AGENCE DU NUMÉRIQUE EN SANTÉ



Hébergement des données de santé : cadre applicable et évolutions

Session Collective

07/10/2026

AGENCE DU NUMÉRIQUE EN SANTÉ

Sommaire

Enjeux et cadre règlementaire

Champ d'application

Mise en œuvre pour un hébergeur : les exigences

Mise en œuvre pour un client : les points d'attention

Point d'actualité

AGENCE
DU NUMÉRIQUE
EN SANTÉ



Enjeux et cadre règlementaire

Cadre règlementaire certification HDS



Art. L.1111-8 *Loi*

Champ d'application
Obligation préalable de certification HDS
Cession des données de santé

Art. R.1111-8-8, R.1111-9 à R1111-11
décret en Conseil d'Etat et avis CNIL

Arrêté du 26 avril 2024

Référentiel de certification HDS

Référentiel d'accréditation des organismes certificateurs

- Toute personne qui **héberge des données de santé à caractère personnel** recueillies à l'occasion d'activités de **prévention, de diagnostic, de soins ou de suivi social et médico-social**, **pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même**
- **L'hébergeur** de données sur support numérique **est titulaire d'un certificat de conformité**.
- Sanctions en **cas de cession à titre onéreux de données de santé** identifiantes ou indirectement identifiantes y compris avec l'accord du patient
- Les activités d'hébergement de données de santé
- Exclusion : cas des données confiées pour un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données (pour une courte durée)
- Les mentions à stipuler dans un contrat d'hébergement

Cadre règlementaire certification HDS

Art. R.1111-10
décret en Conseil d'Etat et avis CNIL

Rôles des acteurs du dispositif

- Rédaction du référentiel HDS et publication de la liste des hébergeurs certifiés : **ANS**

  9 OC (octobre 2026)

- Vérification de conformité aux exigences et délivrance de certificat HDS : **Organismes certificateurs**

  421 certificats (octobre 2026)

- Accrédication des organismes certificateurs : **Comité français d'accréditation** (COFRAC)

AGENCE
DU NUMÉRIQUE
EN SANTÉ



Champ d’application

Comment déterminer qui doit être certifié

1) Etre hébergeur **pour le compte** d'une personne **(qui peut être le patient/usager) …**

2) de **données de santé à caractère personnel**…

3) recueillies **à l'occasion de prévention, soins, suivi social ou médico-social…**

4) dans le cadre d'une des **6 activités** encadrées par le référentiel HDS

Mise à disposition et maintien en condition opérationnelle	sites physiques	Activité 1
	Infrastructures matérielles	Activité 2
	Infrastructures virtuelles	Activité 3
	plateforme d'hébergement d'applications	Activité 4
Administration et l'exploitation du système d'information		Activité 5
Sauvegarde des données de santé notamment dans le cadre d'un archivage		Activité 6

Pour chacune des activités, il convient d'identifier quel(s) acteur(s) la réalise(nt)

Chaque acteur identifié doit être certifié pour la(es)'activité(s) qu'il réalise

AGENCE DU NUMÉRIQUE EN SANTÉ



Mise en œuvre pour un hébergeur

Les exigences

Mise en œuvre pour un hébergeur – démarche

Prendre connaissance du référentiel de certification HDS
profil : responsable de la sécurité des systèmes d'information, DPO

Phase de préparation
profil : responsable de la sécurité des systèmes d'information, DPO
Se mettre en conformité avec les exigences (moyenne de 9/12 mois de mise en conformité en fonction de la maturité en sécurité)

- Certification 27001

Documenter a minima : le domaine d'application, la politique de sécurité, l'analyse de risques et le plan de traitement des risques, la déclaration d'applicabilité des exigences, le plan de traitement des risques et les rapports d'audit interne

- Exigences spécifiques HDS dont :
  - 15 exigences spécifiques à traiter dans le cadre de la certification 27001
  - 13 exigences contractuelles
  - 4 exigences liées à des enjeux de souveraineté

Mise en œuvre pour un hébergeur – démarche

Sélectionner un des organismes certificateurs accrédités pour HDS

Certification

- Audit initial (documentaire et sur site)
  Planifier au plus tôt les audits sur site / disponibilité des personnes interviewées
- Audit(s) complémentaire(s) pour lever des non-conformités,
- Délivrance du certificat HDS dont la validité est de 3 ans
- Audit de surveillance annuel

Nota bene
La gestion de la sécurité n'est pas un projet mais une activité continue. Lors du renouvellement de la certification HDS, l'amélioration continue de cette gestion de la sécurité sera évaluée.

Mise en œuvre pour un hébergeur – les exigences spécifiques

Trois exigences portent sur le domaine d'application du système de management de la sécurité de l'information qui doit prendre en compte de manière explicite le fait que l'hébergeur héberge des données de santé à caractère personnel

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	Complément au chapitre 4 de l'ISO 27001

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.	Complément au chapitre 4 de l'ISO 27001

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.	Complément au chapitre 4 de l'ISO 27001

Mise en œuvre pour un hébergeur – les exigences spécifiques

Une exigence porte sur l'analyse de risques qui doit prendre en compte de manière explicite a minima les risques identifiés dans le référentiel HDS

Exigence n° 05

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

A. Défaillance des supports matériels de l'information due à des menaces physiques et environnementales.

B. Perte de contrôle de supports matériels de l'information, notamment à l'occasion :

   a. De copie des DSCP sur des supports portables ;

   b. De matérialisation éventuelle sous format documents papier ;

   c. De réallocation des espaces de stockage.

C. Dégradation, compromission ou rupture d'un flux d'information interne ou externe sous la responsabilité de l'Hébergeur.

