COMPLIANCE & REGULATORY DOSSIER

Evidence for Diligence Review

Regulatory positioning, privacy and security controls, and interoperability alignment for ARKA's clinical decision-support and administrative-workflow platform.

FDA Non-Device CDS · 21st Century Cures Act §520(o)(1)(E)

HIPAA Privacy & Security Rules

CMS-0057-F Interoperability & Prior Authorization

HL7 FHIR R4 / US Core

AIIE Methodology

SOC 2 (in progress)

DOCUMENT	VERSION	EFFECTIVE	CLASSIFICATION
Compliance Dossier	1.0	May 2026	Confidential

PREPARED BY	OWNER	AUDIENCE	CONTACT
Compliance & Legal	Chief Compliance Officer	Regulators · Payers · Customers	compliance@getarka.health

© 2026 ARKA Health. Confidential — provided for regulatory and payer diligence review. The appropriateness layer for American healthcare · getarka.health

Contents

1 Executive Summary

ARKA is the appropriateness layer for American healthcare — a platform that unifies clinical decision support with coverage and prior-authorization workflows. This dossier sets out ARKA's regulatory posture, the legal basis for our product claims, and the operational controls that keep us compliant as we scale.

ARKA deliberately positions across two regulatory lanes. **ARKA-CLIN** (ordering and emergency-department pathways) is designed as **Non-Device Clinical Decision Support** under §520(o)(1)(E) of the Federal Food, Drug, and Cosmetic Act, as added by the 21st Century Cures Act. **ARKA-INS** (prior authorization, utilization management, and cost transparency) operates as administrative and operational software that is not a medical device. Across both modules, a licensed human remains accountable for every clinical decision.

4 / 4
FDA Non-Device CDS criteria addressed by ARKA-CLIN by design

BAA
ARKA executes Business Associate Agreements and applies HIPAA safeguards

FHIR R4
CMS-0057-F-aligned PARDD and access APIs on HL7 FHIR / US Core

What a reviewer will find in this document

- ✓ A clear, defensible regulatory classification for each module, with the statutory basis stated.
- ✓ A criterion-by-criterion analysis of how ARKA-CLIN satisfies the four Non-Device CDS prongs, and the design controls that enforce each.
- ✓ HIPAA administrative, physical, and technical safeguards, and our data-minimization and de-identification practices.
- ✓ Alignment with the CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F).
- ✓ Traceability of recommendations through the AIIE methodology, with versioning and human-in-the-loop guarantees.
- ✓ An honest statement of limitations — what ARKA is not, and what remains in progress.

GUIDING PRINCIPLE

ARKA's voice is precise, calm, and evidence-first. We do not overpromise. We cite, we disclose limitations, and we keep human accountability explicit in the product UI and in every API response.

2 Purpose, Scope & Intended Audience

This dossier defines ARKA's regulatory posture, the legal basis for our product claims, and the operational controls that keep us compliant. It is written for three audiences:

Audience	What this document gives them
Regulators	The statutory basis for ARKA's Non-Device CDS positioning and the design controls that keep clinical modules outside the device definition.
Payers & UM teams	CMS-0057-F interoperability alignment, prior-authorization API readiness, and medical-necessity workflow guardrails.
Customer compliance & privacy officers	HIPAA safeguards, the shared-responsibility model, audit capabilities, and answers to common diligence questions (Appendix A).

Scope: ARKA's commercial platform (ARKA-CLIN and ARKA-INS). This is a living document; material changes are communicated to customers under contract. See Appendix B for revision history.

3 Regulatory Identity

ARKA is a clinical decision-support (CDS) and administrative-workflow platform. We position deliberately across two regulatory lanes so that each module is assessed under the framework that actually fits its function.

Module	Primary regulatory frame	Rationale
ARKA-CLIN Ordering, ED pathways	Non-Device CDS under the 21st Century Cures Act §520(o)(1)(E)	Recommendations are transparent, reviewable, and intended for licensed clinicians who can independently evaluate the basis for each recommendation.
ARKA-INS PA, utilization, transparency	Administrative / operational software (not a medical device)	Coverage, prior-authorization, and cost-transparency workflows are administrative in nature — they support payment and operations, not diagnosis.

CLIN VS INS

ARKA-CLIN and the ED pathways emphasize **appropriateness at order entry**. ARKA-INS adds coverage, prior authorization, and patient-facing financial estimates. Each module keeps human accountability explicit in the UI and in API card text.

4 FDA Non-Device CDS Compliance

Section 520(o)(1)(E) of the FD&C Act, added by the 21st Century Cures Act, excludes certain clinical decision-support software functions from the definition of a medical *device*. The FDA's September 2022 final guidance, *Clinical Decision Support Software*, interprets these criteria. ARKA's clinical modules are designed to satisfy **all four** statutory criteria.

