Certification des Hébergeurs des données de santé : tout savoir sur les fondamentaux

Frédéric Law-Dune et Emmanuel Clout

Les intervenants

Frédéric Law-Dune
Responsable de projets
ANS

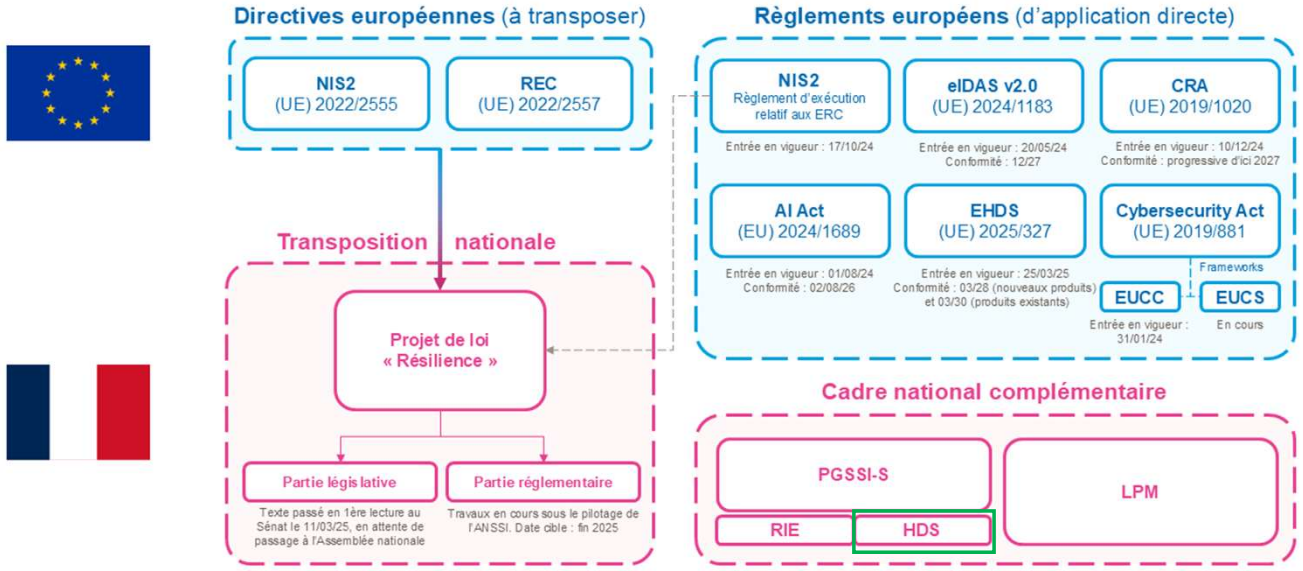
Emmanuel Clout
Directeur de projets
DNS

Sommaire

Enjeux et cadre règlementaire

Réglementation en matière de cybersécurité et enjeux d'une réglementation sectorielle santé, médico-social et social

- **Panorama de la réglementation en matière de cybersécurité**



- **Pourquoi une réglementation complémentaire sectorielle santé, médico-social, social ?**
  - Partage / échange de données de santé => amélioration de la prise en charge
  - Pré-requis au partage/échange : confiance des utilisateurs (patients / professionnels) dans le numérique en santé
  - Niveau très élevé de confidentialité, intégrité, disponibilité, imputabilité des services numériques en santé
  - Contexte d'évolution des attaques cyber dans le secteur de la santé (opportuniste / solutions les plus vulnérables => groupe d'attaquants qui cible les données de santé)

Cadre règlementaire certification HDS

RGPD
mai 2018

Art. L.1111-8 *Loi* Juillet 2018

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

- 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

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

- Les activités d'hébergement de données de santé
- Exclusion : cas des données confiées pour une courte période par les personnes physiques ou morales pour un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données.
- Les mentions à stipuler dans un contrat d'hébergement

