

**KCST**

KELSHAD CYBER SYSTEMS AND TECHNOLOGIES LLC

KST-INTEROP-003-REV2026-10 · PUBLIC BRIEF

Interoperability and Clinical Data Integration

ISSUED

2026-10-17

AUTHOR

Joshua Kelsey Bass, Founder, Chairman and Chief Executive Officer

SUPERSEDES

KST-INTEROP-003-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.

1. Scope and Purpose

This document describes the interoperability design of RxOmniMedLink: the standards the platform is built around, the data-exchange capability that exists today, and the integration architecture that is planned but not yet implemented. It replaces the May 17, 2026 revision, which asserted certified compatibility with third-party electronic health record (EHR) products and a working standards-based export capability. Neither assertion was accurate, and both have been removed.

RxOmniMedLink is built around the HL7 Fast Healthcare Interoperability Resources (FHIR) Release 4 (R4) framework as its design direction. FHIR R4 organizes clinical concepts into modular, predictable JSON resources with stable identifiers, which gives the platform a common internal vocabulary and a defensible path toward future external exchange. Choosing that framework is a design commitment. It is not, by itself, a claim of connectivity to any external system, and this document does not make one.

2. Implemented Capability

The following describes functionality that exists in the alpha build today.

Medication terminology and validation. The platform uses RxNorm and the National Library of Medicine RxNav service for medication terminology, normalization, and validation. Drug concepts inside the system are

carried as RxNorm codes rather than free text, which removes a common source of transcription and name-matching error. Publicly available openFDA data is referenced for safety information presented alongside a medication record.

Identity verification of clinical users. Stripe Identity is used to verify the identity of clinical users to a NIST IAL2 standard before a clinical account is activated.

Secure three-way messaging. Prescriber, pharmacist, and patient can communicate within a single structured thread tied to a prescription record.

Refill coordination and status visibility. Participants in a prescription share visibility into its current status, and refill requests are coordinated through the platform rather than through unstructured phone and fax traffic.

Transport and storage protection. Data in transit is protected with TLS 1.3. Data at rest is encrypted by the managed database provider (Render Postgres) using industry-standard AES-256. This is provider-level encryption. Kelshad Cyber Systems and Technologies LLC has not implemented an application-level field encryption layer for protected health information, and does not represent that it has.

Access control and audit logging. Role-based access control governs which user roles may read or modify which records, and application actions are written to an audit log.

Limitation on the audit log. The audit log is not currently tamper-evident. The `sha384_checksum` column is populated with constant string labels rather than computed digests. Remediation is in progress. Until it ships, no Kelshad Cyber Systems and Technologies LLC document, including this one, claims tamper evidence, immutability, or non-repudiation for audit records.

3. Capability That Does Not Exist Today

Stated plainly, so that no reader is misled by the architecture sections that follow:

- There is **no working FHIR R4 data export**. No export route exists in the backend.
- There is **no integration or tested compatibility with any EHR product from any vendor**. No connection has been established, and no compatibility has been tested.
- There is **no Surescripts connectivity**. Onboarding is not complete, and nothing is transmitted to any pharmacy network.
- There is **no EPCS certification** and no controlled-substance prescribing support. A technical block is being shipped to enforce that restriction in the product.
- There is **no SOC 2 audit**.
- There is **no live protected health information** in the system. All alpha data is synthetic test data.
- There is **no FIPS 140-2 validated PKI signing engine**.

4. Target Architecture: FHIR R4 Resource Model

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

Internal records are intended to map deterministically onto standard FHIR R4 resources, with vocabulary bindings enforced at the schema layer, so that a future export or exchange interface can be added without reshaping the underlying data model.

