AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Référentiel HDS

Exigences

Statut : En concertation | *Classification : Restreinte* | *Version : V1.1.20221027*

Agence du Numérique en Santé
9, rue Georges Pitard – 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/CEI 27001:2013
[SecNumCloud]	Référentiel SecNumCloud v3.2 du 8 mars 2022

Historique des modifications

Version	Date	Commentaire
V1.1	Juin 2018	Version publiée 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
V1.1.20221027	Octobre 2022	Version soumise à concertation ► Définition du champ d'application de l'activité 5 « administration et exploitation du système d'information contenant les données de santé. ► Rappel des exigences contractuelles dont celles mentionnées à l'article R.1111-11 du code de la santé publique. ► Standardisation de la présentation des garanties mises en place par l'hébergeur permettant de couvrir toute défaillance éventuelle de sa part. ► Ajout d'une matrice de correspondance avec le référentiel SecnumCloud. ► Renforcement des exigences relatives au transfert de données hors Union européenne.

SOMMAIRE

1. PREAMBULE

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'une organisation 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 organisations ayant une activité d'hébergeur de données de santé.

Ces organisations contribuent notamment à la mise en œuvre d'un service numérique en santé, tel que défini à l'article L. 1470-1 du code de la santé publique.

Article L1470-1 du code de la santé publique

« Les services numériques en santé régis par le présent titre sont les systèmes d'information ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités.

Les utilisateurs des services numériques en santé sont :

1° Les professionnels de santé et les personnes exerçant sous leur autorité, les établissements et services de santé, le service de santé des armées et tout organisme participant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code ;

2° Les professionnels des secteurs social et médico-social et les établissements ou services des secteurs social et médico-social mentionnés au I de l'article L. 312-1 du code de l'action sociale et des familles ;

3° Les usagers du système de santé. »

2. DEFINITIONS ET CONCEPTS GENERAUX

2.1. Glossaire

2.1.1. Acteur

Tout intervenant, certifié ou pas, susceptible de détenir, d'accéder ou de contrôler une instance des données de santé traitées dans le cadre du service numérique en santé.

2.1.2. Administrateur

Personne ayant un accès privilégié aux données de santé à caractère personnel ou aux moyens de traitement utilisés dans la mise en œuvre du service souscrit.

2.1.3. Administration et exploitation du système d'information contenant les données de santé

L'administration et l'exploitation du système d'information contenant des données de santé mentionnée à l'article R.1111-9 du code la santé publique comporte :

- L'encadrement et la gestion des accès occasionnels des tiers mandatés par le client de l'organisation, par exemple à des fins d'audit, d'expertise, de déploiement ou de maintenance, amenés à accéder via le Socle d'Infrastructure HDS à l'Application métier. Les accès des Utilisateurs finaux et du responsable de traitement ne sont pas concernés. Ces tiers mandatés ne sont pas tenus d'être certifiés HDS.
- Le maintien en condition de sécurité du Socle d'Infrastructure HDS et le centre de support au client. Ces services doivent être adaptés à la criticité des données de santé et aux obligations qui incombent au Responsable de traitement.
- La documentation tenue à jour de la cohérence et de la complétude des garanties de sécurité apportées par les différents acteurs contribuant à la mise en œuvre du service, telle que décrite au chapitre 7 du référentiel de certification

2.1.4. Application métier

Le terme d'application métier (ou « application métier comportant des données de santé à caractère personnel ») désigne l'application utilisée par l'Utilisateur final pour la collecte et le traitement de données de santé à caractère personnel.

2.1.5. 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.

2.1.6. Hébergeur

Prestataire qui concourt à la fourniture d'un service d'hébergement de données de santé à caractère personnel.

2.1.7. Maintien en condition de sécurité

Ce terme désigne la mise en œuvre par l'hébergeur de l'ensemble des mesures techniques et organisationnelles pour garantir la sécurité du socle d'infrastructure HDS et du support client.

2.1.8. Organisation

Le terme organisation désigne dans le cadre du présent référentiel, le candidat à la certification des hébergeurs de données de santé et l'hébergeur disposant d'une certification.

2.1.9. 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.

2.1.10. Service numérique en santé

Système d'information, service ou outil au sens de l'article L1470-1 du CSP.

2.1.11. Service souscrit

Service d'hébergement dont bénéficie le client dans le cadre obtenu par le client auprès de l'organisation

2.1.12. Socle d'infrastructure utilisé pour l'hébergement de données de santé

Le socle d'infrastructure utilisé pour l'hébergement de données de santé (ou « Socle d'Infrastructure HDS ») comprend les infrastructures matérielle et logicielle mentionnées à l'article R.1111-9 du code de la santé publique.

- L'infrastructure matérielle comporte les locaux, le matériel et le réseau interne de l'hébergeur.
- L'infrastructure logicielle comporte l'infrastructure virtuelle, la plateforme logicielle (comprenant entre autres : l'OS, les middleware le système de gestion des bases de données) et la sauvegarde des données de santé.

L'Application Métier est exclue du Socle d'Infrastructure HDS.

2.1.13. Sous-traitant

Le sous-traitant au sens du règlement n°2016/679 désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

2.1.14. Système d'information de santé

Le terme de système d'information de santé (ou « système d'information contenant les données de santé » ou « système d'information utilisé pour le traitement de données de santé ») désigne le socle d'infrastructure utilisé pour l'hébergement de données de santé visées à l'article L.1111-8 du Code de la Santé Publique, ainsi que l'application métier.