Arrêté du 26 avril 2024

Référentiel de certification HDS v2.0

Référentiel d'accréditation des organismes certificateur v2.0

Objectifs

Objectifs

- Pour un client
  - Garantir la bonne gestion de la sécurité de l'hébergement des données de santé recueillies à l'occasion d'une prise en charge confiées à un Hébergeur
  - Depuis la version 2 du référentiel HDS, garantir la transparence au regard des risques de transfert de données en raison de lois extra européennes pour un choix éclairé de son Hébergeur
- Pour un Hébergeur
  - Reconnaissance de la maîtrise de leur gestion de la sécurité adaptée à l'hébergement de données de santé au-delà du territoire national
  - Conformité règlementaire
    La sanction en cas d'hébergement de données de santé à caractère personnel sans certification prévu à l'article L.1111-5-1 du Code de la Santé Publique est de 45k€ d'amende et 3 ans d'emprisonnement

Champ d’application

Comment savoir 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 des fins 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

Méthode

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

Mise en œuvre pour un hébergeur

Mise en œuvre – pour un hébergeur

- Prendre connaissance du référentiel de certification HDS (profil : responsable de la sécurité des systèmes d'information, DPO)
- Phase de préparation
  Se mettre conformité avec les exigences (profil : responsable de la sécurité des systèmes d'information, DPO) – moyenne de 9/12 mois de mise en conformité en fonction de votre maturité
  - 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
    - 3 exigences liées à des enjeux de souveraineté

Mise en œuvre – pour un hébergeur

- Sélectionner un des organismes certificateurs accrédités pour HDS

- Processus général de certification (3/4 mois minimum, 3 à 6 mois de plus en cas de non-conformité)
  - Audit initial (documentaire et sur site)
    Planifier au plus tôt les audits sur site
  - Le cas échéant, 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.

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

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

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

Deux exigences portent sur le fonctionnement du SMSI

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.

Complément au chapitre 8 de l'ISO 27001

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.

Complément au chapitre 8 de l'ISO 27001

Mise en œuvre – pour un hébergeur

Les exigences contractuelles

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.

Mise en œuvre – pour un hébergeur

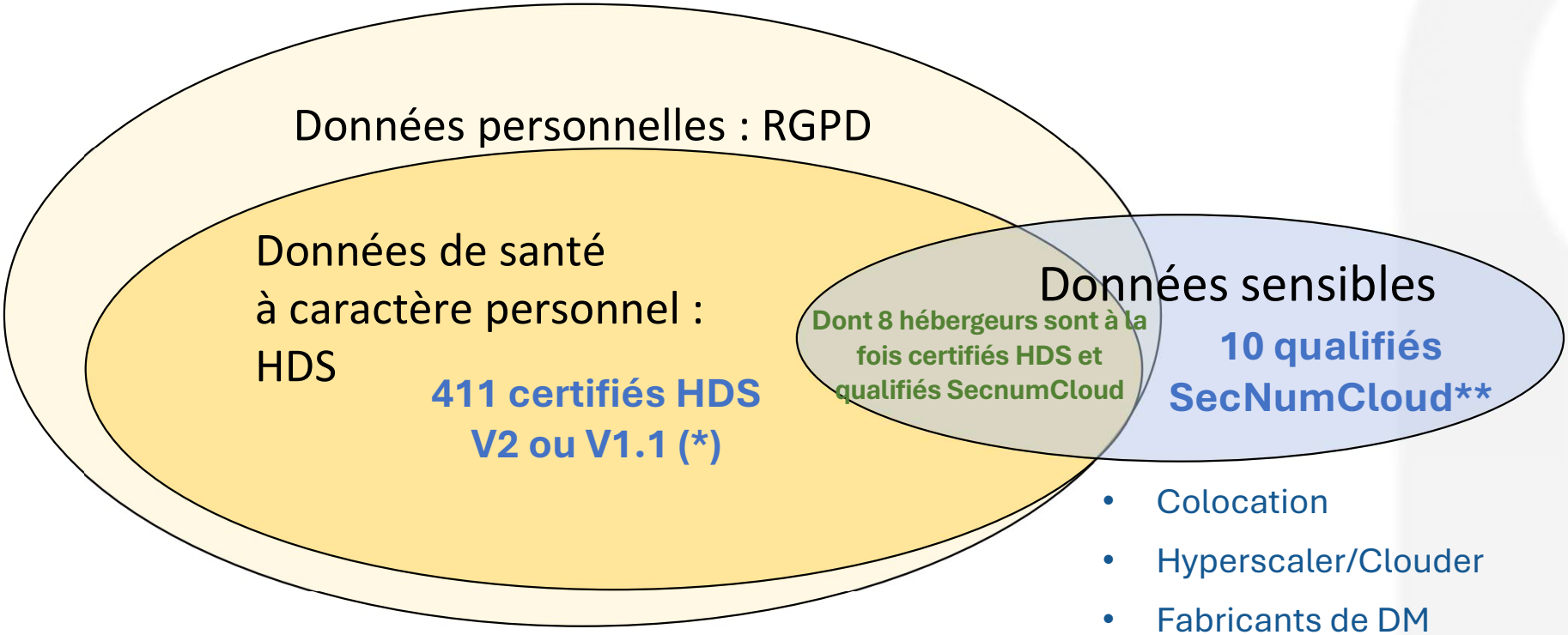
Focus sur l'amélioration de la visibilité en cas de sous-traitance ultérieure