Criterion 1

Not intended to acquire, process, or analyze a medical image, signal, or pattern

ARKA does not ingest medical images, in-vitro-diagnostic signals, or raw device-acquired patterns. It surfaces appropriateness, coverage, and workflow context; it does not perform image acquisition or diagnostic image interpretation. ARKA operates on structured clinical context, orders, and coverage rules.

Criterion 2

Intended for displaying, analyzing, or printing medical information

ARKA displays and analyzes medical information — labs, problem lists, specialty-society guidelines, and payer coverage policies — presenting structured recommendations, payer-aligned factors, and estimates for clinician or administrative review. This is a permitted activity under the statute.

Criterion 3

Intended to support or provide recommendations to a health care professional

ARKA provides recommendations *to* licensed health care professionals (and, where applicable, trained support staff acting under organizational policy). For ARKA-CLIN and ED pathways, the recipients are licensed clinicians at the point of ordering. For ARKA-INS, the recipients are licensed clinicians and trained utilization staff. ARKA does not directly drive treatment without a human in the loop.

Criterion 4 · The critical one

Enabling the professional to independently review the basis for recommendations

ARKA surfaces the basis for every recommendation: the guideline, the rule that fired, the policy citation, and the data inputs used. A clinician can independently review and either accept or reject — they are not expected to rely *primarily* on ARKA to make a clinical diagnosis or treatment decision. The AIIE methodology (Section 8) exposes these traceable, guideline- and policy-linked factors, consistent with transparent CDS expectations.

Design controls we enforce

- ✓ Every recommendation card shows its sources and citations.
- ✓ We avoid directive language ("you must"); we use "consider" and "evidence suggests."
- ✓ Clinician overrides are logged as first-class events, evidencing human agency.
- ✓ The ARKA standard disclaimer appears in the UI, in CDS Hooks card text returned via API, and in exported reports and PDFs.

5 The ARKA Standard Disclaimer

The following text — or a context-appropriate variant — is the standard disclaimer that reinforces ARKA's Non-Device CDS posture and the human-in-the-loop model.

> **ARKA STANDARD DISCLAIMER**
>
> **ARKA provides clinical decision support for licensed health care professionals. Recommendations are advisory, require independent clinical judgment, and do not replace the clinician–patient relationship. ARKA is not a diagnostic device.**

This disclaimer must appear on every clinical recommendation surface in the UI, in CDS Hooks card text returned via the API, and in exported reports and PDFs.

6 HIPAA & Data Privacy

ARKA operates as a **Business Associate** under HIPAA when handling protected health information (PHI) on behalf of covered entities, and will execute a Business Associate Agreement (BAA).

Administrative, physical, and technical safeguards

Safeguard class	Controls implemented
Administrative	Workforce training, periodic access reviews, risk assessments, and a documented incident-response plan.
Physical	SOC 2-aligned cloud data centers; no on-premise PHI by default.
Technical	Encryption at rest (AES-256) and in transit (TLS 1.2+), immutable audit logs, and role-based access control (RBAC).

Minimum necessary & de-identification

- We apply the HIPAA *minimum necessary* standard to PHI access.
- Analytics use de-identified or aggregated data under the Safe Harbor or Expert Determination methods.

> **DATA-HANDLING COMMITMENT**
>
> PHI is processed only to deliver contracted services. ARKA does not sell PHI and does not use PHI for purposes outside the BAA and the underlying services agreement.

7 CMS-0057-F — Interoperability & Prior Authorization

The CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F) establishes requirements for impacted payers that **ARKA-INS is designed to support**.

FHIR-based Prior Authorization API (PARDD)

ARKA-INS supports the Prior Authorization Requirements, Documentation, and Decision (PARDD) API, built on HL7 FHIR. Impacted payers must implement the API requirements by **January 1, 2027**; ARKA-INS is built to be ready ahead of that deadline.

Patient, Provider & Payer-to-Payer Access APIs

ARKA-INS aligns with the Patient Access, Provider Access, and Payer-to-Payer Access API requirements, built on HL7 FHIR R4 and US Core profiles.

Decision timelines

CMS-0057-F shortens prior-authorization decision windows (for example, 72 hours for expedited/urgent requests and 7 calendar days for standard requests). ARKA-INS tracks and surfaces these service-level expectations to help payers and providers stay within the required windows.

Requirement	ARKA-INS support	Standard
Prior Authorization API (PARDD)	Supported	FHIR
Patient / Provider / Payer-to-Payer Access	Aligned	FHIR R4 · US Core
Decision-timeline tracking & SLA surfacing	Built in	72h / 7d

Statutory obligations under CMS-0057-F fall on impacted payers. ARKA-INS provides the technical capabilities to support payer and provider compliance; it does not assume the payer's regulatory obligations.

