ALTNETIX LLC
VitaAI Platform

SECURITY EVENT LOGGING POLICY

Audit Logging, Monitoring, and Alerting Standards

Control Reference	LOG-4
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. Purpose and Legal Basis

This Policy establishes requirements for security event logging across all VitaAI platform components. Comprehensive audit logging is required by HIPAA §164.312(b) (Audit Controls) and supports rapid detection, investigation, and response to security incidents.

2. Log Sources and Events

Log Source	Events Captured	Retention	Storage
VitaAI Audit Middleware	All PHI access, create, update, delete events with	6 years	Azure Blob (WORM)
Authentication Logs	Login success/failure, MFA events, token issuance	6 years	Azure Blob + SQL hot cache
API Request Logs	All API calls with path, method, user, response code	1 year operational	Application Insights
Azure Active Directory	User provisioning, role changes, admin actions	6 years	Azure AD audit logs
Azure Key Vault	Key access, wrap/unwrap, certificate operations	6 years	Azure Monitor
Azure SQL	Query activity, schema changes, failed auth attempts	90 days	Azure SQL Auditing
Infrastructure	App Service start/stop, deployment events, NSG flow logs	1 year	Azure Monitor

3. PHI Audit Event Requirements

All PHI access events must be logged with the following minimum fields per HIPAA §164.312(b):

- User identifier (authenticated user ID or system service account)
- Action type (read, create, update, delete, export)
- Resource identifier (patient ID, record type, record ID)
- Timestamp (UTC, millisecond precision)
- Source IP address and correlation ID
- HTTP response status and outcome (success/failure)

PHI audit logs are stored in an immutable, WORM-protected Azure Blob container. Logs are cryptographically hash-chained to detect tampering. Deletion of

audit logs is not permitted during the 6-year retention period.

4. Log Protection and Integrity

- Audit logs are written to a separate, isolated Azure Blob container with immutability policy
- Hash-chaining ensures each log entry references the hash of the prior entry
- Log access is restricted to the Security Officer and automated pipeline services
- Workforce members with access to production databases cannot modify or delete audit logs
- Log integrity is verified monthly by the Security Officer

5. Alerting and Monitoring

The following events trigger immediate automated alerts to the Security Officer:

- Five or more failed authentication attempts within 10 minutes (brute force)
- Any access to PHI outside of business hours by non-clinical users
- Bulk PHI export (>100 records) by any single user in a 1-hour window
- Administrative account login from unrecognized IP or geography
- Key Vault access failure or unusual key usage pattern

- Application error rate increase >200% above baseline in 5 minutes

6. Log Review Procedures

- Automated anomaly detection runs continuously via Application Insights smart detection
- Security Officer reviews PHI access audit summaries weekly
- Full audit log review is performed quarterly or following a security incident
- Customer-specific audit log reports are available to Covered Entities upon request for HIPAA audit purposes