSI
- Le type de business
- La performance démontrée du SMSI
- La diversité de la technologie utilisée
- La sous-traitance
- Le nombre de sites

3.4. Documents de certification

L'octroi de la certification se traduit par l'émission d'un certificat qui précise la portée de la certification et par la remise d'un programme d'audit qui spécifie la planification des différentes activités de surveillance et les audits de renouvellement.

3.5. Durée et validité du certificat

La durée de validité de la certification est de trois ans à compter de la décision d'octroi. Dans le cas d'une « extension » à une certification ISO 27001 existante, la validité de la certification HDS est celle de la certification ISO 27001.

Le programme d'audit ISO 27001 sur un cycle reste inchangé.

4. Confidentialité

Avant toute intervention de la part de l'équipe d'audit, il convient au prestataire de confirmer à LSTI que les informations qui seront communiquées lors de l'audit ne contiennent aucune donnée de santé à caractère personnel, ni aucune donnée confidentielle ou sensible. Le cas échéant, l'organisme de certification et le candidat doivent définir les modalités d'accès au système devant être audité (engagement de confidentialité, etc.).

Dans le cas d'une incapacité à auditer le système d'information sans accéder à des données de santé à caractère personnel, LSTI confirme que tous auditeurs agissant sous sa responsabilité ont signé une clause de confidentialité leur interdisant de divulguer ou d'utiliser ces données de santé.

L'audité devra informer de tout accès à des données de santé à caractère personnel un professionnel de santé sous sa responsabilité.

Les données de santé à caractère personnel et toutes autres données confidentielles ou sensibles auxquelles l'organisme de certification aurait accès dans le cadre de l'audit ne peuvent être divulguées ou réutilisées par l'organisme de certification, ni par le candidat à la certification.