VITAAI PLATFORM

HIPAA Security Rule Compliance Controls

Technical Implementation Reference | *Confidential*

Version 1.0 | June 2026

Prepared by Altnetix, LLC

CONFIDENTIAL — FOR AUTHORIZED RECIPIENTS ONLY

Table of Contents

1. Executive Summary

VitaAI is a cloud-native healthcare AI platform deployed exclusively on Microsoft Azure. This document maps each requirement of the HIPAA Security Rule (45 CFR Part 164) to the specific technical and administrative controls implemented in the VitaAI platform. All controls described herein are implemented in production code and Azure infrastructure as of the document date.

VitaAI serves healthcare organizations by providing AI-assisted clinical documentation, patient communication, and Epic FHIR R4 integration. The platform handles Protected Health Information (PHI) as defined under HIPAA and is operated in accordance with applicable Business Associate Agreement (BAA) obligations.

Key security commitments:

- 100% Microsoft Azure deployment — inherits Azure HIPAA BAA, SOC 2 Type II, ISO 27001, and FedRAMP High infrastructure certifications
- AES-256-GCM field-level encryption on all PHI strings; envelope key management via Azure Key Vault (RSA-4096 master key)
- Immutable, hash-chained audit logs archived to Azure Blob Storage (WORM) for 6 years
- Multi-factor authentication enforced for all clinical staff via Azure Entra ID and SAML 2.0
- Built-in breach incident management module with HIPAA 60-day notification deadline tracking
- Epic FHIR R4 integration (SMART on FHIR / EHR Launch) using asymmetric JWT assertion auth

2. Administrative Safeguards (45 CFR §164.308)

2.1 Security Management Process (§164.308(a)(1))

Risk Analysis | Required

- Formal HIPAA Security Rule risk assessment conducted annually
- Threat model covers all PHI data flows: patient portal, provider EHR integration, AI transcription pipeline, and audit subsystem
- Vulnerability scanning integrated into CI/CD pipeline; NuGet dependency audit on every build

Risk Management | Required

- Risks tracked in the built-in Breach Incident Management system (see Section 5)
- Remediation timelines assigned by severity classification (Critical / High / Medium / Low)

Sanction Policy | Required

- Workforce violations escalated per documented HR and security policy
- Azure Entra ID accounts disabled immediately upon violation or termination
- Token revocation table (RevokedTokens) invalidates all active sessions within seconds

Information System Activity Review | Required

- AuditMiddleware captures every API request with SHA-256 hash chaining — tamper-evident
- Logs archived to Azure Blob Storage (WORM) for 6 years — exceeds HIPAA 6-year minimum
- Authentication events (login success/failure, password change, kiosk auth, badge auth) separately classified and retained

2.2 Assigned Security Responsibility (§164.308(a)(2))

- Designated Security Officer at Altnetix, LLC is responsible for HIPAA compliance oversight, policy maintenance, and workforce training coordination
- Security Officer has direct authority to initiate incident response and disable accounts

2.3 Workforce Security (§164.308(a)(3))

Authorization / Supervision | Required

- All workforce members with PHI access are credentialed through Azure Entra ID
- Access requires explicit app role assignment: 'Administrator' or 'Clinician'
- Role changes enforced immediately via Azure AD token refresh cycle (no latency)

Termination Procedures | Addressable

- Entra ID account disabled upon termination (blocks all future token issuance)
- All active JWT tokens for that user revoked via RevokedTokens table (jti claim blocklist)
- All active sessions invalidated within 60 minutes (token expiry) or immediately via revocation

Clearance Procedures | Addressable

- Background checks conducted prior to PHI access provisioning for all clinical staff

2.4 Information Access Management (§164.308(a)(4))

Access Authorization | Required

- Role-Based Access Control (RBAC) enforced at API authorization middleware layer

- 'ProviderOnly' policy: requires Administrator or Clinician app role in Entra ID token
- 'PatientOnly' policy: structurally rejects provider tokens — cross-role escalation is impossible
- No shared accounts; every user has a unique identifier logged in every audit record

Access Establishment and Modification | Addressable

- Role assignments managed centrally in Azure Entra ID enterprise application configuration
- Changes take effect on next token acquisition (typically within 60 minutes, or immediately on re-login)