En cas de recours par un Hébergeur à un sous-traitant ultérieur :

- l'Hébergeur reste **responsable de l'ensemble du périmètre** de la prestation d'hébergement (notamment la partie sous-traitée). La certification HDS de l'Hébergeur doit porter sur l'ensemble du périmètre (y compris les parties confiées au sous-traitant ultérieur) (Exigence 06)
- **Les mesures de sécurité relatives aux fournisseurs de l'ISO 27001 s'appliquent.**
  Il convient de noter que le recourt à un sous-traitant ultérieur certifié HDS simplifie le respect de ces mesures
- L'Hébergeur doit **faire figurer les sous-traitants ultérieurs dans la représentation des garanties**, montrant la participation réelle de chacun dans la prestation d'hébergement et les risques d'accès aux données de santé (Exigence 01)

Mise en œuvre pour un client

Quelques chiffres clés de la certification HDS



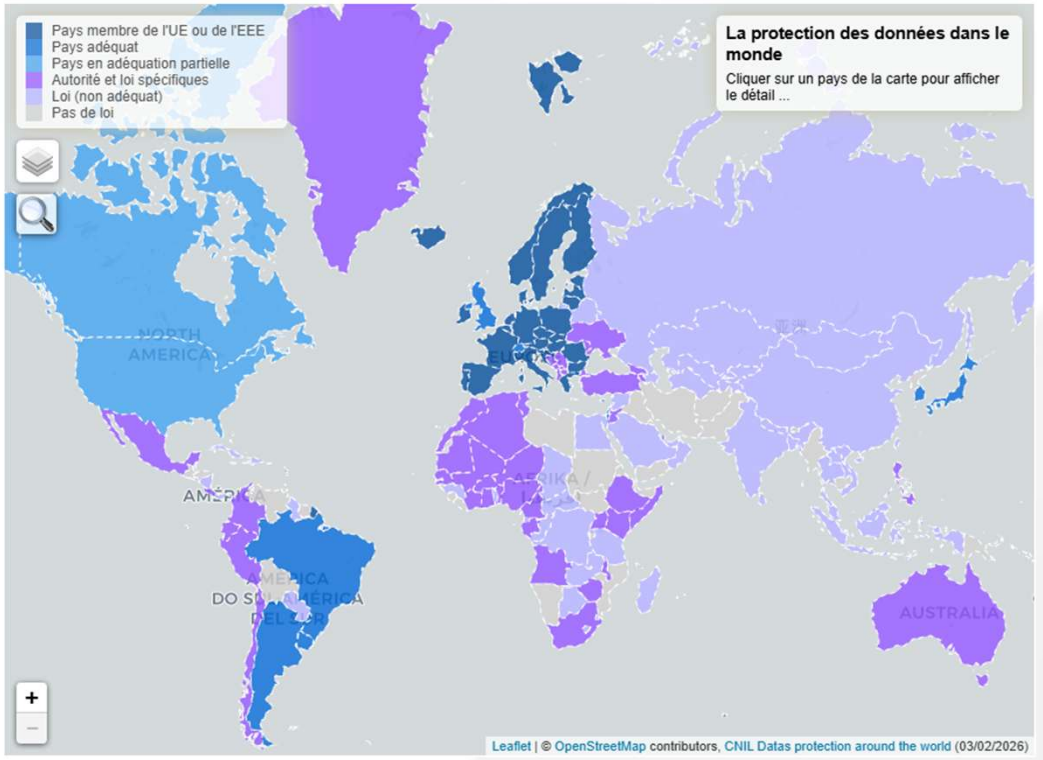
- Colocation
- Hyperscaler/Clouder
- Fabricants de DM
- Editeur de service numérique en santé
- ES/ESMS
- Start up