2.1.15. Utilisateur final

L'Utilisateur final est la personne ou l'entité qui utilise l'application métier dans l'exercice de ses missions pour collecter, modifier, traiter des données de santé à caractère personnel (exemple : application de type dossier patient informatisé, application pour le suivi du diabète, application pour la gestion des informations de santé de personnes handicapées, etc.).

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 au prestataire qui concourt à la fourniture d'un service d'hébergement de données de santé.

L'obligation de certification HDS ne s'applique pas aux personnes à l'origine de la production ou du recueil des données, par exemple les établissements et professionnels de santé.

3.1.2. Nature et origine des données

Les données hébergées doivent être des données à caractère personnel concernant la santé, telles que définies par le RGPD dans son considérant 35 :

« Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.

Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro. »

Sont concernées les données de santé à caractère personnel hébergées pour le compte :

- Des personnes physiques ou morales à l'origine de la production ou du recueil des données
- Du patient lui-même

3.1.3. Motif de 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.

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 des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;

2° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;

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 6 de sauvegarde des données comprend les sauvegardes externalisées et les sauvegardes intrinsèquement nécessaires aux activités 3 à 5.

Le R.1111-8-8 ajoute à l'exception télécom traditionnelle (le traitement fugitif des données lorsqu'elles transitent sur un réseau public) une exception de transcription visant principalement les services d'impression de courriers ou de saisie de comptes-rendus, que ce soit par des opérateurs ou de la reconnaissance vocale.

4. CONDITIONS D'ATTRIBUTION D'UN CERTIFICAT

Exigence n° 01

[EXI 01] La certification d'une organisation nécessite :

- Qu'elle ait mis en œuvre un système de management de la sécurité de l'information certifié selon la norme ISO 27001, complétée des exigences définies au chapitre 5.
- Que les contrats conclus avec ses clients soient conformes aux exigences définies au chapitre 6 EXIGENCES LIEES A LA RELATION CONTRACTUELLE liées à la relation contractuelle et 7 REPRESENTATION DES GARANTIES.

5. EXIGENCES RELATIVES AU SMSI

La numérotation de ce chapitre est alignée sur celle de l'ISO 27001 et commence donc 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 paragraphe 4.1 de l'ISO 27001 s'appliquent.

5.4.2. Compréhension des besoins et des attentes des parties intéressées

Exigence n° 02

[EXI 02] **Exigence supplémentaire par rapport au paragraphe 4.2 de l'ISO 27001**

Les parties intéressées doivent inclure :

- Les personnes dont les données de santé à caractère personnel (DSCP) sont hébergées (personnes concernées au sens de l'article 4 du RGPD).
- Les autres parties ayant des intérêts ou des responsabilités associées au traitement des DSCP, et notamment les professionnels assurant la prise en charge des personnes concernées.

Parmi les exigences des parties intéressées doivent figurer leurs exigences en termes de continuité, de disponibilité et de capacité des services de l'organisation, d'imputabilité des accès aux DSCP et de respect des dispositions du RGPD.

5.4.3. Détermination du domaine d'application du SMSI

Exigence n° 03

[EXI 03] **Exigence supplémentaire par rapport au paragraphe 4.3 de l'ISO 27001**

Le domaine d'application du SMSI doit comprendre l'ensemble des traitements de DSCP assurés par l'organisation. 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 l'ISO 27001 s'appliquent.

5.5. Gouvernance

5.5.1. Gouvernance et engagement

Les exigences énoncées au paragraphe 5.1 de l'ISO 27001 s'appliquent.

5.5.2. Politique

Les exigences énoncées au paragraphe 5.2 de l'ISO 27001 s'appliquent.

5.5.3. Rôles, responsabilités et autorités

Les exigences énoncées au paragraphe 5.3 de l'ISO 27001 s'appliquent.

5.6. Planification

5.6.1. Actions liées aux risques et opportunités

5.6.1.1. Généralités

Les exigences énoncées au paragraphe 6.1.1 de l'ISO 27001 s'appliquent.

5.6.1.2. Appréciation des risques

Exigence n° 04

[EXI 04] **Exigence supplémentaire par rapport au paragraphe 6.1.2 de l'ISO 27001**

Dans l'appréciation des risques, l'organisation doit considérer en priorité les risques encourus par la personne concernée en cas de perte d'intégrité, de confidentialité ou de disponibilité de ses DSCP. Ces risques comportent notamment la perte de chance liée à une prise en charge inappropriée, les risques de réputation ou de discrimination.

Elle doit également prendre en compte les risques encourus par les personnes et organisations assurant la prise en charge médicale de la personne concernée, y compris l'engagement de leur responsabilité médicale et les risques de réputation.

Lors de l'appréciation des risques, l'organisation doit a minima envisager les événements suivants :

A. Défaillance des supports matériels de l'information dues à des menaces physiques et environnementales.
B. Perte de contrôle de supports matériels de l'information, notamment à l'occasion :
    - de copies des DSCP sur des supports portables
    - de matérialisation (éventuelle) sous format documents papier
    - de réallocation des espaces de stockage
C. Défaut de protection des flux d'information internes ou externes sous la responsabilité de l'organisation.
D. Défaillance de la maîtrise des accès attribués, que ce soit aux personnels sous le contrôle de l'organisation où à ceux désignés par ses clients :
    - Attribution, modification et retrait des droits d'accès
    - Distribution des crédits
    - Traçabilité et imputabilité des accès
    - 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 l'incapacité à respecter les engagements de continuité ou de reprise d'activité.
H. Sujétion de l'organisation ou de ses éventuels sous-traitants à des législations extra-européennes pouvant entrainer une violation des DSCP.

