RÉPUBLIQUE FRANÇAISE

Ministère de la santé et de la prévention

Arrêté du XXX 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

NOR : SPRD2325104A

Le ministre de la santé et de la prévention, et le ministre de l'économie et des finances,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, et notamment la notification n° XX en date du XX ;

Vu le code de la santé publique, notamment ses articles L. 1111-8 et R. 1111-10 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu 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 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 13 juillet 2023,

Vu la notification n°…/…/F adressée le … à la Commission européenne,

Arrêtent :

Article 1er

Les articles 1 et 2 de l'arrêté du 11 juin 2018 susvisé sont remplacés par des articles ainsi rédigés :

« *Art. 1.* - Le référentiel relatif à l'accréditation des organismes de certification pour l'hébergement de données de santé à caractère personnel mentionné à l'article R. 1111-10 du code de la santé publique dans sa version modifiée, annexé au présent arrêté, est approuvé.

« *Art. 2.* - Le référentiel relatif à la certification pour l'hébergement de données de santé à caractère personnel mentionné à l'article R. 1111-10 du code de la santé publique dans sa version modifiée, annexé au présent arrêté, est approuvé. »

Article 2

Les dispositions de l'article 2 de l'arrêté du 11 juin 2018 susvisé, dans leur rédaction résultant du présent arrêté, entrent en vigueur dans un délai de six mois à compter de sa publication. Elles sont applicables aux demandes de certificat de conformité et aux demandes de renouvellement d'un tel certificat présentées à un organisme de certification à compter de cette date.

Article 3

Le ministre de la santé et de la prévention et le ministre de l'économie sont chargés, chacun en ce qui les concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait le XXX.

Pour le ministre de la santé et de la prévention et par délégation :

Hela Ghariani

Déléguée au numérique en santé

Pour le ministre de l'économie et des finances et par délégation :

Thomas Courbe

Directeur général des entreprises

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Référentiel de certification Hébergeur de données de santé (HDS)

Exigences

Agence du Numérique en Santé
2 - 10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Documents de référence

Réglementation

Renvoi	Document
[ART_L1111-8]	Articles L. 1111-8 du code de la santé publique relatif à l'hébergement de données de santé https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27/04/2016 (« règlement général sur la protection des données ») https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
[ART R1111-8-8]	Article R. 1111-8-8 du code de la santé publique relatif à l'activité d'hébergement de données de santé https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036656709
[ART R1111-9] à [ART R1111-11]	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. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006196138/#LEGISCTA000036658495

Autres documents

Renvoi	Document
[ISO 27001]	NF ISO/IEC 27001:2023 Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Historique des modifications

Version	Date	Commentaire
V1.1	Juin 2018	Version publiée de 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
V1.1.20230330	Mars 2023	Projet de révision dont les modifications principales sont : ► La définition du champ d'application de l'activité 5 « administration et exploitation du système d'information contenant les données de santé. ► La prise en compte de la version de la norme NF ISO/IEC 27001 : 2023. ► Le rappel des exigences contractuelles mentionnées à l'article R.1111-11 du code de la santé publique. ► La standardisation de la présentation des garanties. ► Le renforcement des exigences relatives au transfert de données hors

		Union européenne.

SOMMAIRE

1. PRÉAMBULE

La présente mise à jour du référentiel de certification pour les Hébergeurs de données de santé vise à tenir compte de nouveaux enjeux et de points d'améliorations du précédent référentiel datant de 2018, identifiés en concertation avec l'écosystème. Cette mise à jour consiste notamment à :

Améliorer la lisibilité des garanties apportées par un Hébergeur certifié sur les prestations qu'il réalise pour un client donné ;
Clarifier les obligations contractuelles de l'Hébergeur définies dans le code de la santé publique ;
Renforcer les exigences de protection des données personnelles au regard des transferts de données hors de l'Union européenne. Sur ce dernier point, il s'agit d'une première étape : des exigences renforcées en termes de souveraineté européenne seront ajoutées au plus tard en 2027, en cohérence avec les futurs référentiels européens (EUCS – European Cybersecurity Certification Scheme for Cloud services).

Dans le cas où l'Hébergeur candidat à la certification HDS a déjà obtenu une certification sur la base du référentiel SecNumCloud 3.2 de l'ANSSI, une matrice de correspondance entre les mesures de l'annexe A de la norme ISO 27001 et les exigences SecNumCloud est mise à disposition des Hébergeurs en annexe 1 du présent référentiel afin de faciliter la candidature d'un Hébergeur qualifié SecNumCloud à la certification HDS.

1.1. Objet du référentiel

Pris en application de l'article R1111-10 du code de la santé publique, le référentiel de certification HDS (ci-après dénommé « référentiel d'exigences » ou « référentiel ») définit les exigences qu'un Hébergeur doit satisfaire pour obtenir la certification d'Hébergeur de données de santé.

1.2. Périmètre d'application du référentiel

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.

2. DEFINITIONS ET CONCEPTS GENERAUX

2.1.1. Acteur

Tout intervenant contribuant à la sécurité des données de santé à caractère personnel, à l'exclusion du responsable de traitement et des sous-traitants d'un Hébergeur certifié lorsqu'ils agissent conformément à la politique de sécurité et sous la surveillance dudit Hébergeur.

2.1.2. 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.

2.1.3. Client de l'Hébergeur

Le client de l'Hébergeur (également dénommé « client ») désigne la personne physique ou morale souscrivant au service mis en œuvre par l'Hébergeur.

2.1.4. Hébergeur

L'Hébergeur, également désigné organisation dans la norme ISO 27001, est le candidat à la certification des Hébergeurs de données de santé ou au renouvellement de sa certification. Il fournit tout ou partie d'un service d'hébergement de données de santé à caractère personnel (ou « données de santé ») au sens de l'article L. 1111-8 du code de la santé publique.

2.1.5. Moyen d'identification électronique

Un moyen d'identification électronique est un élément matériel ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier à un service en ligne.

2.1.6. Responsable de traitement

Cette notion désigne le responsable de traitement au sens du règlement n° 2016/679, soit la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

2.2. Abréviations et acronymes

Acronyme	
CSP	Code de la santé publique
DSCP	Données de Santé à Caractère Personnel
HDS	Hébergeur de Données de Santé
RGPD	Règlement Général sur la Protection des Données
SMSI	Système de Management de la Sécurité de l'Information

3. CHAMP D'APPLICATION

3.1. Applicabilité du référentiel de certification HDS

Le champ d'application du référentiel est défini par les articles L. 1111-8, R. 1111-8-8 et R. 1111-9 du code de la santé publique.

3.1.1. Rôle d'Hébergeur

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.

3.1.2. Nature des données

Les données hébergées doivent être des données à caractère personnel concernant la santé, telles que définies à l'article 4.15 du RGPD.

3.1.3. Contexte du recueil

Sont concernées par la certification HDS les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social.

Ces données de santé à caractère personnel doivent être hébergées pour le compte des personnes physiques ou morales à l'origine de la production ou du recueil des données ou pour le compte du patient lui-même.

3.1.4. Activités réalisées

L'article R. 1111-9 du CSP définit l'activité d'hébergement de données de santé :

Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L. 1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R. 1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes :

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.

L'activité 5 est précisée au paragraphe 2.1.2.

L'activité 6 de sauvegarde des données doit être interprétée comme comprenant uniquement les sauvegardes externalisées. Les sauvegardes intrinsèquement nécessaires aux activités 1 à 5 sont dans le périmètre des activités 1 à 5.

4. CONDITIONS D'ATTRIBUTION D'UN CERTIFICAT

Exigence n° 01

[EXI 01] La certification d'un Hébergeur nécessite :

Qu'il ait mis en œuvre un Système de Management de la Sécurité de l'Information (SMSI) certifié selon la norme ISO 27001, complétée des exigences définies au chapitre 5. ;
Que le domaine d'application de ce SMSI couvre l'ensemble des activités d'hébergement de données de santé de l'Hébergeur ;
Que les contrats conclus avec ses clients répondent aux exigences définies au chapitre 6. ;
Qu'il respecte les exigences relatives à la souveraineté définies au chapitre 7 ;
Qu'il communique à ses clients la présentation des garanties formalisée conformément au chapitre .

5. EXIGENCES RELATIVES AU SMSI

La numérotation de ce chapitre est alignée sur celle de la norme ISO 27001 et commence au point 5.4, correspondant au chapitre 4 de la norme.

5.1. Contexte de l'organisation

5.1.1. Compréhension de l'organisation et de son contexte

Les exigences énoncées au chapitre 4.1 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 02
[EXI 02] Dans la détermination de ses enjeux externes et internes, l'Hébergeur doit prendre en compte le fait que sa mission lui impose la protection des DSCP qui lui sont confiées par ses clients

5.1.2. Compréhension des besoins et des attentes des parties intéressées

Les exigences énoncées au chapitre 4.2 de l'ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 03
[EXI 03] Dans la détermination des exigences des parties intéressées, l'Hébergeur doit prendre en compte le cadre juridique applicable en matière de protection des DSCP.

5.1.3. Détermination du domaine d'application du SMSI

Les exigences énoncées au chapitre 4.3 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 04
[EXI 04] Le domaine d'application du SMSI doit comprendre l'ensemble des traitements de DSCP assurés par l'Hébergeur. Il doit couvrir tous les moyens et processus de traitement des DSCP, notamment les sauvegardes et les transferts de supports matériels de l'information.

5.1.4. Système de management de la sécurité de l'information

Les exigences énoncées au paragraphe 4.4 de la norme ISO 27001 s'appliquent.

5.2. Gouvernance

Les exigences énoncées au chapitre 5 de la norme ISO 27001 s'appliquent.

5.3. Planification

5.3.1. Actions à mettre en œuvre face aux risques et opportunités

5.3.1.1. Généralités

Les exigences énoncées au chapitre 6.1.1 de la norme ISO 27001 s'appliquent.

5.3.1.2. Appréciation des risques

Les exigences énoncées au chapitre 6.1.2 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 05

[EXI 05] Lors de l'appréciation des risques, l'Hébergeur doit a minima envisager les événements suivants :

A. Défaillance des supports matériels de l'information due à des menaces physiques et environnementales.
B. Perte de contrôle de supports matériels de l'information, notamment à l'occasion :
    a. De copie des DSCP sur des supports portables ;
    b. De matérialisation éventuelle sous format documents papier ;
    c. De réallocation des espaces de stockage.
C. Dégradation, compromission ou rupture d'un flux d'information interne ou externe sous la responsabilité de l'Hébergeur.
D. Défaillance de la maîtrise des accès attribués, que ce soit aux personnels sous le contrôle de l'organisation ou à ceux désignés par ses clients :
    a. Attribution, modification et retrait des droits d'accès ;
    b. Distribution des moyens d'identification électroniques ;
    c. Traçabilité et imputabilité des accès ;
    d. Accès occasionnels lors des audits et tests d'intrusion.
E. Défaillance de la maîtrise des interventions, qu'elles soient à l'initiative de l'organisation ou commanditées par un client.
F. Usages imprévus du service, par maladresse ou malveillance.
G. Défaillances matérielles ou logicielles, avec incapacité à respecter les engagements de continuité ou de reprise d'activité.
H. Sujétion de l'Hébergeur ou des éventuels sous-traitants à des législations extra-européennes pouvant entrainer une violation des DSCP.