*Liste de fin avril 2026

**Liste du 12 mai 2026

Exigences de souveraineté des données

- **'Souveraineté' : autonomie d'actions, maîtrise des dépendances financières, réglementaires, technologiques,...**
- **Objectifs du référentiel HDS : "souveraineté des données"**
  - Renforcer la maîtrise des risques d'accès aux données de santé à caractère personnel depuis des pays tiers à l'Espace Economique Européen (EEE)
- **Risques de transfert aux données de santé vers des pays hors EEE :**
  - **En raison des activités d'hébergement**
  - **En raison de la réglementation en vigueur dans les pays hors EEE**
    - Faisant l'objet d'une décision d'adéquation prévue par le RGPD (article 45 RGPD) : pas d'autorisation de transfert préalable
    - Sans décision d'adéquation : transferts possibles moyennant des garanties appropriées prévues par le responsable du traitement ou le sous-traitant et à condition que les personnes concernées disposent de droits opposables et de voies de droit effectives (article 46 du RGPD)
    - Cas particulier des Etats-Unis pour lesquels il existe une décision d'adéquation
      - Cloud Act (2018) : obliger par décision de justice les fournisseurs de service établis sur le territoire des Etats-Unis, par mandat ou assignation, à transmettre les données relatives aux communications électroniques de ses clients, stockées sur des serveurs, qu'ils soient situés aux Etats-Unis ou dans des pays étrangers.
      - Section 702 du Foreign Intelligence Surveillance Act (FISA) : obligation pour des fournisseurs domiciliés aux Etats-Unis de services cloud de fournir aux agences américaines de renseignement des données personnelles étrangères stockées sur des serveurs gérés par ces fournisseurs en respectant une clause de confidentialité



Source : La protection des données dans le monde | CNIL

Besoin pour les clients de distinguer les hébergeurs soumis à des réglementations extraterritoriales d'accès aux données de santé à caractère personnel

Exigences de souveraineté des données

=> Renforcement des exigences de 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 : Mentions obligatoires ajoutées au **contrat** — *exigences 29, 23-3 et 23-2*
  - Entre l'hébergeur, les futurs clients et le public : Tableau à mettre en ligne par l'hébergeur sur son **site internet** — *exigence 31*

Exigences de souveraineté des données

=> Renforcement des exigences de protection des données personnelles au regard des risques de transferts de données hors de l'Espace économique européen

- **Transparence renforcée** entre l'hébergeur et ses clients dans les contrats :

exigence 29

  - Si la prestation d'hébergement implique un transfert y compris un **accès à distance** sans stockage (à des fins de support, par exemple) dans un pays extracommunautaire :
    - L'accès doit être fondé sur une décision d'adéquation de la Commission adoptée en vertu de l'article 45 du RGPD ;
    - En l'absence de décision d'adéquation: des garanties appropriées au sens de l'article 46 du RGPD sont mises en mise en place pour encadrer ce transfert ou toute autre mesure permettant de d'assurer un niveau de protection des données équivalent à celui garanti par le droit de l'Union Européenne.

    => La décision d'adéquation, les garanties appropriées, les mesures mises en oeuvre sont précisées dans le contrat

Exigences de souveraineté des données

=> Renforcement des exigences de protection des données personnelles au regard des risques de transferts de données hors de l'Espace économique européen

- **Transparence renforcée** entre l'hébergeur et ses clients dans les contrats :
  - si l'Hébergeur n'est **soumis à aucune législation** d'un pays tiers lui imposant un transfert de données de santé à caractère personnel — exigence 23-3
  - si l'Hébergeur ou l'un de ses sous-traitants est **soumis à la législation d'un pays tiers** qui n'est pas membre de l'Union européenne ou partie à l'Espace économique européen : — exigence 23-2
    - **la liste des réglementations extra-européennes** en vertu desquelles l'hébergeur ou l'un de ses sous-traitants intervenant dans la prestation d'hébergement est tenu de permettre un transfert de données ou un accès non autorisé aux données de santé à caractère personnel, au sens de l'article 48 du même règlement (transfert fondée sur un accord international / entraide judiciaire);
    - le cas échéant, la **décision d'adéquation** prise en vertu de l'article 45 du règlement n° 2016/679 du 27 avril 2016 ;
    - en l'absence de décision d'adéquation,
      - d'une part, **les mesures mises en œuvre** par l'Hébergeur pour atténuer les risques de transfert de données ou d'accès non autorisé aux données de santé à caractère personnel induits par ces réglementations extra-européennes et,
      - d'autre part, **la description des risques résiduels** de transfert de données à caractère personnel ou d'accès non autorisé à ces données malgré ces mesures.