5.6.1.3. Traitement des risques

Exigence n° 05

[EXI 05] **Exigence supplémentaire par rapport au paragraphe 6.1.3 de l'ISO 27001**

En cas de recours à la sous-traitance, l'organisation doit s'assurer qu'elle maîtrise les changements des mesures techniques et organisationnelles de ses sous-traitants permettant de traiter les risques identifiés.

Exigence n° 06

[EXI 06] **Exigence supplémentaire par rapport au paragraphe 6.1.3 de l'ISO 27001**

Pour toutes les mesures mises en œuvre et faisant l'objet d'une préconisation particulière du référentiel SecNumCloud (voir Annexe 2 : Matrice de correspondance avec SecNumCloud), la déclaration d'applicabilité doit en outre préciser si la mise en œuvre est conforme à cette préconisation.

L'adoption d'une mise en œuvre conforme à SecNumCloud est au libre choix de l'organisation, sauf à ce qu'elle y soit contrainte par un autre cadre. Elle ne la dispense pas de l'évaluation de l'efficacité de la mesure pour atteindre ses objectifs de sécurité.

Si l'organisation n'est pas déjà titulaire d'une qualification SecNumCloud pour le même service, la déclaration de conformité de la réalisation d'une mesure en cohérence avec SecNumCloud n'a pas valeur de qualification. Dans le cadre de ce référentiel, l'auditeur qui contrôle cette conformité n'a pas à être certifié en tant que Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI).

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

Exigence n° 07

[EXI 07] **Exigence supplémentaire par rapport au paragraphe 6.2 de l'ISO 27001**

Les objectifs de sécurité doivent

- être établis en cohérence avec les exigences des parties intéressées.
- comporter l'imputabilité à des personnes physiques des accès aux DSCP et aux systèmes utilisés pour leur traitement. Cette imputabilité concerne toutes les personnes opérant pour le compte de l'organisation ainsi que les intervenants occasionnels mandatés par ses clients. L'imputabilité des accès des administrateurs réguliers des clients relève de la responsabilité de chaque client, même lorsque l'organisation y contribue.
- comporter le respect des obligations du RGPD.

5.7. Support

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

Exigence n° 08

[EXI 08] **Précision au paragraphe 7.3 de l'ISO 27001**

Les contrats de travail des personnels travaillant pour l'organisation doivent inclure une clause de confidentialité. En cas de recours à la sous-traitance, cette exigence s'applique également aux sous-traitants.

5.7.4. Communication

Exigence n° 09

[EXI 09] **Exigence supplémentaire par rapport au paragraphe 7.4 de l'ISO 27001**

L'organisation doit prendre en compte les obligations légales et réglementaires de communication des incidents de sécurité s'appliquant aux utilisateurs de ses services et leur fournir les moyens d'y satisfaire.

Exigence n° 10

[EXI 10] **Exigence supplémentaire par rapport au paragraphe 7.4 de l'ISO 27001**

L'organisation doit communiquer à son client et au responsable de traitement des DSCP :

- Les lois extra-communautaires auxquelles l'Hébergeur est soumis.

- Les mesures mises en œuvre par l'Hébergeur pour atténuer les risques de violation des DSCP induits par ces lois.
- La description des risques résiduels.

Exigence n° 11

[EXI 11] **Exigence supplémentaire par rapport au paragraphe 7.4 de l'ISO 27001**

L'organisation 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.

5.7.5. Informations documentées

5.7.5.1. Généralités

Les exigences énoncées au paragraphe 7.5.1 de l'ISO 27001 s'appliquent.

5.7.5.2. Création et mise à jour

Les exigences énoncées au paragraphe 7.5.2 de l'ISO 27001 s'appliquent.

5.7.5.3. Maîtrise des informations documentées

Exigence n° 12

[EXI 12] **Précision au paragraphe 7.5.3 de l'ISO 27001**

Les durées de conservation des différentes versions des informations documentées constituant la politique de sécurité doivent être définies et formalisées

Exigence n° 13

[EXI 13] **Exigence supplémentaire par rapport au paragraphe 7.5 de l'ISO 27001**

Lorsque des informations documentées sont échangées avec le client, ces informations doivent être la langue de travail choisie par celui-ci.

Les informations documentées comprennent les informations définies dans le chapitre 7.5 de l'ISO 27001, les interfaces, le support de premier niveau, une déclaration d'applicabilité dans la langue de travail et la représentation des garanties telle que décrite au chapitre 7

5.8. Fonctionnement

5.8.1. Planification et contrôle opérationnels

Exigence n° 14

[EXI 14] **Précision par rapport au paragraphe 8.1 de l'ISO 27001**

Les modifications prévues intègrent notamment toutes les modifications des moyens à l'initiative de l'organisation.

Les modifications imprévues intègrent notamment toutes les altérations des ressources mises à disposition par l'organisation, ainsi que tous les changements de leur usage, à l'initiative des bénéficiaires de ces ressources

.

