

**KCST**

KELSHAD CYBER SYSTEMS AND TECHNOLOGIES LLC

KST-SAFETY-005-REV2026-10 • PUBLIC BRIEF

Safety Intelligence and Federal Data Integration

ISSUED

2026-10-17

AUTHOR

Joshua Kelsey Bass, Founder, Chairman and Chief Executive Officer

SUPERSEDES

KST-SAFETY-005-REV2026, issued May 17, 2026

CURRENT STATUS

RxOmniMedLink is in controlled private alpha. Kelshad Cyber Systems and Technologies LLC is not using live protected health information, is not transmitting live prescriptions, and does not support controlled-substance prescribing. We have not completed Surescripts onboarding, the third-party audit and certification required for EPCS under 21 CFR Part 1311, or a SOC 2 audit. This document describes both implemented capability and target architecture, and states plainly which is which.

Section 1: Purpose and scope

1.1 What this document covers

This brief describes how RxOmniMedLink uses two public federal data sources: the National Library of Medicine (NLM) RxNav service, which publishes the RxNorm medication terminology, and openFDA, which publishes drug labeling, enforcement (recall), and adverse event report data. It sets out what is implemented today in controlled private alpha, what is designed but not yet built, and the limits a reader should place on any output derived from these sources.

This document supersedes KST-SAFETY-005-REV2026. The prior revision described an automated clinical decision support system, real-time interaction blocking, and enforcement-driven inventory quarantine as existing capability. Those descriptions were not accurate. They are retained below, corrected and relabeled as target architecture, because the design work behind them is sound and remains our roadmap.

1.2 Data use limitations

The following limitations apply to every feature described in this document, implemented or planned, and they are not waivable by configuration:

- Terminology and safety data drawn from RxNav and openFDA is **reference information only**. It is presented to help a qualified professional look something up faster. It is not a recommendation.
- Federal source data **may be incomplete, delayed, or out of date**. openFDA adverse event reports are voluntary submissions that are not verified for causality, and enforcement records may lag the physical recall. RxNorm releases are periodic, and a newly marketed product may not yet be represented.
- RxOmniMedLink **does not provide clinical decision support**. It does not evaluate a patient's clinical picture, does not rank or triage risk, and does not direct or restrict any clinical action.
- Nothing in the platform is **a substitute for the independent professional judgment** of a licensed prescriber or pharmacist, or for the product labeling supplied by the manufacturer.
- RxOmniMedLink **is not a medical device**, is not registered or listed with the FDA as one, and is not marketed for the diagnosis, cure, mitigation, treatment, or prevention of disease.

Section 2: Implemented capability as of 2026-10-17

2.1 RxNorm and RxNav terminology

The platform uses the NLM RxNav API for medication terminology and for validation of medication entries. Free-text and locally entered medication names are resolved against RxNorm Concept Unique Identifiers (RxCUIs) so that the same product carries the same identifier everywhere in the system. This is normalization and lookup work: it prevents two spellings of one drug from being treated as two drugs. It is not an interaction verdict.

Where a name cannot be resolved to an RxCUI, the entry is surfaced as unresolved rather than silently guessed. A user resolves it manually.

2.2 openFDA reference data

openFDA data is referenced for safety information. Retrieved records are displayed to the user with their source and retrieval context so the user can go to the primary federal record. The platform does not currently score, weight, or threshold this data, and it does not act on it automatically.

Systematic ingestion of the openFDA enforcement (recall) and adverse event report streams is target architecture and is described in Section 3. It is not implemented as of 2026-10-17, and no reader should assume this platform will surface a recall or an adverse event report for a given product.

2.3 Security controls supporting these integrations

- **Transport.** All traffic, including outbound calls to federal endpoints, runs over TLS 1.3.
- **Identity.** Clinical users are verified through Stripe Identity to a NIST IAL2 standard before they are granted a clinical role.
- **Authorization.** Role-based access control governs which users can view or enter medication data.
- **Audit logging.** Access and change events are written to an audit log. **This log is not currently tamper-evident.** The integrity column in the audit schema is presently populated with constant string labels rather than computed digests. Remediation is in progress. Until it ships, no representation of tamper evidence, immutability, or non-repudiation should be read into this control.

- **Encryption at rest.** Data at rest is encrypted by our managed database provider (Render Postgres) using industry-standard AES-256. This is provider-level encryption. Kelshad Cyber Systems and Technologies LLC has not built application-level encryption of protected health information.
- **Vendor agreements.** Business Associate Agreements are in place with the vendors in the data path, including our hosting and database providers. Live protected health information is still not present in the environment.
- **Testing.** A third-party penetration test of the platform has been completed. No SOC 2 audit has been performed.

