SUPPLEMENT AU REGLEMENT DE CERTIFICATION SYSTEMES DE MANAGEMENT

Hébergeurs de données de santé à caractère personnel sur support numérique

Ordonnance N° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel

LSTI SAS - 10, avenue Anita Conti - 35400 Saint-Malo - France
RCS 453 867 863 Saint-Malo - SAS au capital de 1 200 000 €
www.lsti-certification.fr

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 determination 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

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 :

Ordonnance N° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel
Décret N° 2018-137 du 26 févier 2018 relatif à l'hébergement de données de santé à caractère personnel
ISO/IEC 17021-1 « Evaluation de la conformité –Exigences pour les organismes procédant à l'audit et à la certification de systèmes de management – partie 1 exigences »
ISO/IEC 27006 - Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27001 – Sécurité de l'information, cybersécurité et protection de la vie privée- Systèmes de management de la sécurité de l'information -- Exigences
ISO/IEC 27018 Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
ISO/IEC 27017 Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage
ISO/IEC 20000-1 Partie 1 Exigences du système de management des services
Référentiel d'accréditation HDS
Référentiel de certification HDS – Exigences et contrôles

2 CHAMP D'APPLICATION

La certification HDS est délivrée dans le cadre de l'article 1er alinéa II de l'ordonnance N° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel.

La certification est délivrée pour deux types de portées :

- Hébergeur d'infrastructure physique
- Hébergeur infogéreur

Un prestataire peut demander à être certifié pour l'une ou l'autre de ces portées ou pour les deux portées.

Un hébergeur d'infrastructure physique peut exercer les activités suivantes :

1. 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
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

Un hébergeur infogéreur peut exercer les activités suivantes :

3. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information

4. 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
5. L'administration et l'exploitation du système d'information contenant des données de santé
6. La sauvegarde des données de santé

3 PROCEDURE DE CERTIFICATION

3.1 CAS DES HEBERGEURS NON CERTIFIES ISO 27001

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

3.2 CAS DES HEBERGEURS 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 CRITERES DE DETERMINATION 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 en vigueur). 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 DUREE ET VALIDITE 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 CONFIDENTIALITE :

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.
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. Il devra également s'assurer que tous les accès éventuels à des données de santé à caractère personnel par l'auditeur seront être tracés nominativement et horodatés.