5.3.1.3. Traitement des risques

Les exigences énoncées au chapitre 6.1.3 de la norme ISO 27001 s'appliquent en prenant en compte les exigences suivantes.

Exigence n° 06

[EXI 06] En cas de recours à la sous-traitance, l'Hébergeur doit s'assurer qu'il maîtrise les changements des mesures techniques et organisationnelles de ses sous-traitants permettant de traiter les risques identifiés.

Exigence n° 07

[EXI 07] Afin de réduire les risques d'usage imprévu du système, l'Hébergeur doit s'assurer que :

Les interfaces proposées aux clients sont disponibles au moins en langue française ;
Le support de premier niveau est au moins en langue française.

Exigence n° 08

[EXI 08] La déclaration d'applicabilité doit être disponible en langue française pour les auditeurs qui en feront la demande.

5.3.2. Objectifs de sécurité de l'information et plans pour les atteindre

Les exigences énoncées au chapitre 6.2 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 09

[EXI 09] Les objectifs de sécurité de l'information établis par l'Hébergeur doivent intégrer la protection des DSCP qui lui sont confiées par ses clients et comporter le respect des obligations du RGPD.

5.3.3. Planification des modifications

Les exigences énoncées au chapitre 6.3 de la norme ISO 27001 s'appliquent.

5.4. Supports

5.4.1. Ressources

Les exigences énoncées au paragraphe 7.1 de l'ISO 27001 s'appliquent.

5.4.2. Compétence

Les exigences énoncées au paragraphe 7.2 de l'ISO 27001 s'appliquent.

5.4.3. Sensibilisation

Les exigences énoncées au chapitre 7.3 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 10

[EXI 10] Les personnels travaillant pour l'Hébergeur doivent être sensibilisés à la criticité en termes de disponibilité, de confidentialité et d'intégrité des DSCP hébergées.

Cette exigence s'applique également au personnel des sous-traitants éventuels de l'Hébergeur.

5.4.4. Communication

Les exigences énoncées au chapitre 7.4 de la norme ISO 27001 s'appliquent en prenant en compte les exigences suivantes.

Exigence n° 11

[EXI 11] L'Hébergeur doit :

Maintenir une liste des points de contact pour chacun des clients. Ce point de contact doit être en mesure de désigner à l'Hébergeur un professionnel de santé habilité à accéder aux DSCP lorsque cela est nécessaire ;
Etre en capacité de transmettre sans délai cette liste à l'autorité compétente sur demande, notamment en cas de suspension ou de retrait de la certification.

.

Exigence n° 12

[EXI 12] L'Hébergeur doit communiquer à ses clients :

Une copie du certificat de conformité HDS. Cette copie constitue une garantie pour le Client de l'Hébergeur du respect des exigences de conformité ;
Le certificat de ses sous-traitants participant à l'activité d'hébergement lorsqu'ils sont certifiés HDS.

5.4.5. Informations documentées

Les exigences énoncées au chapitre 7.5 de la norme ISO 27001 s'appliquent.

5.5. Fonctionnement

5.5.1. Planification et contrôle opérationnels

Les exigences énoncées au chapitre 8.1 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 13

[EXI 13] L'Hébergeur doit planifier et contrôler la répartition des responsabilités en termes de sécurité de l'information entre l'Hébergeur et son client.

5.5.2. Appréciation des risques

Les exigences énoncées au paragraphe 8.2 de la norme ISO 27001 s'appliquent.

5.5.3. Traitement des risques

Les exigences énoncées au chapitre 8.3 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 14

[EXI 14] En cas de recours à un sous-traitant certifié pour la réalisation de tout ou partie du service d'hébergement, l'Hébergeur doit prévoir une procédure permettant d'encadrer le risque de perte ou de suspension de la certification du sous-traitant.

5.6. Evaluation de la performance

5.6.1. Surveillance, mesurage, analyse et évaluation

Les exigences énoncées au chapitre 9.1 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 15

[EXI 15] L'Hébergeur doit permettre au client d'effectuer les vérifications suivantes du niveau de sécurité proposé :

Si l'Hébergeur met à la disposition du client des ressources qui lui sont spécifiques, le client peut réaliser ou mandater des audits de sécurité technique sur ces seules ressources spécifiques. L'organisation assiste le client ou son intervenant mandaté dans le maintien de la sécurité de l'information durant ces audits ;
Sur demande du client, l'Hébergeur doit lui communiquer la synthèse managériale d'un rapport d'audit technique portant sur les ressources mutualisées dans le cadre du service. Cet audit doit être réalisé par un auditeur indépendant et dater de moins de trois ans ;
L'Hébergeur doit permettre au client de consulter les traces d'accès aux DSCP portées par des ressources spécifiques ou auxdites ressources par les personnels sous son contrôle ;
L'Hébergeur doit définir les modalités permettant à son client de consulter son dernier rapport d'audit de certification HDS.

5.6.2. Audit interne

5.6.2.1. Généralités

Les exigences énoncées au chapitre 9.2.1 de la norme ISO 27001 s'appliquent en prenant en compte l'exigence suivante.

Exigence n° 16
[EXI 16] Les audits internes effectués par l'Hébergeur doivent comprendre a minima : Un audit permettant de déterminer si le SMSI est conforme aux exigences du présent référentiel et est efficacement mis en œuvre et maintenu ; Un audit des traces des accès par les personnes opérant pour le compte de l'organisation aux DSCP ou aux systèmes utilisés pour leur traitement.

5.6.2.2. Programme d'audit interne

Les exigences énoncées au chapitre 9.2.2 de la norme ISO 27001 s'appliquent.

5.6.3. Revue de direction

Les exigences énoncées au chapitre 9.3 de la norme ISO 27001 s'appliquent.

5.7. Amélioration

Les exigences énoncées au chapitre 5.10 de la norme ISO 27001 s'appliquent.

6. EXIGENCES LIEES A LA RELATION CONTRACTUELLE

L'Hébergeur est tenu de fournir à son client un modèle de contrat conforme aux exigences règlementaires.

NOTE - Il est ainsi notamment recommandé à l'Hébergeur, qui agit en tant que sous-traitant de son client, de se référer aux modèles des clauses contractuelles types proposés par la Commission européenne pour inclure dans le contrat les clauses requises au titre de l'article 28 du RGPD (L_2021199FR.01001801.xml (europa.eu)

6.1. Certificat de conformité

Exigence n° 17
[EXI 17] Conformément au 1° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause mentionnant l'indication du périmètre du certificat de conformité obtenu par l'Hébergeur, ainsi ses dates de délivrance et de renouvellement.

6.2. Description des prestations réalisées

Exigence n° 18

[EXI 18] Conformément au 2° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause relative à la description des prestations réalisées, comprenant le contenu des services et résultats attendus notamment aux fins de garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données hébergées.

6.3. Respect des droits des personnes concernées

Exigence n° 19

[EXI 19] Conformément au 4° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause relative aux mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé. Cette clause doit notamment comporter les mentions suivantes : les modalités d'exercice des droits d'accès, de rectification, de limitation, d'opposition, d'effacement et de portabilité des données (lorsqu'ils sont applicables), les modalités de signalement au responsable de traitement d'une violation des données à caractère personnel, les modalités de conduite des audits par le délégué à la protection des données.

6.4. Désignation d'un référent contractuel

Exigence n° 20

[EXI 20] Conformément au 5° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause mentionnant le référent contractuel du client de l'Hébergeur à contacter pour le traitement des incidents ayant un impact sur les données de santé hébergées.

6.5. Les indicateurs de qualité et de performance

Exigence n° 21

[EXI 21] Conformément au 6° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause précisant les indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci.

6.6. Recours à la sous-traitance

Exigence n° 22

[EXI 22] Conformément au 7° de l'article R. 1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit prévoir une information sur les conditions de recours à d'éventuels prestataires techniques externes et les

engagements de l'Hébergeur pour que ce recours assure un niveau de protection équivalent de garantie au regard des obligations pesant sur l'Hébergeur, dans le respect de l'article 28.4 du RGPD.

6.7. Accès aux données de santé à caractère personnel hébergées

Exigence n° 23

[EXI 23] Conformément au 8° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit décrire les modalités retenues pour encadrer les accès aux données de santé à caractère personnel hébergées.

6.8. Modifications ou évolutions techniques

Exigence n° 24

[EXI 24] Conformément au 9° de l'article R. 1111-11 du CSP, le contrat d'hébergement doit préciser les obligations de l'Hébergeur à l'égard de son Client en cas de modifications ou d'évolutions techniques introduites par lui ou imposées par le cadre légal applicable.

Le contrat d'hébergement doit en outre prévoir l'accord préalable du Client dans le cas où ces modifications ou évolutions introduites par l'Hébergeur ne respectent pas :

Les niveaux de service tels que requis au chapitre; 6.5.
Les garanties définies aux chapitres 6.2 et.6.9.

6.9. Garanties

Exigence n° 25

[EXI 25] Conformément au 10° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit prévoir une information sur les garanties et les procédures mises en place par l'Hébergeur permettant de couvrir toute défaillance éventuelle de sa part.

6.10. Interdiction liée au traitement des données hébergées

Exigence n° 26

[EXI 26] Conformément au 11° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit rappeler l'interdiction pour l'Hébergeur d'utiliser les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé.

6.11. Réversibilité

Exigence n° 27

[EXI 27] Conformément aux 12° à 14° de l'article R.1111-11 du CSP, une clause relative à la réversibilité doit en présenter les modalités à la fin de la prestation ou en cas d'arrêt anticipé de la prestation quel qu'en soit le motif, avec a minima :

L'engagement de restitution de la totalité des informations confiées au titre de la prestation ;
L'engagement de destruction de toute copie de ces informations à l'issue de la restitution ;
Les modalités de calcul des coûts et délais pour la restitution des copies ;
Les formats de restitution, lisibles et exploitables à des fins de portabilité des données de santé, et le cas échéant les modalités permettant le déplacement des machines virtuelles/conteneurs.

7. SOUVERAINETE DES DONNEES

Exigence n° 28

[EXI 28] Quelle que soit l'activité d'hébergement de DSCP proposée au Client par l'Hébergeur ou l'un de ses sous-traitants, et dès lors que celle-ci implique un stockage de DSCP, alors l'Hébergeur ou ses sous-traitants doivent stocker ces DSCP exclusivement au sein de l'Espace Economique Européen (EEE), sans préjudice des cas d'accès à distance visée à l'exigence n°29. L'Hébergeur documente et communique au Client la localisation de ce stockage.

