

# JetPatient — Integration Architecture

EDI · FHIR R4 · SFTP · OAuth 2.0 · for TPAs, ASOs, and self-funded plan sponsors

**Audience.** Integration engineers, security architects, and plan-data stewards at TPAs and self-funded plan sponsors. This spec is the reference you implement against; the marketing page at [jetpatient-tpas.html](https://jetpatient.com/tpas.html) is the conversation starter, this is the conversation finisher.

## 1. Architecture overview

JetPatient is a plan-agnostic bundled-care navigation layer. It receives tokenized eligibility and claims feeds from your TPA, runs PREDICT scoring against the population, and surfaces a ranked outreach cohort to the sponsor's benefits team inside Guardian. Routed cases flow back through standard 835 / 837 transactions so the TPA remains the plan-of-record. There is no shadow ledger.

Three planes:

(a) **Data plane** — EDI 834 / 837 / 820 / 835 / 270 / 271; FHIR R4 alternatives.

(b) **Identity plane** — OAuth 2.0 client-credentials + SAML 2.0 SSO + SCIM.

(c) **Application plane** — Guardian Console (SPA), PREDICT inference API, member outreach engine.

## 2. Data plane · EDI transactions

| Txn     | Name                             | Direction        | Cadence                        | Required    |
|---------|----------------------------------|------------------|--------------------------------|-------------|
| 834     | Benefit enrollment & maintenance | TPA → JetPatient | Monthly full + mid-cycle delta | Yes         |
| 837     | Health-care claim (I + P)        | TPA → JetPatient | 36–60mo bulk + monthly delta   | Yes         |
| 820     | Premium / fee remittance         | Sponsor → TPA    | Per pay-cycle                  | Optional    |
| 835     | Claim payment / advice           | JetPatient → TPA | Per routed case (wrap only)    | Wrap only   |
| 270/271 | Eligibility inquiry / response   | Bidirectional    | Real-time                      | Recommended |

### 2.1 Companion-guide deltas vs. CAQH CORE

Our 834 companion guide aligns with the CAQH CORE Phase IV companion-guide template, with three deltas: (a) tokenized member identifier in REF\*0F rather than NM1\*IL\*SSN; (b) plan-tier code in REF\*ZZ qualifier; (c) JetPatient routing flag in REF\*Q5 for sponsors that pre-flag opted-in members. Full companion guide ships under MSA.

### 2.2 837 claim history bulk load

Initial bulk: 36–60 months of de-identified institutional and professional claims, segmented by procedure family. Acceptable file size up to 8 GB per drop; larger files split per HIPAA chunk-size conventions. SFTP delivery preferred; HTTPS multipart upload supported. Format: standard 837 with no proprietary extensions.

## 3. Data plane · FHIR R4 (alternative to EDI)

For TPAs that have stood up CMS Patient Access APIs (per CMS-9115-F), JetPatient supports FHIR R4 as an alternative transport for the same data. Supported resources: Patient, Coverage, ExplanationOfBenefit, Claim, Encounter, Organization, Practitioner. SMART-on-FHIR launch supported for sponsor-side Guardian sign-in.

### Example: Patient resource fetch

```
GET /fhir/r4/Patient?identifier=https://jetpatient.com/tokens|<TOKEN>
```

Authorization: Bearer <oauth\_access\_token>  
Accept: application/fhir+json

Response 200 OK

```
{
  "resourceType": "Patient",
  "id": "jp-tok-9f3d...",
  "identifier": [
    { "system": "https://jetpatient.com/tokens", "value": "jp-tok-9f3d..." }
  ],
  "meta": {
    "security": [{ "system": "http://hl7.org/fhir/v3/ActReason", "code": "HOPERAT" }]
  }
}
```

4. Identity plane · OAuth · SAML · SCIM

Machine-to-machine authentication for the data plane uses OAuth 2.0 client-credentials flow with mTLS pinning at the JetPatient edge. Human authentication for the Guardian Console uses SAML 2.0 with Just-In-Time provisioning, or SCIM 2.0 for full lifecycle management. Auth0 is our default IdP broker; Okta, Azure AD, and Ping Identity are tested and supported.

|                |                                                                                          |
|----------------|------------------------------------------------------------------------------------------|
| OAuth grant    | client_credentials with audience claim; access tokens TTL 15 min; refresh tokens TTL 24h |
| Token endpoint | POST https://auth.jetpatient.com/oauth/token                                             |
| mTLS           | Required for production; client certificate pinned at edge; rotation cadence 90 days     |
| SAML SSO       | SP-initiated and IdP-initiated both supported; SCIM 2.0 user provisioning available      |
| RBAC roles     | Plan Admin · Benefits Manager · Read-Only · Broker · TPA — defined in §6                 |
| MFA            | TOTP and FIDO2 WebAuthn; mandatory for Plan Admin and Benefits Manager roles             |

