



SOUVERAINETÉ & CONFORMITÉ

Données sensibles dans le cloud

conformité et chiffrement souverain

Comprendre ce que couvrent réellement HDS, SecNumCloud et le futur schéma EUCS, mesurer l'exposition au Cloud Act et concevoir une architecture de chiffrement qui tient devant un auditeur. Un guide opérationnel pour les équipes qui hébergent des données de santé, financières ou stratégiques dans le cloud.

11 pages · Grille d'analyse réglementaire, comparatif des référentiels, matrice de décision chiffrement et checklist d'audit incluses

6

activités d'hébergement couvertes par la certification HDS

3

niveaux d'assurance prévus par le schéma européen EUCS

72h

délai de notification d'une violation de données à la CNIL

SOMMAIRE

Ce que vous allez trouver dans ce document

Ce document part du contexte réglementaire européen pour descendre jusqu'aux choix d'architecture concrets — certifications, modèles de transfert, gestion des clés — et se conclut par une feuille de route de mise en conformité actionnable.

01	Synthèse — l'essentiel en une page	p.3
02	Un paysage réglementaire sous tension	p.4
03	Certification HDS : périmètre réel	p.5
04	HDS, SecNumCloud, EUCS : comparatif	p.6
05	Cloud Act et transferts RGPD	p.7
06	Architecture de chiffrement BYOK et HYOK	p.8
07	Grille d'auto-évaluation	p.9
08	Feuille de route en 5 étapes	p.10
09	Conclusion & à propos de Move2Cloud	p.11

À qui s'adresse ce document ? CTO, RSSI, DPO, architectes cloud et responsables plateforme d'ETI, de grands comptes et d'éditeurs SaaS manipulant des données de santé, des données personnelles sensibles ou des actifs stratégiques — en particulier ceux engagés dans une migration ou une mise en conformité d'un SI déjà hébergé chez un hyperscaler.

SYNTHÈSE

L'essentiel en une page

Héberger des données sensibles dans le cloud ne relève plus du choix de fournisseur, mais d'une architecture de clés que l'on doit pouvoir démontrer.

Les données de santé, financières et stratégiques migrent vers le cloud plus vite que les cadres qui les encadrent. Le référentiel HDS couvre **6 activités d'hébergement** distinctes et impose, depuis sa révision de **2024**, la localisation du stockage et du traitement dans l'Union européenne ; le référentiel SecNumCloud **3.2** de l'ANSSI y ajoute des critères capitalistiques et juridiques ; le schéma européen EUCS, qui prévoit **3 niveaux d'assurance**, n'est toujours pas adopté.

La pression ne vient plus seulement des autorités de contrôle mais des contrats. DORA s'applique au secteur financier depuis **janvier 2025** et impose un registre des prestataires TIC critiques et des clauses de sortie ; NIS2 étend des obligations équivalentes à des milliers d'entités ; et depuis l'arrêt Schrems II, tout transfert hors UE exige une analyse d'impact documentée, y compris sous le Data Privacy Framework. Les clients grands comptes et les appels d'offres publics reprennent désormais ces exigences en annexe technique, bien avant qu'un régulateur ne se manifeste.

La bonne nouvelle est que la conformité se joue moins sur le drapeau du fournisseur que sur la maîtrise des clés et le découpage des traitements. BYOK, HYOK, HSM externalisé, confidential computing et chiffrement applicatif permettent de conserver des charges de travail sur un hyperscaler tout en rendant les données inexploitable sans une clé restée sous contrôle européen. Ce document fournit les critères pour décider quelle donnée relève de quel modèle, et comment documenter ce choix.

6

activités d'hébergement couvertes
par le référentiel HDS

3

niveaux d'assurance prévus par le
schéma EUCS (Basic,
Substantial, High)

72h

délai RGPD de notification d'une
violation de données à la CNIL

La question que traite ce document n'est pas « quel cloud est souverain ? » mais « quelles données, sous quelles clés, accessibles par qui, et comment le prouver à un auditeur ? ». Les sections suivantes proposent une méthode de classification, une grille d'exposition au Cloud Act, trois patterns d'architecture de chiffrement et une checklist de mise en conformité applicable sur un SI déjà hébergé.