Exigence n° 29

[EXI 29] Lorsque la prestation proposée par l'Hébergeur ou l'un de ses sous-traitants implique un accès à distance depuis un pays qui ne fait pas partie de l'Espace Economique Européen (EEE), cet accès doit être fondé sur une décision d'adéquation de la Commission adoptée vertu de l'article 45 du RGPD[1] ou, à défaut, sur l'une des garanties appropriées prévues à l'article 46 du règlement.

Dans ce dernier cas, l'hébergeur informe son client de l'absence de décision d'adéquation, d'une part, et des garanties appropriées au sens de l'article 46 du RGPD mises en place pour encadrer cet accès à distance, d'autre part.

L'hébergeur indique au client et documente les garanties appropriées mises en place, ainsi que le cas échéant, tout autre mesure permettant d'assurer un niveau de protection des données équivalent à celui garanti par le droit de l'Union Européenne.

S'agissant des mesures supplémentaires mentionnées à l'exigence n° 29, l'hébergeur doit tenir compte des recommandations du comité européen de la protection des données 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE (version 2.0, adoptée le 18 juin 2021).

Exigence n° 30

[1] La liste des pays assurant un niveau de protection adéquat est consultable sur le site de la CNIL : www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

[EXI 30] Lorsque l'Hébergeur, ou l'un de ses sous-traitants intervenant dans la prestation d'hébergement, est soumis à la législation d'un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 45 du RGPD, l'Hébergeur doit indiquer dans le contrat qui le lie à son client et porter à la connaissance de l'organisme certificateur :

- La liste des réglementations extra-européennes en vertu desquelles l'Hébergeur, ou l'un de ses sous-traitants intervenant dans la prestation d'hébergement, serait tenu de permettre un accès non autorisé par le droit de l'Union aux DSCP, au sens de l'article 48 du RGPD ;
- Les mesures mises en œuvre par l'Hébergeur pour atténuer les risques d'accès non autorisé aux DSCP induits par ces réglementations extra-européennes ;
- La description des risques résiduels d'accès non autorisés aux DSCP via des réglementations extra-européennes qui demeureraient malgré ces mesures.

S'agissant de ces mesures mises en œuvre pour atténuer les risques d'accès mentionnées à l'exigence n° 30, l'hébergeur tient compte des lignes directrices du comité européen de la protection des données 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE (version 2.0, adoptée le 18 juin 2021).

Exigence n° 31

[EXI 31] L'Hébergeur doit rendre publiques et mettre à jour la cartographie des transferts des DSCP vers un pays n'appartenant pas à l'Espace Economique Européen y compris les accès distants éventuels mentionnés à l'exigence n° 29 ainsi que la description des risques d'accès non autorisé visés par l'exigence n° 30. Les modalités d'information du public doivent prendre la forme suivante :

- Dans le cas où l'activité certifiée bénéficie d'une qualification SecNumCloud (version 3.2), l'Hébergeur doit communiquer l'information suivante : « Aucun risque d'accès imposé par la législation d'un pays tiers en violation du droit de l'Union » ;

- Dans le cas où l'activité certifiée ne bénéficie pas d'une qualification SecNumCloud (version 3.2) et ne comporte pas de transfert de DSCP vers un pays n'appartenant pas à l'Espace Economique Européen, l'Hébergeur doit communiquer l'information suivante : « Aucun transfert de données de santé à caractère personnel vers un pays tiers à l'espace économique européen »;

- Dans le cas où l'activité certifiée ne bénéficie pas d'une qualification SecNumCloud (version 3.2) et comporte un ou plusieurs transferts de DSCP vers un pays n'appartenant pas à l'Espace Economique Européen ou un risque d'accès non autorisé visé par l'exigence n°30, l'Hébergeur doit communiquer les informations figurant dans le tableau fourni au chapitre 8.

L'Hébergeur doit mettre ces informations à la disposition du public de manière lisible sur une page dédiée d'un site internet accessible et communiquer l'URL de la page à l'organisme certificateur. Cette URL a vocation à être publiée dans la liste des hébergeurs certifiés sur le site de l'ANS.

8. REPRESENTATION DES GARANTIES

Ce chapitre a pour finalité d'apporter aux clients des Hébergeurs de données de santé davantage de transparence s'agissant du périmètre de la prestation de service couvert par la certification HDS. Il permet aux clients d'un service d'avoir connaissance des différents acteurs sur lesquels leur fournisseur de service s'appuie pour délivrer sa prestation.

Ainsi, cette représentation standard permet de lister les acteurs qui participent au traitement des DSCP dans le cadre de la prestation de service d'hébergement proposée.

Raison sociale de l'acteur	Rôle dans le cadre de la prestation d'hébergement (Hébergeur/sous-traitant de l'Hébergeur)	Certifié HDS (oui/non/exempté)	Qualifié SecNumCloud 3.2	Activités d'hébergement sur laquelle l'acteur intervient	Accès aux données de santé à caractère personnel depuis des pays tiers à l'Espace Economique Européen, par l'Hébergeur ou l'un de ses sous-traitants (exigence n° 29 du référentiel HDS)	Hébergeur ou sous-traitant soumis à un risque d'accès aux données de santé à caractère personnel depuis des pays tiers à l'Espace Economique Européen, imposé par la législation d'un pays tiers en violation du droit de l'Union (exigence n° 30 du référentiel HDS)
	□ Hébergeur □ Sous-traitant	□ Oui □ Non □ Exempté	□ Oui, aucun risque d'accès non autorisé aux données visé par l'exigence n°30 du référentiel HDS □ Non		□ Oui □ Non, aucun accès aux données depuis un pays tiers à l'Espace Economique Européen Si oui, préciser le pays concerné : -couvert par	□ Oui □ Non Si oui, préciser le pays concerné :

					une décision d'adéquation au sens de l'article 45 du RGPD : XX (préciser le pays) - non couvert par une décision d'adéquation au sens de l'article 45 du RGPD : XX (préciser le pays)	

9. SYNTHÈSE DES EXIGENCES

Exigence n° 01

[EXI 01] La certification d'un Hébergeur nécessite :

Qu'il ait mis en œuvre un Système de Management de la Sécurité de l'Information (SMSI) certifié selon la norme ISO 27001, complétée des exigences définies au chapitre 5. ;
Que le domaine d'application de ce SMSI couvre l'ensemble des activités d'hébergement de données de santé de l'Hébergeur ;
Que les contrats conclus avec ses clients répondent aux exigences définies au chapitre 6. ;
Qu'il respecte les exigences relatives à la souveraineté définies au chapitre 7 ;
Qu'il communique à ses clients la présentation des garanties formalisée conformément au chapitre .

Exigence n° 02

[EXI 02] Dans la détermination de ses enjeux externes et internes, l'Hébergeur doit prendre en compte le fait que sa mission lui impose la protection des DSCP qui lui sont confiées par ses clients.

Exigence n° 03

[EXI 03] Dans la détermination des exigences des parties intéressées, l'Hébergeur doit prendre en compte le cadre

juridique applicable en matière de protection des DSCP.

Exigence n° 04

[EXI 04] Le domaine d'application du SMSI doit comprendre l'ensemble des traitements de DSCP assurés par l'Hébergeur. Il doit couvrir tous les moyens et processus de traitement des DSCP, notamment les sauvegardes et les transferts de supports matériels de l'information.

Exigence n° 05

[EXI 05] Lors de l'appréciation des risques, l'Hébergeur doit a minima envisager les événements suivants :

A. Défaillance des supports matériels de l'information due à des menaces physiques et environnementales.
B. Perte de contrôle de supports matériels de l'information, notamment à l'occasion :
    a. De copie des DSCP sur des supports portables ;
    b. De matérialisation (éventuelle) sous format documents papier ;
    c. De réallocation des espaces de stockage.
C. Dégradation, compromission ou rupture d'un flux d'information interne ou externe sous la responsabilité de l'Hébergeur.
D. Défaillance de la maîtrise des accès attribués, que ce soit aux personnels sous le contrôle de l'organisation ou à ceux désignés par ses clients :
    a. Attribution, modification et retrait des droits d'accès ;
    b. Distribution des moyens d'identification électroniques ;
    c. Traçabilité et imputabilité des accès ;
    d. Accès occasionnels lors des audits et tests d'intrusion.
E. Défaillance de la maîtrise des interventions, qu'elles soient à l'initiative de l'organisation ou commanditées par un client.
F. Usages imprévus du service, par maladresse ou malveillance.
G. Défaillances matérielles ou logicielles, avec incapacité à respecter les engagements de continuité ou de reprise d'activité.
H. Sujétion de l'Hébergeur ou des éventuels sous-traitants à des législations extra-européennes pouvant entrainer une violation des DSCP.

Exigence n° 06

[EXI 06] En cas de recours à la sous-traitance, l'Hébergeur doit s'assurer qu'il maîtrise les changements des mesures techniques et organisationnelles de ses sous-traitants permettant de traiter les risques identifiés.

Exigence n° 07

[EXI 07] Afin de réduire les risques d'usage imprévu du système, l'Hébergeur doit s'assurer que :

Les interfaces proposées aux clients sont disponibles au moins en langue française ;

Le support de premier niveau est au moins en langue française. .

Exigence n° 08

[EXI 08] La déclaration d'applicabilité doit être disponible en langue française pour les auditeurs qui en feront la demande.

Exigence n° 09

[EXI 09] Les objectifs de sécurité de l'information établis par l'Hébergeur doivent intégrer la protection des DSCP qui lui sont confiées par ses clients et comporter le respect des obligations du RGPD.

Exigence n° 10

[EXI 10] Les personnels travaillant pour l'Hébergeur doivent être sensibilisés à la criticité en termes de disponibilité, de confidentialité et d'intégrité des DSCP hébergées.

Cette exigence s'applique également au personnel des sous-traitants éventuels de l'Hébergeur.

Exigence n° 11

[EXI 11] L'Hébergeur doit :

Maintenir une liste des points de contact pour chacun des clients. Ce point de contact doit être en mesure de désigner à l'Hébergeur un professionnel de santé habilité à accéder aux DSCP lorsque cela est nécessaire.
Être en capacité de transmettre sans délai cette liste à l'autorité compétente sur demande, notamment en cas de suspension ou de retrait de la certification.

.

Exigence n° 12

[EXI 12] L'Hébergeur doit communiquer à ses clients :

Une copie du certificat de conformité HDS. Cette copie constitue une garantie pour le Client de l'Hébergeur du respect des exigences de conformité ;
Le certificat de ses sous-traitants participant à l'activité d'hébergement lorsqu'ils sont certifiés HDS.

Exigence n° 13

[EXI 13] L'Hébergeur doit planifier et contrôler la répartition des responsabilités en termes de sécurité de l'information entre l'Hébergeur et son client.