Exigences de souveraineté des données

=> Renforcement des exigences de protection des données personnelles au regard des risques de transferts de données hors de l'Espace économique européen

- **Transparence renforcée** entre l'hébergeur, les futurs clients et le public
  - L'hébergeur doit **rendre public et mettre à jour un descriptif détaillé de tout transfert de données de santé** à caractère personnel hors EEE ainsi que toute soumission à un risque d'accès à ses données au titre d'une législation étrangère
  - Un tableau devra être mis en ligne et tenu à jour par l'hébergeur. Le site internet de l'ANS pointera vers le tableau des risques de tous les hébergeurs certifiés HDS

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 : 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 :

Mise en œuvre – pour un client

Identifier pour les sous-traitants Hébergeurs qui réalisent tout ou partie des activités d'hébergement.

Exiger de leur part d'être certifiés HDS a minima pour les activités d'hébergement nécessaires à la prestation qu'ils vous fournissent et le vérifier soit

- En consultant la liste publiée sur le site de l'ANS des Hébergeurs avec la liste les activités concernées et le lien vers les risques en matière de transfert des données hors EEE.
- En demandant ces informations aux Hébergeurs qui ont l'obligation de vous les fournir.

Cas particulier des Hébergeurs en cours de certification.

La certification HDS est requise dès lors qu'il y a hébergement de données de santé réelles.

A l'issue d'un appel d'offres, il est possible de retenir un Hébergeur qui n'est pas encore certifié HDS et de le faire héberger les environnements qui contiennent des données fictives (ex environnement de développement)

Néanmoins, cet Hébergeur devra être certifié avant de pouvoir héberger un environnement qui contient des données de santé à caractère personnel réelles.

Point d’actualité

Loi SREN et évolution référentiel certification HDS 2.0 => 2.1

- **Article 32 de la loi visant à Sécuriser et Réguler l'espace numérique (SREN) du 21 mai 2024 modifie les dispositions du CSP sur le HDS :**
- obligation de certification HDS pour un hébergeur qui conserve des données dans le cadre d'un **service d'archivage électronique**
- impose de préciser **par décret les dispositions** du CSP sur l'hébergement de données de santé:
  - obligation de stocker les données dans l'UE (déjà dans le référentiel v2.0)
  - nouvelles stipulations dans le contrat conclu entre l'hébergeur et son client face aux risques de transfert de données à caractère personnel ou d'accès non autorisé
- A l'occasion de la publication du décret HDS article 32 : modifications rédactionnelles pour lister les droits des patients prévus par le RGPD

- **Publication au Journal Officiel du décret HDS (ici) le 24 mars 2026**
- **Impact sur le référentiel de certification HDS v2**

Transition référentiel certification HDS 2.0 => 2.1

Quel impact pour un hébergeur déjà certifié v2.0 ?

- **Cas 1 : si l'hébergeur n'est soumis à aucune législation d'un pays tiers lui imposant un transfert de données de santé à caractère personnel**

  => il doit l'indiquer dans le contrat d'hébergement conclu avec chacun de ses clients (nouveaux et existants) (Exigence 23-2).