Section 3: Target architecture

Target architecture. The following describes the intended design. It is not implemented as of 2026-10-17.

3.1 Design principles

1. **Authoritative fetching over stale local tables.** Safety and terminology lookups should be served from a fresh query to the federal source, or from a short-lived cache with an explicit age shown to the user, rather than from an unmaintained local copy.
2. **Deterministic coding at every boundary.** Every medication field entering the system should carry an RxCUI and, where applicable, a National Drug Code before it reaches any downstream consumer.
3. **Visible, attributed alerts.** Where a potential interaction or an enforcement record is surfaced, it should be shown with its source, its retrieval time, and the reminder that it is reference information requiring professional review. Any workflow interruption is designed to prompt review, not to render a clinical determination.

3.2 Planned openFDA and RxNav pipeline

The intended pipeline runs federal lookups on an asynchronous worker tier separate from request-handling threads, with a short-lived cache in front of the upstream API, strict JSON schema validation of every response before it is admitted to internal processing, per-call timeouts, and structured error logging. When an upstream endpoint is unavailable and the cache misses, the intended behavior is to display an explicit "safety reference unavailable" state instructing the user to consult the primary source directly. The system is designed never to present an empty result as a clean result.

Planned RxNav endpoints include `/REST/rxcui.json` for name to identifier resolution and `/REST/interaction/list.json` for retrieval of documented interaction pairs. Planned openFDA streams include the drug enforcement and drug label endpoints.

3.3 Terminology mapping and current status

The target architecture marker above applies to every row in this table except where the status column states otherwise. The table is included here so the full intended mapping can be read in one place.

DATA CONTEXT	SOURCE REGISTRY	IDENTIFIER	STATUS
Active compounds	NLM RxNorm	RxCUI	Implemented

DATA CONTEXT	SOURCE REGISTRY	IDENTIFIER	STATUS
Commercial packages	FDA NDC Directory	10 or 11 digit NDC	Target architecture
Enforcement events	openFDA enforcement	FDA event record ID	Target architecture
Adverse reaction terms	openFDA reaction fields	Reported term	Target architecture

3.4 Planned privacy handling for outbound queries

The intended model is data minimization at the boundary: no patient identifier is included in any outbound query to a federal endpoint, and internal correlation of a lookup to a record is carried by a one-way salted digest rather than by an identifier of clinical or commercial value. This design is not yet exercised against live data, because the environment contains synthetic test data only.

3.5 Explicitly out of scope

The following appeared in the prior revision and are withdrawn rather than relabeled, because they describe activity Kelshad Cyber Systems and Technologies LLC is not positioned to perform:

- Automated matching of enforcement records against live pharmacy inventory. There is no pharmacy network connectivity. Surescripts onboarding is not complete, and nothing is transmitted to any pharmacy network.
- Automated hard blocking of an order on the basis of a retrieved interaction record. Blocking a clinical action on an automated determination is decision support, and the platform does not do it.
- Any representation of Epic, Cerner, or other EHR compatibility. None has been tested or established.
- FHIR R4 data export of safety records. HL7 FHIR R4 is the design direction for the platform's data model, but no export route exists in the backend.

Section 4: Regulatory position

HIPAA. RxOmniMedLink is built toward HIPAA-aligned controls, including access control, audit logging, transport encryption, and data minimization consistent with the HIPAA Security Rule technical safeguards at 45 CFR 164.312. Kelshad Cyber Systems and Technologies LLC makes no claim of HIPAA certification, and no such certification exists in United States law. Business Associate Agreements are in place with the vendors in the data path. No live protected health information is processed.

Controlled substances. The platform does not support controlled-substance prescribing. A technical block enforcing this is being shipped. There is no EPCS certification, and no third-party audit under 21 CFR Part 1311 has been performed or begun.

Medical device status. The safety reference features described here are informational lookups against public federal data with full source attribution. Should Kelshad Cyber Systems and Technologies LLC pursue predictive or interpretive safety features in the future, their regulatory status will be assessed under current FDA clinical decision support guidance before any release, and this document will be revised before any such feature reaches a user.

Section 5: Document control

Kelshad Cyber Systems and Technologies LLC is a Florida limited liability company, document number L26000296916, EIN 42-2712869, located at 7901 4th Street North, Suite 300, St. Petersburg, FL 33702.

Questions, corrections, and verification requests: info@kelshad.com, (813) 982-8779.

This document will be revised when a described target capability ships, when the audit log integrity remediation is verified, or when any statement in it ceases to be accurate, whichever comes first.

KST-SAFETY-005-REV2026-10 · Classification: Public · This brief is not a certification, audit report, or legal advice. Questions about any statement: info@kelshad.com