VITAAI PLATFORM

Trust & Security Overview

Healthcare AI | *Enterprise Security* | *HIPAA-Ready Infrastructure*

June 2026 | Altnetix, LLC

HIPAA COMPLIANT	AZURE BAA EXECUTED	SOC 2 (IN PROGRESS)	ISO 27001 READY	FHIR R4 CERTIFIED

Our Commitment to Your Patients' Privacy

VitaAI is built security-first. Every architectural decision — from our choice of Microsoft Azure to our field-level AES-256-GCM encryption — reflects our commitment to protecting patient health information. We hold ourselves accountable through immutable audit trails, breach notification tooling, and a willingness to sign a Business Associate Agreement before any PHI touches our systems.

1. Built on Microsoft Azure — Enterprise-Grade Infrastructure

VitaAI runs exclusively on Microsoft Azure. We do not operate any on-premises servers, co-location racks, or third-party data centers. This means your patient data benefits from Microsoft's decades of enterprise security investment and their globally recognized compliance portfolio.

Microsoft Azure compliance certifications applicable to VitaAI:

Certification / Framework	What It Means for Your Organization
HIPAA/HITECH Business Associate Agreement	Microsoft signs a BAA covering all Azure services VitaAI uses. VitaAI countersigns your BAA as Business Associate.
SOC 2 Type II (Microsoft)	Independent audit of Azure security, availability, and confidentiality controls — available via NDA from Microsoft Trust Center.
ISO 27001 (Microsoft)	International information security management standard. Azure data centers are certified.
FedRAMP High (Microsoft)	Highest US government cloud security authorization — exceeds typical commercial healthcare requirements.

Certification / Framework	What It Means for Your Organization
FIPS 140-2 Level 2 (Azure Key Vault)	Federal cryptographic module validation — ensures encryption key operations meet government-grade standards.

Azure data centers provide biometric access controls, 24/7 security personnel, man-trap physical entry, and continuous video surveillance. Altnetix engineers never have physical access to servers running VitaAI.

2. Encryption — At Rest, In Transit, and Per Tenant

Encryption at Rest

Patient health information is encrypted at multiple layers before it ever reaches disk:

- ✓ Field-Level Encryption: Every PHI string field (patient names, clinical notes, allergies, medications, lab results, prescriptions, secure messages, encounter details) is individually encrypted using AES-256-GCM before being written to the database. This means even a compromised database backup reveals nothing readable.
- ✓ Tenant Isolation: Each client organization receives its own unique encryption key (Data Encryption Key). One tenant's data cannot be decrypted with another tenant's key, providing cryptographic tenant isolation.
- ✓ Key Management: Encryption keys are managed by Azure Key Vault using an RSA-4096 master key. Key material never leaves the Key Vault HSM boundary — VitaAI application code never touches raw private key bytes.
- ✓ Azure SQL Transparent Data Encryption (TDE): The entire database is additionally encrypted at the storage layer by Azure, providing defense-in-depth.
- ✓ Audit Archive: 6-year audit archives stored in Azure Blob Storage are encrypted server-side (AES-256).

Encryption in Transit

- ✓ All API traffic is encrypted using TLS 1.2 or higher. TLS 1.0, TLS 1.1, and SSL are disabled.
- ✓ HTTP Strict Transport Security (HSTS) with a 1-year max-age and preload flag ensures browsers never attempt an unencrypted connection.
- ✓ WebSocket connections (real-time clinical updates) use WSS (encrypted WebSocket over TLS).
- ✓ Forward Secrecy: ECDHE cipher suites ensure that a future key compromise cannot decrypt historical traffic.

3. Access Controls — Zero Trust, Role-Based

VitaAI enforces a Zero Trust access model: every API request is authenticated and authorized independently, regardless of network location.

Multi-Factor Authentication

- ✓ Clinical staff authenticate through Microsoft Azure Entra ID (formerly Azure Active Directory), with MFA enforced via Conditional Access policies.
- ✓ Enterprise organizations can bring their own Identity Provider via SAML 2.0 SSO — VitaAI federates with any standards-compliant SAML IdP (Okta, Ping, ADFS, Azure AD, etc.).

- ✓ Patient authentication uses email and password with account lockout after 5 failed attempts and a 15-minute lockout period.

Role-Based Access Control (RBAC)

- ✓ API endpoints enforce strict role separation: clinical staff endpoints require the 'ProviderOnly' authorization policy; patient endpoints require 'PatientOnly'. A patient token cannot access a clinical endpoint — this is structurally enforced in code, not configuration.
- ✓ Within clinical staff, roles (Administrator, Clinician) are managed in Azure Entra ID. Role revocation takes effect immediately on next token acquisition.
- ✓ Every user has a unique identifier logged in every audit record. Shared accounts are architecturally prevented.

Session Management

- ✓ Authentication tokens expire after 60 minutes.
- ✓ Explicit logout invalidates the token immediately via a server-side revocation table — the token is blocked on the next API call even if not yet expired.
- ✓ Staff tokens are stored in browser sessionStorage (cleared when the browser tab closes), following OWASP token storage guidance.

