VITAAI PLATFORM

HIPAA Security Rule Self-Assessment Checklist

45 CFR Part 164 — Administrative, Physical, and Technical Safeguards

Assessment Date: June 2026 | Assessor: Altnetix, LLC Security Officer | Version 1.0

46	5	3	4
Implemented (✓)	Partial (◑)	Gap (✗)	N/A

Legend: ✓ Implemented = control fully operational in production. ◑ Partial = control exists but has identified improvement areas. ✗ Gap = control not yet implemented; remediation required. N/A = not applicable to this platform.

Part 1 — Administrative Safeguards (§164.308)

Requirement	Status	Implementation Notes / Remediation
§164.308(a)(1) — Security Management Process		
§164.308(a)(1)(ii)(A) Risk Analysis (R): Conduct accurate and thorough assessment of potential risks and vulnerabilities to PHI.	✓ Implemented	Annual HIPAA risk assessment conducted; threat model covers patient portal, EHR integration, AI transcription, and audit subsystem.
§164.308(a)(1)(ii)(B) Risk Management (R): Implement security measures to reduce risks to reasonable and appropriate level.	✓ Implemented	Risks tracked in Breach Incident Management module; remediation timelines assigned by severity.
§164.308(a)(1)(ii)(C) Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply.	✓ Implemented	Documented sanction policy; Entra ID accounts disabled immediately on policy violation; token revocation table invalidates all active sessions.
§164.308(a)(1)(ii)(D) Information System Activity Review (R): Implement procedures to regularly review records of information system activity.	✓ Implemented	AuditMiddleware logs every API request; SHA-256 hash-chained; 6-year WORM archive; weekly review cadence with anomaly alerting.
§164.308(a)(2) — Assigned Security Responsibility		
§164.308(a)(2) Identify the security official responsible for policies and procedures (R).	✓ Implemented	Designated Security Officer at Altnetix, LLC; documented responsibility for HIPAA compliance oversight, policy maintenance, and incident response.
§164.308(a)(3) — Workforce Security		
§164.308(a)(3)(ii)(A) Authorization and/or Supervision (A): Implement procedures for authorization/supervision of workforce.	✓ Implemented	All PHI-access users credentialed through Azure Entra ID; explicit app role assignment required (Administrator or Clinician).
§164.308(a)(3)(ii)(B) Workforce Clearance Procedure (A): Implement procedures to determine appropriate access for workforce.	✓ Implemented	Background checks conducted prior to PHI access provisioning for all clinical staff.
§164.308(a)(3)(ii)(C) Termination Procedures (A): Implement procedures for terminating access upon employment termination.	✓ Implemented	Entra ID account disabled on termination; all active tokens revoked via RevokedTokens (jti blocklist); sessions invalidated within 60 min.

Requirement	Status	Implementation Notes / Remediation
§164.308(a)(4) — Information Access Management		
§164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Functions (R): Implement policies for clearinghouse functions.	N/A	VitaAI is not a healthcare clearinghouse. N/A.
§164.308(a)(4)(ii)(B) Access Authorization (A): Implement policies for authorizing access to ePHI.	✓ Implemented	RBAC enforced at API middleware; ProviderOnly and PatientOnly policies; cross-role access architecturally prevented.
§164.308(a)(4)(ii)(C) Access Establishment and Modification (A): Implement procedures for granting/modifying access.	✓ Implemented	Roles managed in Azure Entra ID enterprise app; changes effective immediately on next token acquisition.
§164.308(a)(5) — Security Awareness and Training		
§164.308(a)(5)(ii)(A) Security Reminders (A): Periodic security updates for workforce.	✓ Implemented	Annual HIPAA security training for all PHI-access workforce; platform change security briefings for technical staff.
§164.308(a)(5)(ii)(B) Protection from Malicious Software (A): Procedures for guarding against malicious software.	✓ Implemented	Endpoint protection required on all workforce devices; NuGet audit and OWASP dependency check in CI/CD pipeline.
§164.308(a)(5)(ii)(C) Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies.	✓ Implemented	UserLoginFailed events logged; rate limiting 10 auth/min; account lockout after 5 failures; automated anomaly alerting.
§164.308(a)(5)(ii)(D) Password Management (A): Procedures for creating, changing, and safeguarding passwords.	✓ Implemented	NIST 800-63B: 12+ chars, mixed case, digit, special char, 6 unique. JWT signing keys validated >= 32 chars at startup.
§164.308(a)(6) — Security Incident Procedures		
§164.308(a)(6)(ii) Response and Reporting (R): Identify and respond to security incidents; mitigate harmful effects; document incidents.	✓ Implemented	Built-in Breach Incident Management API (BreachController); full lifecycle tracking; HHS/individual notification deadline tracking; audit trail.
§164.308(a)(7) — Contingency Plan		
§164.308(a)(7)(ii)(A) Data Backup Plan (R): Create and maintain retrievable exact copies of ePHI.	✓ Implemented	Azure SQL geo-redundant automated backups (35-day PITR); Blob Storage WORM archive (6-year); Key Vault geo-redundant.