Exigence n° 14

[EXI 14] En cas de recours à un sous-traitant certifié pour la réalisation de tout ou partie du service d'hébergement, l'Hébergeur doit prévoir une procédure permettant d'encadrer le risque de perte ou de suspension de la certification du sous-traitant.

Exigence n° 15

[EXI 15] L'Hébergeur doit permettre au client d'effectuer les vérifications suivantes du niveau de sécurité proposé :

Si l'Hébergeur met à la disposition du client des ressources qui lui sont spécifiques, le client peut réaliser ou mandater des audits de sécurité technique sur ces seules ressources spécifiques. L'organisation assiste le client ou son intervenant mandaté dans le maintien de la sécurité de l'information durant ces audits ;
Sur demande du client, l'Hébergeur doit lui communiquer la synthèse managériale d'un rapport d'audit technique portant sur les ressources mutualisées dans le cadre du service. Cet audit doit être réalisé par un auditeur indépendant et dater de moins de trois ans ;
L'Hébergeur doit permettre au client de consulter les traces d'accès aux DSCP portées par des ressources spécifiques ou auxdites ressources par les personnels sous son contrôle ;
L'Hébergeur doit définir les modalités permettant à son client de consulter son dernier rapport d'audit de certification HDS.

Exigence n° 16

[EXI 16] Les audits internes effectués par l'Hébergeur doivent comprendre a minima :

Un audit permettant de déterminer si le SMSI est conforme aux exigences du présent référentiel et est efficacement mis en œuvre et maintenu ;
Un audit des traces des accès par les personnes opérant pour le compte de l'organisation aux DSCP ou aux systèmes utilisés pour leur traitement.

Exigence n° 17

[EXI 17] Conformément au 1° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause mentionnant l'indication du périmètre du certificat de conformité obtenu par l'Hébergeur, ainsi que ses dates de délivrance et de renouvellement.

Exigence n° 18

[EXI 18] Conformément au 2° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause relative à la description des prestations réalisées, comprenant le contenu des services et résultats attendus notamment aux fins de garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des

données hébergées.

Exigence n° 19

[EXI 19] Conformément au 4° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause relative aux mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé. Cette clause doit notamment comporter les mentions suivantes : les modalités d'exercice des droits d'accès, de rectification, de limitation, d'opposition, d'effacement et de portabilité des données (lorsqu'ils sont applicables), les modalités de signalement au responsable de traitement d'une violation des données à caractère personnel, les modalités de conduite des audits par le délégué à la protection des données.

Exigence n° 20

[EXI 20] Conformément au 5° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause mentionnant le référent contractuel du client de l'Hébergeur à contacter pour le traitement des incidents ayant un impact sur les données de santé hébergées.

Exigence n° 21

[EXI 21] Conformément au 6° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit comporter une clause précisant les indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci.

Exigence n° 22

[EXI 22] Conformément au 7° de l'article R. 1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit prévoir une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'Hébergeur pour que ce recours assure un niveau de protection équivalent de garantie au regard des obligations pesant sur l'Hébergeur, dans le respect de l'article 28.4 du RGPD.

Exigence n° 23

[EXI 23] Conformément au 8° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit décrire les modalités retenues pour encadrer les accès aux données de santé à caractère personnel hébergées.

Exigence n° 24

[EXI 24] Conformément au 9° de l'article R. 1111-11 du CSP, le contrat d'hébergement doit préciser les obligations de l'Hébergeur à l'égard de son Client en cas de modifications ou d'évolutions techniques introduites par lui ou imposées par

le cadre légal applicable.

Le contrat d'hébergement doit en outre prévoir l'accord préalable du Client dans le cas où ces modifications ou évolutions introduites par l'Hébergeur ne respectent pas :

Les niveaux de service tels que requis au chapitre; 6.5.
Les garanties définies aux chapitres 6.2 et 6.9.

Exigence n° 25

[EXI 25] Conformément au 10° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit prévoir une information sur les garanties et les procédures mises en place par l'Hébergeur permettant de couvrir toute défaillance éventuelle de sa part.

Exigence n° 26

[EXI 26] Conformément au 11° de l'article R.1111-11 du CSP, le contrat d'hébergement conclu entre l'Hébergeur et son Client doit rappeler l'interdiction pour l'Hébergeur d'utiliser les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé.

Exigence n° 27

[EXI 27] Conformément aux 12° à 14° de l'article R.1111-11 du CSP, une clause relative à la réversibilité doit en présenter les modalités à la fin de la prestation ou en cas d'arrêt anticipé de la prestation quel qu'en soit le motif, avec a minima :

L'engagement de restitution de la totalité des informations confiées au titre de la prestation ;
L'engagement de destruction de toute copie de ces informations à l'issue de la restitution ;
Les modalités de calcul des coûts et délais pour la restitution des copies ;
Les formats de restitution, lisibles et exploitables à des fins de portabilité des données de santé, et le cas échéant les modalités permettant le déplacement des machines virtuelles/conteneurs.

Exigence n° 28

[EXI 28] Quelle que soit l'activité d'hébergement de DSCP proposée au Client par l'Hébergeur ou l'un de ses sous-traitants, et dès lors que celle-ci implique un stockage de DSCP, alors l'Hébergeur ou ses sous-traitants doivent stocker ces DSCP exclusivement au sein de l'Espace Economique Européen (EEE), sans préjudice des cas d'accès à distance visée à l'exigence n°29. L'Hébergeur documente et communique au Client la localisation de ce stockage.

Exigence n° 29

[EXI 29] Lorsque la prestation proposée par l'Hébergeur ou l'un de ses sous-traitants implique un accès à distance depuis un pays qui ne fait pas partie de l'Espace Economique Européen (EEE), cet accès doit être fondé sur une décision

d'adéquation de la Commission adoptée vertu de l'article 45 du RGPD[2] ou, à défaut, sur l'une des garanties appropriées prévues à l'article 46 du règlement.

Dans ce dernier cas, l'hébergeur informe son client de l'absence de décision d'adéquation, d'une part, et des garanties appropriées au sens de l'article 46 du RGPD mises en place pour encadrer cet accès à distance, d'autre part.

L'hébergeur indique au client et documente les garanties appropriées mises en place, ainsi que le cas échéant, tout autre mesure permettant d'assurer un niveau de protection des données équivalent à celui garanti par le droit de l'Union Européenne.

Exigence n° 30

[EXI 30] Lorsque l'Hébergeur, ou l'un de ses sous-traitants intervenant dans la prestation d'hébergement, est soumis à la législation d'un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 45 du RGPD, l'Hébergeur doit indiquer dans le contrat qui le lie à son client et porter à la connaissance de l'organisme certificateur :

- La liste des réglementations extra-européennes en vertu desquelles l'Hébergeur, ou l'un de ses sous-traitants intervenant dans la prestation d'hébergement, serait tenu de permettre un accès non autorisé par le droit de l'Union aux DSCP, au sens de l'article 48 du RGPD ;
- Les mesures mises en œuvre par l'Hébergeur pour atténuer les risques d'accès non autorisé aux DSCP induits par ces réglementations extra-européennes ;
- La description des risques résiduels d'accès non autorisés aux DSCP via des réglementations extra-européennes qui demeureraient malgré ces mesures
- .

Exigence n° 31

[EXI 31] L'Hébergeur doit rendre publique et mettre à jour la cartographie des transferts des DSCP vers un pays n'appartenant pas à l'Espace Economique Européen y compris les accès distants éventuels mentionnés à l'exigence n° 29 ainsi que la description des risques d'accès non autorisé visés par l'exigence n° 30. Les modalités d'information du public doivent prendre la forme suivante :

- Dans le cas où l'activité certifiée bénéficie d'une qualification SecNumCloud (version 3.2), l'Hébergeur doit communiquer l'information suivante : « aucun risque d'accès imposé par la législation d'un pays tiers en violation du droit de l'Union »

- Dans le cas où l'activité certifiée ne bénéficie pas d'une qualification SecNumCloud (version 3.2) et ne comporte pas de transfert de DSCP vers un pays n'appartenant pas à l'Espace Economique Européen, l'Hébergeur doit communiquer l'information suivante : « aucun transfert de données de santé à caractère personnel vers un pays tiers à l'espace économique européen »;

- Dans le cas où l'activité certifiée ne bénéficie pas d'une qualification SecNumCloud (version 3.2) et comporte un ou plusieurs transferts de DSCP vers un pays n'appartenant pas à l'Espace Economique Européen ou un risque

[2] La liste des pays assurant un niveau de protection adéquat est consultable sur le site de la CNIL : www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

d'accès non autorisé visé par l'exigence n°30, l'Hébergeur doit communiquer les informations figurant dans le tableau fourni au chapitre 8.

L'Hébergeur doit mettre ces informations à la disposition du public de manière lisible sur une page dédiée d'un site internet accessible et communiquer l'URL de la page à l'organisme certificateur. Cette URL a vocation à être publiée dans la liste des hébergeurs certifiés sur le site de l'ANS.

Annexe 1 : Matrice de correspondance avec SecNumCloud

La matrice ci-dessous explicite la correspondance entre chaque mesure de l'annexe A de la norme ISO 27001 et le chapitre d'exigences du référentiel SecNumCloud v3.2. Attention, la correspondance ne signifie pas qu'il existe une équivalence entre une mesure ISO 27001 et une exigence SecNumCloud 3.2.

L'appréciation de l'efficacité des mesures reste à réaliser pour la certification HDS.

