VitaAI Platform

Client Deployment Architecture

Enterprise-Grade Isolation. Purpose-Built Healthcare Infrastructure.

June 2026

Prepared by Altnetix, LLC

POWERED BY

Microsoft Azure

HIPAA COMPLIANT | DEDICATED INFRA | SOC 2 READY | FHIR R4 CERTIFIED

Your Own Azure Environment. No Shared Infrastructure.

Every VitaAI enterprise client receives a completely dedicated Azure deployment. Your organization's PHI never shares compute, storage, database, or encryption keys with any other client. This document describes what gets provisioned, how it connects, and the step-by-step process from contract signature to go-live.

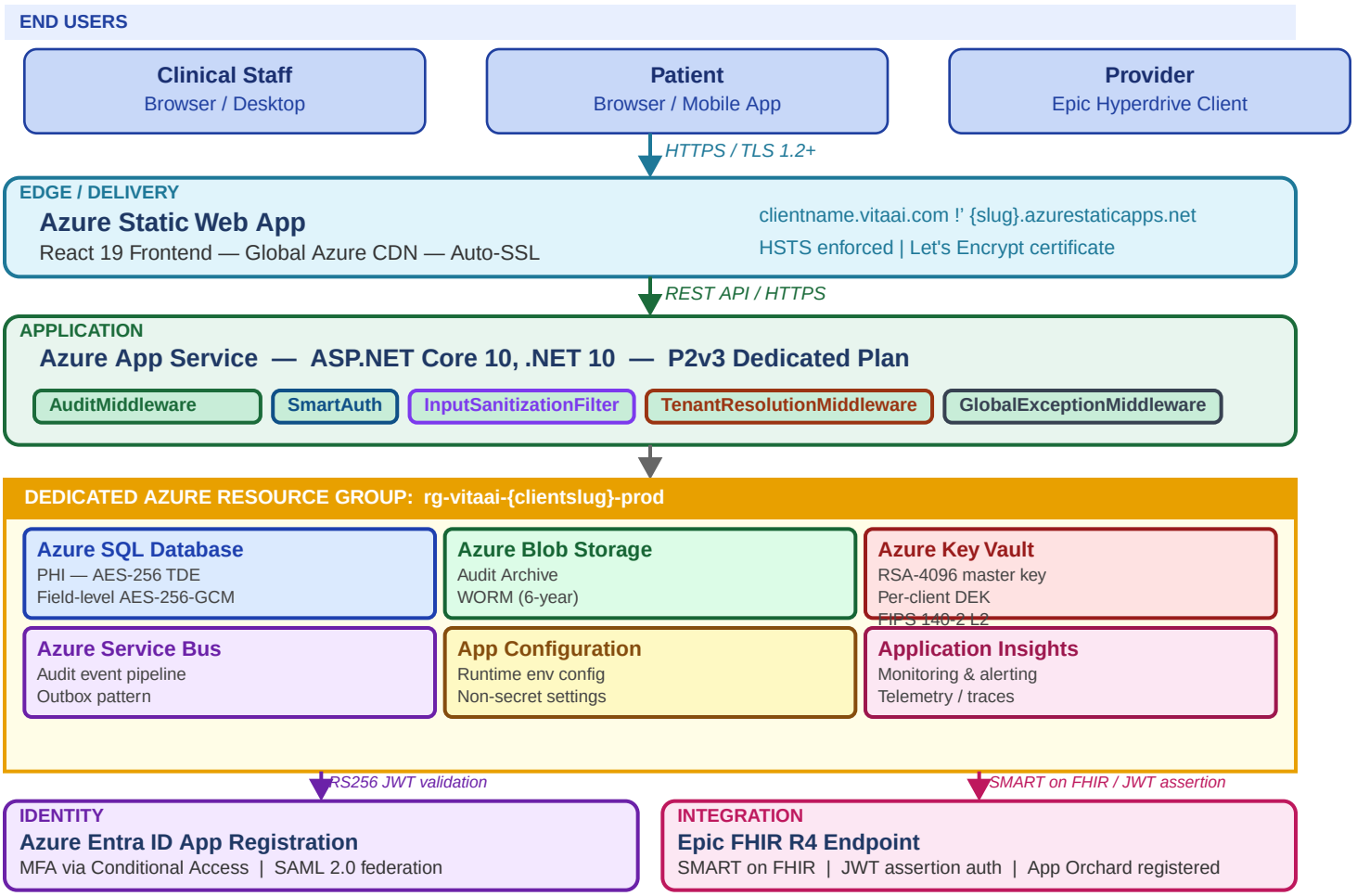
What Your Dedicated Deployment Includes:

- **Dedicated Azure Resource Group**
  Complete logical isolation enforced by Azure RBAC — rg-vitaai-{clientslug}-prod
- **Dedicated Azure SQL Database**
  Your PHI never co-mingles with another organization's data. No shared schema, no shared queries.
- **Dedicated Azure Key Vault**
  Your encryption keys are yours alone — RSA-4096 master key + per-client AES-256-GCM DEK
- **Dedicated App Service Plan**
  No noisy-neighbor CPU/memory contention — P2v3 dedicated compute (2 vCores, 7 GB RAM)
- **Dedicated Entra ID App Registration**
  Your SSO configuration, your users, your app roles (Administrator, Clinician)
- **Custom Subdomain**
  clientname.vitaai.com with auto-SSL, or bring your own domain via CNAME
- **Epic FHIR R4 Integration**
  Configured per your Epic tenant credentials — App Orchard registered, JWT assertion auth

No Multi-Tenancy at the Infrastructure Layer

Unlike multi-tenant SaaS platforms that share a single database and rely on application-level tenant filters, VitaAI provisions a physically separate Azure SQL Database instance for each client. There is no WHERE clause or row-level filter that could inadvertently expose another client's data.

Architecture Overview — Per-Client Azure Deployment



Key Data Flows:

- App Service !' SQL: TLS + EF Core field-level AES-256-GCM
- App Service !' Key Vault: Managed Identity (no secrets in code)
- App Service !' Service Bus: Audit event outbox
- Service Bus !' Blob: WORM audit archive

Deployment Process — Contract to Go-Live

Eight phases from resource provisioning to client handoff

Phase 01 — Pre-Provisioning

Days 1–2 | 4–8 hours

Owner: Altnetix Ops

- Collect client intake form: tenant name, subdomain, admin email, SSO type, Epic Y/N
- Create Azure Resource Group: rg-vitaai-{clientslug}-prod with subscription RBAC
- Register Entra ID application: configure app roles (Administrator, Clinician)
- Generate RSA-4096 master encryption key in new Azure Key Vault instance
- Generate 256-bit per-client DEK; wrap with master key; store as Tenants--{slug}--Dek
- Configure Managed Identity on App Service — zero-credential Key Vault access

Phase 02 — Infrastructure Provisioning

Days 2–3 | 2–4 hours

Owner: Altnetix Ops

- Deploy Azure SQL Database (General Purpose, 4 vCores, geo-redundant backup, TDE enabled)
- Deploy Azure Blob Storage (LRS, WORM immutability policy, 6-year retention)
- Deploy Azure Service Bus namespace (Standard tier, audit-events queue)
- Deploy Azure App Configuration + Application Insights workspace
- Deploy Azure Static Web App (Standard tier) + App Service Plan (P2v3) + App Service

Phase 03 — Application Deployment

Days 3–4 | 2–3 hours

Owner: Altnetix DevOps

- Set Key Vault secrets: Jwt:Key, AzureAd:ClientSecret, Resend:ApiKey
- Set App Service env vars: ASPNETCORE_ENVIRONMENT, KeyVault:Uri, AzureAd:*, CorsOrigins
- Deploy backend API via GitHub Actions CI pipeline to App Service
- Run EF Core migrations — creates AuditLogs, BreachIncidents, RevokedTokens, EpicTenantConfigs tables
- Deploy React frontend build to Azure Static Web App (swa deploy)

Phase 04 — DNS & Domain Configuration

Days 4–5 | 1–2 hrs + DNS propagation

Owner: Altnetix + Client IT

- Create Static Web App custom domain: {clientslug}.vitaai.com
- Client IT adds CNAME: {clientslug}.vitaai.com !’ {swa}.azurestaticapps.net
- Verify domain ownership via TXT record; auto-SSL provisioned (Let's Encrypt via Azure CDN)
- Configure CORS on App Service: AllowedOrigins = https://{clientslug}.vitaai.com
- Verify HTTPS redirect (HTTP !’ 301), HSTS header (max-age=31536000), and CSP headers

Deployment Process (continued)

