Practical Guide to HDS Migration

From Preparation to DNS Cutover

1. Who this guide is for

This guide is intended for teams operating a production healthcare platform on hosting that either does not comply with HDS requirements or does not meet their sovereignty criteria, and that are preparing to migrate to HDS-certified hosting located in France, as considered in this guide. The cutover steps described apply to any hosting migration; however, the preliminary checks are specific to this starting point.

It provides an operational roadmap: how to choose a suitable hosting provider, which steps to follow, which checkpoints to validate, and which mistakes to avoid. It is not intended as legal advice. Depending on the nature, scope, and risks of the processing activities involved, support from the Data Protection Officer (DPO), the Information Security Officer (CISO/IS Manager), or legal counsel may be required.

2. Choosing the right hosting provider for your migration

assessed to prepare the migration and maintain the expected level of compliance after the cutover.

HDS certification scope. HDS certification covers six distinct activities. A provider may be certified for all or only part of this scope. Verify that every activity the provider performs as part of the service is covered by its certificate, and that any remaining activities are handled by organisations providing the required guarantees. For a fully managed service covering the entire hosting chain, certification across all six activities helps reduce gaps in certification scope.

HDS contractual framework. The service must be governed by a contract containing the clauses required by the French Public Health Code, particularly regarding the scope of the services, security, responsibilities, end-of-service provisions, and reversibility. These provisions may be included either in the main contract or in a dedicated appendix. They should be reviewed before any data transfer takes place.

Managed operations. A hosting provider that supplies infrastructure alone leaves customers responsible for configuring and operating the layers above it. Depending on the contractual scope of the service, a managed platform can take responsibility for part of these operations (for example, isolation, infrastructure updates, technical monitoring, or backups), reducing the number of components the customer must configure and maintain. Encryption should be considered separately depending on whether it applies to the infrastructure, databases, object storage, or the application itself.

Reversibility, in both directions. Two separate checks are required. With the current hosting provider, verify that all data can be retrieved in a usable format before leaving. Technical lock-in can prevent the migration itself. With the target provider, the same exit guarantee should exist to avoid creating the same dependency elsewhere.

HDS certification alone does not guarantee protection against the application of extra-European legislation. This risk should be assessed based on the hosting provider's and its subcontractors' legal structure, any potential remote access or data transfers, and the contractual information provided. Decree No. 2026–209 of 24 March 2026 strengthens the information obligations on these points from 26 September 2026 onwards.

3. Migration Steps and Checkpoints

Each phase includes its own verification points. These are operational migration checks, not a compliance assessment.

Step 1 – Assessment and Inventory. Identify everything that will be migrated before making any changes.

- ☐ Health data identified and inventoried, including data volumes
- ☐ Backups identified and included within the migration scope
- ☐ File and storage formats identified (conversion may be required)
- ☐ Application dependencies and external services documented
- ☐ Reversibility of the current hosting provider verified (data export is possible)

Step 2 – Preparation. Put the necessary framework in place before transferring any data.

- ☐ Hosting agreement and HDS-related contractual clauses reviewed and approved
- ☐ Test and production environments provisioned
- ☐ Database, volume, and storage encryption mechanisms verified and configured in line with the chosen architecture
- ☐ User access and permissions configured
- ☐ Rollback plan defined and tested in case the cutover fails
- ☐ Backup restoration tests completed
- ☐ Roles and responsibilities verified (controller, processor, sub-processor), and contractual documentation updated
- ☐ Customers informed of the change of hosting provider in accordance with the terms of their data processing agreements, within a timeframe allowing them to exercise any contractual rights available to them

When a SaaS provider hosting health data on behalf of its customers migrates to a new hosting provider, it changes sub-processors within the meaning of Article 28 of the GDPR. Depending on whether the authorisation provided in the contract is general or specific, the change requires either prior notification allowing customers to object or prior written

authorisation. The new hosting provider must be bound by equivalent obligations, and the record of processing activities must be updated.

Step 3 – Data Transfer and Synchronisation.

- ☐ Databases, files, and stored objects transferred
- ☐ Data formats converted where necessary (e.g. files originating from third-party storage)
- ☐ Data integrity, completeness, and consistency verified between the source and target environments

Step 4 – Application Deployment.