SECTION 02

Un paysage réglementaire sous tension

Entre un référentiel HDS révisé, un schéma EUCS encore inachevé et une extraterritorialité américaine intacte, les équipes doivent décider aujourd'hui d'architectures qui seront auditées demain. Trois dynamiques expliquent pourquoi le sujet ne peut plus être traité en fin de projet.

1. Le référentiel HDS s'est durci

La révision du référentiel HDS publiée en 2024 impose la localisation du stockage et du traitement des données de santé dans l'Union européenne, ainsi que la transparence sur tout accès réclamé par une autorité d'un pays tiers. Les certificats existants doivent être réalignés au prochain cycle d'audit.

2. EUCS : une souveraineté renvoyée à plus tard

Lancé par l'ENISA en 2020, le schéma EUCS prévoit trois niveaux d'assurance (Basic, Substantial, High) mais reste à l'état de projet, les exigences d'immunité aux lois extraterritoriales ayant été sorties du socle obligatoire. Aucun certificat EUCS n'est délivrable aujourd'hui.

3. Le Cloud Act n'a pas disparu avec le DPF

Le Cloud Act de 2018 autorise les autorités américaines à requérir des données détenues par un fournisseur soumis au droit des États-Unis, quel que soit le pays de stockage. Le Data Privacy Framework de 2023 légalise le transfert au sens du RGPD mais ne neutralise pas cet accès.

« La conformité ne se démontre pas avec un logo de certification, mais avec la cartographie des clés et de ceux qui peuvent les lire. »

Les sections suivantes détaillent ce que couvre réellement chaque référentiel, comment mesurer l'exposition juridique d'une charge de travail et quelles architectures de chiffrement résistent à un contrôle.

SECTION 03

Certification HDS : périmètre réel

La certification HDS, issue de l'article L.1111-8 du code de la santé publique, a remplacé l'ancien agrément en 2018 : elle repose sur un socle ISO 27001, complété par des exigences inspirées d'ISO 20000-1 et ISO 27018 et par des obligations propres au secteur de la santé.

POINT DE VIGILANCE	CE QUE CELA IMPLIQUE CONCRÈTEMENT
Périmètre de services	La certification ne couvre pas l'intégralité du catalogue d'un fournisseur : seuls les services listés en annexe du certificat sont éligibles, et un service managé récent y figure rarement dès sa mise sur le marché.
Six activités distinctes	Les activités 1 et 2 concernent les sites et infrastructures physiques, les activités 3 à 6 la virtualisation, la plateforme applicative, l'administration et la sauvegarde : un hébergeur d'infrastructure ne porte pas les responsabilités de l'infogéreur.
Chaîne de sous-traitance	Chaque maillon qui accède techniquement aux données de santé doit être couvert ; un éditeur déployant sur un IaaS certifié reste responsable de ses propres activités d'exploitation et doit être certifié à ce titre.

À retenir : Exigez systématiquement le certificat HDS lui-même, pas le logo : vérifiez l'organisme certificateur accrédité, les numéros d'activités couvertes et l'annexe listant les services certifiés. Si votre éditeur SaaS exploite la plateforme, il doit détenir sa propre certification sur les activités 4 à 6 — celle de son IaaS ne le couvre pas.

Ce que la certification HDS ne dit pas

Le référentiel actuel encadre les pratiques de l'hébergeur : gouvernance de la sécurité, gestion des accès, traçabilité, sauvegarde, réversibilité, désignation d'un délégué à la protection des données et information du patient. Il n'impose en revanche ni le chiffrement des données au repos sous une clé maîtrisée par le client, ni, dans sa version en vigueur, une localisation exclusive dans l'Union européenne ou une immunité à l'égard des lois extraterritoriales. Autrement dit, un hébergeur certifié HDS peut être une filiale européenne d'un groupe soumis au droit américain : la certification atteste la maturité des processus, pas l'étanchéité juridique. C'est précisément ce manque que les travaux de refonte du référentiel, portés par l'Agence du numérique en santé, cherchent à combler en y introduisant des critères de localisation et de protection contre les accès de pays tiers. Tant que cette nouvelle version n'est pas opposable, l'exposition juridique se traite ailleurs : dans l'analyse de transfert et dans l'architecture de clés.