Phases 5–8: SSO, Epic FHIR, Smoke Testing, and Client Handoff

Phase 05 — SSO Configuration

Days 5–6 | 2–4 hours

Owner: Altnetix + Client IdP Team

- Export SAML SP metadata: https://api.{clientslug}.vitaai.com/saml/metadata
- Provide SP metadata to client's IT team (Okta / ADFS / Azure AD / Ping Identity)
- Receive IdP metadata XML; upload to VitaAI SamlConfigService via admin API
- Configure claim mapping: email, givenname, surname, role !' Clinician/Administrator
- Test IdP-initiated and SP-initiated SSO; verify ProviderOnly API endpoint access

Phase 06 — Epic FHIR Integration

Days 6–8 | 4–8 hrs + Epic IT coordination

Owner: Altnetix + Client Epic Team

- Register VitaAI in Epic App Orchard; generate RSA key pair for JWT assertion auth
- Store private key in Key Vault as epic-{clientslug}-private-key
- Insert EpicTenantConfig: ClientId, PrivateKey ref, TokenEndpoint, FhirBaseUrl, IsEnabled=true
- Test EHR Launch (Hyperdrive): SMART auth !' patient context !' VitaAI encounter view
- Test nightly sync: Patient, Encounter, Observation, Condition, MedicationRequest FHIR resources

Phase 07 — Smoke Testing & Validation

Days 8–9 | 4–6 hours

Owner: Altnetix QA

- Auth smoke: provider login (Entra/SAML), patient login, logout + token revocation (HTTP 401)
- PHI audit: create encounter !' verify ContainsPHI=true, SHA-256 hash chain integrity
- Encryption check: query raw SQL — confirm PHI columns are ciphertext (not plaintext)
- Audit archive: flush batch !' verify JSONL blob in Blob Storage with WORM immutability
- Security: confirm HTTP 429 on rate limit, HTTPS redirect, HSTS + CSP headers present

Phase 08 — Client Handoff

Days 9–10 | 2–4 hours

Owner: Altnetix Account Team

- Provision admin user accounts for client's IT administrator in Entra ID
- Deliver admin portal credentials, architecture doc, and HIPAA Security Controls doc
- Execute Business Associate Agreement (if not already signed pre-deployment)
- Schedule 30-day check-in call; transition to ongoing support team

Deployment Timeline

Typical Go-Live: 10 Business Days from Contract Signature

Phase	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8	Day 9	Day 10
Pre-Provisioning	Day 1–2									
Infrastructure		Day 2–3								
App Deployment			Day 3–4							
DNS & Domain				Day 4–5						
SSO Configuration					Day 5–6					
Epic FHIR (optional)						Day 6–8				
Smoke Testing								Day 8–9		
Client Handoff									Day 9–10	

** Epic FHIR integration depends on client Epic IT availability — may extend timeline to Day 14.*

** DNS propagation may add 12–24 hours to the domain configuration phase.*

** Expedited deployments possible in 5 business days for clients without SAML or Epic integration.*

10	8	5	0
Business Days Typical Go-Live	Deployment Phases	Days Go-Live Simple Deployments	PHI Shared With Other Clients

Security Architecture — Complete Client Isolation

Data Isolation

- Every client's PHI lives in a dedicated Azure SQL Database instance — no shared database, no shared schema, no multi-tenancy at the data layer.
- PHI is encrypted with a per-client AES-256-GCM Data Encryption Key. One client's DEK cannot decrypt another client's data.
- Azure SQL Transparent Data Encryption (TDE) encrypts the database at rest — storage media removed from a data center is unreadable.

Key Management Isolation

- Each client's Azure Key Vault is provisioned as a dedicated resource containing only that client's secrets and encryption keys.
- The RSA-4096 master encryption key is generated fresh per client. Key material never leaves the Key Vault HSM boundary.
- App Service accesses Key Vault via Managed Identity — no client secrets, no passwords, no credentials in environment variables or code.

Compute Isolation

- Each client runs on a dedicated Azure App Service Plan (P2v3 — 2 vCores, 7 GB RAM). No shared process space, memory, or CPU with other clients.
- App Service environment variables (database connection string, Key Vault URI, AzureAd tenant) are scoped exclusively to that client's App Service.
- Blue/green deployment slots enable zero-downtime updates. Maintenance windows are schedulable per client.

Identity Isolation

- Each client has a dedicated Entra ID App Registration. Clinical staff roles (Administrator, Clinician) are managed within that registration only.
- Patient accounts are scoped to the client's database. A patient at Client A cannot access Client B — enforced at both application and database layers.
- SAML configurations load at runtime per subdomain. Cross-tenant SSO token acceptance is architecturally impossible.