- ☐ Applications deployed (e.g. from a Git repository)
- ☐ Scheduled tasks (CRON jobs) reconfigured
- ☐ Monitoring, logging, and alerting implemented (access, errors, security events)

Step 5 – Cutover to the Target Environment. This phase carries the highest risk of service disruption. Depending on the architecture, it may include a final synchronisation, a temporary write freeze, a routing change, or a DNS cutover.

- ☐ DNS TTL reduced sufficiently in advance—before the previous TTL expires—to minimise the time during which caches continue using the previous DNS resolution
- ☐ Cutover window scheduled during a period of low traffic
- ☐ Cutover completed, with data consistency and service availability actively monitored

Step 6 – Post-Cutover Validation and Decommissioning of the Original Hosting Environment.

- ☐ Encryption of stored data verified according to the planned mechanisms
- ☐ Backups operational and located in accordance with the defined scope
- ☐ Monitoring and alerting operational
- ☐ Service validated from the users' perspective
- ☐ Exit scope with the original hosting provider documented in writing: databases, files, backups, logs, and test environments
- ☐ Data returned and subsequently deleted once integrity has been verified on the target environment
- ☐ Written confirmation of data deletion obtained in accordance with the terms of the hosting agreement

4. Common Mistakes

Overlooking backup requirements. Backups containing health data remain subject to the same requirements as the data they contain. Their hosting, location, encryption, retention period, restoration procedures, and any subcontracting arrangements must all be included within the scope of the assessment.

Assuming that using an HDS-certified hosting provider automatically makes the entire service compliant. HDS certification covers only the hosting activities listed on the certificate. The data controller remains responsible, in particular, for the lawfulness of the processing, access management, application security, and compliance with data subjects' rights, while each processor remains responsible for the obligations falling within its own scope.

Underestimating format conversion. File formats, APIs, metadata, or access mechanisms specific to the source environment may require conversion or adaptation before they can be used in the target environment. This should be anticipated during the inventory phase, not at the time of the transfer.

Ignoring the reversibility of the current hosting provider. Technical lock-in on the source platform can prevent data extraction and delay the entire migration. This is a prerequisite check, not something to discover at the last minute.

Improvising the cutover. Without reducing the DNS TTL in advance, selecting an appropriate cutover window, and controlling the final synchronisation, the cutover becomes the most visible point of friction for users. Proper preparation reduces the risk of perceived downtime or data inconsistencies.

5. Customer Experience: Madietenligne

This case illustrates the operational sequence described above. Before the migration, the Madietenligne platform already met HDS requirements. The objective of the migration was to simplify operations rather than to remediate a compliance issue.

From an execution standpoint, the complete migration—including both test and production environments—was completed in less than fifteen days. It involved transferring and synchronising 500 GB of data, adapting file formats previously stored on Azure, deploying PHP and Node.js applications from a Git repository, and reconfiguring scheduled tasks and monitoring on the target platform. In this case, the DNS cutover was the only potential service interruption; from the users' perspective, the transition was seamless.

"*We migrated all test and production environments in under 15 days.*" — Eddy Montus, Co-founder of Madietenligne

6. Legal Framework and References

This guide is intended as an operational preparation tool. It does not constitute legal advice. The regulatory references are provided for information only. Their applicability depends on the nature of the data being processed and on the specific circumstances of each organisation.

Sources

- Order of 26 April 2024 approving the HDS Certification Framework (Version 2), published in the Official Journal of the French Republic on 16 May 2024.
- Decree No. 2026-209 of 24 March 2026 amending certain provisions of the French Public Health Code relating to the hosting of personal health data (Official Journal of 26 March 2026), adopted pursuant to Article 32 of Law No. 2024-449 of 21 May 2024. Paragraphs 2 and 3 of Article 1 (creation of Article R.1111-9-1 and amendment of Article R.1111-11) enter into force on 26 September 2026.
- French Public Health Code, Articles L.1111-8, R.1111-8-8, and R.1111-9 to R.1111-11, as well as Article R.1111-9-1 from 26 September 2026 onwards.
- French Digital Health Agency (ANS) – HDS Certification Framework and the official list of certified HDS hosting providers (including certified activities and the applicable version of the framework).
- Madietenligne customer case study, published on Clever Cloud.