Data Security Overview

ARKA Health, Inc. — clinical decision support, built for hospital security review

Version 1.0 · June 2026
Distribution: unrestricted

NO PHI
in demo environment — 100% synthetic data

AES-256 / TLS 1.2+
encryption everywhere, at rest & in transit

MFA REQUIRED
all systems; FIDO2 keys for administrators

6-YEAR
retention of security audit evidence

ARCHITECTURE & DATA PROTECTION

- **Encryption by default.** AES-256 at rest across databases, object storage, and backups; TLS 1.2+ (1.3 preferred) with HSTS on every public endpoint. Keys held in managed KMS; rotation and custody documented.
- **Tenant isolation.** Row-level security keyed to tenant identity; server-side authorization on every request; isolation covered by automated tests in CI.
- **Structured-data-only CDS.** ARKA-CLIN consumes scoped FHIR R4 prefetch via SMART on FHIR / CDS Hooks. No bulk record ingestion; integration scopes are minimum-necessary by design.
- **No PHI outside production.** Development, demo, and analytics environments use synthetic or de-identified data only — enforced by policy, seed tooling, and CI guards.

ACCESS CONTROL

- **MFA on everything.** Multi-factor authentication on all production, code, and data systems; phishing-resistant FIDO2 hardware keys for administrative access.
- **Least privilege.** Role-based access from a documented matrix; quarterly access reviews; 24-hour deprovisioning on separation; break-glass access alarmed and audited.
- **Attributable identity.** Unique accounts only — no shared credentials; secrets vaulted, never in source code, scanned for in CI.

MONITORING & RESPONSE

- **Immutable audit trail.** Authentication, record-level PHI access, admin actions, and deployments logged append-only, clock-synced, and retained 6 years.
- **Tested incident response.** Severity-classified plan with 1-hour containment objective for suspected ePHI events; customer notice within 10 business days, per BAA; annual tabletop incl. ransomware.
- **Resilience.** Immutable cross-region backups (35-day PITR + 12-month archives), quarterly restore tests, 72-hour restoration standard for critical systems.

COMPLIANCE PROGRAM STATUS

HIPAA (Privacy · Security · Breach) — **Program in force**
Full policy suite adopted; BAA ready; annual NIST 800-30 risk analysis complete.

SOC 2 (Security · Availability · Conf.) — **In progress**
Type I targeted Dec 2026; Type II report mid-2027. Report under NDA on issuance.

HITRUST e1 — **Roadmap active**
MyCSF self-assessment Q1 2027; validated assessment H1 2027.

2025 HIPAA Security Rule NPRM — **Adopted as baseline**
MFA, universal encryption, asset inventory, 6-mo scans, annual pen test, segmentation.

WHAT WE SIGN

- **Business Associate Agreement.** Attorney-drafted template per 45 C.F.R. §§ 164.314(a), 164.504(e): 10-business-day breach notice, subcontractor flow-down, NIST 800-88 return/destruction.
- **Honest claims, verifiable posture.** We never state “certified” before an auditor or assessor has issued the artifact — and we put that rule in writing for hospital diligence teams.

DILIGENCE PACKAGE (UNDER NDA)

- **21 controlled documents.** Governance charter, HIPAA privacy & security policy suite, risk assessment, SOC 2 / HITRUST readiness, certification roadmap, no-PHI demo attestation.
- **Request access.** security@getarka.health — typical turnaround 2 business days.

ARKA Health, Inc.
privacy@getarka.health · security@getarka.health · www.getarka.health/security