Requirement	Status	Implementation Notes / Remediation
§164.308(a)(7)(ii)(B) Disaster Recovery Plan (R): Restore loss of data.	✓ Implemented	Azure SQL failover groups (RTO < 1hr, RPO < 5 min); App Service blue/green deployment; DR tested annually.
§164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (R): Enable continuation of critical business processes for PHI during emergency.	✓ Implemented	Emergency access credentials in Azure Key Vault; break-glass procedure documented; emergency events auto-flagged in audit.
§164.308(a)(7)(ii)(D) Testing and Revision Procedures (A): Implement procedures for periodic testing of contingency plans.	◑ Partial	DR procedures tested annually. Gap: results not formally documented and versioned. Remediation: create DR test report template and archive results.
§164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis (A): Assess relative criticality of applications and data.	◑ Partial	Informal criticality ranking exists. Gap: formal BIA (Business Impact Analysis) document not published. Remediation: complete BIA document by Q3 2026.
§164.308(a)(8) — Evaluation		
§164.308(a)(8) Evaluation (R): Perform periodic technical and non-technical evaluation of security standards.	✓ Implemented	Annual HIPAA self-assessment; external penetration testing annually; automated vulnerability scanning in CI/CD.
§164.308(b) — Business Associate Contracts and Other Arrangements		
§164.308(b)(1) Business Associate Contracts (R): Written contract or arrangement satisfactory assurances.	✓ Implemented	Microsoft Azure BAA executed (covers SQL, Blob, Service Bus, Key Vault, App Insights, Azure OpenAI). BAA template available for covered entities.
§164.308(b)(4) Written Contract or Other Arrangement (R): Document satisfactory assurances.	✓ Implemented	BAA inventory maintained; all subprocessors reviewed annually. Standard BAA template maintained.

Part 2 — Physical Safeguards (§164.310)

Requirement	Status	Implementation Notes / Remediation
§164.310(a) — Facility Access Controls		
§164.310(a)(2)(i) Contingency Operations (A): Establish procedures to allow physical access to support data restoration.	✓ Implemented	Azure-managed data centers; break-glass procedure provides emergency API access; documented in emergency mode operations plan.
§164.310(a)(2)(ii) Facility Security Plan (A): Implement policies to safeguard facility and equipment from unauthorized physical access.	✓ Implemented	VitaAI is 100% cloud-native on Azure. Azure data centers: biometric access, man-trap, 24/7 security, video surveillance — ISO 27001 certified.
§164.310(a)(2)(iii) Access Control and Validation Procedures (A): Implement procedures to control and validate a person's access.	✓ Implemented	Azure Conditional Access enforces device compliance; MDM enrollment required for admin portal access; remote wipe via Intune.
§164.310(a)(2)(iv) Maintenance Records (A): Implement policies for maintenance of security-relevant facility components.	✓ Implemented	Azure infrastructure maintenance managed by Microsoft; change management records maintained via Azure Activity Log.
§164.310(b) — Workstation Use		
§164.310(b) Workstation Use (R): Implement policies specifying proper functions and physical attributes of workstations.	✓ Implemented	Workforce policy: full-disk encryption (BitLocker/FileVault), screen lock after 5 min, MDM enrollment, EDR required.
§164.310(c) — Workstation Security		
§164.310(c) Workstation Security (R): Implement physical safeguards for workstations that access ePHI.	✓ Implemented	Azure AD Conditional Access enforces device posture; clear-screen policy; endpoint protection policy enforced via MDM.
§164.310(d) — Device and Media Controls		
§164.310(d)(2)(i) Disposal (R): Implement policies for final disposition of ePHI and/or hardware.	✓ Implemented	No PHI on portable media; Azure-managed disposal; NIST 800-88 media sanitization policy for any workforce devices.
§164.310(d)(2)(ii) Media Re-Use (R): Implement procedures for removal of ePHI from	✓ Implemented	No PHI stored on portable media. Enrolled devices wiped via Intune before reassignment.

