ALTNETIX LLC

VitaAI Platform

ENCRYPTION DOCUMENTATION

Cryptographic Controls and Key Management

Control Reference	APPS-2
Document Version	1.0
Effective Date	June 1, 2026
Next Review	June 1, 2027
Classification	Confidential – Internal & Customer Use
Maintained by	Altnetix LLC Security & Compliance Team
Contact	compliance@altnetix.com

1. Overview and Policy

Altnetix LLC implements encryption as a foundational security control across all layers of the VitaAI platform. This document describes all cryptographic standards, key management procedures, and implementation details required by HIPAA §164.312(a)(2)(iv) (encryption and decryption) and §164.312(e)(2)(ii) (encryption in transit).

2. Encryption at Rest

Database Layer

Azure SQL Database employs Transparent Data Encryption (TDE) with AES-256 encryption applied automatically to all database files, backups, and transaction logs. Database encryption keys are stored in Azure Key Vault under customer-managed key (CMK) configuration for enterprise accounts.

Blob Storage

Azure Blob Storage uses Azure Storage Service Encryption with AES-256-bit keys managed by Microsoft or customer-managed keys via Key Vault. WORM-protected audit log containers use immutability policies with separate encryption key hierarchies.

Field-Level Encryption (PHI)

Highly sensitive PHI fields (Social Security Numbers, dates of birth, patient identifiers) are encrypted at the application layer before database storage using AES-256-GCM. Per-tenant Data Encryption Keys (DEKs) are wrapped by Key Encryption Keys (KEKs) stored exclusively in Azure Key Vault. DEKs are cached in memory for up to 30 minutes; they are never written to disk.

3. Encryption in Transit

TLS Configuration

All communications between clients and the VitaAI API are encrypted using TLS 1.2 or TLS 1.3. TLS 1.0 and 1.1 are disabled at all layers. HTTPS is strictly enforced with HTTP Strict Transport Security (HSTS) at max-age=31536000; includeSubDomains; preload.

Approved Cipher Suites (TLS 1.2)

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F) — forward secret, AEAD
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030) — forward secret, AEAD

All CBC-mode and static-RSA cipher suites are disabled to eliminate padding oracle and BEAST attack vectors.

TLS 1.3 Cipher Suites

- TLS_AES_128_GCM_SHA256 — mandatory per RFC 8446
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Internal Service Communication

All internal API-to-service communications (SignalR, Service Bus, Key Vault, Azure SQL) use TLS 1.2+ with certificate validation enforced. Private endpoints are used to keep internal traffic off the public internet.

4. Key Management

Cryptographic key management follows NIST SP 800-57 guidelines:

- All production keys are stored exclusively in Azure Key Vault (FIPS 140-2 Level 2)
- Key hierarchy: Master Key (KEK) !’ Data Encryption Key (DEK) !’ Field-level encryption
- DEK rotation is performed annually or upon suspected compromise
- Key access is restricted to the Platform service identity via Azure RBAC
- Key access is logged and audited in Azure Monitor with 6-year retention
- Development environments use separate key stores; production keys are never used in dev

5. Certificate Management

TLS certificates are issued by GeoTrust TLS RSA CA G1 (DigiCert). Certificates are RSA 2048-bit with SHA-256 signatures. Certificates are monitored for expiration with automated 60-day advance renewal. Certificate Transparency logging is enabled for all issued certificates. DNS CAA records restrict certificate issuance to DigiCert.

6. Compliance Mapping

Requirement	Standard	Implementation
Encryption at rest	HIPAA §164.312(a)(2)(iv)	AES-256 via Azure TDE + field-level
Encryption in transit	HIPAA §164.312(e)(2)(ii)	TLS 1.2+ enforced, CBC suites disabled
Key management	NIST SP 800-57	Azure Key Vault, annual rotation
Certificate management	NIST SP 800-57	DigiCert, 2-year certs, auto-renewal
HSTS enforcement	OWASP / Qualys SSL A+	max-age=31536000, preload registered