Exigence n° 15
[EXI 15] **Exigence supplémentaire par rapport au paragraphe 8.1 de l'ISO 27001** L'organisation doit s'assurer qu'elle maintient les garanties de sécurité de l'information : ► Lors de modifications prévues, comme la délivrance du service à de nouveaux clients. ► Lors de modifications imprévues, comme les modifications de configuration ou d'usage du service par un client. De telles modifications peuvent entraîner des répercussions sur les services auxquels il a souscrit, mais éventuellement aussi sur ceux rendus aux autres clients

Exigence n° 16
[EXI 16] **Exigence supplémentaire par rapport au paragraphe 8.1 de l'ISO 27001** L'organisation doit s'assurer qu'elle dispose des documentations que le client doit lui fournir pour lui permettre d'assurer son service dans le respect de ses objectifs de sécurité.

5.8.2. Appréciation des risques

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

5.8.3. Traitement des risques

Exigence n° 17
[EXI 17] **Exigence supplémentaire par rapport au paragraphe 8.3 de l'ISO 27001** L'organisation, si elle délègue une partie du traitement des DSCP à un fournisseur certifié HDS, doit avoir défini une procédure de traitement du risque de perte ou de suspension de la certification dudit fournisseur.

5.9. Evaluation des performances

5.9.1. Surveillance, mesures, analyse et évaluation

Exigence n° 18
[EXI 18] **Exigence supplémentaire par rapport au paragraphe 9.1 de l'ISO 27001.** 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 un rapport d'audit externe indépendant datant de moins de trois ans sur les ressources mutualisées participant au service rendu. ► 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

Exigence n° 19

[EXI 19] **Exigence supplémentaire par rapport au paragraphe 9.2 de l'ISO 27001**

Les audits internes effectués par l'organisation doivent comprendre a minima :

- Un audit de conformité et de bon fonctionnement de son SMSI
- 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.

5.9.3. Revue de direction

Les exigences énoncées au paragraphe 9.3 de l'ISO 27001 s'appliquent.

5.10. Amélioration

5.10.1. Non-conformités et actions correctives

Les exigences énoncées au paragraphe 10.1 de l'ISO 27001 s'appliquent.

5.10.2. Amélioration continue

Les exigences énoncées au paragraphe 10.2 de l'ISO 27001 s'appliquent.

6. EXIGENCES LIEES A LA RELATION CONTRACTUELLE

6.1. Certificat de conformité

Exigence n° 20

[EXI 20] Conformément au 1° de l'article R.1111-1 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° 21

[EXI 21] 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. Pays d'hébergement – souveraineté des données

Exigence n° 22

[EXI 22] Le client doit être mis en mesure de choisir dans la liste des lieux d'hébergement proposés par l'Hébergeur, les pays dans lesquels ces données pourront être effectivement traitées. Conformément au 3° de l'article R1111-11 du CSP, une clause du contrat d'hébergement conclu entre l'hébergeur et son client doit mentionner l'indication des lieux d'hébergement choisis par le Client.

Exigence n° 23

[EXI 23] Les lieux d'hébergement proposés au Client par l'Hébergeur doivent être localisés dans des pays membres de l'Espace Economique Européen, ou des pays assurant un niveau de protection adéquat au sens de l'article 45 du RGPD, à l'exclusion des autres dispositions prévues aux articles 46 et 47 du RGPD.

6.4. Respect du droit des personnes concernées

Exigence n° 24

[EXI 24] Conformément au 4° de l'article R.1111-1 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 du droit des personnes concernées par les données de santé. Cette clause doit a minima comporter les mentions suivantes : les modalités d'exercice des droits de portabilité des données, les modalités de signalement au responsable de traitement de la violation des données à caractère personnel, les modalités de conduite des audits par le délégué à la protection des données.

6.5. Désignation d'un référent contractuel

Exigence n° 25

[EXI 25] Conformément au 5° de l'article R.1111-1 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 hébergée.

6.6. Les indicateurs de qualité et de performance

Exigence n° 26

[EXI 26] Conformément au 6° de l'article R.1111-1 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.

6.7. Recours à la sous-traitance

Exigence n° 27

[EXI 27] 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.

6.8. Accès aux données de santé à caractère personnel hébergées

Exigence n° 28

[EXI 28] 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.

6.9. Modifications ou évolutions techniques

Exigence n° 29

[EXI 29] 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 5.2 ;
- les garanties définies aux chapitres 5.3 et 5.4.

6.10. Garanties

Exigence n° 30

[EXI 30] 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.

6.11. Interdiction liée au traitement des données hébergées

Exigence n° 31

[EXI 31] 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.

6.12. Réversibilité

Exigence n° 32

[EXI 32] Conformément aux 12° à 14° de l'article R.1111-11 du CSP, une clause relative à la réversibilité doit présenter les modalités de réversibilité 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 procédures, coûts et délais pour cette restitution et la destruction 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. REPRESENTATION DES GARANTIES

Ce chapitre précise comment doivent être représentées les garanties prévues à l'article R.1111-11 du CSP.

Ces garanties se déclinent comme suit.

- L'identification de l'Hébergeur comme administrateur de la sécurité du service ;
- La liste des acteurs participant au service fourni ;
- La liste des instances des données de santé à caractère personnel utilisées ;
- La conformité des acteurs dans la prise en compte des objectifs de sécurité pour chaque instance
- la synthèse des risques résiduels
- Les chapitres suivants explicitent ces cinq parties.

