

**KCST**

KELSHAD CYBER SYSTEMS AND TECHNOLOGIES LLC

KST-EPCS-004-REV2026-10 · PUBLIC BRIEF

Controlled Substance Prescribing: Position and Target Architecture

ISSUED

2026-10-17

AUTHORJoshua Kelsey Bass, Founder, Chairman and Chief
Executive Officer**SUPERSEDES**

KST-EPCS-004-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. Notice

RxOmniMedLink DOES NOT SUPPORT CONTROLLED SUBSTANCE PRESCRIBING.

Kelshad Cyber Systems and Technologies LLC (KCST) holds no EPCS certification under 21 CFR Part 1311. No third-party audit or certification of RxOmniMedLink for the electronic prescribing of controlled substances has been completed, and none has been started.

Do not use RxOmniMedLink to prescribe any controlled substance, in any schedule, for any patient, under any circumstance. The platform is not lawful for that purpose and is not built for that purpose. A technical block that refuses controlled substance orders is in development and has not shipped as of 2026-10-17. Until it does, the prohibition rests on this notice and on the fact that RxOmniMedLink has no connection to any pharmacy network and transmits nothing.

Prescribers who need to issue a controlled substance order must use a separate application that holds a current third-party audit or certification for EPCS, in accordance with 21 CFR 1311.300.

This document exists because the version it supersedes claimed a capability KCST does not have. That document has been withdrawn in full and nothing in it should be relied upon.

The purpose of this replacement is narrower: to state our position without qualification, to describe what the platform actually does today, and to set out our understanding of what a conforming EPCS implementation would require. Understanding a regulatory regime and meeting it are different things. This document is an account of the first only.

2. Why We State This Plainly

KCST adopted the following principle on 2026-08-07, and it governs every public document we issue:

Disclosure is a credibility asset, not a concession. A counterparty who discovers an overclaim later is far more damaged, and does far more damage, than a counterparty who knows our real position now.

In healthcare infrastructure, the cost of an overclaim is not reputational alone. A hospital network, pharmacy group, or provider practice that relies on a vendor's assertion of EPCS conformance inherits federal exposure it did not knowingly accept. A vendor claim is not a defense. The registrant who signs the prescription carries the liability.

We would rather be the vendor that says "not yet, and here is exactly where we are" than the vendor whose customer learns the truth during an audit, a Drug Enforcement Administration inquiry, or a diversion investigation. This position is not costless: it removes RxOmniMedLink from consideration for any procurement that requires EPCS today. We accept that outcome as the correct one, and ask to be evaluated on what we have built and on the honesty of our description of it.

3. What Is True Today

The following describes the state of RxOmniMedLink as of 2026-10-17.

3.1 Nothing is transmitted anywhere. RxOmniMedLink has no Surescripts connectivity. Onboarding is not complete. No prescription of any kind, controlled or otherwise, is transmitted to any pharmacy network from this platform. There is no transmission path a controlled substance order could take.

3.2 No live patient data. The platform holds no live protected health information. All data in the alpha environment is synthetic test data.

3.3 Terminology and identification. Medication identification and validation use RxNorm and the National Library of Medicine RxNav service. Safety information references openFDA data. These sources are not, and are not represented as, a substitute for a certified EPCS application.

3.4 Supporting controls. Identity verification for clinical users is performed through Stripe Identity to a NIST IAL2 standard. Role-based access control and audit logging are implemented. TLS 1.3 protects data in transit. Data at rest is encrypted by our managed database provider (Render Postgres) using industry-standard AES-256; this is provider-level encryption, not application-level PHI encryption built by KCST. Access controls are operated to HIPAA-aligned standards. KCST makes no claim of HIPAA certification, because no such certification exists in United States law.

3.5 Implemented clinical collaboration. Secure three-way messaging among prescriber, pharmacist, and patient is implemented, as are refill coordination and shared prescription-status visibility. The platform is built around the HL7 FHIR R4 framework as a design direction.

3.6 Known limitations we are disclosing rather than deferring.

- **The controlled substance block described in Section 4 has not shipped.** It is in active development. As of 2026-10-17 there is no implemented technical control preventing a controlled substance from being entered in the prescribing workflow. Because nothing is transmitted (3.1) and no live patient data is present (3.2), the practical exposure in the alpha environment is contained, but we will not describe an unshipped control as an operating one.
- **The audit trail is not currently tamper-evident.** The `sha384_checksum` column in the audit log is populated with constant string labels rather than computed digests. Repair is in progress. Until that work ships and is verified, no KCST document, including this one, claims tamper evidence, immutability, or non-repudiation for any log.
- No SOC 2 audit has been performed.
- No integration or compatibility with Epic, Cerner, or any other EHR vendor has been tested or established.
- No FHIR R4 data export exists. There is no export route in the backend.

4. The Controlled Substance Block

Target architecture. The following describes a control that is in development and is not implemented as of 2026-10-17. It is not a statement of current capability.

4.1 Refusal in the backend. The prescribing workflow is being changed to refuse any medication identified as a controlled substance. The refusal is to be enforced server-side, not in the user interface alone, so that it cannot be bypassed by a client-side change or a direct API call.