Mesure Annexe A	Exigences SecNumCloud applicables
5.1 – Politiques de sécurité de l'information	5.2 – Politique de sécurité de l'information
5.2 – Fonctions et responsabilités liées à la sécurité de l'information	6.1 – Fonctions et responsabilités liées à la sécurité de l'information.
5.3 – Séparation des tâches	6.2 – Séparation des tâches
5.4 – Responsabilités de la direction	Pas d'exigence liée
5.5 – Contacts avec les autorités	6.3 – Relations avec les autorités
5.6 – Contacts avec des groupes d'intérêt spécifiques	6.4 – Relations avec les groupes de travail spécialisés
5.7 – Surveillance des menaces	Pas d'exigence liée

Mesure Annexe A	Exigences SecNumCloud applicables
5.8 – Sécurité de l'information dans la gestion de projet	6.5 – La sécurité de l'information dans la gestion de projet
5.9 – Inventaire des informations et autres actifs associés	8.1 – Inventaire et propriété des actifs
5.10 – Utilisation correcte des informations et autres actifs associés	8.4 – Marquage et manipulation de l'information
5.11 – Restitution des actifs	8.2 – Restitution des actifs
5.12 – Classification des informations	8.3 - Identification
5.13 – Marquage des informations	8.4 – Marquage et manipulation de l'information
5.14 – Transfert des informations	10.2 – Chiffrement des flux
5.15 – Contrôle d'accès	9.1 – Politiques et contrôle d'accès
5.16 – Gestion des identités	9.2 – Enregistrement et désinscription des utilisateurs
5.17 – Informations d'authentification	10.3 – Hachage des mots de passe
5.18 – Droits d'accès	9.2 – Enregistrement et désinscription des utilisateurs 9.4 – Revue des droits d'accès utilisateurs
5.19 – Sécurité de l'information dans les relations avec les fournisseurs	15.1 – Identification des tiers

Mesure Annexe A	Exigences SecNumCloud applicables
5.20 – Sécurité de l'information dans les accords conclus avec les fournisseurs	15.2 – La sécurité dans les accords conclus avec des tiers 15.5 – Engagements de confidentialité
5.21 – Gestion de la sécurité de l'information dans la chaîne d'approvisionnement des technologies de l'information et de la communication (TIC)	15.1 – Identification des tiers 15.3 – Surveillance et revue des services des tiers
5.22 – Surveillance, révision et gestion des changements des services fournisseurs	15.3 – Surveillance et revue des services des tiers
5.23 – Sécurité de l'information dans l'utilisation de services en nuage	15.1 – Identification des tiers 15.3 – Surveillance et revue des services des tiers 19.6 – Immunité au droit extra-communautaire (d)
5.24 – Planification et préparation de la gestion des incidents de sécurité de l'information	16.1 – Responsabilités et procédures
5.25 – Évaluation des événements de sécurité de l'information et prise de décision	16.3 – Appréciation des événements liés à la sécurité de l'information et prise de décision
5.26 – Réponse aux incidents de sécurité de l'information	16.4 – Réponse aux incidents liés à la sécurité de l'information
5.27 – Tirer des enseignements des incidents de sécurité de l'information	16.5 – Tirer des enseignements des incidents liés à la sécurité de l'information
5.28 – Collecte de preuves	16.6 – Recueil de preuves
5.29 – Sécurité de l'information pendant une perturbation	Pas d'exigence liée
5.30 – Préparation des TIC pour la continuité d'activité	17.4 – Disponibilité des moyens de traitement de l'information

Mesure Annexe A	Exigences SecNumCloud applicables
5.31 – Exigences légales, statutaires, réglementaires et contractuelles	18.1 – Identification de la législation et des exigences contractuelles applicables
5.32 – Droits de propriété intellectuelle	Pas d'exigence liée
5.33 – Protection des enregistrements	Pas d'exigence liée
5.34 – Protection de la vie privée et des données à caractère personnel (DCP)	19.5 – Protection des données à caractère personnel
5.35 – Révision indépendante de la sécurité de l'information	18.2 – Revue indépendante de la sécurité de l'information
5.36 – Conformité aux politiques, règles et normes de sécurité de l'information	18.3 – Conformité avec les politiques et les normes de sécurité 18.4 – Examen de la conformité technique
5.37 – Procédures d'exploitation documentées	12.1 – Procédures d'exploitation documentées
6.1 – Sélection des candidats	7.1 – Sélection des candidats
6.2 – Termes et conditions d'embauche	7.2 – Conditions d'embauche
6.3 – Sensibilisation, apprentissage et formation à la sécurité de l'information	7.3 – Sensibilisation, apprentissage et formation à la sécurité de l'information
6.4 – Processus disciplinaire	7.4 – Processus disciplinaire
6.5 – Responsabilités après la fin ou le changement d'un emploi	7.5 – Rupture, terme ou modification du contrat de travail

Mesure Annexe A	Exigences SecNumCloud applicables
6.6 – Accords de confidentialité ou de non-divulgation	15.5 – Engagements de confidentialité
6.7 – Travail à distance	12.12 – Administration (c) 12.13 – Télédiagnostic et télémaintenance des composants de l'infrastructure
6.8 – Déclaration des événements de sécurité de l'information	16.2 – Signalements liés à la sécurité de l'information
7.1 – Périmètres de sécurité physique	11.1 – Périmètres de sécurité physique
7.2 – Les entrées physiques	11.2 – Contrôle d'accès physique 11.5 – Zones de livraison et de chargement
7.3 – Sécurisation des bureaux, des salles et des équipements	Pas d'exigence liée
7.4 – Surveillance de la sécurité physique	11.2.1 – Zones privées (h) 11.2.2 – Zones sensibles (h)
7.5 – Protection contre les menaces extérieures et environnementales	11.3 – Protection contre les menaces extérieures et environnementales
7.6 – Travail dans les zones sécurisées	11.4 – Travail dans les zones privées et sensibles
7.7 – Bureau propre et écran vide	Pas d'exigence liée
7.8 – Emplacement et protection des matériels	11.10 – Matériel en attente d'utilisation

Mesure Annexe A	Exigences SecNumCloud applicables
7.9 – Sécurité des actifs hors des locaux	Pas d'exigence liée
7.10 – Supports de stockage	11.8 – Sortie des actifs
7.11 – Services supports	11.3 – Protection contre les menaces extérieures et environnementales 11.7 – Maintenance des matériels
7.12 – Sécurité du câblage	11.6 – Sécurité du câblage
7.13 – Maintenance du matériel	11.7 – Maintenance des matériels
7.14 – Élimination ou recyclage sécurisé(e) du matériel	11.9 – Recyclage sécurisé du matériel
8.1 – Terminaux finaux des utilisateurs	12.12 - Administration
8.2 – Droits d'accès privilégiés	9.3 – Gestion des droits d'accès
8.3 – Restriction d'accès aux informations	9.7 – Restriction des accès à l'information
8.4 – Accès aux codes sources	Pas d'exigence liée
8.5 – Authentification sécurisée	9.5 – Gestion des authentifications des utilisateurs

Mesure Annexe A	Exigences SecNumCloud applicables
8.6 – Dimensionnement	Pas d'exigence liée
8.7 – Protection contre les programmes malveillants (malware)	12.4 – Mesures contre les codes malveillants
8.8 – Gestion des vulnérabilités techniques	12.11 – Gestion des vulnérabilités techniques
8.9 – Gestion des configurations	18.2.1 – Revue initiale 18.2.2 – Revue des changements majeurs
8.10 – Suppression des informations	11.9 – Recyclage sécurisé du matériel 19.4 – Fin de contrat
8.11 – Masquage des données	Pas d'exigence liée
8.12 – Prévention de la fuite de données	12.14 – Surveillance des flux sortants de l'infrastructure 19.6 – Immunité au droit extracommunautaire
8.13 – Sauvegarde des informations	12.5 – Sauvegarde des informations 17.5 – Sauvegarde de la configuration de l'infrastructure technique 17.6 – Mise à disposition d'un dispositif de sauvegarde des données du commanditaire
8.14 – Redondance des moyens de traitement de l'information	17.1 – Organisation de la continuité d'activité 17.2 – Mise en œuvre de la continuité d'activité 17.3 – Vérifier, revoir et évaluer la continuité d'activité
8.15 – Journalisation	12.6 – Journalisation des événements 12.7 – Protection de l'information journalisée 12.9 – Analyse et corrélation des événements
8.16 – Activités de surveillance	13.3 – Surveillance des réseaux

Mesure Annexe A	Exigences SecNumCloud applicables
8.17 – Synchronisation des horloges	12.8 – Synchronisation des horloges
8.18 – Utilisation de programmes utilitaires à privilèges	Pas d'exigence liée
8.19 – Installation de logiciels sur des systèmes opérationnels	12.10- Installation de logiciels sur des systèmes en exploitation
8.20 – Sécurité des réseaux	13.1 – Cartographie du système d'information 13.2 – Cloisonnement des réseaux
8.21 – Sécurité des services réseau	9.6 – Accès aux services d'administration 13.2 – Cloisonnement des réseaux (d,e)
8.22 – Cloisonnement des réseaux	13.2 – Cloisonnement des réseaux
8.23 – Filtrage web	13.2 – Cloisonnement des réseaux (c)
8.24 – Utilisation de la cryptographie	10.4 – Non-répudiation 10.5 – Gestion des secrets 10.6 – Racines de confiance
8.25 – Cycle de vie de développement sécurisé	14.1 – Politique de développement sécurisé
8.26 – Exigences de sécurité des applications	5.3 – Appréciation des risques
8.27 – Principes d'ingénierie et d'architecture des systèmes sécurisés	Pas d'exigence liée

Mesure Annexe A	Exigences SecNumCloud applicables
8.28 – Codage sécurisé	18.2.2 – Revue initiale 18.2.3 – Revue des changements majeurs
8.29 – Tests de sécurité dans le développement et l'acceptation	14.6 – Test de la sécurité et conformité du système
8.30 – Développement externalisé	14.5 – Développement externalisé
8.31 – Séparation des environnements de développement, de test et opérationnels	12.3 – Séparation des environnements de développement, de test et d'exploitation 14.4 – Environnement de développement sécurisé
8.32 – Gestion des changements	12.2 – Gestion des changements 14.2 – Procédures de contrôle des changements de système 14.3 – Revue technique des applications après changement appliqué à la plateforme d'exploitation
8.33 – Informations de test	14.7 – Protection des données de test
8.34 – Protection des systèmes d'information pendant les tests d'audit	Pas d'exigence liée

Deux exigences de SecNumCloud ne sont pas corrélées à des mesures de référence de la norme ISO 27001, mais se retrouvent partiellement dans les exigences contractuelles ou les exigences supplémentaires relatives au SMSI :

- Les exigences concernant le contenu de la convention de service (19.1 de SecNumCloud) ;
- L'exigence de localisation des données (19.2 de SecNumCloud).

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Statut : En cours de validation | *Classification : Publique* | *Version : v2023 – à valider*

Agence du Numérique en Santé
2-10 Rue d'Oradour-sur-Glane – 75015 Paris T. 01
58 45 32 50
esante.gouv.fr

Documents de référence

Référence n°1 : NF EN ISO/IEC 17021-1:2015

Évaluation de la conformité -- Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management

Référence n°2 : NF ISO/IEC 27001:2022

Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information - Exigences

Référence n°3 : Référentiel de certification HDS exigences v2023

Référence n°4 : IAF MD1 version en vigueur

Document d'exigences IAF pour la certification multi-sites par échantillonnage

Référence n°5 : IAF MD2 version en vigueur

Document d'exigences IAF pour le transfert d'une certification sous accréditation de systèmes de management

Référence n°6 : IAF MD4 version en vigueur

Document d'exigences IAF pour l'utilisation de techniques d'audit assistées par ordinateur (« TAAO ») pour la certification sous accréditation de systèmes de management

Référence n°7 : IAF MD5 version en vigueur

Détermination du temps d'audit des systèmes de management de la qualité et des systèmes de management environnemental

Référence n°8 : IAF MD11 version en vigueur

Document d'exigences IAF pour l'application de la norme ISO/IEC 17021 pour les audits de Systèmes de Management Intégrés (SMI)

Les documents d'exigences IAF sont disponibles sur le site de l'IAF.