2.5 Security Awareness and Training (§164.308(a)(5))

- Annual HIPAA security training required for all workforce members with PHI access
- Phishing awareness training conducted quarterly
- Security briefings on significant platform changes provided to technical staff
- New employee HIPAA orientation prior to PHI access provisioning

2.6 Security Incident Procedures (§164.308(a)(6))

Incident Response | Required

- Built-in Breach Incident Management API (BreachController) with full lifecycle tracking
- Incident classification workflow: Suspected → Confirmed → Ruled Out
- Breach type taxonomy: Unauthorized Access, Lost Device, Hacking, Insider Threat, Accidental Disclosure
- Compliance dashboard tracks overdue HHS notification (>60 days from discovery) and overdue individual notification with automatic alerting
- HHS OCR submission IDs recorded per incident; media notification tracked for breaches affecting >500 individuals in a state
- All breach events emit a BreachIncidentReported audit event with PHI flag set — full audit chain preserved

2.7 Contingency Plan (§164.308(a)(7))

Data Backup | Required

- Azure SQL Database: automated geo-redundant backups with 35-day point-in-time restore
- Azure Blob Storage (audit archive): locally redundant with WORM immutability policies
- Application configuration and secrets: Azure Key Vault with geo-redundancy

Disaster Recovery Plan | Required

- Azure App Service: supports blue/green deployment for zero-downtime releases
- Azure SQL failover groups: RTO < 1 hour, RPO < 5 minutes
- DR procedures tested annually; results documented

Emergency Mode Operation | Required

- Emergency access credentials stored in Azure Key Vault with restricted policy
- Break-glass procedure documented, access events automatically flagged in audit system
- Critical clinical read paths remain accessible during planned maintenance windows

2.8 Evaluation (§164.308(a)(8))

- Annual HIPAA Security Rule self-assessment conducted against current implementation
- External penetration testing conducted annually by qualified third party
- Automated vulnerability scanning on every CI/CD build (NuGet audit, OWASP dependency check)

- Application security review performed for significant feature changes

2.9 Business Associate Contracts (§164.308(b))

- Microsoft Azure Business Associate Agreement (BAA) executed — covers Azure SQL, Azure Blob Storage, Azure Service Bus, Azure Key Vault, Application Insights, Azure OpenAI Service
- BAA template available for covered entity clients (see companion document)
- BAAs required from all third-party subprocessors with access to PHI
- BAA inventory maintained and reviewed annually

3. Physical Safeguards (45 CFR §164.310)

3.1 Facility Access Controls (§164.310(a))

VitaAI is a 100% cloud-native platform. No PHI is processed or stored on Altnetix-managed physical infrastructure. Physical data center security is provided by Microsoft Azure.

- Azure data centers hold ISO 27001, SOC 2 Type II, and FedRAMP High certifications
- Physical access controls: biometric authentication, man-trap entries, 24/7 security personnel, video surveillance
- Microsoft publishes physical security details in their Trust Center documentation

3.2 Workstation Use (§164.310(b))

- Workforce workstations must have full-disk encryption enabled (BitLocker on Windows, FileVault on macOS)
- Screen lock enforced after 5 minutes of inactivity via group policy
- MDM enrollment (Microsoft Intune) required for any device accessing the administrative portal
- Azure AD Conditional Access policies enforce device compliance posture before granting API access

3.3 Workstation Security (§164.310(c))

- Endpoint protection (EDR) required on all workforce devices with PHI access
- Operating system patches applied within 30 days of release; critical patches within 72 hours
- Clear-screen and clear-desk policies enforced in any shared office environment

3.4 Device and Media Controls (§164.310(d))

- No PHI stored on portable media (USB drives, external disks) — all data resides in Azure-managed services
- Remote wipe capability enabled via Microsoft Intune for all enrolled devices
- Device tracking enforced via x-device-id custom header, logged in every audit event
- Device disposal follows NIST 800-88 media sanitization guidelines

4. Technical Safeguards (45 CFR §164.312)

4.1 Access Control (§164.312(a))

4.1.1 Unique User Identification (§164.312(a)(2)(i))

Every user is assigned a unique, non-reusable identifier:

- Providers: Azure Entra ID Object ID (oid claim) — globally unique, Microsoft-managed, persists across password changes
- Patients: Internal UUID (uid claim in JWT) — generated at registration, immutable for the life of the account
- All audit log entries include UserId and EntraObjectId — shared or anonymous access is architecturally prevented

4.1.2 Emergency Access Procedure (§164.312(a)(2)(ii))

- Emergency access credentials stored in Azure Key Vault with restricted access policy (requires Security Officer authorization)
- Emergency access events automatically generate a high-severity audit event with PHI flag set
- Break-glass procedure documented in internal runbook and tested annually

4.1.3 Automatic Logoff (§164.312(a)(2)(iii))

- Provider JWT tokens expire after 60 minutes (configurable; enforced server-side)
- Patient JWT tokens expire after 60 minutes
- Microsoft Entra ID tokens governed by Azure AD session policy (1-hour default with Conditional Access)
- MSAL (Microsoft Authentication Library) enforces silent token refresh; interactive re-authentication required when refresh fails
- Explicit logout: JWT ID (jti claim) inserted into RevokedTokens table; all subsequent requests with that token rejected with HTTP 401 regardless of expiration
- Patient tokens stored in browser sessionStorage (cleared on tab close) per OWASP token storage guidance

4.1.4 Encryption and Decryption (§164.312(a)(2)(iv))

Multi-layer encryption architecture — see Section 6 for full encryption table.

- Field-Level PHI Encryption: AES-256-GCM applied to 25+ PHI string fields across 11 clinical entities
- Envelope encryption: per-tenant Data Encryption Keys (DEKs) wrapped with RSA-4096 master key in Azure Key Vault — key material never leaves Key Vault HSM
- DEKs cached in-process for maximum 30 minutes to limit exposure window
- Azure SQL Transparent Data Encryption (TDE): AES-256 encryption of entire database at rest
- Azure Blob Storage: AES-256 server-side encryption for all audit archive blobs
- Authentication tag in AES-GCM provides tamper detection on every encrypted field

4.2 Audit Controls (§164.312(b))

AuditMiddleware is registered in the ASP.NET Core middleware pipeline and executes for every HTTP request. The implementation uses a transactional outbox pattern to guarantee no audit events are lost, even under application failure.

Fields captured per audit event:

Field	Description	Example
EventId	Globally unique event GUID	a3b2-...
UserId	Internal user UUID	usr_8a4f...
EntraObjectId	Azure AD object ID	b97c-...
ActionType	Semantic event classification	PHIAccess_Encounter_GET
Path	HTTP request path	/api/encounter/42
Method	HTTP verb	GET
StatusCode	HTTP response code	200
IpAddress	Client IP (X-Forwarded-For resolved)	10.0.1.45
UserAgent	Browser/device identifier	Mozilla/5.0 ...
DeviceId	x-device-id custom header	kiosk-room-3
CorrelationId	Trace ID for log correlation	0HN4G...
ContainsPHI	Boolean PHI route flag	true
Hash	SHA-256 hash of record + previous hash	a3f8...
PreviousHash	Hash of prior record (chain integrity)	9d21...

- PHI route auto-detection: 20+ path patterns automatically flagged (/patient, /encounter, /prescription, /labresult, /vitals, /medication, /demographics, /transcript, etc.)
- Authentication events separately classified: UserLoginSuccess, UserLoginFailed, UserLogout, PasswordChange, KioskAuthSuccess, KioskAuthFailed, BadgeAuthSuccess, BadgeAuthFailed
- Hash-chained immutability: modification of any audit record breaks the SHA-256 chain — tamper detection is automatic
- Retention: WORM-protected Azure Blob Storage (6 years); hot SQL cache for operational queries
- Delivery: Transactional outbox → Azure Service Bus → batch SQL + blob write — no events lost under API crash

