

**KCST**

KELSHAD CYBER SYSTEMS AND TECHNOLOGIES LLC

KST-CRYPTO-002-REV2026-10 • PUBLIC BRIEF

Data Encryption and Infrastructure Architecture

ISSUED

2026-10-17

AUTHOR

Joshua Kelsey Bass, Founder, Chairman and Chief Executive Officer

SUPERSEDES

KST-CRYPTO-002-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: Scope and Purpose

This brief describes how RxOmniMedLink protects data in transit and at rest, what cryptographic controls are running in the controlled private alpha environment today, and what remains designed but unbuilt. It supersedes KST-CRYPTO-002-REV2026 in full. The superseded revision described a cryptographic architecture that was in substantial part aspirational and presented it as operational. This revision separates the two.

The intended readers are prospective clinical partners, security reviewers, and counsel performing diligence. It is written so that a reviewer can tell, section by section, whether a control is running or planned. Where a control is planned, the engineering design is retained rather than deleted, because the design work has value and a reader is better served by an accurate roadmap than by a silent omission.

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

The controls in this section are in place in the alpha environment. They operate against synthetic test data only. No live protected health information (PHI) has been entered into or processed by the platform.

2.1 Data in Transit: TLS 1.3

All client and service connections to RxOmniMedLink are carried over TLS 1.3. Application traffic negotiates authenticated encryption with associated data (AEAD) cipher suites, principally TLS_AES_256_GCM_SHA384 and TLS_CHACHA20_POLY1305_SHA256, the latter being favored by resource-constrained mobile clients. TLS 1.3 removes static RSA key exchange, so every session derives unique ephemeral keys and past sessions are not retroactively readable if a long-term server key is later exposed. The handshake completes in a single round trip, which lowers latency on mobile connections without weakening the negotiation.

2.2 Data at Rest: Provider-Managed AES-256

Persistent application data is stored in a managed PostgreSQL instance operated by Render. Render encrypts that storage at rest using industry-standard AES-256.

This is provider-level encryption. It is important to state the boundary precisely:

- The encryption at rest is performed by the managed database provider, at the storage layer.
- Kelshad Cyber Systems and Technologies LLC has **not** built application-layer or field-level PHI encryption. Individual columns are not separately encrypted by the application before they reach the database.
- Key custody for at-rest encryption sits with the provider, not with KCST. KCST does not operate a hardware security module, a customer master key, or an envelope encryption scheme today.

Provider-level AES-256 protects against loss of the underlying physical media and against certain classes of infrastructure compromise. It does not, by itself, protect a record from an actor who has legitimate credentials to the running database. Application-layer encryption addressing that threat is described in Section 4 as target architecture.

2.3 Access Control and Audit Logging

Role-based access control (RBAC) governs which authenticated principals may read or write which records. Prescriber, pharmacist, and patient roles carry distinct permission sets, and the secure three-way messaging channel among those parties is scoped by the same role model.

The platform writes an audit log of security-relevant events. Readers should note the following limitation, stated here rather than buried: **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 over row content. Repair is in progress. Until that work ships and is verified, no KCST document, including this one, asserts tamper evidence, immutability, or non-repudiation for the audit trail. What exists today is audit logging: a durable record of events, adequate for operational review, not adequate as a cryptographic integrity guarantee.

2.4 Third-Party Services in the Data Path

- **Stripe Identity** performs identity verification for clinical users to a NIST IAL2 standard.
- **RxNorm and NLM RxNav** supply medication terminology and validation.
- **openFDA** data is referenced for safety information.

Business Associate Agreements are in place with the vendors in the platform's data path. They are a precondition for handling live PHI, which the platform does not yet do.

Section 3: Explicit Non-Claims

The following are stated so that no reader infers them from adjacent technical detail. As of 2026-10-17, RxOmniMedLink has:

- No EPCS certification, and no third-party audit for 21 CFR Part 1311 has been performed or begun.
- No controlled-substance prescribing support. It is unsupported, and a technical block enforcing this is being shipped.
- No Surescripts connectivity. Onboarding is incomplete and nothing is transmitted to any pharmacy network.
- No SOC 2 audit.
- No live protected health information. Synthetic test data only.
- No Epic, Cerner, or other EHR integration. No compatibility with any EHR vendor has been tested or established.
- No FIPS 140-2 validated PKI signing engine.
- No working FHIR R4 data export. No export route exists in the backend.