8 AIIE — Appropriateness & Interoperability Inference Engine

AIIE is ARKA's methodology for turning guidelines and policies into traceable, reviewable recommendations — the engine behind Criterion 4.

Traceability
Every output links to the source guideline/policy, its version, the specific rule fired, and the patient-context inputs used.

Versioning
Guidelines and policies are versioned; ARKA records which version produced each result.

Human-in-the-loop
AIIE never auto-executes clinical actions; a licensed professional makes the decision.

9 Evidence & Citations

ARKA's recommendations cite recognized sources: specialty-society guidelines, peer-reviewed literature, and payer medical policies. We maintain a versioned evidence library so that the basis for any recommendation can be reproduced and reviewed.

10 Security Program

SOC 2 Type II — in progress / targeted | **Encryption at rest & in transit** | **RBAC & least privilege** | **Immutable audit logging** | **Vulnerability management** | **Penetration testing**

Certifications marked "in progress" are stated honestly and are not represented as complete. ARKA aligns its security program with NIST guidance.

11 Medical-Necessity Alignment (ARKA-INS)

ARKA-INS aligns clinical documentation with payer medical-necessity criteria to reduce denials and accelerate approvals.

How it works

Maps clinical facts to payer policy criteria · flags gaps before submission · surfaces the specific policy language that applies.

Guardrails

ARKA does not fabricate clinical facts. It surfaces what the policy requires and what the chart shows. The clinician attests to medical necessity — not ARKA.

12 Audit & Logging

- ✓ Immutable audit logs for recommendations, overrides, and data access.
- ✓ Tamper-evident storage; retention configured per customer policy.
- ✓ Logs are exportable to support customer compliance reviews.

13 Roles & Responsibilities

Party	Responsibility
Customer (covered entity)	Clinical use decisions and final medical judgment.
ARKA (business associate)	Safeguards PHI and provides traceable, reviewable clinical decision support.
Shared	Incident-response coordination and audit cooperation.

14 Limitations & Honest Disclosures

WHAT ARKA IS NOT

- ARKA is **not** a diagnostic device and makes **no** diagnostic claims.
- ARKA does **not** replace clinical judgment.
- Coverage estimates are **estimates**, not guarantees of payment.
- SOC 2 and certain certifications are **in progress** where noted — we do not overclaim.

These disclosures are an intentional part of ARKA's compliance posture. Stating limitations plainly reinforces the Non-Device CDS positioning and sets accurate expectations with clinicians, payers, and patients.

15 Standards & Frameworks Mapping

Framework	How ARKA maps to it	Status
FDA Non-Device CDS — Cures Act §520(o)(1)(E)	ARKA-CLIN designed to satisfy all four statutory criteria; 2022 FDA CDS guidance applied.	By design
HIPAA Privacy & Security Rules	Business Associate; administrative, physical, and technical safeguards; minimum necessary.	Implemented
CMS-0057-F Interoperability & Prior Authorization	PARDD and access APIs; decision-timeline tracking.	Ready ahead of deadline
HL7 FHIR R4 / US Core	Interoperability profiles for access and prior-authorization APIs.	Aligned
SOC 2 Trust Services Criteria	Type II program covering security controls.	In progress
NIST security guidance	Security program aligned to NIST controls.	Alignment

A Appendix A — FAQ for Compliance Officers

Q. Is ARKA an FDA-regulated device?

ARKA's clinical modules are designed as Non-Device Clinical Decision Support under the 21st Century Cures Act. We do not make diagnostic-device claims.

Q. Do you sign BAAs?

Yes. ARKA operates as a Business Associate and will execute a BAA.

Q. Where is PHI stored?

In SOC 2-aligned cloud infrastructure with encryption at rest and in transit and access controls.

Q. Can we audit?

Yes. We provide exportable audit logs and this living compliance document.

Q. How does ARKA keep a clinician "in the loop"?

Recommendations are advisory and cite their basis. Clinician overrides are logged as first-class events, and AIIE never auto-executes clinical actions.

Q. Are coverage and cost estimates guarantees of payment?

No. Estimates are estimates. ARKA surfaces what payer policy requires and what the chart shows; the clinician attests to medical necessity.

B Appendix B — Document Control & Revision History

Version	Date	Summary of changes	Owner
1.0	May 2026	Initial consolidated compliance dossier for regulatory and payer diligence review.	Compliance & Legal

This is a living document; updates are tracked by Compliance & Legal and material changes are communicated to customers under contract. Questions: compliance@getarka.health.

STANDARD DISCLAIMER

ARKA provides clinical decision support for licensed health care professionals. Recommendations are advisory, require independent clinical judgment, and do not replace the clinician–patient relationship. ARKA is not a diagnostic device.

© 2026 ARKA Health · Confidential — provided for regulatory and payer diligence review · getarka.health