SECTION 04

HDS, SecNumCloud, EUCS : comparatif

HDS, SecNumCloud et EUCS ne répondent pas à la même question : le premier encadre un secteur, le deuxième qualifie un niveau de confiance incluant des critères juridiques, le troisième vise à harmoniser l'évaluation de la cybersécurité des services cloud à l'échelle européenne.

RÉFÉRENTIEL	STATUT	CE QU'IL GARANTIT	À RÉSERVER À
HDS	Certification obligatoire en droit français	Maturité des processus d'hébergement et d'exploitation des données de santé à caractère personnel, sur un socle ISO 27001	Toute charge hébergeant ou exploitant des données de santé pour le compte d'un responsable de traitement
SecNumCloud	Qualification ANSSI, volontaire	Exigences techniques et organisationnelles renforcées, assorties de critères d'immunité aux droits extra-européens (localisation, capital, gouvernance)	Données stratégiques, systèmes d'information d'importance vitale, secrets industriels et besoins étatiques
EUCS	Schéma européen en cours d'élaboration au titre du Cybersecurity Act	Niveaux d'assurance gradués et reconnaissance mutuelle entre États membres, destinés à remplacer les schémas nationaux	Anticipation de la trajectoire de conformité : à cartographier aujourd'hui, pas à exiger contractuellement

Piège fréquent : Confondre « cloud de confiance » et qualification effective : une offre opérée en France sous licence d'une technologie américaine n'est pas qualifiée tant que l'ANSSI n'a pas délivré l'attestation, et aucune certification, HDS comprise, ne dispense de réaliser l'analyse de transfert exigée par le chapitre V du RGPD.

Articuler les référentiels sans empiler les coûts

Empiler les référentiels coûte cher et retarde les mises en production. La démarche efficace consiste à segmenter : identifier les charges réellement concernées par chaque obligation, puis dimensionner le niveau d'exigence en conséquence. Une plateforme de santé peut parfaitement combiner un socle HDS pour les environnements de production traitant des données de patients, un cloud public non qualifié pour les environnements de développement alimentés par des jeux de données anonymisés, et une enclave SecNumCloud réservée aux traitements les plus sensibles ou aux secrets d'exploitation. Cette segmentation suppose une classification formelle des données et des flux inter-zones explicitement contrôlés — sans quoi la zone la moins exigeante finit par recevoir, par copie ou par log, les données que l'on prétendait isoler.

SECTION 05

Cloud Act et transferts RGPD

Le CLOUD Act de 2018 oblige tout fournisseur relevant de la juridiction américaine à remettre aux autorités les données en sa « possession, garde ou contrôle », quel que soit le pays où ces données sont physiquement stockées.

Le critère décisif : le contrôle, pas la géographie

Ce n'est pas la localisation du datacenter qui détermine l'exposition, mais le lien de contrôle entre l'entité réquisitionnée et les données. Une filiale européenne détenue par une société mère américaine reste dans le champ dès lors qu'elle peut techniquement accéder aux données en clair.

Le transfert ne se limite pas au stockage

Au sens du RGPD, un accès distant depuis un pays tiers constitue déjà un transfert. Support de niveau 3, astreinte administrateur, télémétrie produit, journaux d'exploitation et métadonnées de facturation sont autant de flux à inventorier au même titre que la base de données elle-même.

Des mesures supplémentaires réellement opposables

Depuis Schrems II, les recommandations du Comité européen de la protection des données identifient le chiffrement robuste, avec des clés détenues et administrées exclusivement dans l'UE par une entité hors d'atteinte du droit tiers, comme la mesure supplémentaire la plus solide — à condition qu'elle soit effective.

VECTEUR D'EXPOSITION	MESURE DE RÉDUCTION
Accès administrateur distant	Restreindre l'exploitation à des équipes situées dans l'UE, journaliser et approuver chaque accès via un mécanisme de type lockbox.
Télémétrie, journaux et sauvegardes	Désactiver les remontées optionnelles, cantonner les logs à la région et chiffrer les sauvegardes avec une clé distincte de celle du service.

SECTION 06

Architecture de chiffrement BYOK et HYOK

Entre le chiffrement au repos activé par défaut et la maîtrise exclusive des clés, il existe trois modèles distincts dont les garanties juridiques sont très inégales.

