

**KCST**

KELSHAD CYBER SYSTEMS AND TECHNOLOGIES LLC

KST-PRIVACY-006-REV2026-10 · PUBLIC BRIEF

Data Privacy Governance and the Zero PHI Commercialization Mandate

ISSUED

2026-10-17

AUTHOR

Joshua Kelsey Bass, Founder, Chairman and Chief Executive Officer

SUPERSEDES

KST-PRIVACY-006-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: The Zero PHI Commercialization Mandate

1.1 The commitment

Kelshad Cyber Systems and Technologies LLC does not sell, license, rent, trade, or otherwise commercialize protected health information. This is unconditional. It is not contingent on volume, funding pressure, acquisition, partnership terms, or a future change of business model.

Concretely, the company will not:

- sell or license patient records, clinical indicators, prescription histories, or derived health datasets to any third party;
- share or disclose protected health information for advertising, marketing, lead generation, or audience targeting;
- monetize behavioral or usage metadata that describes an identifiable patient;
- permit a third party to extract, mine, or resell customer data as a condition of any integration or vendor agreement.

No live protected health information exists in the platform today. When protected health information is eventually entrusted to RxOmniMedLink, it will exist to execute the clinical workflow the user requested. Nothing else.

1.2 Why this is stated first

Most privacy documents lead with control inventories. Controls change as a platform matures. A commercialization stance is a matter of business model, and a business model is a decision, not an engineering artifact. Covered entities evaluating RxOmniMedLink are entitled to know that decision before they read anything about ciphers or key management.

1.3 Scope and enforcement

The mandate binds Kelshad Cyber Systems and Technologies LLC, its employees and contractors, and any subcontractor or vendor that touches customer data. It will be expressed as an affirmative term in each customer agreement and in each Business Associate Agreement the company executes, so that it is contractually enforceable by the customer and not merely a published intention.

Section 2: Scope and purpose of this document

This brief describes the privacy governance posture of RxOmniMedLink, the medication coordination platform operated by Kelshad Cyber Systems and Technologies LLC. It supersedes KST-PRIVACY-006-REV2026 in full. The prior revision contained capability claims that were aspirational or inaccurate, including an assertion that the privacy infrastructure had already been audited. No audit of that infrastructure has been performed. That claim is withdrawn.

This document is public. It is not a certification, an attestation, or a legal opinion, and it does not create warranties beyond those in an executed agreement.

Section 3: What is implemented today

RxOmniMedLink is in controlled private alpha and operates exclusively on synthetic test data. No live protected health information has been loaded into any environment.

Implemented and in use:

- **Identity verification.** Stripe Identity verifies clinical users to a NIST IAL2 standard.
- **Medication terminology.** RxNorm and the NLM RxNav services provide medication naming and validation.
- **Safety reference data.** openFDA data is referenced for safety information.
- **Transport encryption.** TLS 1.3 protects data in transit.
- **Encryption at rest.** The managed database provider (Render Postgres) encrypts stored data using industry-standard AES-256. This is provider-level encryption. Kelshad Cyber Systems and Technologies LLC has not built application-level field encryption for protected health information, and this document does not claim it.
- **Access control.** Role-based access control governs what each account may read and write.
- **Audit logging.** Application events are written to an audit log. See Section 6 for the current, material limitation of that log.
- **Clinical coordination.** Secure three-way messaging among prescriber, pharmacist, and patient, refill coordination, and shared prescription-status visibility are working features.

The platform is designed around the HL7 FHIR R4 framework as a design direction. There is no FHIR R4 data export route in the backend today.

3.1 What is explicitly not claimed

The following are stated plainly so that no reader is misled: no EPCS certification and no third-party audit under 21 CFR Part 1311; no controlled-substance prescribing support, and a technical block is being shipped to enforce that; no Surescripts connectivity and nothing transmitted to any pharmacy network; no SOC 2 audit; no Epic, Cerner, or other EHR integration, and no tested compatibility with any EHR vendor; no FIPS 140-2 validated PKI signing engine.

Section 4: HIPAA-aligned controls and the BAA gate

4.1 Terminology

Kelshad Cyber Systems and Technologies LLC describes its work as implementing **HIPAA-aligned controls**. The company does not describe itself or RxOmniMedLink as "HIPAA compliant", "HIPAA certified", or as having achieved "full HIPAA compliance". No HIPAA certification exists in United States law. Any vendor claiming one is describing something that cannot be granted.

4.2 Business Associate Agreements

Business Associate Agreements are in place with the vendors in the platform's data path. No live protected health information exists in the platform today.

The governing rule going forward is simple and it is a gate, not a goal: **a Business Associate Agreement is executed with each covered entity and with each vendor in the data path before any protected health information is processed**. No pilot, demonstration, or convenience exception is available against this rule.

