HDS and Digital Sovereignty: 10 Points to Verify

A Practical Framework for Assessing a Health Data Hosting Provider

This framework brings together ten questions to ask a health data hosting provider, along with the reason each one matters. It is designed to structure an assessment, without providing a score or legal opinion. Starting point: HDS certification confirms that a defined scope of hosting activities complies with the requirements of the HDS framework. However, it does not, by itself, eliminate exposure to extraterritorial legislation. These are two distinct issues, which this framework addresses separately.

No.	Criterion	Question to Ask the Provider	Why It Matters
A. What HDS Certification Confirms			
1	HDS Certification	Is the HDS certificate currently valid and issued by a certification body accredited by COFRAC or an equivalent European accreditation body?	An expired certificate, or one issued by a non-accredited certification body, does not constitute valid HDS certification.
2	Scope of the Six HDS Activities	Does the certification cover all the activities actually performed as part of the service, including operations management and backups?	Some providers are certified for only part of the HDS scope. Partial certification may be sufficient if it exactly matches the activities performed by the provider. Any remaining activities must be identified and, where they fall within the scope of HDS hosting, covered by a provider holding the appropriate HDS certification.
B. What HDS Certification Does Not Cover (Legal Sovereignty)			
3	Data Location	In which countries and datacentres are health data and their backups actually stored, and is all storage located exclusively within the European Economic Area (EEA)?	A provider may store data in France while still being subject to non-European legislation because of its parent company.
4	Protection Against Non-European Legislation	Are the provider, its parent companies and its subcontractors subject to non-European legislation (such as the Cloud Act or FISA) that could require access to the data? What safeguards (legal status, ownership structure, operational control and location, and, where applicable, SecNumCloud qualification) help mitigate this risk?	HDS certification alone does not eliminate the risk of data access ordered by a foreign authority. French Decree No. 2026-209 of 24 March 2026 strengthens the regulatory framework (EEA data storage, rules governing data transfers, customer information regarding risks and mitigation measures), but it documents this risk rather than removing it. Two distinct aspects must therefore be considered: legal immunity, which depends on the provider's legal status (exclusive application of European law, ownership structure, absence of subsidiaries subject to non-European jurisdictions) and may also be demonstrated through SecNumCloud qualification; and technological independence from non-European providers, which SecNumCloud qualification alone does not guarantee. For the most sensitive data, the

No.	Criterion	Question to Ask the Provider	Why It Matters
			CNIL recommends choosing a provider that is exclusively subject to European law and offers an appropriate level of protection.
5	Location of Operations	From which country, and by which teams, is the platform administered and operated?	Remote access from a non-EEA country constitutes an international data transfer under the GDPR. It must therefore be governed by an appropriate legal mechanism (an adequacy decision or appropriate safeguards) and does not, in itself, mean that the data is effectively exposed. The HDS framework requires providers to document the countries concerned, the safeguards implemented, the applicable non-European legislation and any residual risks, and to disclose this information to the customer in the contract.
C. Operations, Commitments and Exit Strategy			
6	Allocation of Responsibilities	Which obligations remain the customer's responsibility once the hosting service has been entrusted to the provider?	The certification is held by the hosting provider and covers the hosting component only. It does not cover the customer's applications or its obligations under the GDPR.
7	Backup and Disaster Recovery	How are backups and service continuity ensured (Recovery Point Objective (RPO) / Recovery Time Objective (RTO))?	Backup is one of the activities covered by the HDS framework, but it does not, on its own, guarantee business continuity, which is a separate matter. Contractually defined RPO and RTO targets make it possible to measure the acceptable level of data loss and the target recovery time.
8	Reversibility	Can all data be retrieved in a usable format, allowing the customer to leave the platform without technical dependency?	Insufficient reversibility creates vendor lock-in, which can increase the cost or duration of a migration and make it more difficult to switch providers—for example, when migrating to a sovereign solution.
9	Transparency	Does the provider publish a mapping of data transfers outside the European Economic Area and document its commitments and security measures?	The revised HDS framework already requires providers to publish and keep up to date a mapping of transfers outside the EEA, remote access locations and the risks of data access by non-European states. This obligation is also incorporated into the French Public Health Code through Decree No. 2026-209 of 24 March 2026, with a deferred entry into force for these provisions (six months after publication in the Official Journal). If this information is not available, the applicable version of the HDS framework should be verified and the provider should be asked how it complies with its transparency obligations.
10	Managed Operations	Does the platform provide encryption, isolation, backups, monitoring and updates as managed services, or must these layers be configured by the customer?	The more the provider limits its service to infrastructure layers, the more responsibility the customer assumes for configuring, operating and monitoring the upper layers. This division of responsibilities must be clearly defined to avoid gaps in coverage.

Disclaimer

This framework is intended as a decision-making aid to structure the assessment of a health data hosting provider. It does not constitute legal advice. The regulatory references cited are provided for information only; their applicability depends on the nature of the data being processed and the specific circumstances of each organisation. For sensitive processing activities, the support of a Data Protection Officer (DPO) or legal counsel is recommended.

Sources

- French Decree No. 2026–209 of 24 March 2026 amending provisions of the French Public Health Code relating to the hosting of health data (Journal Officiel, 26 March 2026). The provisions relating to storage location and transfer mapping become applicable six months after publication.
- CNIL – Recommendations on health data hosting; guidance dated 19 July 2024 on the risks of access to sensitive data by foreign authorities.
- French Digital Health Agency (ANS) – HDS Certification Framework for Health Data Hosting Providers.
- French Court of Auditors – Recommendation to align the HDS framework with SecNumCloud requirements.
- French Public Health Code, Articles L.1111–8, R.1111–9–1 and R.1111–11.