BYOK : un contrôle de gouvernance, pas une barrière cryptographique

Avec le BYOK, la clé est générée par le client puis importée dans le module matériel du fournisseur. Elle y est manipulée en clair au moment des opérations cryptographiques : le contrôle apporté est essentiellement contractuel et opérationnel — traçabilité des appels, rotation maîtrisée, capacité de révocation entraînant une destruction cryptographique des données. Il ne constitue pas une barrière face à une réquisition visant le fournisseur, puisque celui-ci dispose techniquement du matériel de clé. C'est un bon niveau de maîtrise pour la gouvernance interne et la séparation des environnements, pas une réponse au risque extraterritorial.

HYOK et clés externalisées : le coût réel de l'étanchéité

Les mécanismes de clés externes — store de clés déporté, service de key management hors cloud, chiffrement applicatif côté client — maintiennent le matériel de clé dans un HSM que le fournisseur n'administre pas ; chaque opération déclenche un appel sortant. Le coût est réel : latence ajoutée sur le chemin critique, dépendance stricte à la disponibilité du broker de clés, complexité des caches et des plans de reprise, et surtout perte des fonctions managées qui supposent un accès en clair (indexation, recherche, analytique native). Avant de généraliser ce modèle, il faut tester la coupure volontaire du broker et mesurer le temps de retour à la normale.

À retenir : Documentez pour chaque flux une seule réponse : qui peut déchiffrer, avec quelle clé et sous quelle juridiction. C'est ce tableau, et non le niveau de certification du fournisseur, qui tiendra devant un auditeur ou une autorité de contrôle.

La hiérarchie opérationnelle est simple à poser. Le chiffrement au repos géré par le fournisseur reste le défaut pour l'immense majorité des charges : il protège contre la perte de support et le vol physique. Le BYOK s'applique dès qu'il faut prouver la traçabilité des opérations cryptographiques et disposer d'un levier de révocation. Le HYOK, le store de clés externe ou le chiffrement applicatif côté client se réservent aux données dont la lecture par un tiers serait inacceptable — et dont l'indisponibilité temporaire est préférable à la divulgation. Chacun de ces choix doit être consigné dans l'analyse de transfert, avec les tests de révocation et de restauration associés : une architecture de clés qui n'a jamais été éprouvée n'est pas une mesure supplémentaire, c'est une intention.

SECTION 07

Grille d'auto-évaluation

Passez ces six points en revue avant d'engager une nouvelle charge sensible dans le cloud, ou avant votre prochain audit HDS ou contrôle CNIL.

- ☐ **Disposez-vous d'une classification à jour des données hébergées, distinguant les données de santé à caractère personnel, les données financières et les données stratégiques ?** Sans classification, aucune exigence réglementaire ne peut être rattachée à un traitement précis et les mesures de protection sont appliquées au hasard.
- ☐ **Avez-vous obtenu et lu le certificat HDS de chacun de vos fournisseurs, avec l'organisme certificateur, les activités couvertes et l'annexe des services certifiés ?** Le logo ne vaut pas preuve : seul le certificat permet de vérifier que les services réellement utilisés entrent dans le périmètre.
- ☐ **Avez-vous formalisé une analyse de transfert (TIA) documentant l'exposition de chaque fournisseur et de ses sous-traitants à une juridiction extraterritoriale ?** Le chapitre V du RGPD l'exige indépendamment de toute certification, et c'est le premier document demandé lors d'un contrôle.
- ☐ **Connaissez-vous, pour chaque charge sensible, qui détient matériellement les clés de chiffrement et où s'exécutent les opérations cryptographiques ?** Un chiffrement dont les clés restent sous le contrôle du fournisseur n'apporte aucune garantie supplémentaire face à une réquisition.
- ☐ **Avez-vous testé, en conditions réelles, la révocation d'une clé puis la restauration du service associé ?** Une architecture BYOK ou HYOK jamais éprouvée relève de l'intention et ne résistera pas à l'examen d'un auditeur.
- ☐ **Tenez-vous à jour la liste des sous-traitants ultérieurs de vos fournisseurs, avec un plan de réversibilité chiffré en charge et en délai ?** L'exposition réelle se joue souvent au deuxième rang de la chaîne, et une dépendance non réversible interdit toute décision de sortie.

