

GALIMED AI — Care Intelligence Platform

Supplemental content for Microsoft Marketplace certification · Security, compliance and data residency · 29 July 2026

1. What the product is, and what it is not

GALIMED is a clinical workflow and care-coordination platform for healthcare professionals and organisations. It assists documentation and triage; it does not diagnose, does not prescribe, and takes no autonomous medical decision.

Safety rule enforced in the code. No output of the platform carries medical weight until a registered physician has validated it. The constraint is applied server-side, stated on screen, printed on the exported document, and returned in every API response — not only written in the terms of service.

2. Data residency

Health data for patients and hospitals in the United States is stored in the United States (Azure East US 2). All other health data is stored in the European Union (Azure France Central). Routing is decided by the application at write time and verified in production every day.

3. Authentication and access control

- Microsoft Entra ID single sign-on; JWT sessions for the application; scoped API keys for machine access
- Two-factor authentication: TOTP and WebAuthn / FIDO2 passkeys
- Identity verification (KYC) of every practitioner through Stripe Identity; hospitals additionally provide registration and licence documents
- Role-based access control across nine roles; an API key is refused outright when it lacks the required scope, never served partial data

4. Platform security

- TLS 1.2+ in transit; encryption at rest on Azure Cosmos DB and Azure Storage
- Secrets held in Azure Key Vault under managed identity; no secret in clear in the application
- Strict Content Security Policy, security headers, rate limiting
- Request correlation and audit logging in Azure Application Insights
- Billing webhooks authenticated: Stripe signature, PayPal, and Microsoft Entra JWT for Marketplace

5. Compliance position

Framework	Status	Basis
GDPR (EU), DPA and BAA	In place	Record of processing, contractual DPA/BAA, data-subject rights, minimisation
HDS (French health data hosting)	In progress	Runs on Microsoft Azure, itself HDS-certified. GALIMED does not claim the certification in its own name until the certificate is issued.
ISO/IEC 27001	On track	ISMS under construction; internal audit before certification audit
SOC 2 (Type I then II)	Planned	Controls defined; observation period then independent audit
HIPAA (USA)	On track	HIPAA-oriented controls, BAA, audit logging, dedicated US deployment profile

6. How a buyer gets started

After purchase, Microsoft redirects the buyer to the GALIMED activation page. Signing in with the Microsoft Entra account that made the purchase links the subscription automatically. Team members are invited from the administration console; each practitioner completes identity verification once. Every workspace opens with a guided tour, and a narrated video walkthrough exists for each one, in English and French.

7. Integration

A public REST API is available with scoped keys: analyses, physician-validated prescriptions, patient record, and an HL7 FHIR R4 Patient resource. Calendar synchronisation with Outlook and Google is built in. Webhooks are signed with HMAC-SHA256.

8. Support

support@galimedai.org · Documentation and tutorials: www.galimedai.org/faq-tuto-en.html · Security and compliance: www.galimedai.org/compliance-en.html