- **Cas 2 : si l'hébergeur effectue un transfert de données de santé à caractère personnel vers un pays tiers à l'Union Européenne ou à l'Espace Economique européen pour lequel il existe une décision d'adéquation de la Commission Européenne (Exigence 23-1)**

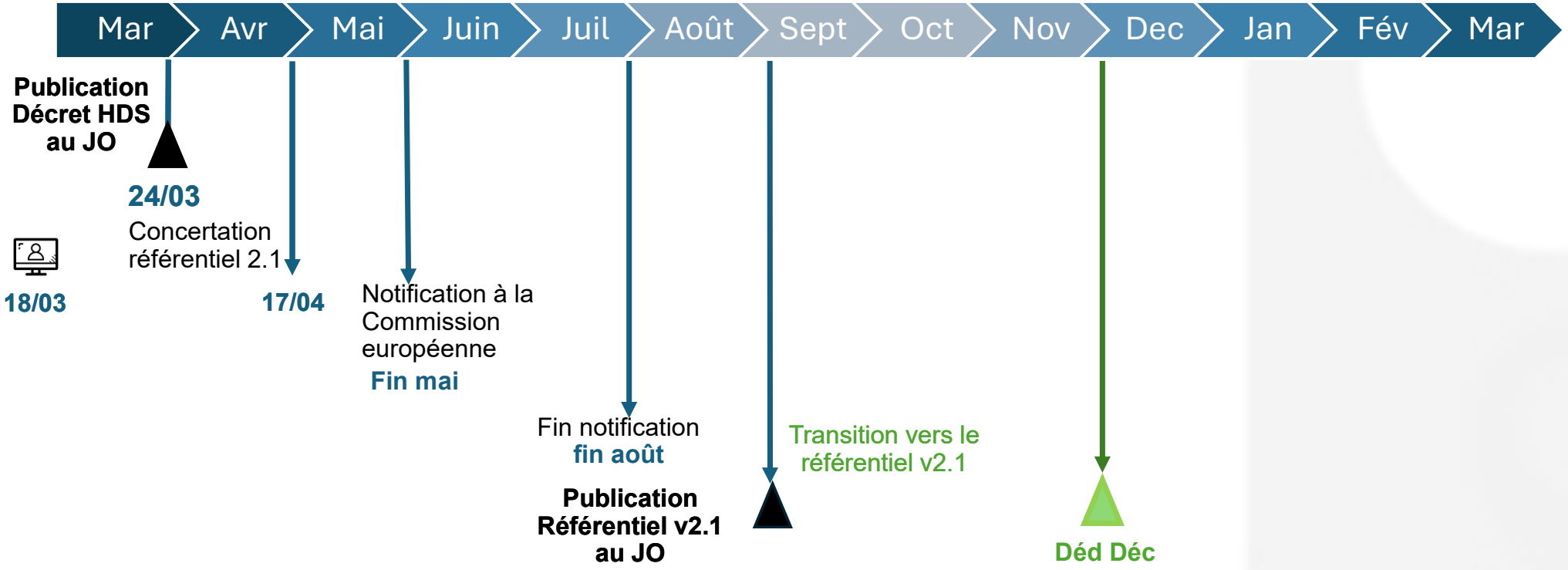
  => il doit indiquer dans le contrat les informations relatives à ce transfert (motif du transfert, type de données de santé à caractère personnel, pays vers lequel les données sont transférées,...).

- **Cas 3 : si l'hébergeur a une activité d'archivage électronique (Activité 6),**

  => cette activité d'archivage électronique doit être certifiée conformément au référentiel de certification HDS.

Ces exigences étant compatibles avec la certification v2.0, nous vous recommandons d'anticiper dès aujourd'hui ces modifications.

Transition référentiel certification HDS 2.0 => 2.1



Les audits réalisés 3 mois après la date de publication du référentiel au JO (audit initial, de surveillance, de renouvellement) sont réalisés selon la version v2.1.
Les certificats émis à la suite de ces audits sont émis selon la version 2.1.

Annexes

Ressources

- Cadre juridique
  https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549
  https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006196138/#LEGISCTA000036658495

- Référentiel
  https://esante.gouv.fr/produits-services/hds
- Liste des Hébergeurs certifiés HDS
  https://esante.gouv.fr/offres-services/hds/liste-des-hebergeurs-certifies
- Liste des organismes certificateurs HDS
  https://esante.gouv.fr/offres-services/hds/liste-des-organismes-de-certification
- FAQ
  https://esante.gouv.fr/faq/resultats?f%5B0%5D=filtrez_par_offre%3A2630&f%5B1%5D=produit%3A543

- La protection des données dans le monde
  https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

AGENCE DU NUMÉRIQUE EN SANTÉ

LE VILLAGE DE LA E-SANTÉ

Pour plus d'information retrouvez nous sur esante.gouv