Requirement	Status	Implementation Notes / Remediation
electronic media before re-use.		
§164.310(d)(2)(iii) Accountability (A): Maintain a record of the movements of hardware and electronic media.	◑ Partial	Device tracking via x-device-id audit header. Gap: formal hardware asset inventory for workforce endpoints not maintained. Remediation: Intune device inventory report to serve as formal register.
§164.310(d)(2)(iv) Data Backup and Storage (A): Create a retrievable exact copy of ePHI, when needed, before movement of equipment.	✓ Implemented	All PHI in Azure-managed services; no local copies; Azure automated backups cover all PHI at rest.

Part 3 — Technical Safeguards (§164.312)

Requirement	Status	Implementation Notes / Remediation
§164.312(a) — Access Control		
§164.312(a)(1) Access Control (R): Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to authorized persons.	✓ Implemented	API-level RBAC with ProviderOnly and PatientOnly authorization policies; JWT authentication required on all PHI endpoints.
§164.312(a)(2)(i) Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity.	✓ Implemented	Providers: Azure Entra ID Object ID (oid claim, globally unique). Patients: internal UUID (uid claim). All audit records include UserId + EntraObjectId.
§164.312(a)(2)(ii) Emergency Access Procedure (R): Establish procedures for obtaining necessary ePHI during emergency.	✓ Implemented	Emergency credentials in Azure Key Vault with restricted policy; break-glass procedure documented; emergency events auto-flagged in audit log.
§164.312(a)(2)(iii) Automatic Logoff (A): Implement procedures that terminate an electronic session after a period of inactivity.	✓ Implemented	JWT tokens expire after 60 minutes; MSAL enforces silent refresh; explicit logout inserts jti into RevokedTokens (HTTP 401 on next use).
§164.312(a)(2)(iv) Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt ePHI.	✓ Implemented	AES-256-GCM field-level encryption on 25+ PHI fields across 11 entities; envelope encryption via Azure Key Vault RSA-4096 master key; Azure SQL TDE.
§164.312(b) — Audit Controls		
§164.312(b) Audit Controls (R): Implement hardware, software, and/or procedural mechanisms that record and examine activity in systems that contain or use ePHI.	✓ Implemented	AuditMiddleware logs every request (UserId, EntraObjectId, ActionType, Path, IP, DeviceId, CorrelationId, PHI flag, SHA-256 hash). Hash-chained immutability. 6-year WORM Blob archive.
§164.312(c) — Integrity		
§164.312(c)(1) Integrity (R): Implement policies and procedures to protect ePHI from improper alteration or destruction.	✓ Implemented	AES-256-GCM authentication tag on every encrypted field (tamper detection). SHA-256 hash chain on audit logs. TLS 1.2+ in transit. InputSanitizationFilter at API boundary.

Requirement	Status	Implementation Notes / Remediation
§164.312(c)(2) Mechanism to Authenticate ePHI (A): Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	✓ Implemented	GCM authentication tag proves ePHI integrity on decryption. Any modification of ciphertext produces AuthTagMismatch exception. Audit log hash chain provides forensic integrity.
§164.312(d) — Person or Entity Authentication		
§164.312(d) Person or Entity Authentication (R): Implement procedures to verify that a person or entity seeking access is the one claimed.	✓ Implemented	Three auth pathways: Azure Entra ID (RS256, MFA via Conditional Access), SAML 2.0 (signed assertions), Patient JWT (HS256 + account lockout + rate limiting). SmartAuth routing prevents cross-role token reuse.
§164.312(e) — Transmission Security		
§164.312(e)(1) Transmission Security (R): Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	✓ Implemented	TLS 1.2+, HTTPS redirect enforced in all non-dev environments, HSTS max-age=31536000 with preload, WSS for WebSocket, ECDHE cipher suites for forward secrecy.
§164.312(e)(2)(i) Integrity Controls (A): Implement security measures to ensure electronically transmitted ePHI is not improperly modified without detection.	✓ Implemented	TLS AEAD cipher suites provide transmission integrity. HTTPS redirect and HSTS prevent downgrade. CSP connect-src whitelist prevents unauthorized API endpoints.
§164.312(e)(2)(ii) Encryption (A): Implement a mechanism to encrypt ePHI whenever deemed appropriate.	✓ Implemented	All ePHI transmission encrypted via TLS 1.2+. End-to-end: field-level AES-256-GCM at rest, TLS in transit, no unencrypted PHI ever leaves Azure boundary.