SOMMAIRE

10. INTRODUCTION

10.1. Objet du document

Ce document s'adresse aux organismes de certification souhaitant être accrédités pour la certification des Hébergeurs de données de santé. Il décrit le processus d'accréditation des organismes de certification et le processus de certification des hébergeurs.

10.2. Structure du document

Ce document est organisé en sept parties et deux annexes :

- introduction du document ;
- description du champ d'application du référentiel d'accréditation ;
- description des normes applicables au sein du référentiel d'accréditation ;
- liste des acronymes utilisés dans le référentiel d'accréditation ;
- description des conditions, critères et modalités d'accréditation des organismes de certification ;
- définition des responsabilités des organismes d'accréditation ;
- description des conditions, critères et modalités de certification des hébergeurs.

Annexes

- annexe A présentant les éléments nécessaires permettant de déterminer la durée d'audit pour la certification HDS ;
- annexe B présentant les modèles de documents à utiliser par les organismes de certification pour envoyer des informations à l'autorité compétente.
- .

10.2.1. Définitions

10.2.1.1. Acteur

Tout intervenant contribuant à la sécurité des données de santé à caractère personnel, à l'exclusion du responsable de traitement et des sous-traitants d'un Hébergeur certifié lorsqu'ils agissent conformément à la politique de sécurité et sous la surveillance dudit Hébergeur

10.2.1.2. 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 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.

10.2.1.3. Client de l'Hébergeur

Le client de l'Hébergeur (également dénommé « client ») désigne la personne physique ou morale souscrivant au service mis en œuvre par l'Hébergeur.

10.2.1.4. Hébergeur

L'Hébergeur, également désigné organisation dans la norme ISO 27001, est le candidat à la certification des Hébergeurs de données de santé ou au renouvellement de sa certification. Il fournit tout ou partie d'un service d'hébergement de données de santé à caractère personnel (ou « données de santé »).

10.2.1.5. Moyen d'identification électronique

Un moyen d'identification électronique est un élément matériel ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier à un service en ligne.

10.2.1.6. Responsable de traitement

Le responsable de traitement au sens du règlement n°2016/679 désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

11. CHAMP D'APPLICATION

11.1. Applicabilité du référentiel de certification HDS

Le champ d'application du référentiel est défini par les articles L. 1111-8, R. 1111-8-8 et R. 1111-9 du code de la santé publique.

11.1.1. Rôle d'Hébergeur

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.

11.1.2. Nature des données

Les données hébergées doivent être des données à caractère personnel concernant la santé, telles que définies à l'article 4.15 du RGPD.

11.1.3. Contexte du recueil

Sont concernées par la certification HDS, les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social.

Ces données de santé à caractère personnel doivent être hébergées pour le compte :

des personnes physiques ou morales à l'origine de la production ou du recueil des données ;

ou du patient lui-même.

11.1.4. Activités réalisées

L'article R. 1111-9 du CSP définit l'activité d'hébergement de données de santé.

Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L. 1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R. 1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes :

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.

L'activité 5 est précisée au paragraphe 2.1.2.

L'activité 6 de sauvegarde des données doit être interprétée comme comprenant uniquement les sauvegardes externalisées. Les sauvegardes intrinsèquement nécessaires aux activités 1 à 5 sont dans le périmètre des activités 1 à 5.

12. RÉFÉRENCES NORMATIVES

Les documents, listés ci-dessous sont référencés de manière normative dans le présent référentiel et sont indispensables pour son application.

NF EN ISO 27001:2023, *Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information - Exigences*

NF EN ISO/IEC 17021-1:2015, *Évaluation de la conformité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences*

Dans la suite du document, les références à ces normes se feront de la manière suivante :

- NF ISO 27001 pour la norme NF EN ISO 27001:2023 ;
- NF ISO 17021-1 pour la norme NF EN ISO/IEC 17021-1:2015.

13. ACRONYMES UTILISÉS

COFRAC	Comité Français d'Accréditation
DdA	Déclaration d'Applicabilité documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées et applicables au Système de Management de la Sécurité de l'Information d'un organisme
HDS	Hébergeur de Données de Santé
IAF	International Accreditation Forum
CEI / IEC	Commission Electrotechnique Internationale / International Electronical Commission
ISO	International Organization for Standardization
OC	Organisme de Certification

14. CONDITIONS, CRITÈRES ET MODALITÉS D'ACCRÉDITATION

Les conditions, critères et modalités d'accréditation s'appuient sur les standards de la norme NF ISO 17021-1. L'accréditation atteste de la compétence, de l'impartialité et de la fiabilité d'un organisme à vérifier la conformité à des exigences établies et formalisées. L'accréditation constitue un contrôle dit de deuxième niveau qui vise à contrôler la façon dont opère le contrôleur.

14.1. Conditions et critères d'accréditation

Les organismes de certification habilités à délivrer des certificats de conformité HDS doivent être accrédités par une instance nationale d'accréditation telle que définie dans le règlement CE 765/2008 (le COFRAC en France ou son équivalent dans les autres pays signataires des accords multilatéraux de reconnaissance internationaux) conformément au présent référentiel d'accréditation qui sera revu régulièrement afin d'intégrer notamment les évolutions technologiques au sein des systèmes d'information de santé, ainsi que les mutations des métiers de l'hébergement.

L'application et le respect des exigences du référentiel d'accréditation permettent de garantir que les organismes accrédités sont compétents pour délivrer les certifications HDS.

L'accréditation porte sur l'évaluation des organismes souhaitant être certifiés hébergeurs de données de santé à caractère personnel.

Pour qu'un organisme puisse être accrédité pour délivrer des certifications HDS, il doit être accrédité selon les exigences de la norme NF ISO 17021-1 et appliquer les règles en vigueur pour l'audit et la certification des systèmes de management de la sécurité des systèmes d'information selon la norme ISO 27001. En outre, le présent référentiel d'accréditation définit les exigences spécifiques qui s'appliquent à la certification HDS.

14.2. Exigences d'accréditation

14.2.1. Exigences générales

14.2.1.1. Domaine contractuel et juridique

Les exigences du §5.1 de la norme NF ISO 17021-1 s'appliquent.

14.2.1.2. Gestion de l'impartialité

Les exigences du §5.2 de la norme NF ISO 17021-1 s'appliquent.

14.2.1.3. Responsabilité et financement

Les exigences du §5.3 de la norme NF ISO 17021-1 s'appliquent.

14.2.2. Exigences structurelles

14.2.2.1. Compétence du personnel

Les exigences du §7.1 de la norme NF ISO 17021-1 s'appliquent.

Lors de la sélection de l'équipe d'audit, l'organisme de certification veille à ce que les compétences apportées à chaque mission soient appropriées. L'équipe doit avoir une connaissance suffisante des aspects de sécurité de l'information, d'hébergement de données sensibles et des services proposés par les hébergeurs de données de santé.

En particulier, les auditeurs de l'organisme de certification qui participent aux activités de certification HDS doivent être en mesure de démontrer qu'ils possèdent des compétences dans les domaines de la sécurité des systèmes d'information et notamment des systèmes d'information de santé.

La direction de l'organisme de certification doit définir les processus et disposer des ressources nécessaires pour lui permettre de déterminer si oui ou non les auditeurs sont compétents pour les tâches qu'ils doivent accomplir dans le cadre de la certification HDS. L'organisme de certification doit être en mesure de communiquer à ses clients les compétences de son personnel impliqué dans les activités de certification.

14.2.2.2. Personnel intervenant dans les activités de certification

Les exigences du §7.2 de la norme NF ISO 17021-1 s'appliquent.

L'équipe d'auditeurs peut être renforcée par des experts techniques. Ces experts techniques ne se substituent pas aux auditeurs, mais accompagnent ces derniers sur les questions d'adéquation entre la sécurité et les dispositifs utilisés dans le contexte de l'hébergement de données de santé.

Il est recommandé que les experts aient des compétences spécifiques dans le domaine de la santé acquises à l'occasion d'une formation ou d'un projet.

L'organisme de certification doit avoir une procédure permettant :

- de sélectionner des auditeurs et des experts techniques sur la base de leurs compétences, leurs formations, leurs qualifications et leur expérience ;
- d'évaluer la conduite des auditeurs et des experts techniques lors des audits de certification et de surveillance.

14.2.2.3. Intervention d'auditeurs et d'experts techniques externes individuels

Les exigences du §7.3 de la norme NF ISO 17021-1 s'appliquent.

14.2.2.4. Enregistrements relatifs au personnel

Les exigences du §7.4 de la norme NF ISO 17021-1 s'appliquent.

14.2.2.5. Externalisation

Les exigences du §7.5 de la norme NF ISO 17021-1 s'appliquent.

14.2.3. Exigences relatives aux informations

14.2.3.1. Informations accessibles au public

Les exigences du §8.1 de la norme NF ISO 17021-1 s'appliquent.

14.2.3.2. Documents de certification

Les exigences du §8.2 de la norme NF ISO 17021-1 s'appliquent.

L'organisme de certification fournit à chacun de ses clients certifiés hébergeurs de données de santé à caractère personnel les documents attestant de leur certification.

Ces documents doivent :

- préciser le périmètre du service certifié au regard des activités définies dans le chapitre 2 « Champ d'application », notamment la liste des activités certifiées;
- spécifier les normes ISO pour lesquelles l'organisme est déjà certifié et dont il respecte les exigences en vigueur (NF ISO 27001).
- préciser la localisation (a minima le pays) de tous les sites entrant dans le périmètre de certification.

Lorsqu'une certification ISO 27001 est délivrée par un OC différent de celui qui délivre la certification HDS, le certificat doit comporter une mention explicite indiquant qu'il est valable sous condition d'obtention d'une certification ISO 27001 valide pour le même périmètre.

Nota bene

En cas de recours à des sous-traitants, les sites de ces derniers ne figurent pas sur le certificat.

14.2.3.3. Référence à la certification et utilisation des marques

Les exigences du §8.3 de la norme NF ISO 17021-1 s'appliquent.

14.2.3.4. Confidentialité

Les exigences du §8.4 de la norme NF ISO 17021-1 s'appliquent.

Avant toute intervention de la part de l'équipe d'audit, l'organisme de certification doit s'assurer avec le candidat que les informations qui seront communiquées durant 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 ou d'autres données confidentielles ou sensibles, l'organisme de certification doit en informer le candidat, un accord de confidentialité doit être établi et un professionnel de santé intervenant sous la responsabilité du client doit être informé.

Le chapitre 8.4.2 de la norme NF ISO 17021-1 est complété ainsi : 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.

14.2.3.5. Echanges d'informations avec l'autorité compétente

14.2.3.5.1. Rapport de suspension HDS

L'organisme de certification doit communiquer en français ou en anglais à l'autorité compétente toute décision de suspension de certification d'un hébergeur de données de santé.

Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été suspendue doivent être communiquées :

- désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été suspendue ;
- numéro d'identifiant du certificat suspendu ;
- date de suspension du certificat ;
- raisons de la suspension de la certification HDS.

L'envoi des informations doit être réalisé par voie électronique en complétant le modèle proposé en Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

14.2.3.5.2. Rapport de retrait HDS

L'organisme de certification doit communiquer en français ou en anglais à l'autorité compétente toute décision de retrait de certification d'un hébergeur de données de santé.

Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été retirée doivent être communiquées :

- désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été retirée ;
- numéro d'identifiant du certificat retiré ;
- date de retrait du certificat ;
- raisons du retrait de la certification HDS.

L'envoi des informations doit être réalisé par voie électronique en complétant le modèle de l'Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

14.2.3.5.3. Répertoire clients HDS

L'organisme de certification doit fournir, a minima une fois par mois, un rapport des certifications valides, suspendues et retirées, à l'autorité compétente. Ce rapport, en français ou en anglais, doit contenir les données suivantes pour chaque hébergeur de données de santé :

- désignation ou raison sociale de l'hébergeur de données de santé ;
- numéro d'identifiant du certificat ;
- périmètre de la certification (liste des activités) ;
- adresse du site certifié et dans le cas d'une certification multi-sites, indiquer l'adresse du siège social, ainsi que celles de tous les sites rattachés ;
- état de la certification (valide, suspendue ou retirée) ;
- date de la certification.
- URL ou contact afin de permettre la vérification du certificat auprès de l'OC.
- URL de la page de déclaration des transferts des DSCP conformément à l'exigence 31 du référentiel de certification

L'envoi du répertoire doit être réalisé par voie électronique en complétant le modèle de l'Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

14.2.3.5.4. Rapport annuel HDS

Les exigences du § 8.5 de la norme NF ISO 17021-1 s'appliquent.

Chaque année, l'organisme de certification doit fournir à l'autorité compétente un rapport annuel en français ou en anglais comprenant :

- une synthèse anonymisée des certifications HDS, des audits réalisés et des non-conformités relevées.
- une synthèse des difficultés rencontrées lors de la certification des hébergeurs et des éventuelles propositions de modifications à apporter aux référentiels de certification et d'accréditation ;
- des indicateurs sur la procédure de certification HDS, tels que :
- nombre d'hébergeurs de données de santé en cours de certification ;
- nombre d'hébergeurs de données de santé ayant échoué à la certification ;
- nombre de renouvellements de certification ;
- durée moyenne des audits.

L'envoi du rapport annuel doit être réalisé par voie électronique entre le 1er et le 31 janvier de l'année suivante, en complétant le modèle proposé en Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

14.2.4. Exigences du processus de certification

14.2.4.1. Activités préalables à la certification

14.2.4.1.1. Demande de certification

Les exigences du § 9.1.1 de la norme NF ISO 17021-1 s'appliquent.

Dans le cas d'un transfert de certificat, le guide IAF MD 2 s'applique. En complément, l'organisme de certification récepteur devra informer l'autorité compétente de tout transfert de certificat et indiquer le nom de l'organisme de certification émetteur.

14.2.4.1.2. Revue de la demande

Les exigences du § 9.1.2 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.1.3. Programme d'audit

Les exigences du § 9.1.3 de la norme NF ISO 17021-1 s'appliquent.

Le chapitre 9.1.3.1 est complété par l'exigence suivante : la description du périmètre de certification doit préciser la liste des activités énumérées au chapitre 11. pour lesquelles le candidat demande une certification afin de déterminer le type de certification HDS.

14.2.4.1.4. Détermination du temps d'audit

Les exigences du § 9.1.4 de la norme NF ISO 17021-1 s'appliquent. En complément, les exigences des guides IAF MD 4 et MD 5 s'appliquent.

La détermination de la durée d'audit doit être réalisée en appliquant la méthode et les tableaux, de l'« Annexe A : Tableau de durée d'audit pour la certification HDS » du présent document.

Si après calculs le résultat obtenu n'est pas un nombre entier, le nombre de jours doit être arrondi à la demi-journée la plus proche (par ex. : 5,3 jours d'audit deviennent 5,5 jours d'audit, et 5,2 jours d'audit deviennent 5 jours d'audit).

14.2.4.1.5. Echantillonnage multiple

Les exigences du § 9.1.5 de la norme NF ISO 17021-1 s'appliquent. En complément, le guide IAF MD 1 s'applique.

14.2.4.1.6. Normes de systèmes de management multiples

Les exigences du § 9.1.6 de la norme NF ISO 17021-1 s'appliquent, ainsi que le guide IAF MD 11.

14.2.4.2. Planification des audits

Les exigences du § 9.2 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.3. Certification initiale

Les exigences du § 9.3 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.4. Réalisation des audits

Les exigences du § 9.4 de la norme NF ISO 17021-1 s'appliquent.

Des représentants de l'Agence du Numérique en Santé peuvent assister en tant qu'observateurs à la réalisation d'un audit.

14.2.4.5. Décision de certification

Les exigences du § 9.5 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.6. Maintien de la certification

Les exigences du § 9.6 de la norme NF ISO 17021-1 s'appliquent.

La certification est délivrée pour une durée de 3 ans. Les hébergeurs certifiés doivent déposer auprès de l'organisme de certification une demande de recertification au plus tard 3 mois avant la date de fin de validité de la certification.

14.2.4.7. Appels

Les exigences du § 9.7 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.8. Plaintes

Les exigences du § 9.8 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.9. Enregistrements relatifs au client

Les exigences du § 9.9 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.10. Exigences du système de management pour les organismes de certification

14.2.4.10.1. Options

Les exigences du § 10.1 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.10.2. Exigences du système de management conformément à la norme ISO 9001

Les exigences du § 10.2 de la norme NF ISO 17021-1 s'appliquent.

14.2.4.10.3. Exigences générales du système de management

Les exigences du § 10.3 de la norme NF ISO 17021-1 s'appliquent.

14.2.5. Modalités d'évaluation

L'annexe B de la norme NF ISO 17021-1 s'applique.

15. RESPONSABILITÉS DES ORGANISMES D'ACCRÉDITATION

Les missions des organismes d'accréditation (le COFRAC, en France, et ses homologues européens), consistent à s'assurer que les organismes qu'ils accréditent sont compétents et impartiaux et qu'ils le demeurent dans le temps, quel que soit le contexte.

Pour attester de cette compétence, l'organisme d'accréditation réalise des évaluations régulières du fonctionnement de ces organismes accrédités. Les évaluations sont constituées d'une revue documentaire ainsi que d'une intervention des évaluateurs en tant que témoins d'un audit pour vérifier à la fois la qualité des procédures et la façon dont elles sont appliquées.

15.1. Processus d'accréditation

Le processus d'accréditation est conforme à la norme NF ISO 17021-1.

Si l'organisme de certification est déjà accrédité pour la norme NF ISO 17021-1, une extension majeure de la portée d'accréditation à un nouveau domaine doit être réalisée. Cela conduit à une évaluation au siège de l'organisme et au moins à une observation d'activité.

Si l'organisme de certification n'est pas déjà accrédité pour la norme NF ISO 17021-1, le processus d'accréditation initial doit être appliqué.

Après recevabilité favorable de la demande d'accréditation par l'instance nationale d'accréditation pour la certification HDS (recevabilité opérationnelle), les organismes certificateurs en cours de demande d'accréditation sont autorisés à délivrer des certificats pendant douze (12) mois.

L'accréditation doit être obtenue dans un délai maximum de douze (12) mois, à compter de la date de notification de la décision positive de recevabilité opérationnelle.

Si l'accréditation n'est pas obtenue dans ce délai, l'organisme de certification en informe ses clients pour qu'ils prennent contact avec un autre organisme de certification pour obtenir un nouveau certificat.

Les certificats émis pendant la période des douze (12) mois devront être réémis sous accréditation s'ils ont été initialement délivrés dans les mêmes conditions que celles ayant permis de prononcer l'accréditation.

La portée d'accréditation est exprimée comme suit :

Objet de la certification	Référence de certification	Référentiel d'accréditation
Systèmes de management de la sécurité des systèmes d'information des hébergeurs de données de santé	Référentiel de Certification HDS Exigences (version en vigueur)	Référentiel d'accréditation HDS (version en vigueur)

15.2. Processus de suspension de l’accréditation

15.2.1. Décision de suspension

Dans le cas d’une suspension de l’accréditation à l’initiative de l’organisme d’accréditation, ce dernier en informe sans délai l’organisme de certification et l’autorité compétente en précisant : le nom de l'organisme de certification, la date de suspension, les motivations de la décision de suspension et la date à laquelle l’accréditation sera retirée si les conditions de levée de la suspensions ne sont pas respectées.

La décision de suspension est notifiée par lettre recommandée avec accusé de réception et précise la portée de la suspension de l’accréditation, les motivations de la décision de suspension de l’organisme d’accréditation, ainsi que les conditions dans lesquelles l’organisme pourra lever la suspension de l’accréditation de l’organisme de certification.

Si l’organisme de certification ne transmet pas les réponses demandées par l’organisme d’accréditation dans les délais impartis spécifiés dans la décision de suspension, l’accréditation est retirée pour les activités de certification d’hébergeur de données de santé à caractère personnel.

Dès la réception de la décision de suspension de son accréditation, l’organisme de certification a l’obligation d’informer ses clients et cesser toute nouvelle référence à l’accréditation. Un organisme dont l’accréditation est suspendue ne doit plus réaliser d’audit de certification, ni rendre de décisions relatives au certificat d’hébergeur de donnée de santé.

15.2.2. Levée de suspension

Dans le cas d’une suspension à l’initiative de l’organisme d’accréditation, les conditions de levée de la suspension sont spécifiées dans la décision de suspension adressée à l’organisme de certification.

La décision de levée de suspension ne peut être émise qu’à la suite d’une évaluation de l’organisme de certification sur site ou à l’examen par l’organisme d’accréditation d’un rapport d’audit interne transmis par l’organisme de certification. Si le rapport ne fournit pas d’éléments suffisants pour démontrer la conformité aux exigences d’accréditation, l'organisme de certification est informé par courrier que sa suspension ne pourra être levée qu’au vu des résultats d'une évaluation sur site. La décision de levée de suspension est notifiée par l’organisme d’accréditation. Une nouvelle attestation d'accréditation mentionnant la date de prise d'effet de la levée de suspension est établie et l'annexe technique définissant les activités pour lesquelles l'accréditation a été accordée est mise à jour. La date de fin de validité de l’accréditation est inchangée par rapport à l’accréditation initiale.

L’envoi de la notification de levée de suspension à l’autorité compétente doit être réalisé par voie électronique en précisant : le nom de l'organisme de certification, la date de suspension (le cas échéant), les motivations de la décision de suspension et la date de levée de la suspension.