4.3 Technical safeguard mapping (45 CFR 164.312)

STATUTORY AREA	APPROACH	STATUS AS OF 2026-10-17
Unique user identification, 164.312(a)(2)(i)	Distinct account identifiers for every actor, enforced by role-based access control	Implemented
Person or entity authentication, 164.312(d)	Stripe Identity verification of clinical users to NIST IAL2	Implemented
Transmission security, 164.312(e)(1)	TLS 1.3 for external communication paths	Implemented
Encryption at rest, 164.312(a)(2)(iv)	AES-256 provider-level encryption via the managed database provider	Implemented at provider level; application-level PHI encryption not built
Audit controls, 164.312(b)	Application audit logging of access and change events	Implemented, with the integrity limitation in Section 6
Integrity, 164.312(c)(1)	Verifiable digests over audit records	Not satisfied; remediation in progress
Emergency access, 164.312(a)(2)(iii)	Break-glass access under multi-party authorization	Target architecture

STATUTORY AREA	APPROACH	STATUS AS OF 2026-10-17
Automatic logoff, 164.312(a)(2)(iii)	Sliding inactivity timeout across web and mobile sessions	Target architecture

Administrative and physical safeguards under 45 CFR 164.308 and 164.310 are inherited in part from the hosting provider and are otherwise target architecture. The prior revision described biometric-controlled, FIPS 140-2 Level 3 data center facilities under direct company control. That description was not accurate and has been removed.

Section 5: Target architecture

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

5.1 De-identification and ingress sanitization

A de-identification stage at ingress will apply the Safe Harbor method of 45 CFR 164.514(b)(2), removing the eighteen enumerated identifiers from payloads before records are written to secondary indexes used for analytics or support. Clinical codes (RxNorm) would be preserved; direct identifiers would be replaced with keyed tokens.

5.2 Data minimization and retention

Retention limits will bound the lifetime of transient operational records, with scheduled deletion on expiry and automated scrubbing of accidental identifier capture from application logs before they are persisted. Specific retention windows will be published once the deletion pipeline is implemented and tested, rather than asserted in advance.

5.3 Multi-tenant isolation

Tenant separation is intended to be enforced at the database tier through a tenant identifier on every row, combined with query-level restrictions that prevent cross-tenant reads. Per-tenant key separation is a design objective. The company does not today operate customer-managed keys, hardware security modules, or hardware-backed tenant isolation, and the prior revision's description of those mechanisms as operational was incorrect.

5.4 Re-identification resistance

Keyed tokenization of direct identifiers, using a secret held outside the application database, is the intended defense against linkage of platform records to external demographic datasets. This is a design commitment, not a shipped control.

5.5 FHIR R4 export

A conformant FHIR R4 export route is on the roadmap so that customers can retrieve their own data in a standard format. No export route exists in the backend today.

Section 6: Audit trail integrity

The audit log currently carries a `sha384_checksum` column that is populated with constant string labels rather than computed digests. It therefore provides no cryptographic verification of record integrity.

This is a defect, it is known, and repair is in progress. Until the corrected digest computation ships and is verified, Kelshad Cyber Systems and Technologies LLC makes no claim of tamper evidence, immutability, or non-repudiation for the audit trail, in this document or any other. The audit log is useful for operational review. It is not, at present, forensic evidence.

Section 7: Security assessment posture

Threat modeling to date covers cross-tenant data access, identifier leakage into application logs, insider access to stored records, and credential exposure. Mitigations for several of these are target architecture rather than shipped controls, as noted above.

A **third-party penetration test** of the platform has been completed. No SOC 2 examination has been performed or scheduled. Results of any future independent assessment will be summarized in a revision of this document.

Section 8: Social commitment

Kelshad Cyber Systems and Technologies LLC intends to direct a fixed share of platform profits to community initiatives once the platform generates revenue. RxOmniMedLink is in private alpha and produces no revenue today, so this is a stated forward commitment and not a description of current activity. It will be reported on when it becomes operative.

Section 9: Revision statement

This revision withdraws the following claims made in KST-PRIVACY-006-REV2026: that the privacy infrastructure had already been audited; that the platform had achieved full HIPAA compliance or complete safeguard coverage; that hardware-backed multi-tenant isolation, customer-managed keys, FIPS 140-2 Level 3 facilities, and an operating de-identification engine were in production; that audit trails were immutable or non-repudiable; and that the platform is transmitting or routing live prescriptions. It also corrects the legal entity name and removes references to standards belonging to unrelated entities.

The Zero PHI Commercialization Mandate is retained without qualification. It was true then and it is true now.

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

Questions about this document, or requests for the current control status ahead of the next revision, should be directed to info@kelshad.com.