Guide pratique de la migration HDS

De la préparation à la bascule DNS

1. À qui s'adresse ce guide

Ce guide s'adresse aux équipes qui exploitent une plateforme de santé en production sur un hébergement non conforme aux exigences HDS ou ne répondant pas à leurs critères de souveraineté, et qui préparent une migration vers un hébergement certifié HDS, situé en France dans le cas présenté ici. Les étapes de bascule décrites valent pour tout changement d'hébergement ; les vérifications préalables, elles, sont celles qu'appelle ce point de départ.

Il décrit un déroulé opérationnel : comment choisir un hébergeur adapté, quelles étapes suivre, quels points contrôler, et quelles erreurs éviter. Il ne constitue pas un avis juridique. Selon la nature, l'ampleur et les risques du traitement, l'appui du délégué à la protection des données, du responsable de la sécurité des systèmes d'information ou d'un conseil juridique peut être nécessaire.

2. Choisir un hébergeur adapté à une migration

Le choix de l'hébergeur se fait avant la migration et conditionne sa réussite. Quatre critères doivent notamment être examinés pour préparer la migration et maintenir le niveau de conformité attendu après la bascule.

Périmètre de la certification. La certification HDS distingue six activités. Un prestataire peut être certifié pour tout ou partie de ce périmètre. Il faut vérifier que les activités qu'il réalise dans le cadre de la prestation sont bien couvertes par son certificat, et que les éventuelles autres activités sont prises en charge par des acteurs disposant des garanties requises. Pour une prestation managée couvrant l'ensemble de la chaîne, une certification sur les six activités permet de limiter les ruptures de périmètre.

Cadre contractuel HDS. La prestation doit être encadrée par un contrat comportant les clauses exigées par le Code de la santé publique, notamment concernant le périmètre des prestations, la sécurité, les responsabilités, la fin de l'hébergement et la réversibilité. Ces dispositions peuvent figurer dans le contrat principal ou dans une annexe dédiée. Leur examen doit être anticipé avant le transfert des données.

Exploitation managée. Un hébergeur qui ne fournit que l'infrastructure laisse au client la charge de configurer et d'exploiter les couches par-dessus. Une plateforme managée peut prendre en charge une partie de ces opérations (par exemple l'isolation, les mises à jour de l'infrastructure, la supervision technique ou les sauvegardes) selon le périmètre contractuel de la prestation, et réduire ainsi le nombre d'opérations restant à configurer et à maintenir côté client. Le chiffrement mérite d'être distingué selon qu'il porte sur l'infrastructure, les bases de données, le stockage objet ou l'application elle-même.

Réversibilité, dans les deux sens. Deux vérifications distinctes. Côté hébergeur actuel : peut-on récupérer l'intégralité des données dans un format exploitable pour partir ? Un verrouillage technique peut empêcher la migration elle-même. Côté hébergeur cible : la même garantie de sortie doit exister, pour ne pas reproduire la dépendance ailleurs.

La certification HDS ne suffit pas, à elle seule, à garantir une protection contre l'application de législations extra-européennes. Ce risque doit être examiné à partir de la structure juridique de l'hébergeur et de ses sous-traitants, des transferts et accès distants possibles, ainsi que des informations contractuelles fournies. Le décret n° 2026-209 du 24 mars 2026 renforce les obligations d'information sur ces points à compter du 26 septembre 2026.

3. Étapes et points de contrôle

Chaque étape porte ses éléments de vérification. Ce sont des contrôles opérationnels de migration, pas une évaluation de conformité.

Étape 1 – État des lieux et cartographie. Inventorier ce qui va migrer avant de bouger quoi que ce soit.

- ☐ Données de santé recensées, avec leurs volumes
- ☐ Sauvegardes localisées et intégrées au périmètre de migration
- ☐ Formats de fichiers et de stockage identifiés (une conversion peut être nécessaire)
- ☐ Dépendances applicatives et services externes listés
- ☐ Réversibilité de l'hébergeur actuel vérifiée (extraction possible)

Étape 2 – Préparation. Mettre en place le cadre avant le transfert.

- ☐ Contrat d'hébergement et clauses relatives au périmètre HDS examinés et validés
- ☐ Environnements de test et de production provisionnés
- ☐ Modalités de chiffrement des bases, volumes et espaces de stockage vérifiées et configurées conformément à l'architecture retenue
- ☐ Accès et droits configurés
- ☐ Plan de retour arrière défini et testé en cas d'échec de la bascule
- ☐ Tests de restauration des sauvegardes réalisés
- ☐ Qualification des rôles vérifiée (responsable de traitement, sous-traitant, sous-traitant ultérieur) et documentation contractuelle mise à jour
- ☐ Clients informés du changement d'hébergeur selon les modalités de leurs contrats de sous-traitance, dans un délai leur permettant d'exercer les droits qui y sont prévus

Un éditeur SaaS qui héberge des données de santé pour le compte de ses clients change, en migrant, de sous-traitant ultérieur au sens de l'article 28 du RGPD. Selon que l'autorisation prévue au contrat est générale ou spécifique, le changement suppose une information préalable ouvrant une faculté d'objection, ou une autorisation écrite préalable. Le nouvel hébergeur doit être tenu par des obligations équivalentes, et le registre des traitements mis à jour.

Étape 3 – Transfert et synchronisation.

