PulseGuard AI Security & Compliance

Enterprise-Ready Infrastructure for Healthcare AI

KEY SECURITY COMMITMENTS

- ✓ HIPAA-compliant Azure infrastructure with Microsoft BAA
- ✓ Read-only by default for 60-90 day pilots
- ✓ **ZERO PHI in development, demos, or non-production environments**
- ✓ Executed BAAs for all customer relationships
- ✓ Immutable audit trail for all provider actions

1. PROGRAM OVERVIEW

Comprehensive HIPAA compliance program with executed Business Associate Agreements (BAAs) for all pilots and production deployments. Read-only access by default during pilot phase. Writebacks (note text, messages, orders) enabled only after explicit site approval and governance review. Strict environment separation between sandbox, staging, and production. No PHI permitted in development environments or public demonstrations.

2. ARCHITECTURE & DATA FLOW

Integration: Primary connection via Redox Engine supporting both FHIR (DiagnosticReport, Observation) and HL7 (ORU) formats for imaging results, laboratory data, microbiology cultures, encounters, and diagnoses.

Result Linking Logic: Hierarchical matching algorithm prioritizing encounter references, then accession/order numbers, then time/location heuristics. All linking rationale stored for audit compliance.

Processing Pipeline: Event-driven architecture with idempotent processing, versioned result/task records, and complete audit logging of all user interactions and system decisions.

Data Boundaries: All PHI processed within PulseGuard's HIPAA-eligible Azure environment (US regions only), covered by Microsoft BAA and PulseGuard-customer BAA.

3. SECURITY CONTROLS

- Azure HIPAA-eligible services only
- TLS 1.2+ for all data in transit
- AES-256 encryption at rest
- Azure Key Vault managed keys
- Role-based access control (RBAC)
- Multi-factor authentication required
- Centralized audit logging
- Retention per site policy (default 12 months, extendable to meet regulatory requirements)
- Encrypted backups with quarterly restore testing

4. INCIDENT RESPONSE

- 24/7 monitoring and alerting
- Automated vulnerability scanning
- Monthly security patching cycles
- CRITICAL CVE remediation within 72 hours
- Third-party dependency tracking via Dependabot
- Incident lifecycle: detect → triage → contain → eradicate → recover → review
- Breach notification per BAA and HIPAA requirements
- Annual tabletop exercises (third-party facilitated)

5. COMPLIANCE ROADMAP

Current:	HIPAA compliance program operational, BAAs executed, security policies documented
Q1 2025:	SOC 2 Type I audit scheduled with independent auditor (firm selection in progress)
Q3 2025:	SOC 2 Type II certification (12 months post-pilot completion)
Ongoing:	Support for customer security questionnaires, architecture reviews, and annual attestations

6. PHI HANDLING & MINIMUM NECESSARY

Data access strictly limited to detection, task assignment, and audit functions. De-identification protocols enforced outside production environments. Optional writebacks require both site

governance approval and explicit user action. All data flows documented and available for customer review.

End-to-End Flow: Inbound read-only via Redox (FHIR/HL7) → AI detection and task creation → Provider action recording → Optional writeback (post-approval) → Complete audit trail maintained.

CONTACTS

Security & Compliance: Yuriy Savytskyy, Chief Technology Officer - yuriy.savytskyy@pulseguardai.com

General Inquiries: info@pulseguardai.com