Audit & Logging Isolation

- Audit logs for each client are written to that client's dedicated Azure Blob Storage account. No log data from other clients is in scope.
- WORM immutability policies on Blob containers prevent deletion or modification for 6 years — exceeding HIPAA minimum retention requirements.
- Application Insights telemetry is tagged with the tenant slug. Separate Application Insights workspace is available on request.

Network Isolation

- CORS policy restricts API access to the client's subdomain only (https://{clientslug}.vitaai.com). Requests from other origins receive HTTP 403.
- Azure Application Gateway with WAF (Web Application Firewall) protection is available as an add-on for enhanced DDoS and injection defense.
- Inter-service communication within the Resource Group uses Azure private endpoints on Standard/Premium tiers, keeping traffic off the public internet.

Azure Resources Provisioned Per Client

All resources deployed in a dedicated Resource Group — rg-vitaai-{clientslug}-prod

Azure Resource	SKU / Tier	Purpose	Est. Cost
Azure Resource Group	N/A (free)	Logical container + RBAC boundary	$0
App Service Plan (P2v3)	Premium v3 P2	API compute — 2 vCores, 7 GB RAM dedicated	~$150/mo
Azure App Service	Included in plan	ASP.NET Core 10 API runtime + deployment slots	Incl.
Azure SQL Database	General Purpose, 4 vCores	PHI data store, geo-redundant automated backups	~$370/mo
Azure Static Web App	Standard	React 19 frontend, global CDN, auto-SSL	~$9/mo
Azure Key Vault	Standard (HSM optional)	Encryption keys, secrets management	~$5–10/mo
Azure Blob Storage	LRS + WORM policy	Audit log archive (6-year WORM immutability)	~$2–5/mo
Azure Service Bus	Standard	Audit event streaming pipeline	~$10/mo
Azure App Configuration	Standard	Runtime environment configuration	~$1.20/mo
Application Insights	Pay-as-you-go	Monitoring, tracing, alerting (5 GB free)	~$5–15/mo
Azure AD App Registration	Free	Provider SSO + RBAC role management	$0
Entra ID P1 (per user)	P1 license	MFA + Conditional Access per clinical user	~$6/user
Total Base Infrastructure Cost			**~$560–600/mo + $6/user/mo (MFA)**

- Costs are estimates based on Azure public pricing as of June 2026. Actual costs vary by region, usage, and reserved capacity.
- Epic FHIR integration requires no additional Azure resources — uses the client's existing Epic license.
- Add-ons: Azure Application Gateway (WAF), Azure Front Door (global load balancing), Entra ID P2 (PIM, Identity Protection).
- 1-year reserved pricing can reduce App Service and SQL Database costs by up to 40%.

Reserved Capacity Savings: 1-year reserved pricing can reduce App Service and SQL Database costs by up to 40%. Contact Altnetix for volume pricing on multi-client enterprise agreements.

Ready to Deploy?

Altnetix deploys VitaAI in as little as 5–10 business days. Our team handles all Azure provisioning, deployment, SSO, and Epic integration.

What Altnetix Handles End-to-End:

- All Azure resource provisioning (App Service, SQL Database, Key Vault, Service Bus, Static Web App)
- Backend API and React frontend deployment with full production configuration
- Encryption key generation (RSA-4096 master + per-client AES-256 DEK) and Key Vault setup
- EF Core database migration and initial schema setup
- CORS, HTTPS, HSTS, Content Security Policy, and security header configuration
- SAML 2.0 or Azure Entra ID SSO configuration and end-to-end testing
- Epic FHIR R4 App Orchard registration, JWT assertion setup, and integration testing
- Full smoke testing and security validation checklist before client handoff

Your IT Team's Involvement Is Limited To:

- Providing your SAML IdP metadata (if using enterprise SSO — Okta, ADFS, Ping, or Azure AD)
- Coordinating Epic App Orchard registration (if using Epic FHIR integration)
- Approving a DNS CNAME record for your subdomain (clientname.vitaai.com)
- Reviewing and signing the Business Associate Agreement

Altnetix, LLC

Contact our deployment team:

deployments@altnetix.com

www.altnetix.com

Documents included with this package:

- HIPAA Security Controls (VTA-SEC-001)
- Trust & Security Overview
- Business Associate Agreement Template
- Security Self-Assessment Checklist (VTA-SEC-004)
- Client Deployment Architecture (this document)

This document describes the standard VitaAI enterprise deployment architecture as of June 2026. Architecture details, Azure SKUs, and pricing estimates are subject to change without notice. Specific client configurations may vary. Pricing estimates do not constitute a binding quote.