D. Défaillance de la maîtrise des accès attribués, que ce soit aux personnels sous le contrôle de l'organisation ou à ceux désignés par ses clients :

   a. Attribution, modification et retrait des droits d'accès ;

   b. Distribution des moyens d'identification électroniques ;

   c. Traçabilité et imputabilité des accès ;

   d. Accès occasionnels lors des audits et tests d'intrusion.

E. Défaillance de la maîtrise des interventions, qu'elles soient à l'initiative de l'organisation ou commanditées par un client.

F. Usages imprévus du service, par maladresse ou malveillance.

G. Défaillances matérielles ou logicielles, avec incapacité à respecter les engagements de continuité ou de reprise d'activité.

H. Sujétion de l'Hébergeur ou des éventuels sous-traitants à des législations extra-européennes pouvant entrainer une violation des DSCP.

Version en cours

Complément au chapitre 6 de l'ISO 27001

Mise en œuvre pour un hébergeur – les exigences spécifiques

Quatre exigences portent sur le plan de traitement des risques

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.	Complément au chapitre 6 de l'ISO 27001
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	Complément au chapitre 6 de l'ISO 27001
Exigence n° 08 [EXI 08] La déclaration d'applicabilité doit être disponible en langue française pour les auditeurs qui en feront la demande.	Complément au chapitre 6 de l'ISO 27001
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.	Complément au chapitre 6 de l'ISO 27001

Présentation

Mise en œuvre pour un hébergeur – les exigences spécifiques

Trois exigences portant sur les besoins de sensibilisation du personnel de l'Hébergeur et les besoins de communication entre l'Hébergeur et ses clients

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.

Complément au chapitre 7 de l'ISO 27001

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.

Complément au chapitre 7 de l'ISO 27001

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.

Complément au chapitre 7 de l'ISO 27001

Version de consultation

Mise en œuvre pour un hébergeur – les exigences spécifiques

Deux exigences portent sur l'évaluation de la performance du SMSI

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.

Complément au chapitre 9 de l'ISO 27001

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.

Complément au chapitre 9 de l'ISO 27001

Mise en œuvre pour un hébergeur – les exigences spécifiques

13 exigences contractuelles qui correspondent à des obligations (article R.1111-11 du Code de la Santé Publique)

Exemple

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.

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036658473/2022-01-01

Code de la santé publique

Réduire

EN VIGUEUR DEPUIS LE 19 AVRIL 2026

Sous-section 2 : Hébergement des données de santé à caractère personnel sur support numérique soumis à certification

Version à la date d'aujourd'hui

Article R1111-11

VERSION EN VIGUEUR DU 01 AVRIL 2018 AU 26 SEPTEMBRE 2026

Modifié par Décret n°2018-137 du 26 février 2018 - art. 2

I.-Le contrat d'hébergement mentionné au dernier alinéa du I de l'article L. 1111-8 est conclu entre l'hébergeur et son client. Il contient au moins les clauses suivantes :

1° L'indication du périmètre du certificat de conformité obtenu par l'hébergeur, ainsi que ses dates de délivrance et de renouvellement ;

Mise en œuvre pour un hébergeur – les exigences spécifiques

Quatre exigences pour renforcer la protection des données personnelles au regard des risques de transferts de données hors de l'Espace économique européen



- **Localisation obligatoire des infrastructures de stockage des données dans l'EEE** — *exigence 28*



- **Transparence renforcée**
  - Entre l'hébergeur et ses clients : Communications obligatoires de l'hébergeur vers ses clients — *exigences 29 et 30*



  - Entre l'hébergeur, les futurs clients et le public : Tableau à mettre en ligne par l'hébergeur — *exigence 31*

AGENCE DU NUMÉRIQUE EN SANTÉ



Mise en œuvre pour un client

Les points d’attention

Mise en œuvre pour un client

En cas de recours à un tiers pour héberger des données de santé vérifier que ce tiers est certifié HDS

Points à vérifier dans le contrat

- Présence d'une description des prestations réalisées, comprenant le contenu des services et résultats attendus notamment aux fins de garantir la sécurité des données (exigence 18 et 2° de l'art. R1111-11 du CSP)
- Présence d'une description du périmètre du certificat de conformité obtenu par l'Hébergeur, ainsi que ses dates de délivrance et de renouvellement (exigence 17 et 1° de l'art. R1111-11 du CSP)

Vérifier que

- Le certificat est toujours valide (en consultant le site de l'ANS ou en interrogeant l'organisme certificateur)
- Les prestations réalisées sont dans le périmètre du certificat
  A titre d'exemple : dans le cadre d'un contrat HDS, le stockage des données est obligatoirement au sein de l'Espace Economique Européen (EEE).

AGENCE
DU NUMÉRIQUE
EN SANTÉ



Actualités

Evolution du référentiel HDS

Loi SREN et évolution référentiel certification HDS 2.0 => 2.1



A partir de mars 2027, les contrats devront comporter de nouvelles mentions : anticiper leur mise à jour dès aujourd'hui !

Retrouvez une description exhaustive des impacts de la nouvelle version ici

https://esante.gouv.fr/webinaires/certification-hds-avancement-transition-v2-et-point-d-actualite-sur-la-publication-du-decret-sren

Merci d'avoir suivi ce webinaire !

Nous vous invitons à répondre à ce rapide questionnaire et nous laisser votre avis

Hébergement des données de santé : cadre applicable et évolutions

07/10/2026



Un besoin ? Une question ?
Ecrivez-nous : innovation@esante.gouv.fr

Abonnez-vous à notre page LinkedIn dédiée aux entreprises du numérique en santé : Engagé pour la e-santé