- ☐ Transfert des bases de données, fichiers et objets stockés
- ☐ Conversion des formats si nécessaire (ex. fichiers issus d'un stockage tiers)
- ☐ Intégrité, complétude et cohérence des données vérifiées entre la source et la cible

Étape 4 – Déploiement applicatif.

- ☐ Applications déployées (ex. via un dépôt Git)
- ☐ Tâches planifiées (CRON) reconfigurées
- ☐ Supervision, journalisation et alertes mises en place (accès, erreurs, événements de sécurité)

Étape 5 – Bascule vers l'environnement cible. Cette étape concentre le principal risque d'interruption. Selon l'architecture, elle peut comprendre une synchronisation finale, un gel temporaire des écritures, une modification du routage ou une bascule DNS.

- ☐ TTL DNS réduit suffisamment en amont, avant l'expiration de l'ancien TTL, afin de limiter la durée de conservation de l'ancienne résolution par les caches qui respectent cette valeur
- ☐ Fenêtre de bascule planifiée sur une période de faible trafic
- ☐ Bascule effectuée, cohérence des données et disponibilité du service surveillées

Étape 6 – Validation post-bascule et clôture de l'hébergement d'origine.

- ☐ Chiffrement des données stockées vérifié selon les mécanismes prévus
- ☐ Sauvegardes opérationnelles et localisées conformément au périmètre
- ☐ Supervision et alertes fonctionnelles
- ☐ Service vérifié côté utilisateurs
- ☐ Périmètre de sortie chez l'hébergeur d'origine défini par écrit : bases, fichiers, sauvegardes, journaux, environnements de test
- ☐ Restitution puis suppression des données engagées, une fois l'intégrité vérifiée côté cible
- ☐ Preuve écrite de la suppression obtenue, dans les termes prévus par le contrat d'hébergement

4. Erreurs fréquentes

Négliger le régime des sauvegardes. Les sauvegardes contenant des données de santé restent soumises aux exigences applicables à ces données. Leur hébergement, leur localisation, leur chiffrement, leur durée de conservation, leur restauration et leur éventuelle sous-traitance doivent être intégrés au périmètre étudié.

Croire que le recours à un hébergeur certifié suffit à rendre l'ensemble du service conforme. La certification couvre les activités d'hébergement indiquées sur le certificat. Le responsable de traitement demeure notamment responsable de la licéité du traitement, de la gestion des habilitations, de la sécurité applicative et du respect des droits des personnes, tandis que chaque sous-traitant conserve les obligations relevant de son périmètre.

Sous-estimer la conversion de format. Les formats, API, métadonnées ou mécanismes d'accès propres à l'environnement d'origine peuvent nécessiter une conversion ou une adaptation avant d'être exploitables sur la cible. À anticiper dès la cartographie, pas au moment du transfert.

Ignorer la réversibilité de l'hébergeur d'origine. Un verrouillage technique côté départ peut bloquer la sortie et retarder toute la migration. C'est une vérification préalable, pas une découverte de dernière minute.

Improviser la bascule. Sans réduction préalable du TTL, sans fenêtre choisie ni synchronisation finale maîtrisée, la bascule devient le point de friction visible pour les utilisateurs. Une préparation adaptée réduit le risque d'indisponibilité ou d'incohérence perçue.

5. Retour d'expérience : Madietenligne

Ce cas illustre la **séquence opérationnelle** décrite plus haut. La plateforme Madietenligne satisfaisait déjà aux exigences HDS avant la bascule, et la migration visait à alléger l'exploitation, pas à corriger une non-conformité.

Côté exécution, la bascule complète (environnements de test et de production) s'est déroulée en moins de quinze jours. Elle a impliqué le transfert et la synchronisation de 500 Go, l'adaptation des formats de fichiers auparavant stockés sur Azure, le déploiement des applications PHP et Node via un dépôt Git, et la reprise des tâches planifiées et de la supervision sur la plateforme cible. La bascule DNS a constitué, dans ce cas, l'unique interruption possible ; côté utilisateurs, la transition a été transparente.

« *On a migré l'ensemble des environnements de test et de prod en moins de 15 jours.* » — Eddy Montus, cofondateur de Madietenligne

6. Cadre et sources

Ce guide est un outil de préparation opérationnelle. Il ne constitue pas un avis juridique. Les références réglementaires sont fournies à titre d'information ; leur application dépend de la nature des données traitées et de la situation propre à chaque organisation.

Sources

- Arrêté du 26 avril 2024 portant approbation du référentiel de certification HDS (version 2), publié au Journal officiel du 16 mai 2024.
- Décret n° 2026-209 du 24 mars 2026 portant modification de certaines dispositions du code de la santé publique relatives à l'hébergement de données de santé à caractère personnel (JO du 26 mars 2026), pris en application de l'article 32 de la loi n° 2024-449 du 21 mai 2024. Les 2° et 3° de son article 1er (création de l'article R. 1111-9-1 et modification de l'article R. 1111-11) entrent en vigueur le 26 septembre 2026.

- Code de la santé publique, articles L. 1111-8, R. 1111-8-8, et R. 1111-9 à R. 1111-11, ainsi que R. 1111-9-1 à compter du 26 septembre 2026.
- Agence du numérique en santé (ANS) - référentiel de certification des hébergeurs de données de santé et liste officielle des hébergeurs certifiés (activités et version du référentiel couvertes).
- Témoignage client Madietenligne publié sur clever.cloud.