7.1. Administrateur de la sécurité

L'administrateur de la sécurité du service est une organisation certifiée selon le présent référentiel. Il garantit et maintient dans la durée :

- La cohérence et de la complétude des garanties de sécurité apportées par les différents acteurs avec les objectifs de sécurité spécifiques du service numérique de santé.
- La véracité des rôles et des garanties exprimés dans la table de conformité.
- De la véracité de la synthèse des risques résiduels

7.2. Acteurs du service fourni

Outre l'administrateur de la sécurité ces acteurs sont tous les intervenants, certifiés ou pas, susceptibles de détenir, d'accéder ou de contrôler une instance des DSCP traitées dans le cadre du service. A chaque acteur on associe un code identifiant qui sera utilisé dans la table de conformité ainsi qu'un descriptif de son rôle.

7.3. Instances des données de santé

Depuis la collecte des DSCP jusqu'à leur présentation à des utilisateurs finaux, elles sont répliquées en un certain nombre d'instances. Plusieurs copies techniques, par exemple les données de production et leurs sauvegardes, peuvent représenter une même instance tant qu'elles sont sous le contrôle des mêmes acteurs selon la même politique de sécurité.

Pour chaque instance on précise quels acteurs y ont accès.

7.4. Conformité des acteurs

La conformité des acteurs dans la prise en compte des objectifs de sécurité est décrite dans une table dont :

- Les colonnes correspondent aux instances des données de santé
- Les lignes correspondent aux objectifs de sécurité

7.4.1. Objectifs de sécurité

Les objectifs de sécurité sont a minima les suivants (en réponse aux risques identités au chapitre 5.6.1.2) :

A. Sécurité physique et environnementale
   La sécurité physique et environnementale inclut notamment les contrôles d'accès physique, la sécurité des câblages et la continuité dans le maintien des conditions de fonctionnement des matériels (alimentation électrique, climatisation, etc.)
B. Maîtrise des supports matériels

La maîtrise des supports matériels concerne le maintien de leur sécurité lors d'interventions, de transferts ou de réaffectations.

C. Protection des flux d'information
Ceci concerne les flux au sein de l'instance, entre instances ou avec les utilisateurs et systèmes tiers, selon le niveau d'intervention de l'organisation. La sécurité des câblages relève de la sécurité physique et environnementale.

D. Maîtrise des accès
Il s'agit ici de l'attribution et du contrôle des accès logiques aux moyens de traitement ou de transfert de l'information. Les accès physiques relèvent de la sécurité physique et environnementale.

E. Maîtrise des interventions
Il s'agit ici de la planification et du contrôle des interventions des administrateurs autorisés sur les moyens de traitement ou de transfert de l'information, ainsi que sur les composants logiciels mis à disposition par l'organisation.

F. Robustesse aux usages imprévus, que ces usages proviennent de tiers privilégiés (par exemple d'autres clients de l'organisation) ou d'intrus

G. Garantie de continuité ou de reprise d'activité en cas de défaillance, selon les niveaux de service prévus par l'organisation

H. Protection contre des lois extra-européennes.

7.4.2. Conformité des acteurs

Chaque case de cette table précise les acteurs qui prennent en charge l'objectif de sécurité identifié en ligne pour l'interface identifiée en colonne.

Plusieurs acteurs peuvent contribuer à un même objectif sur une même instance. Par exemple, les sauvegardes peuvent être effectuées à la fois au niveau applicatif par l'acteur opérant une machine virtuelle et au niveau de la machine virtuelle elle-même.

Pour chacun de ces acteurs une couleur indique son niveau de conformité.

Les couleurs font partie de la représentation normalisée de la table de conformité :

Niveau	Description
Non conforme	L'acteur contribue à cet objectif, est soumis à l'obligation de certification et n'est pas actuellement certifié.
Exempté	L'acteur contribue à cet objectif mais n'est pas soumis à une obligation de certification selon le présent référentiel.
Certifié	Il peut également s'agir d'un sous-traitant agissant exclusivement sous le contrôle d'un acteur certifié.
Certifié et qualifié SecNumCloud	L'acteur contribue à cet objectif selon un SMSI formalisé et certifié conformément au présent référentiel

7.5. Commentaire

Le commentaire justifie en des termes intelligibles les particularités du tableau de synthèse et récapitule les éventuels risques résiduels qui ne seraient pas pris en charge par un acteur certifié. Il est rédigé sous la responsabilité de l'administrateur de la sécurité.

7.6. Représentation normalisée

Administrateur de la sécurité : _____

Acteurs du service

Code	Identité	Rôle
…		

Instances des données de santé

Code	Description	Acteurs
…		

Conformité dans la prise en compte des objectifs de sécurité

Légende	Non conforme	Exempté	Certifié HDS	Certifié HDS et qualifié SecNumCloud

A – Sécurité physique et environnementale			
B – Maîtrise des supports matériels			
C – Protection des flux d'information			
D – Maîtrise des accès			
E – Maîtrise des interventions			
F – Robustesse aux usages imprévus			
G – Continuité ou reprise d'activité			
H – Protection contre des lois extra-européennes			

Commentaire

…

8. SYNTHESE DES EXIGENCES

8.1. Conditions d'attribution d'un certificat

Exigence n° 01

[EXI 01] La certification d'une organisation nécessite :

- Qu'elle ait mis en œuvre un système de management de la sécurité de l'information certifié selon la norme ISO 27001, complétée des exigences définies au chapitre 5.
- Que les contrats conclus avec ses clients soient conformes aux exigences définies au chapitre 6 EXIGENCES LIEES A LA RELATION CONTRACTUELLE liées à la relation contractuelle et 7 REPRESENTATION DES GARANTIES.