En cas de refus de la levée de la suspension, l'organisme de certification peut faire appel de la décision auprès de l'organisme d'accréditation.

15.3. Processus de retrait de l'accréditation

Dans le cas d'un retrait de l'accréditation, l'organisme d'accréditation informe sans délai l'organisme de certification et l'autorité compétente, de toute mesure de retrait d'accréditation.

L'envoi de la notification de retrait à l'autorité compétente doit être réalisé par voie électronique en précisant : le nom de l'organisme de certification, la date de suspension (le cas échéant), les motivations de la décision de retrait de l'accréditation et la date à laquelle l'accréditation a été retirée.

Le retrait de l'accréditation prend effet à la date de notification du retrait par l'organisme d'accréditation. La décision est communiquée à l'organisme de certification par lettre recommandée avec accusé de réception, précisant les motivations de la décision.

L'organisme n'est plus autorisé à délivrer de certificats ni à maintenir les certificats existants.

L'organisme de certification dont l'accréditation a été retirée doit cesser toutes les activités liées à la certification d'hébergeur de données de santé et en informer immédiatement l'autorité compétente et ses clients pour que ces derniers puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue.

L'organisme d'accréditation a la possibilité d'intervenir sur le site de l'organisme de certification afin de s'assurer que les activités liées à la certification d'hébergeurs de données de santé ont été suspendues et que l'autorité compétente et les clients ont été informés.

15.4. Transfert de certification à un nouvel organisme de certification à la suite d'un retrait

Le nouvel organisme de certification qui reçoit une demande de transfert doit appliquer les dispositions décrites dans le §16. du présent document. En particulier, le guide IAF MD2 s'applique. S'il est dans l'impossibilité de se procurer le dossier du client auprès de l'organisme précédent, la demande du client sera traitée comme une certification initiale. Dans tous les cas, il revient à l'organisme de certification « récepteur » d'évaluer les éléments fournis et d'établir si le cycle de certification peut être repris à la même étape de certification que celle dans laquelle il se trouvait avec l'organisme de certification initial.

15.5. Cessation d'activité d'un organisme de certification

L'organisme d'accréditation informe sans délai l'autorité compétente, de toute annonce de cessation d'activité d'un organisme de certification.

L'organisme de certification est également tenu d'informer l'autorité compétente, ainsi que les clients concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue.

16. CONDITIONS, CRITÈRES ET MODALITÉS DE CERTIFICATION

16.1. Conditions et critères de certification

Un candidat souhaitant obtenir une certification HDS devra répondre aux exigences du référentiel de certification HDS et faire une demande de certification auprès d'un organisme de certification accrédité conformément au référentiel d'accréditation HDS.

La certification d'un hébergeur nécessite :

- qu'il ait mis en œuvre un Système de Management de la Sécurité de l'Information (SMSI) certifié selon la norme ISO 27001, complétée des exigences définies au chapitre 5 du référentiel de certification;
- que le domaine d'application de ce SMSI couvre l'ensemble des activités d'hébergement de données de santé de l'Hébergeur ;
- que les contrats conclus avec ses clients répondent aux exigences définies au chapitre 6 du référentiel de certification ;
- qu'il respecte les exigences relatives à la souveraineté définies au chapitre 7 du référentiel de certification ;
- qu'il communique à ses clients la présentation des garanties formalisée conformément au chapitre 8 du référentiel de certification.

Un hébergeur qui a déjà obtenu une certification ISO 27001 peut faire prévaloir cette certification s'il remplit les conditions citées dans le chapitre 16.2..

Un candidat disposant déjà de cette certification est évalué sur le périmètre des exigences du référentiel de certification non couvertes par la certification. La certification déjà obtenue fait l'objet d'une vérification selon les modalités définies au chapitre 16.2..

Le certificat HDS est délivré pour 3 ans : la date de fin de validité peut être différente de la date de fin de validité du certificat ISO 27001.

Le certificat HDS comporte une mention explicite indiquant qu'il est valable sous condition d'une certification ISO 27001 valide pour le même périmètre.

Dans le contrat entre l'OC et son client, les mentions suivantes doivent apparaitre :

- Le client est informé qu'en cas de non-conformité relative à une exigence de l'ISO 27001 constatée à l'occasion d'un audit HDS, cette information est transmise à l'OC qui a certifié le client selon l'ISO 27001.
- Le client a l'obligation d'informer immédiatement l'OC de toute mesure de suspension, retrait, résiliation ou transfert de son certificat ISO 27001.

Ces engagements font l'objet d'une vérification lors des audits de surveillance.

16.2. Equivalence

Si le candidat souhaite faire prévaloir la certification selon la norme NF ISO 27001 qu'il a déjà obtenue, cette certification doit remplir toutes les conditions ci-dessous :

- le périmètre d'application de la certification dont dispose l'hébergeur doit inclure le périmètre pour lequel le candidat demande une certification HDS ;
- les rapports d'audit : le rapport d'audit initial et les rapports d'audit de surveillance de la certification dont l'équivalence est demandée doivent être fournis sur demande de l'organisme de certification ;
- pour un candidat disposant d'une certification ISO 27001, la déclaration d'applicabilité (DdA) du système de gestion de la sécurité des informations de l'organisation doit expressément inclure :
- la justification détaillée de toute exclusion de contrôles de l'ISO 27001 ;
- la justification détaillée de tout contrôle non applicable ;
- la certification doit :
- être en cours de validité ;
- avoir été délivrée par un organisme de certification accrédité par une instance nationale d'accréditation telle que définie dans le règlement (CE) n° 765/2008 pour la délivrance de ces certificats et dont l'accréditation doit être en cours de validité (le COFRAC en France ou son équivalent dans les autres pays signataires des accords multilatéraux de reconnaissance internationaux) ;
- ne pas faire l'objet d'une procédure de suspension ou de retrait ;
- ne pas faire l'objet d'une demande de transfert.

Les conditions ci-dessus doivent faire l'objet d'une vérification par l'organisme de certification recevant la demande de certification HDS, qui doit enregistrer les informations reçues (copies des certificats notamment) et justifier les résultats de cette vérification en indiquant quelle(s) certification(s) est (sont) acceptée(s) par l'OC préalablement à l'audit initial du candidat.

Les certifications obtenues selon des normes internationales équivalentes aux normes françaises indiquées ci-dessus pourront être reconnues selon les mêmes conditions. Il s'agit notamment des certifications de conformité aux normes ISO 27001 et ISO 17021 dans d'autres langues que le français.

16.3. Sous-traitance

En cas de recours à des sous-traitants par l'hébergeur, la représentation des garanties décrite au chapitre 8 du référentiel de certification HD s'applique.

Annexe A : Tableau de durée d'audit pour la certification HDS

Le tableau de temps d'audit ci-dessous fournit le cadre qui doit être utilisé pour la planification de l'audit de certification HDS en identifiant un point de départ basé sur le nombre total de personnes travaillant sous le contrôle de l'organisation pour tous les postes impliqués dans le service d'hébergement de données de santé et en ajustant les facteurs importants.

L'OC doit fournir la détermination du temps d'audit et les justificatifs au client. Ceux-ci font partie intégrante du contrat et doivent être tenus à disposition de l'organisme d'accréditation sur demande.

Le point de départ pour déterminer le temps d'audit d'une certification HDS doit reposer sur le nombre réel d'employés impliqués dans le service d'hébergement de données de santé, puis pourra être ajusté en fonction de facteurs significatifs s'appliquant au client à auditer.

Nombre de personnes impliquées dans le service d'hébergement de données de santé	Durée d'audit de la certification HDS (étape 1 + étape 2) A+B		
	(A) Durée d'audit NF ISO 27001	(B) Durée d'audit des exigences hors NF ISO 27001	Durée totale de l'audit de certification HDS
0			0,5[3]
1 – 10	5	2	7
11 - 15	6	2	8
16 - 25	7	2	9
26 - 45	8,5	2	10,5
46 - 65	10	3	13
66 - 85	11	3	14
86 - 125	12	3	15
126 - 175	13	3	16
176 - 275	14	3	17
276 - 425	15	3	18
426 - 625	16,5	4	20,5
626 - 875	17,5	4	21,5
876 - 1175	18,5	4	22,5
1176 - 1550	19,5	4	23,5
1551 – 2025	21	4	25

[3] Aucun facteur de réduction ne peut s'appliquer sur cette ligne

Nombre de personnes impliquées dans le service d'hébergement de données de santé	Durée d'audit de la certification HDS (étape 1 + étape 2) A+B		
	(A) Durée d'audit NF ISO 27001	(B) Durée d'audit des exigences hors NF ISO 27001	Durée totale de l'audit de certification HDS
2026 – 2675	22	4	26
2676 – 3450	23	4	27
3451 – 4350	24	5	29
4351 – 5450	25	5	30
5451 – 6800	26	5	31
6801 – 8500	27	5	32
8501 - 10700	28	5	33
10700	Suivre la progression ci-dessus	Suivre la progression ci-dessus	Suivre la progression ci-dessus

La durée d'audit HDS pourra être ajustée à la hausse ou à la baisse en fonction de facteurs spécifiques selon les bonnes pratiques en vigueur pour le calcul des durées d'audit d'un SMSI. Ces facteurs sont la complexité du SMSI, la nature du service concerné, la preuve d'une mise en œuvre préalable d'un SMSI, la complexité technologique mise en œuvre, le recours à des sous-traitants, la nature des développements éventuels et le nombre de sites. Les modifications apportées au SMSI sont un facteur à prendre en compte pour le calcul des durées des audits de surveillance et de recertification.

Selon les règles de bonnes pratiques en vigueur pour le calcul des durées d'audit d'un SMSI, la réduction maximale de la durée d'audit est de 30%, l'augmentation maximale de la durée d'audit est de 100%. Ces limites s'appliquent au calcul de la durée d'audit HDS.

Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente

Rapport annuel HDS

Nom de l'organisme de certification	Date : *jj/mm/aaaa*

Synthèse des certifications HDS, des audits réalisés et des non-conformités relevées

Synthèse des difficultés rencontrées lors de la certification HDS

Propositions d'amélioration de la certification HDS

Indicateurs sur la procédure de certification HDS

Nombre de certifications délivrées	Nombre d'échecs	Nombre de renouvellements	Nombre de suspensions	Nombre de retraits	Nombre de certifications

					transférées
XXXX	*XXXX*	*XXXX*	*XXXX*	*XXXX*	*XXXX*

Répertoire clients HDS

Nom de l'organisme de certification : *XXXX*

Date : *jj/mm/aaaa*

Identifiant du Certificat	Nom hébergeur de données de santé	Périmètre de la certification (liste des activités)	URL de la page de déclaration des risques de transfert des DSCP conformément à l'exigence 31	Adresse des sites	Date de certification	Etat du certificat	URL de publication du certificat ou Contact OC

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv.fr