Comment lire vos réponses : Deux « non » appellent un plan de remédiation documenté ; trois « non » ou plus signalent une exposition réglementaire à traiter en priorité, avant tout nouveau déploiement.

SECTION 08

Feuille de route en 5 étapes

Cette trajectoire se mène par incréments, sans interrompre les plateformes existantes : chaque étape produit un livrable exploitable immédiatement, même si la suivante est repoussée.

1

Cartographier les données sensibles

Recensez les traitements, leur nature (santé, financière, stratégique), leur base légale et leur niveau de criticité. Rattachez chaque jeu de données aux services cloud qui le stockent, le traitent ou le sauvegardent, y compris les logs et les environnements de test.

2

Vérifier les certifications réelles

Collectez les certificats HDS, attestations SecNumCloud et rapports d'audit de chaque fournisseur, et confrontez les activités et services couverts à votre usage réel. Identifiez les zones non couvertes, notamment chez les éditeurs SaaS exploitant la plateforme.

3

Conduire l'analyse de transfert

Documentez pour chaque fournisseur et sous-traitant ultérieur son rattachement juridictionnel, les mécanismes de transfert invoqués et les mesures techniques et organisationnelles complémentaires. Concluez par une décision motivée, maintenir, renforcer ou relocaliser, pour chaque traitement.

4

Concevoir l'architecture de clés

Appliquez la hiérarchie définie : chiffrement géré par le fournisseur par défaut, BYOK dès que la traçabilité et la révocation sont requises, HYOK ou chiffrement côté client pour les données dont la divulgation serait inacceptable. Formalisez la gouvernance des clés, rôles, rotation, séparation des pouvoirs.

5

Éprouver et gouverner

Organisez des exercices de révocation et de restauration, mesurez les impacts applicatifs et consignez les résultats dans le dossier de conformité. Intégrez ces tests au cycle d'audit annuel et rattachez-les au plan de réversibilité du fournisseur concerné.

CONCLUSION

Conformité démontrable plutôt que souveraineté déclarative

Les organisations qui traitent ces sujets de front ne gagnent pas seulement un certificat : elles gagnent la capacité de documenter, devant un auditeur comme devant un comité d'investissement, pourquoi telle donnée est hébergée à tel endroit, sous quel contrôle cryptographique et avec quel levier de sortie. Cette traçabilité transforme un risque diffus en décisions explicites, arbitrables et révisables.

Le paysage réglementaire continuera de bouger — montée en charge d'EUCCS, évolution du référentiel HDS, jurisprudence sur les transferts. Les architectures qui traverseront ces changements ne sont pas les plus souveraines sur le papier, mais les plus explicites : périmètres délimités, clés maîtrisées là où cela compte, dépendances connues et réversibilité testée. C'est un travail d'ingénierie autant que de conformité, et il se mène mieux en amont qu'en réaction à un contrôle.

Move2Cloud	est un cabinet de conseil spécialisé en infrastructure, cloud et transformation IT. Nous accompagnons les organisations dans l'audit, la mise en conformité et la sécurisation de leur environnement cloud.
Contact	Move2Cloud — Paris · move2cloud.fr
Prochaine étape	Un audit de quelques semaines suffit généralement à transformer les « non » de la grille précédente en un plan de remédiation chiffré : cartographie des données sensibles, revue des certificats et des contrats, analyse de transfert et schéma cible de gestion des clés.

Sources

ANSSI — Référentiel SecNumCloud v3.2 (2022) — Ministère de la Santé / ANS — Référentiel de certification Hébergeur de Données de Santé — ENISA — European Cybersecurity Certification Scheme for Cloud Services (EUCCS), projet de schéma — CNIL — Doctrine et recommandations sur les transferts de données hors UE — EDPB — Recommandations 01/2020 sur les mesures complémentaires (post-Schrems II)

Document rédigé à titre d'exemple et d'illustration par Move2Cloud à des fins pédagogiques. Le schéma EUCCS reste en cours d'adoption : ses niveaux d'assurance et ses exigences d'immunité peuvent évoluer. Ce document ne constitue pas un conseil juridique.