8.2. Exigences relatives au SMSI

Exigence n° 02

[EXI 02] **Exigence supplémentaire par rapport au paragraphe 4.2 de l'ISO 27001**

Les parties intéressées doivent inclure :

- Les personnes dont les données de santé à caractère personnel (DSCP) sont hébergées (personnes concernées au sens de l'article 4 du RGPD).
- Les autres parties ayant des intérêts ou des responsabilités associées au traitement des DSCP, et notamment les professionnels assurant la prise en charge des personnes concernées.

Parmi les exigences des parties intéressées doivent figurer leurs exigences en termes de continuité, de disponibilité et de capacité des services de l'organisation, d'imputabilité des accès aux DSCP et de respect des dispositions du RGPD.

Exigence n° 03

[EXI 03] **Exigence supplémentaire par rapport au paragraphe 4.3 de l'ISO 27001**

Le domaine d'application du SMSI doit comprendre l'ensemble des traitements de DSCP assurés par l'organisation. 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° 04

[EXI 04] **Exigence supplémentaire par rapport au paragraphe 6.1.2 de l'ISO 27001**

Dans l'appréciation des risques, l'organisation doit considérer en priorité les risques encourus par la personne concernée en cas de perte d'intégrité, de confidentialité ou de disponibilité de ses DSCP. Ces risques comportent notamment la perte de chance liée à une prise en charge inappropriée, les risques de réputation ou de discrimination.

Elle doit également prendre en compte les risques encourus par les personnes et organisations assurant la prise en charge médicale de la personne concernée, y compris l'engagement de leur responsabilité médicale et les risques de réputation.

Lors de l'appréciation des risques, l'organisation doit a minima envisager les événements suivants :

A. Défaillance des supports matériels de l'information dues à des menaces physiques et environnementales.
B. Perte de contrôle de supports matériels de l'information, notamment à l'occasion :
    - de copies des DSCP sur des supports portables
    - de matérialisation (éventuelle) sous format documents papier
    - de réallocation des espaces de stockage
C. Défaut de protection des flux d'information internes ou externes sous la responsabilité de l'organisation.

D. Défaillance de la maîtrise des accès attribués, que ce soit aux personnels sous le contrôle de l'organisation où à ceux désignés par ses clients :
   - Attribution, modification et retrait des droits d'accès
   - Distribution des crédits
   - Traçabilité et imputabilité des accès
   - 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 l'incapacité à respecter les engagements de continuité ou de reprise d'activité.
H. Sujétion de l'organisation ou de ses éventuels sous-traitants à des législations extra-européennes pouvant entrainer une violation des DSCP.

Exigence n° 05

[EXI 05] **Exigence supplémentaire par rapport au paragraphe 6.1.3 de l'ISO 27001**

En cas de recours à la sous-traitance, l'organisation doit s'assurer qu'elle maîtrise les changements des mesures techniques et organisationnelles de ses sous-traitants permettant de traiter les risques identifiés.

Exigence n° 06

[EXI 06] **Exigence supplémentaire par rapport au paragraphe 6.1.3 de l'ISO 27001**

Pour toutes les mesures mises en œuvre et faisant l'objet d'une préconisation particulière du référentiel SecNumCloud (voir Annexe 2 : Matrice de correspondance avec SecNumCloud), la déclaration d'applicabilité doit en outre préciser si la mise en œuvre est conforme à cette préconisation.

Exigence n° 07

[EXI 07] **Exigence supplémentaire par rapport au paragraphe 6.2 de l'ISO 27001**

Les objectifs de sécurité doivent

- être établis en cohérence avec les exigences des parties intéressées.
- comporter l'imputabilité à des personnes physiques des accès aux DSCP et aux systèmes utilisés pour leur traitement. Cette imputabilité concerne toutes les personnes opérant pour le compte de l'organisation ainsi que les intervenants occasionnels mandatés par ses clients. L'imputabilité des accès des administrateurs réguliers des clients relève de la responsabilité de chaque client, même lorsque l'organisation y contribue.
- comporter le respect des obligations du RGPD.

Exigence n° 08

[EXI 08] **Précision au paragraphe 7.3 de l'ISO 27001**

Les contrats de travail des personnels travaillant pour l'organisation doivent inclure une clause de confidentialité. En cas de recours à la sous-traitance, cette exigence s'applique également aux sous-traitants.

Exigence n° 09

[EXI 09] **Exigence supplémentaire par rapport au paragraphe 7.4 de l'ISO 27001**

L'organisation doit prendre en compte les obligations légales et réglementaires de communication des incidents de sécurité s'appliquant aux utilisateurs de ses services et leur fournir les moyens d'y satisfaire.

Exigence n° 10

[EXI 10] **Exigence supplémentaire par rapport au paragraphe 7.4 de l'ISO 27001**

L'organisation doit communiquer à son client et au responsable de traitement des DSCP :

- Les lois extra-communautaires auxquelles l'Hébergeur est soumis.
- Les mesures mises en œuvre par l'Hébergeur pour atténuer les risques de violation des DSCP induits par ces lois.
- La description des risques résiduels.