Part 4 — Organizational Requirements & Breach Notification

Requirement	Status	Implementation Notes / Remediation
§164.314 — Organizational Requirements		
§164.314(a)(1) Business Associate Contracts (R): Contracts must meet requirements of §164.308(b).	✓ Implemented	Microsoft Azure BAA executed; standard covered entity BAA template prepared; subprocessor BAAs required.
§164.314(a)(2)(i) Implementation Specifications (R): Contract must require BA to implement safeguards, report incidents, ensure subcontractors comply, authorize termination.	✓ Implemented	BAA template contains all required provisions: safeguard obligations, breach reporting (60-day), subcontractor requirements, termination for cause, return/destroy PHI.
§164.314(b) Requirements for Group Health Plans (R).	N/A	VitaAI is not a group health plan. N/A.
§164.316 — Policies, Procedures and Documentation		
§164.316(a) Policies and Procedures (R): Implement reasonable and appropriate policies and procedures to comply with standards.	✓ Implemented	HIPAA security policies documented; annual review cycle; changes communicated to workforce.
§164.316(b)(1) Documentation (R): Maintain written policies, procedures, and records for 6 years.	◑ Partial	Policies and incident records maintained. Gap: formal document management system with version history and 6-year retention tracking not yet implemented. Remediation: implement SharePoint/Confluence documentation library with retention labels by Q4 2026.
§164.316(b)(2)(ii) Availability (R): Make documentation available to those responsible for implementing procedures.	✓ Implemented	Security documentation maintained in internal wiki; available to all relevant workforce.
§164.316(b)(2)(iii) Updates (R): Review and update documentation in response to environmental or operational changes.	✓ Implemented	Annual review cycle; security Officer responsible for updates; changes logged.
§164.400-414 — Breach Notification Rule		
§164.402 Breach Definition (R): Identify breaches per HIPAA definition.	✓ Implemented	BreachController supports Suspected / Confirmed / Ruled Out classification aligned with HIPAA breach definition and risk assessment framework.
§164.404 Individual Notification (R): Notify affected individuals within 60 days of discovery.	✓ Implemented	IndividualsNotifiedAt field tracked per incident. Compliance dashboard flags overdue individual notifications (>60 days from DiscoveredAt).

Requirement	Status	Implementation Notes / Remediation
§164.406 Media Notification (R): Notify prominent media outlets for breaches affecting >500 individuals in a state.	✓ Implemented	MediaNotifiedAt field tracked per incident; dashboard flags applicable breaches.
§164.408 HHS Notification (R): Notify HHS of breaches.	✓ Implemented	HhsNotifiedAt and HhsSubmissionId fields tracked per incident; dashboard flags overdue HHS notifications. Annual submission of sub-500 breaches supported.
§164.412 Law Enforcement Delay (A): Delay notification if law enforcement requests.	✗ Gap	Gap: no formal documented procedure for handling law enforcement delay requests. Remediation: add law enforcement delay acknowledgment field to BreachIncident model; document procedure in incident response plan by Q3 2026.
§164.414 Burden of Proof (R): Business Associate bears burden of demonstrating breach did not occur.	◑ Partial	Hash-chained audit logs provide strong forensic evidence. Gap: formal breach risk assessment documentation template (4-factor HIPAA test) not standardized. Remediation: create breach risk assessment form template by Q3 2026.

Part 5 — Remediation Plan Summary

The following items have been identified as requiring remediation. All items are classified as low-to-moderate risk given the compensating controls already in place.

Section	Gap / Improvement	Priority	Target Date
§164.308(a)(7)	Formalize DR test report template; archive annual DR test results with version control.	**Medium**	Q3 2026
§164.308(a)(7)	Complete and publish Business Impact Analysis (BIA) document with application criticality rankings.	**Medium**	Q3 2026
§164.310(d)	Implement formal hardware asset inventory using Intune device inventory as system of record.	**Low**	Q3 2026
§164.316(b)	Implement document management library (SharePoint/Confluence) with 6-year retention labels for HIPAA policies.	**Medium**	Q4 2026
§164.412	Add law enforcement delay field to BreachIncident model; document procedure in incident response plan.	**Low**	Q3 2026
§164.414	Create standardized HIPAA breach risk assessment form (4-factor test template).	**Medium**	Q3 2026
Technical	Migrate Service Bus auth from SharedAccessKey to Managed Identity.	**Medium**	Q3 2026
Technical	Migrate patient SAML JWT from localStorage to sessionStorage.	**Low**	Q3 2026
Technical	Implement automated RevokedTokens pruning job (ExpiresAt-based cleanup).	**Low**	Q4 2026

Assessment Sign-Off

Security Officer Altnetix, LLC Signature: _____ Date: _____	**Next Review Date** June 2027 Assessment ID: VTA-HIPAA-SA-2026-01 Document ID: VTA-SEC-004