AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Référentiel de certification Hébergeur de données de santé (HDS)

Exigences

Statut : Validé | *Classification : Publique* | *Version : v2.0*

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
[ARTR 1111-9] 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
V2.0	Avril 2024	Version publiée par l'arrêté du 26 avril 2024 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 Ecart avec la version publiée par l'arrêté : correction du lien vers le chapitre 8 dans l'exigence 01.

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. Définitions

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

Acronyme	
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 8

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.

5.4. Contexte de l'organisation

5.4.1. 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

5.4.2. 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.

5.4.3. 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.

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

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

5.5. Gouvernance

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

5.6. Planification

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

5.6.1.1. Généralités

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

5.6.1.2. 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 àceux 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.

5.6.1.3. 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.

5.6.2. 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.

5.6.3. Planification des modifications

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

5.7. Supports

5.7.1. Ressources

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

5.7.2. Compétence

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

5.7.3. 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.

5.7.4. 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.

5.7.5. Informations documentées

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

5.8. Fonctionnement

5.8.1. 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.

5.8.2. Appréciation des risques

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

5.8.3. 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.

5.9. Evaluation de la performance

5.9.1. 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.

5.9.2. Audit interne

5.9.2.1. 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.

5.9.2.2. Programme d'audit interne

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

5.9.3. Revue de direction

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

5.10. 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 que 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

[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 extraeuropéennes 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,

[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

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 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)	□ Oui □ Non Si oui, préciser le pays concerné:

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 8

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 àceux 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 ;
- 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.

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 ;

[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

- La description des risques résiduels d'accès non autorisés aux DSCP via des réglementations extraeuropéennes qui demeureraient malgré ces mesures.

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.

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
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
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

Mesure Annexe A	Exigences SecNumCloud applicables
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
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
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

Mesure Annexe A	Exigences SecNumCloud applicables
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
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
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

Mesure Annexe A	Exigences SecNumCloud applicables
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
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
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

Mesure Annexe A	Exigences SecNumCloud applicables
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).