Exigence n° 11

[EXI 11] **Exigence supplémentaire par rapport au paragraphe 7.4 de l'ISO 27001**

L'organisation 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 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] **Précision au paragraphe 7.5.3 de l'ISO 27001**

Les durées de conservation des différentes versions des informations documentées constituant la politique de sécurité doivent être définies et formalisées

Exigence n° 13

[EXI 13] **Exigence supplémentaire par rapport au paragraphe 7.5 de l'ISO 27001**

Lorsque des informations documentées sont échangées avec le client, ces informations doivent être la langue de travail choisie par celui-ci.

Les informations documentées comprennent les informations définies dans le chapitre 7.5 de l'ISO 27001, les interfaces, le support de premier niveau, une déclaration d'applicabilité dans la langue de travail et la représentation des garanties telle que décrite au chapitre 7

Exigence n° 14

[EXI 14] **Précision par rapport au paragraphe 8.1 de l'ISO 27001**

Les modifications prévues intègrent notamment toutes les modifications des moyens à l'initiative de l'organisation.

Les modifications imprévues intègrent notamment toutes les altérations des ressources mises à disposition par l'organisation, ainsi que tous les changements de leur usage, à l'initiative des bénéficiaires de ces ressources

.

Exigence n° 15

[EXI 15] **Exigence supplémentaire par rapport au paragraphe 8.1 de l'ISO 27001**

L'organisation doit s'assurer qu'elle maintient les garanties de sécurité de l'information :

- Lors de modifications prévues, comme la délivrance du service à de nouveaux clients.
- Lors de modifications imprévues, comme les modifications de configuration ou d'usage du service par un client. De telles modifications peuvent entraîner des répercussions sur les services auxquels il a souscrit, mais éventuellement aussi sur ceux rendus aux autres clients

Exigence n° 16

[EXI 16] **Exigence supplémentaire par rapport au paragraphe 8.1 de l'ISO 27001**

L'organisation doit s'assurer qu'elle dispose des documentations que le client doit lui fournir pour lui permettre d'assurer son service dans le respect de ses objectifs de sécurité.

Exigence n° 17

[EXI 17] **Exigence supplémentaire par rapport au paragraphe 8.3 de l'ISO 27001**

L'organisation, si elle délègue une partie du traitement des DSCP à un fournisseur certifié HDS, doit avoir défini une procédure de traitement du risque de perte ou de suspension de la certification dudit fournisseur.

Exigence n° 18

[EXI 18] **Exigence supplémentaire par rapport au paragraphe 9.1 de l'ISO 27001.**

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 un rapport d'audit externe indépendant datant de moins de trois ans sur les ressources mutualisées participant au service rendu.
- 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° 19

[EXI 19] **Exigence supplémentaire par rapport au paragraphe 9.2 de l'ISO 27001**

Les audits internes effectués par l'organisation doivent comprendre a minima :

- Un audit de conformité et de bon fonctionnement de son SMSI
- 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.

8.3. Exigences liées à la relation contractuelle

Exigence n° 20

[EXI 20] Conformément au 1° de l'article R.1111-1 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.

Exigence n° 21

[EXI 21] 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° 22

[EXI 22] Le client doit être mis en mesure de choisir dans la liste des lieux d'hébergement proposés par l'Hébergeur, les pays dans lesquels ces données pourront être effectivement traitées. Conformément au 3° de

l'article R1111-11 du CSP, une clause du contrat d'hébergement conclu entre l'hébergeur et son client doit mentionner l'indication des lieux d'hébergement choisis par le Client.

Exigence n° 23

[EXI 23] Les lieux d'hébergement proposés au Client par l'Hébergeur doivent être localisés dans des pays membres de l'Espace Economique Européen, ou des pays assurant un niveau de protection adéquat au sens de l'article 45 du RGPD, à l'exclusion des autres dispositions prévues aux articles 46 et 47 du RGPD.

Exigence n° 24

[EXI 24] Conformément au 4° de l'article R.1111-1 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 du droit des personnes concernées par les données de santé. Cette clause doit a minima comporter les mentions suivantes : les modalités d'exercice des droits de portabilité des données, les modalités de signalement au responsable de traitement de la violation des données à caractère personnel, les modalités de conduite des audits par le délégué à la protection des données.

Exigence n° 25

[EXI 25] Conformément au 5° de l'article R.1111-1 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 hébergée.

Exigence n° 26

[EXI 26] Conformément au 6° de l'article R.1111-1 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° 27

[EXI 27] 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.

Exigence n° 28

[EXI 28] 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° 29

[EXI 29] 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 5.2 ;
- les garanties définies aux chapitres 5.3 et 5.4.

Exigence n° 30

[EXI 30] 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° 31

[EXI 31] 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° 32

[EXI 32] Conformément aux 12° à 14° de l'article R.1111-11 du CSP, une clause relative à la réversibilité doit présenter les modalités de réversibilité 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 procédures, coûts et délais pour cette restitution et la destruction 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.

Annexe 1 : Exemple de représentation des garanties

Les données de cette représentation sont uniquement des exemples permettant d'en illustrer la forme.

