ISO 27001 and HDS: How we built a security-first infrastructure for health data

August 4, 2025

At Epigene Labs, data security is embedded into the architecture of everything we build. We're proud to announce that our organization is now ISO/IEC 27001:2022 certified, and officially certified for Health Data Hosting (Hébergeur de Données de Santé – HDS). These certifications are not just compliance milestones – they're proof that our infrastructure, processes, and governance are aligned with international best practices in cybersecurity.

Trust and scalability begin with how you handle health data

Security certifications are not the end, they're the foundation. They provide assurance that we have robust and repeatable controls in place to protect **health data**, but our mission goes beyond compliance.

We're building a resilient, privacy-preserving platform that can scale across borders and regulatory regimes.

Whether you're a **healthcare** provider, research institution, or technical partner, you can trust that our systems are built to:

- Maintain the privacy, integrity, and availability of data
- Support GDPR and HIPAA-aligned data processing principles
- Enable secure integrations through APIs, SSO, and role-based access
- Adapt rapidly to new threats and compliance requirements

What do these certifications actually mean for health data security?

ISO 27001 is the leading international standard for Information Security Management Systems (ISMS). It defines a risk-based methodology for implementing and continuously improving security controls across people, processes, and technology.

This includes areas such as:

- Identity and access management (IAM)
- Network segmentation and secure architecture
- Incident response and recovery procedures
- Secure software development lifecycle (SSDLC)
- Business continuity planning (BCP)

ISO 27001 and HDS: How we built a security-first infrastructure for health data

August 4, 2025

Our ISMS is aligned with ISO 27001:2022 and audited by an independent accredited body. It ensures we systematically assess risks related to **health data**, implement mitigating controls, and monitor the effectiveness of those controls over time.

HDS Certification goes one step further. Mandated by French law (Article L.1111-8 of the French Public Health Code), HDS ensures that any provider hosting or processing personally identifiable health data complies with strict security, availability, and traceability requirements.

We are certified under both:

- **Scope 3**: Provision and operational maintenance of the application hosting platform for the information system
- **Scope 4**: Provision and operational maintenance of the virtual infrastructure of the information system used for processing health data
- **Scope 5**: Administration and operation of the information system containing health data
- **Scope 6**: Offsite backup of health data

This dual certification confirms that we comply with the expectations of CNIL and ANS regarding encryption, data isolation, logging, system hardening, and data residency in France or the EU.

Security architecture and operational controls

Achieving these certifications required a full-stack review and reinforcement of our infrastructure. Key components of our security program include:

- **Zero Trust Architecture (ZTA)**: We enforce strong authentication, least privilege access, and contextual authorization across all systems and services.
- **Infrastructure as Code (IaC)**: All infrastructure is provisioned using Terraform and continuously validated through security linters and policy-as-code (e.g. Open Policy Agent).
- **Cloud-native security controls**: We use DevSecOps solutions to monitor configuration drift, vulnerability exposure, and runtime threats across our cloud environments.
- **Automated patch management**: Regular updates are deployed with CI/CD pipelines, and critical vulnerabilities are addressed with SLAs defined in our ISMS risk treatment plan.

Why health data security matters – especially in the medical sector

Health data is not only sensitive, it is increasingly targeted by advanced persistent threats (APT) and ransomware groups. Unlike other industries, **healthcare** cannot afford downtime or breaches – every second of exposure puts lives and privacy at risk.
For a startup, reaching this level of compliance and operational security is a significant achievement.

ISO 27001 and HDS: How we built a security-first infrastructure for health data

August 4, 2025

It reflects:

- A mature DevSecOps culture across engineering and operations
- An auditable ISMS with documented controls and continuous improvement loops
- Executive-level support for long-term investment in security and privacy engineering

Security is not a feature – it's infrastructure.

If you're interested in our architecture, partnerships, or certifications, get in touch.
We're always open to sharing how we build secure systems for sensitive data.

Authors: Mathieu Guery & Benjamin Millot