# PREDICT — Compliance Attestation

HIPAA · SOC 2 Type II · EU AI Act readiness · ERISA fiduciary alignment

***Maturity disclosure.*** *PREDICT v0.1 is a working pipeline trained on simulated cohorts and is not approved for production use. The metrics below are v1.0 target spec, validated against the simulated test set. First real-world readout is targeted Q3 2026. See predict-methodology.html for the full Model Card.*

## HIPAA

JetPatient executes a HIPAA Business Associate Agreement with every self-funded plan sponsor, every TPA partner, and every sub-processor. All PHI is encrypted with TLS 1.3 in transit and AES-256 at rest. Member identifiers are tokenized at the TPA boundary before reaching the PREDICT inference layer. Audit logs are retained for seven years and exportable on request.

## SOC 2 Type II

Schellman is engaged as our SOC 2 Type II auditor; the current observation period began 2026-01-01 and concludes 2026-09-30. The first Type II report is targeted for issuance Q4 2026. SOC 2 Type I report is available under NDA — request via trust@jetpatient.com. Pending the Type II report, our security whitepaper, penetration-test summary, and sub-processor list are available in the Trust Center.

## EU AI Act readiness

Under the EU AI Act (in force 2026), PREDICT is classified as a high-risk AI system per Annex III §5(a) (access to essential services — health insurance). JetPatient maintains a conformity assessment file covering: risk management system (Art. 9), data governance (Art. 10), technical documentation (Art. 11), record-keeping (Art. 12), transparency (Art. 13), human oversight (Art. 14), accuracy/robustness/cybersecurity (Art. 15). Full conformity-assessment package available under NDA.

## ERISA fiduciary alignment

PREDICT outputs are advisory; the plan sponsor and the plan's fiduciary committee retain sole authority over benefit-design and outreach decisions. JetPatient does not exercise discretionary authority over plan administration. The model card, validation pack, and quarterly fairness audit are the standard artifacts a fiduciary committee can place in the plan's investment-committee minutes to evidence prudent-process review under ERISA §404(a)(1)(B).

## Anti-Kickback Statute (AKS) posture

JetPatient's plan-agnostic pricing model (no PEPM, pay-per-routed-case) and the absence of any provider-side revenue share for plan referrals have been reviewed against AKS safe-harbor guidance. A summary memo is available for plan counsel under NDA.

## Sub-processors

| Sub-processor | Function | Region | Audit |
|---|---|---|---|
| AWS | Compute, storage, networking | us-east-1, us-west-2 | SOC 2, ISO 27001, HITRUST |
| Snowflake | Data warehouse | us-east, us-west | SOC 2, HITRUST |
| Databricks | Model training pipeline | us-east | SOC 2, ISO 27001 |

| Sub-processor | Function | Region | Audit |
|---|---|---|---|
| Datadog | Observability, log retention | us1 | SOC 2 |
| Auth0 | SSO / SAML / MFA | us | SOC 2, ISO 27001 |
| Twilio (SendGrid) | Transactional email | us | SOC 2 |

## Incident response

Security incidents are triaged 24×7 by an on-call team with a documented escalation matrix. Confirmed PHI incidents are reported to affected covered entities within 24 hours, well inside the HIPAA 60-day notification window. The most recent tabletop exercise was completed 2026-03-08; the incident-response runbook is available under NDA via the Trust Center.

## Contact

All compliance correspondence: **trust@jetpatient.com**. Security incidents (24×7): **security@jetpatient.com**.