KCST does not describe this platform, or any platform, as certified under HIPAA. No such certification exists in United States law, and any vendor offering one is describing something other than a legal status. The phrase KCST uses is **HIPAA-aligned controls**, meaning controls designed with reference to the HIPAA Security Rule technical safeguards at 45 CFR 164.312, without any claim of certification, attestation, or third-party validation.

Section 4: Target Architecture

Target architecture. The following describes the intended design. It is not implemented as of 2026-10-17. Nothing in this section may be read as a statement of current capability.

4.1 Application-Layer Field Encryption

The intended design adds AES-256-GCM encryption of high-sensitivity fields in application memory before those values reach the database engine, layered above the provider-level at-rest encryption already in place. GCM is selected over ECB or CBC because it is an AEAD mode: each ciphertext carries an authentication tag, so alteration of stored data is detectable at decryption time rather than silently accepted.

4.2 Envelope Encryption and Key Management

The intended key hierarchy separates a customer master key (CMK) held in a managed key service from short-lived data encryption keys (DEKs) generated per encryption task. The plaintext DEK encrypts the payload locally and is zeroed from memory immediately; the CMK-wrapped DEK is stored alongside the ciphertext. Planned rotation cadences are 365 days for customer master keys with retired keys retained in decrypt-only state, 90 days for high-risk application keys, and single-session lifetime for ephemeral session keys.

Where a FIPS 140-2 validated cryptographic module or hardware security module is referenced in KCST planning material, it is a target-architecture requirement for a future production environment. KCST operates no FIPS 140-2 validated module today and makes no FIPS validation claim.

4.3 Network Segmentation and Mutual TLS

The intended production topology places internal services in an isolated private network with mutual TLS between microservices, backed by an internal private certificate authority, so that each service presents a signed X.509 identity before peer access. Edge termination is intended to run on hardened reverse-proxy nodes enforcing TLS 1.3 exclusively, HTTP Strict Transport Security with preload, and a restricted cipher list. This topology is designed, not deployed.

4.4 Tamper-Evident Audit Trail

The intended design computes a SHA-384 digest over the canonical serialization of each audit row, chained to the digest of the preceding row, so that deletion or modification of any entry is detectable by recomputation. This replaces the constant-label placeholder described in Section 2.3. Only after this ships and is independently verified will KCST describe the audit trail as tamper-evident.

4.5 Interoperability

RxOmniMedLink is built around the HL7 FHIR R4 framework as a design direction. A FHIR R4 export route is planned. None exists in the backend today.

Section 5: Regulatory Posture

Encryption in transit and at rest is one technical safeguard among several contemplated by the HIPAA Security Rule. KCST's position is that implemented controls (TLS 1.3, provider-managed AES-256, RBAC, audit logging) constitute progress toward HIPAA-aligned technical safeguards, and that alignment is not compliance, certification, or attestation, none of which KCST holds.

Regarding the HITECH breach notification safe harbor: the safe harbor turns on whether affected data was rendered unusable, unreadable, or indecipherable in accordance with HHS guidance at the time of a breach. KCST does not assert safe harbor eligibility. The question is currently moot, because the platform holds no live PHI. It will be reassessed, with counsel, before any live PHI is accepted, and that reassessment depends on the application-layer work in Section 4.1.

KCST makes no FedRAMP claim of any kind.

Section 6: Threat Model Notes

Two observations are offered as reasoning rather than as claims of protection.

First, symmetric key strength ages comparatively well against quantum cryptanalysis. Grover's algorithm reduces the effective security of a symmetric key by roughly half, so a 256-bit key retains on the order of 128 bits of margin. This is a property of AES-256 as an algorithm and is independent of who operates the key.

Second, side-channel resistance depends on constant-time implementations in the underlying cryptographic libraries and on hardware-accelerated instruction paths. KCST relies on the platform and library

implementations of these primitives and has not performed independent side-channel testing. A third-party penetration test of the platform has been completed.

Section 7: Document Control

This document is public and may be redistributed unmodified. It will be revised when any control listed in Section 4 moves into production, when any item in Section 3 ceases to be accurate, or on the next scheduled review, whichever is earliest. Statements in superseded revisions should 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-CRYPTO-002-REV2026-10 · Classification: Public · This brief is not a certification, audit report, or legal advice. Questions about any statement: info@kelshad.com