4.3 Integrity Controls (§164.312(c))

- Data integrity at rest: AES-256-GCM authentication tag on every encrypted PHI field — any modification of ciphertext produces an authentication failure
- Audit integrity: SHA-256 hash chain — modification or deletion of any audit record breaks the chain, providing forensic evidence of tampering
- Transmission integrity: TLS 1.2+ with AEAD cipher suites provides message authentication in transit — data cannot be modified in flight without detection
- API input validation: InputSanitizationFilter rejects HTML/script injection patterns; 16 KB maximum per string field enforced at API boundary
- EF Core model validation enforces data type constraints before database writes

4.4 Person or Entity Authentication (§164.312(d))

Three authentication pathways, all requiring cryptographic proof of identity:

Pathway	Technology	Token Algorithm	MFA	Key Authority
Provider (Internal)	Azure Entra ID	RS256 (asymmetric)	Conditional Access (required)	Microsoft
Provider (Enterprise SSO)	SAML 2.0 via external IdP	RSA-SHA256 signed assertion	Per enterprise IdP policy	Enterprise IdP
Patient	Email + password JWT	HS256 (symmetric)	Email OTP available	Azure Key Vault

- Password requirements (NIST 800-63B compliant): 12+ characters, uppercase, lowercase, digit, special character, 6 unique characters minimum
- Account lockout: 5 consecutive failed attempts triggers 15-minute lockout (ASP.NET Identity)
- Rate limiting: 10 authentication requests per minute per IP; 5 password operations per 5 minutes per IP (returns HTTP 429)
- SmartAuth routing: validates token issuer claim to route to correct validator — cross-role token reuse structurally prevented at middleware layer
- SAML assertion validation: certificate trust chain verified; replay attacks prevented via assertion ID tracking

4.5 Transmission Security (§164.312(e))

- HTTPS enforcement: UseHttpsRedirection() active in all non-development environments — all HTTP requests receive HTTP 301 redirect to HTTPS
- HSTS: Strict-Transport-Security header with max-age=31536000 (1 year), includeSubDomains, preload — eliminates protocol downgrade attacks
- TLS version: .NET 10 on Azure App Service enforces TLS 1.2 minimum; TLS 1.0/1.1 and SSL 3.0 disabled
- Forward secrecy: ECDHE cipher suites ensure past sessions cannot be decrypted if long-term key is compromised
- Content Security Policy: strict CSP blocks mixed content; connect-src whitelist restricts API calls to authorized Azure endpoints
- SignalR WebSocket: connections upgrade to WSS (TLS-encrypted WebSocket); access tokens validated before upgrade
- X-Content-Type-Options: nosniff prevents MIME-type sniffing attacks

5. Breach Notification Rule (45 CFR §164.400–414)

VitaAI includes a built-in Breach Incident Management module that enforces HIPAA breach notification obligations and provides a full audit trail of incident response activities.

Capability	Implementation
Incident classification	Workflow: Suspected → Confirmed → Ruled Out
Breach type taxonomy	Unauthorized Access, Lost Device, Hacking, Insider Threat, Accidental Disclosure, Other
Individual notification tracking	IndividualsNotifiedAt field; dashboard flags overdue (>60 days from discovery)
HHS OCR notification tracking	HhsNotifiedAt field; HHS submission ID recorded; dashboard flags overdue
Media notification tracking	MediaNotifiedAt for breaches affecting >500 individuals in a state
PHI types involved	Structured JSON array per incident (name, SSN, MRN, DOB, diagnosis, etc.)
Containment documentation	Free-text containment actions and root cause fields
Affected count	Numerical estimate of individuals affected
Audit trail	Every incident creation/update emits BreachIncidentReported audit event with PHI flag
Reporter tracking	ReportedByUserId and ReportedByName recorded for accountability

All incident records are protected by the same RBAC controls as clinical PHI — access restricted to ProviderOnly policy (Administrator and Clinician roles). Breach incident data is included in the standard audit log retention policy (6-year WORM archive).