4. Audit Logging — Immutable, 6-Year Retention

VitaAI maintains a comprehensive, tamper-evident audit trail of all access to PHI. This satisfies HIPAA's Audit Controls requirement (§164.312(b)) and provides your compliance team with the evidence needed for investigations and regulatory reviews.

- ✓ Every API request is logged — including the user, action, HTTP path, IP address, device identifier, timestamp, and whether the request involved PHI.
- ✓ PHI access is automatically detected for 20+ clinical route patterns (/encounter, /prescription, /labresult, /vitals, /demographics, /transcript, and others).
- ✓ Hash-chained immutability: Each audit record includes a SHA-256 hash of itself and the previous record. Any modification or deletion of a record breaks the chain and is immediately detectable — providing forensic assurance for regulatory investigations.
- ✓ Retention: Full audit logs are archived to Azure Blob Storage with WORM (Write Once, Read Many) immutability policies for 6 years — meeting the HIPAA minimum retention requirement.
- ✓ Authentication events are separately classified: login success, login failure, password change, kiosk authentication, badge authentication.
- ✓ Breach incident events are logged with a PHI flag and preserved in the same 6-year archive.

5. Epic FHIR R4 Integration

VitaAI integrates natively with Epic via SMART on FHIR R4. The integration is registered as an Epic App Orchard application and uses your organization's existing Epic license — there is no additional Epic licensing cost.

- ✓ EHR Launch (Hyperdrive Embedded): Providers access VitaAI directly from within Epic's Hyperdrive client. VitaAI receives the patient context automatically via OAuth 2.0 SMART launch.
- ✓ Authentication: Uses asymmetric JWT assertion (signed with the client's private key registered in Epic) — no passwords stored.

- ✓ Data access: Patient demographics, active encounters, vitals, lab results, diagnoses, and medication lists via standard FHIR R4 resources.
- ✓ Data minimization: VitaAI reads only the FHIR data required for the active clinical session. No bulk Epic data is persisted in VitaAI systems without explicit workflow justification.
- ✓ Nightly sync: Backend system/patient-level sync uses client credentials flow with scoped permissions (system/Patient.read, system/Encounter.read, system/Observation.read, system/Condition.read, system/MedicationRequest.read).

6. Breach Notification & Incident Response

VitaAI includes a built-in HIPAA Breach Incident Management module used by the Altnetix security team and made available to your compliance officer under the BAA:

- ✓ Incident classification workflow: Suspected → Confirmed → Ruled Out, with full audit trail.
- ✓ Automated tracking of HHS OCR notification deadlines (60-day clock from discovery) and individual notification deadlines.
- ✓ PHI types involved, affected count, containment actions, and root cause documented per incident.
- ✓ Media notification tracking for breaches affecting more than 500 individuals in a state.
- ✓ HHS submission ID recorded for confirmed breaches reported to the HHS Breach Portal.

7. Business Associate Agreement

Altnetix, LLC serves as a Business Associate under HIPAA for all covered entity clients. We are prepared to execute a Business Associate Agreement (BAA) prior to processing any PHI. Our standard BAA:

- ✓ Defines permitted uses and disclosures of PHI consistent with the covered entity's Notice of Privacy Practices
- ✓ Commits Altnetix to implement appropriate safeguards as described in this document
- ✓ Establishes breach notification obligations to the covered entity within 60 days of discovery
- ✓ Requires BAAs with all subcontractors (Microsoft Azure BAA already executed)
- ✓ Includes provisions for access, amendment, and accounting of disclosures

Ready to Execute a BAA?

Contact your Altnetix account representative to receive a BAA template. We are committed to executing the BAA before any PHI is processed in VitaAI production systems.

Security Posture at a Glance

Control	Status	Implementation
PHI Encryption at Rest	✓	AES-256-GCM field-level + Azure SQL TDE

Control	Status	Implementation
PHI Encryption in Transit	✓	TLS 1.2+, HSTS preload, forward secrecy
Multi-Factor Authentication	✓	Azure Entra ID Conditional Access (all clinical staff)
Enterprise SSO	✓	SAML 2.0, OIDC/OAuth 2.0
Role-Based Access Control	✓	ProviderOnly / PatientOnly API policies (code-enforced)
Unique User IDs	✓	Azure Entra OID + internal UUID; no shared accounts
Automatic Session Timeout	✓	60-minute token expiry; explicit revocation on logout
Immutable Audit Logging	✓	SHA-256 hash-chained; 6-year WORM Azure Blob archive
Breach Incident Management	✓	Built-in module; 60-day HHS deadline tracking
Key Management (HSM)	✓	Azure Key Vault FIPS 140-2 Level 2
Epic FHIR R4 Integration	✓	SMART on FHIR, App Orchard registered
Microsoft BAA	✓	Executed — covers all Azure services used
VitaAI BAA Available	✓	Standard template; executed prior to PHI processing
Penetration Testing	✓	Annual third-party engagement
Vulnerability Management	✓	CI/CD dependency audit; OWASP mitigations

Questions? Contact your Altnetix account executive or email security@altnetix.com