Administrateur de la sécurité : Fournisseur Bravo

Acteurs du service

Code	Identité	Rôle
Alpha	Fournisseur Alpha	Opérateur du service numérique en santé En contrat direct avec le responsable de traitement
Bravo	Fournisseur Bravo	Sous-traitant de Alpha Administrateur unique du service
Charlie	Fournisseur Charlie	Sous-traitant de Bravo

Instances des données de santé

Code	Description	Acteurs
PRIM	Site primaire	Alpha, Bravo
BACK	Sauvegardes	Bravo, Charlie

Conformité dans la prise en compte des objectifs de sécurité

Légende	Non conforme	Exempté	Certifié HDS	Certifié HDS et qualifié SecNumCloud

	PRIM	BACK
A – Sécurité physique et environnementale	Bravo	Charlie
B – Maîtrise des supports matériels	Bravo	Bravo Charlie
C – Protection des flux d'information	Alpha Bravo	Bravo
D – Maîtrise des accès	Alpha Bravo	Bravo Charlie
E – Maîtrise des interventions	Alpha Bravo	Bravo Charlie
F – Robustesse aux usages imprévus	Alpha Bravo	Bravo

	PRIM	BACK
G – Continuité ou reprise d'activité	Alpha Bravo	Bravo
H – Protection contre des lois extra-européennes	Alpha Bravo	Bravo Charlie

Commentaire

Dans cet exemple, on pourrait rappeler pourquoi Alpha est exempté de certification.

Annexe 2 Matrice de correspondance avec SecNumCloud

Comme prévu au 5.6.1.35.6.1, l'organisation peut choisir de revendiquer la conformité au référentiel d'exigences SecNumCloud dans la mise en œuvre de tout ou partie des mesures de l'annexe A à l'ISO 27001.

La table de correspondance ci-dessous explicite pour chaque mesure de l'annexe A quels chapitres d'exigences dans SecNumCloud doivent être respectés pour une telle revendication.

La mise en œuvre d'une mesure selon SecNumCloud n'atteste pas de l'efficacité de celle-ci pour atteindre les objectifs de sécurité propres au contexte de l'organisation. L'appréciation de l'efficacité des mesures reste de la responsabilité de l'organisation.

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 – Relations avec les autorités	6.3 – Relations avec les autorités
5.6 – Relations avec les groupes de travail spécialisés	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 de l'information et des actifs associés	8.1 – Inventaire et propriété des actifs
5.10 – Utilisation correcte de l'information ou des 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 – Transferts d'information	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 secrètes 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 – Chaîne d'approvisionnement des produits et des services informatiques	15.1 – Identification des tiers 15.3 – Surveillance et revue des services des tiers
5.22 – Surveillance, revue et gestion des changements des services des fournisseurs	15.3 – Surveillance et revue des services des tiers
5.23 – Sécurité de l'information pour les 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 – Préparation et planification du management des incidents	16.1 – Responsabilités et procédures
5.25 – Appréciation des événements liés à la 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 liés à la sécurité de l'information	16.4 – Réponse aux incidents liés à la sécurité de l'information
5.27 – Tirer des enseignements des incidents liés à la 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

Mesure Annexe A	Exigences SecNumCloud applicables
5.29 – Continuité de la sécurité de l'information	Pas d'exigence liée
5.30 – Disponibilité des TIC pour la continuité d'activité	17.4 – Disponibilité des moyens de traitement de l'information
5.31 – Exigences légales, 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	19.5 – Protection des données à caractère personnel
5.35 – Revue indépendante de la sécurité de l'information	18.2 – Revue indépendante de la sécurité de l'information
5.36 – Conformité avec les politiques, les règles et les 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 – Achèvement ou modification des responsabilités associées à un contrat de travail	7.5 – Rupture, terme ou modification du contrat de travail
6.6 – Engagements de confidentialité ou de non-divulgation	15.5 – Engagements de confidentialité
6.7 – Télétravail	12.12 – Administration (c) 12.13 – Télédiagnostic et télémaintenance des composants de l'infrastructure
6.8 – Signalement des événements liés à la 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 – Contrôle d'accès physique	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 – Politique du bureau propre et de l'écran verrouillé	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 – Gestion des supports de stockage	11.8 – Sortie des actifs
7.11 – Services généraux	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 des matériels	11.7 – Maintenance des matériels
7.14 – Mise au rebut ou réutilisation des supports	11.9 – Recyclage sécurisé du matériel
8.1 – Terminaux des utilisateurs	12.12 - Administration
8.2 – Gestion des droits d'accès à privilèges	9.3 – Gestion des droits d'accès
8.3 – Restriction d'accès à l'information	9.7 – Restriction des accès à l'information
8.4 – Accès aux codes sources des programmes	Pas d'exigence liée
8.5 – Authentification sécurisée	9.5 – Gestion des authentifications des utilisateurs

Mesure Annexe A	Exigences SecNumCloud applicables
8.6 – Dimensionnement des ressources	Pas d'exigence liée
8.7 – Mesures contre les logiciels malveillants	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 – Effacement des informations	11.9 – Recyclage sécurisé du matériel 19.4 – Fin de contrat
8.11 – Masquage de données	Pas d'exigence liée
8.12 – Protection contre les fuites 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 – Supervision	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 en exploitation	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 de 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 des accès Internet	13.2 – Cloisonnement des réseaux (c)
8.24 – Mesures cryptographiques	10.4 – Non-répudiation 10.5 – Gestion des secrets 10.6 – Racines de confiance
8.25 – Politique 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 de la sécurité des systèmes	Pas d'exigence liée
8.28 – Codage sécurisé	18.2.2 – Revue initiale 18.2.3 – Revue des changements majeurs
8.29 – Test de la sécurité du système en développement et en recette	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 d'exploitation	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 – Protection des données de test	14.7 – Protection des données de test
8.34 – Protection des systèmes d'information durant les tests d'audit	Pas d'exigence liée

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

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