6. Encryption Architecture

Component	Technology	Key Size	Key Storage	Scope
Field-Level PHI Encryption	AES-256-GCM	256-bit DEK	Azure Key Vault (wrapped by RSA-4096 master key)	25 PHI fields across 11 clinical entities
Database at Rest	Azure SQL TDE	AES-256	Azure-managed (HSM)	Entire SQL database
Audit Archive	Azure Blob SSE	AES-256	Azure-managed	All audit JSONL blobs (WORM)
Data in Transit	TLS 1.2+	128–256-bit session	Ephemeral (PFS)	All API and WebSocket traffic
JWT Signing (Patient)	HMAC-SHA256	256-bit	Azure Key Vault	Patient authentication tokens
JWT Signing (Provider)	RS256 (Entra ID)	RSA-2048+	Microsoft HSM (Entra ID)	Provider authentication tokens
SAML Assertions	RSA-SHA256	IdP-managed	Enterprise Identity Provider	Enterprise SSO assertions

Envelope Encryption Detail: Each tenant is provisioned with a unique 256-bit Data Encryption Key (DEK). The DEK is wrapped (encrypted) using an RSA-4096 master key stored in Azure Key Vault. The unwrapping operation (private key operation) occurs inside Key Vault — the plaintext master key material never leaves the Key Vault HSM boundary. Decrypted DEKs are cached in application memory for a maximum of 30 minutes, then discarded and re-fetched on demand.

7. Azure Infrastructure Compliance Inheritance

Microsoft Azure is a HIPAA-eligible cloud service provider. By deploying exclusively on Azure and executing a Microsoft BAA, VitaAI inherits the following compliance certifications for all underlying infrastructure layers:

Azure Service	VitaAI Usage	Microsoft Compliance Certifications
Azure SQL Database	Primary PHI data store	HIPAA/HITECH BAA, SOC 2 Type II, ISO 27001, FedRAMP High, PCI DSS
Azure Blob Storage	Audit archive (WORM, 6-year)	HIPAA/HITECH BAA, SOC 2 Type II, ISO 27001, FedRAMP High
Azure Key Vault	Encryption keys, platform secrets	HIPAA/HITECH BAA, SOC 2 Type II, FIPS 140-2 Level 2 HSM
Azure Service Bus	Audit event streaming pipeline	HIPAA/HITECH BAA, SOC 2 Type II, ISO 27001
Azure Entra ID	Provider authentication, RBAC, SSO	HIPAA/HITECH BAA, SOC 2 Type II, ISO 27001, FedRAMP High
Azure OpenAI Service	AI-assisted clinical transcription	HIPAA/HITECH BAA (when BAA configured), SOC 2 Type II
Azure App Service	API hosting and runtime	HIPAA/HITECH BAA, SOC 2 Type II, ISO 27001, FedRAMP High
Application Insights	Platform monitoring and telemetry	HIPAA/HITECH BAA, SOC 2 Type II

Azure compliance documentation and audit reports are available at the Microsoft Trust Center: https://www.microsoft.com/en-us/trust-center

8. Ongoing Compliance Posture

Program	Frequency	Scope
HIPAA Security Rule Self-Assessment	Annual	All §164.308, §164.310, §164.312 safeguards
External Penetration Testing	Annual	API authentication, authorization, injection, data exposure
Vulnerability Scanning (CI/CD)	Every deployment	NuGet dependency audit, OWASP dependency check
DR / Contingency Plan Test	Annual	Azure SQL failover, blob restore, emergency access
HIPAA Security Training	Annual + new-hire	All workforce with PHI access
BAA Review	Annual	All subprocessors and vendors with PHI access
Audit Log Review	Weekly (automated alerting)	Anomalous auth failures, off-hours PHI access, burst access patterns
Breach Response Drill	Annual	Incident classification, notification timelines, HHS reporting

Identified Improvement Areas

- Migrate Service Bus authentication from connection string (SharedAccessKey) to Managed Identity for zero-secret credential model
- Patient token storage: migrate from localStorage to sessionStorage for SAML/patient JWT tokens to reduce persistent XSS exposure window
- Implement automated RevokedTokens pruning job (ExpiresAt-based cleanup currently requires manual execution)
- Pursue formal SOC 2 Type II audit to provide third-party attestation of security controls

Document Control

Field	Value
Document Title	HIPAA Security Rule Compliance Controls — VitaAI Platform
Version	1.0
Effective Date	June 2026
Next Review Date	June 2027
Owner	Altnetix, LLC — Security Officer
Classification	Confidential — Authorized Recipients Only
Document ID	VTA-SEC-001