INTERNAL RECORD	TARGET FHIR R4 RESOURCE	VOCABULARY BINDING	TARGET PROFILE
Patient demographics	Patient	ISO 3166 and US extensions	US Core Patient
Clinical user identity	Practitioner	National Provider Identifier	US Core Practitioner
Facility record	Organization	Employer Identifier / Tax ID	US Core Organization
Prescription order	MedicationRequest	RxNorm	US Core MedicationRequest

The intended semantic policy is strict binding to recognized coding systems rather than local free text: RxNorm for therapeutic products, SNOMED CT for clinical findings and diagnostic status, and LOINC for laboratory observations. Custom fields and non-standard extensions are to be excluded from the transit layer by design. No transit layer exists today, so this is a specification rather than an operating rule.

No export route implementing this model exists in the backend. When one is built, this document will be revised to move that capability into Section 2, and the claim will be made only after the route is demonstrable.

5. Target Architecture: Authorization Model

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

Any future exchange with an external clinical system is intended to use the SMART on FHIR authorization framework rather than a proprietary credential exchange. The intended sequence is a standard OAuth 2.0 authorization code flow: the clinical user launches the application from an authorized context, authenticates against the identity provider of the host system, approves the requested scopes, and the application exchanges the resulting authorization code for a short-lived access token.

Scope requests are intended to follow least privilege, requesting only the resource types and operations a given transaction requires, for example a read-only patient demographic scope where no write is needed. Tokens are intended to be short-lived and bound to a single session.

6. Target Architecture: Integration Security Controls

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

The planned integration boundary would place schema validation ahead of application logic. Inbound payloads would be validated against FHIR R4 structural definitions at the edge and rejected on structural anomaly before reaching internal services. Planned controls at that boundary include network isolation for integration workloads, mutual TLS between the edge and ingestion services, and text sanitization of human-readable narrative fields to prevent script and injection payloads carried inside otherwise valid clinical resources.

The threat model driving those controls covers structured-data injection through nested payloads, token replay and session hijacking, and spoofed resource submission. These are design targets. A third-party penetration test of the platform has been completed. Their effectiveness has not otherwise been independently evaluated.

7. Data Handling and Privacy Commitments

Kelshad Cyber Systems and Technologies LLC does not sell, rent, or license patient data, and does not process patient data for secondary profiling, advertising, or resale. Clinical data is used only to perform the workflow the user requested.

The platform operates HIPAA-aligned controls. No HIPAA certification exists in United States law, and this company does not claim any such certification, nor does it represent that it has achieved full compliance with HIPAA. Alignment is a description of controls, not a credential.

Business Associate Agreements are in place with the vendors in the platform's data path. The platform still does not process live protected health information during the controlled private alpha.

8. External Representation Policy

This company does not describe, certify, or characterize the behavior, requirements, or acceptance criteria of another vendor's system. Statements in the superseded revision about how specific EHR platforms authenticate, route, or validate requests were removed for that reason, in addition to being untested. Any future statement about connectivity to a named third-party system will be published only after that connectivity exists, has been tested, and is permitted by the agreement governing it.

9. Roadmap

Near-term interoperability work, in order of priority: repair of the audit-log checksum implementation so that tamper evidence can be claimed honestly; and implementation of a FHIR R4 export route against the resource model in Section 4. Longer-term direction includes automated translation of legacy HL7 v2 messages into FHIR R4 structures.

Kelshad Cyber Systems and Technologies LLC commits a share of future platform revenue to community initiatives, including workforce safety support and youth mentorship. The platform is in private alpha and is not generating revenue, so this is a stated commitment for the future rather than a description of a program now in operation.

10. Document Control

This document supersedes KST-INTEROP-003-REV2026 in full. Any earlier copy asserting EHR vendor compatibility, a working FHIR export, tamper-evident audit records, or HIPAA certification is withdrawn and must not be relied upon.

Kelshad Cyber Systems and Technologies LLC Florida document number L26000296916, EIN 42-2712869
7901 4th Street North, Suite 300, St. Petersburg, FL 33702 info@kelshad.com | (813) 982-8779

KST-INTEROP-003-REV2026-10 · Classification: Public · This brief is not a certification, audit report, or legal advice. Questions about any statement: info@kelshad.com