5. Application plane

| Surface                | Audience                            | Transport         | Latency target                  |
|------------------------|-------------------------------------|-------------------|---------------------------------|
| Guardian Console (SPA) | Benefits Manager, TPA Admin, Broker | HTTPS + WSS       | < 300 ms p95                    |
| PREDICT inference API  | Sponsor batch + Guardian outreach   | HTTPS REST        | < 800 ms per 1k members         |
| Member outreach engine | End member via SMS + email          | SendGrid + Twilio | Best effort                     |
| Webhook callbacks      | TPA event consumer                  | HTTPS POST        | 5 retries · exponential backoff |
| Member portal          | Routed-case member                  | HTTPS             | < 400 ms p95                    |

6. Security architecture

|                 |                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------|
| Data in transit | TLS 1.3 (minimum); mTLS at integration edge; HSTS preload                                           |
| Data at rest    | AES-256-GCM; per-tenant KMS-managed keys; backup encryption identical                               |
| Tokenization    | FPE (format-preserving encryption) at TPA boundary; raw member identifiers never reach JetPatient c |

|                    |                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------|
| Network isolation  | Per-tenant VPC + PrivateLink available for >5,000-life sponsors                                 |
| Logging            | Audit log immutable, exportable; 7-year retention; SIEM integration via syslog or Splunk HEC    |
| Vulnerability mgmt | Snyk continuous scan; quarterly pen-test by an independent third party (most recent 2026-03-08) |
| Incident response  | 24×7 on-call; PHI incident notification within 24 hours (well inside HIPAA's 60-day window)     |
| Sub-processors     | AWS, Snowflake, Databricks, Auth0, Datadog, SendGrid — BAA chain documented in Trust Center     |

7. RBAC role hierarchy

| Role             | Scope                         | Read                   | Write                              | Audit-log export |
|------------------|-------------------------------|------------------------|------------------------------------|------------------|
| Plan Admin       | Sponsor-wide                  | All                    | All                                | Yes              |
| Benefits Manager | Sponsor-wide ops              | All members + outcomes | Outreach, network selection        | Self             |
| Read-Only        | Sponsor-wide read             | All                    | None                               | No               |
| Broker           | Sponsor-of-record only        | Limited                | Outreach proposals (approval req.) | Self             |
| TPA              | Cross-sponsor by relationship | Integration health     | Eligibility re-sync, claim acks    | Self             |

8. Sandbox · UAT · go-live

|                    |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| Sandbox host       | https://sandbox.jetpatient.com — full functional parity with prod, isolated tenant    |
| Sandbox creds      | Issued under MSA + BAA; client_id + client_secret + mTLS certificate bundle           |
| Test data          | Synthetic 5,000-member census with full 60mo claims history; replenished weekly       |
| Postman collection | Available on request — covers 834 ingestion, 837 bulk load, FHIR R4 fetch, OAuth flow |
| UAT length         | 10 business days typical; covers happy-path + 6 edge-case scenarios                   |
| Go-live gate       | All UAT scenarios pass + sponsor sign-off + integration runbook signed by both teams  |
| Time to live       | Typical 14–21 days from BAA execution for carve-out; 60–90 days for wrap arrangement  |

9. Operational SLAs

| Metric                        | Target                            | Measurement window |
|-------------------------------|-----------------------------------|--------------------|
| Data-plane uptime             | 99.9%                             | rolling 90-day     |
| Guardian Console uptime       | 99.9%                             | rolling 90-day     |
| PREDICT inference latency     | < 800ms p95 per 1k members        | rolling 7-day      |
| 834 ingest acknowledgment     | < 15 min                          | per file           |
| Outreach delivery (SMS)       | 99% within 5 min of trigger       | rolling 24h        |
| Incident notification (Sev-1) | < 15 min                          | per incident       |
| Status page                   | status.jetpatient.com (24×7 live) | —                  |

## 10. Contact

**Integration questions:** [integrations@jetpatient.com](mailto:integrations@jetpatient.com)

**Security & compliance:** [trust@jetpatient.com](mailto:trust@jetpatient.com)

**Incident response (24x7):** [security@jetpatient.com](mailto:security@jetpatient.com)

**Status page:** [status.jetpatient.com](https://status.jetpatient.com)