4.2 Fail closed. Identification of a drug as non-controlled is to be a positive requirement, not a default. If the medication cannot be resolved against our terminology sources, if a lookup fails, if a service is unreachable, or if the control status is ambiguous for any reason, the order is refused. An unknown drug is to be treated as a prohibited drug. The design admits no override path, no administrative exception, and no configuration flag that relaxes the behavior for a tenant, a practice, or an individual prescriber.

4.3 Attempts are recorded. Each refused attempt is to be written to the audit log with the requesting user, the timestamp, the drug as submitted, the reason for refusal, and the originating session, and surfaced to account administrators. A pattern of attempts is information a clinical organization needs. The value of this record depends on the audit log integrity repair described in 3.6.

5. EPCS Target Architecture

Target architecture. The following describes our reading of the applicable requirements and the intended design. It is not implemented as of 2026-10-17. Nothing in this section is a statement of conformance, a claim of capability, or a commitment to deliver.

If KCST were to pursue EPCS capability, 21 CFR Part 1311 Subpart C would govern the work. Our present understanding of what it demands is set out below, alongside an honest accounting of the distance between each requirement and our current state.

5.1 Identity proofing of the prescriber. The regulation requires identity proofing of individual practitioners through a credential service provider or certification authority meeting specified assurance levels, or through an institutional practitioner acting under the conditions the rule sets out. Our existing Stripe Identity verification reaches an IAL2 standard but is not, on its own, the identity proofing the DEA rule contemplates, and we do not present it as such. A conforming design would require a credential issuance path separate from ordinary account creation, plus out-of-band verification of state licensure and DEA registration.

5.2 Logical access control and separation of duties. Access to the signing function may not be granted by a single actor. The rule requires that the entry granting signing authority be made by one individual and approved by a second, with the roles of identity verification, access administration, and prescribing held separately. Our current role-based access control model does not implement this two-party provisioning step. Adding it would require a distinct authorization workflow with its own audit record, not a permission flag.

5.3 Two-factor authentication at the moment of signing. Signing a controlled substance order requires two of three independent factors: something the practitioner knows, something the practitioner has (a hard token meeting the applicable federal standard), and something the practitioner is (a biometric meeting the rule's separate biometric requirements). The authentication must occur at the act of signing, not merely at session start. RxOmniMedLink does not implement this.

5.4 Signing and record integrity. A conforming implementation binds the exact content of the order to the prescriber's credential at the instant of signature, using a cryptographic module validated to the applicable FIPS standard. **KCST does not operate a FIPS 140-2 validated PKI signing engine and has never operated one.** Any prior statement to the contrary was incorrect. The record must be preserved such that alteration after signing is detectable.

5.5 Internal audit trail. The rule requires that the application record specified events, run its own internal audit against auditable events, and generate a report for review when one occurs. This depends on an audit log whose integrity can be demonstrated. As stated in 3.6, ours cannot be demonstrated today. Fixing the checksum implementation is a prerequisite to any further work in this area, not a detail within it.

5.6 Transmission. A controlled substance order must reach the pharmacy without alteration in content, and the rule constrains intermediary handling. This presumes pharmacy network connectivity. KCST has none.

5.7 Under evaluation, not committed. We are examining decentralized verifiable credentials (W3C Verifiable Credentials) as a possible approach to portable practitioner licensure attestation. This is exploratory research: not built, not scheduled, and not a substitute for any requirement above.

6. The Path to Certification

We are not going to publish a date we cannot keep, so this section commits to none.

The sequence is fixed by the regulation, not by us. Under 21 CFR 1311.300, an application may not be used for the electronic prescribing of controlled substances until it has been reviewed by a qualified third party, either through a certification process or an audit performed by a person qualified to conduct SysTrust, WebTrust, or SAS 70 style engagements, and found to meet the Part 1311 requirements. That review is a precondition, and it is not something a vendor performs on itself.

Ahead of any such engagement, KCST would need at minimum to: ship and verify the controlled substance block; complete the audit log integrity repair; complete Surescripts onboarding; build the identity proofing, two-party access provisioning, two-factor signing, and validated cryptographic signing capabilities described in Section 5; and demonstrate all of it against a live-data environment we do not yet operate.

Each of those is substantial. Together they are a program of work, not a release. We will report progress in future revisions of this document, and will not announce a schedule until the work underneath it is real.

Until that day arrives and a completed third-party audit or certification exists to point to, **RxOmniMedLink must not be used to prescribe controlled substances**. If that changes, it will be announced here first, with the auditor named and the report date stated.

7. Document Control and Contact

This document supersedes KST-EPCS-004-REV2026 ("Controlled Substances E-Prescribing (EPCS) Security Framework", issued May 17, 2026) in its entirety. That document contained claims of EPCS capability, audit status, and cryptographic infrastructure that were not accurate. It has been withdrawn and should not be circulated or relied upon.

This brief is descriptive and is not legal advice. Readers evaluating their own obligations should consult 21 CFR Part 1311 directly and take advice from qualified counsel.

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

Questions, corrections, and challenges to any statement in this document are welcome and will be answered. If you believe something here is inaccurate, tell us and we will correct it.

KST-EPCS-004-REV2026-10 · Classification: Public · This brief is not a certification, audit report, or legal advice. Questions about any statement: info@kelshad.com