SAPIENT PREDICTIVE ANALYTICS PTE LTD

CARDINEX EXECUTIVE SUMMARY

ZK-Private Cardiology AI on Cardano

By Sapient Predictive Analytics Pte Ltd

---

1. Executive Summary

Modern cardiology AI requires large and diverse datasets—ECG waveforms, PPG signals, cardiac MRI, echocardiography, and demographic markers. Hospitals, however, cannot safely contribute this data to external AI systems without exposing patient identities or breaching privacy laws.

Cardinex solves this through a zero-knowledge privacy layer built on Cardano.

Hospitals keep all raw cardiac data locally inside their infrastructure. Cardinex provides tools that:

1. **encrypt and summarize local cardiac datasets**,
2. **generate zero-knowledge proofs (ZKPs)** that validate consent, authenticity, and structural dataset integrity,
3. **submit only proofs and non-identifying hashes** to Cardano, and
4. allow **Sapient's AI models** to analyze encrypted or pseudonymized cardiac data **without ever receiving patient identities**.

This creates a cryptographically safe path for hospitals to contribute high-value cardiology data while maintaining full control and legal compliance.

Cardinex unlocks a future where medical AI can grow stronger without exposing the people it aims to protect.

---

2. Background: The Data Bottleneck in Cardiology AI

Cardiology AI systems—especially for early arrhythmia detection, MRI segmentation, and hemodynamic prediction—depend on training data collected across diverse populations and imaging devices.

However:

- Hospitals cannot transfer identifiable patient data to third-party AI systems.
- Even anonymization is risky; ECG patterns and MRI contours can be re-identifiable.
- Compliance (HIPAA, PDPA, GDPR) heavily restricts data sharing.
- Many promising AI models fail to reach clinical readiness due to insufficient variety in training datasets.

This creates a **data-access bottleneck**, limiting model accuracy and slowing adoption of clinically useful AI tools.

Cardinex addresses this bottleneck using **zero-knowledge proofs**, enabling hospitals to contribute encrypted cardiac datasets without revealing sensitive information.

3. Clinical Data Flow: Keeping Patients Invisible

The cardinal rule of Cardinex:

Raw patient data stays inside the hospital. Always.

Cardinex's architecture ensures:

- patient identity never touches the blockchain,
- no cardiac waveform, MRI slice, echo volume, or demographic record is transmitted to Sapient,
- all cryptographic proving happens **locally**,
- only encrypted bundles or anonymized feature sets are sent for AI analysis.

4. Trust & Privacy Model

To give both hospitals and regulators confidence, Cardinex follows a strict privacy model.

4.1 Patient Identity Model

Patients are never placed on-chain or revealed to Sapient. The clinic controls identity and consent.

Each patient has:

- a local keypair (or delegated consent via clinic identity),
- a **signed consent document**,
- no blockchain presence.

4.2 Consent Proof Model

Cardano only sees:

- **consent_policy_hash**: a hash of the predefined consent template,
- **ZKP** proving:

> "There exists a valid patient (or clinic) signature over a consent document consistent with this dataset's declared policy."

No signatures, names, or documents are visible on-chain.

4.3 Data Integrity Proof Model

ZK circuits verify that:

- the dataset originates from the clinic,
- the encrypted or committed metadata matches the dataset,
- the consent policy used is valid.

Cardinex does **not** pass judgement on dataset "usefulness";

our only concern is privacy, consent, and structural integrity,

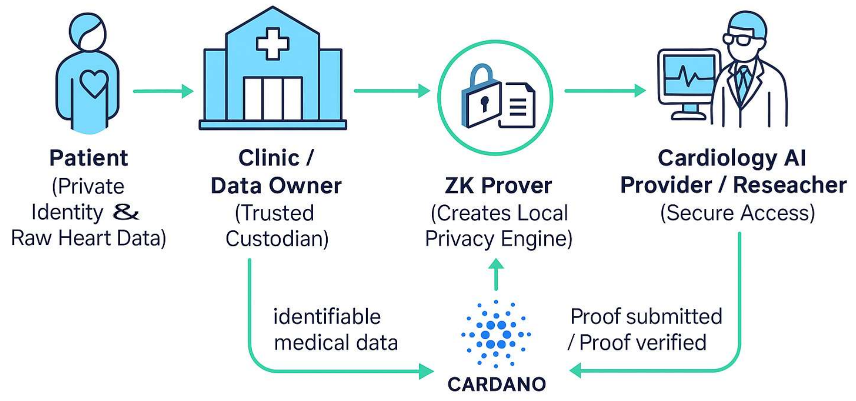
so hospitals can contribute as much data as possible.

5. System Architecture Overview

CARDINEX

Predict. Detect. Protect.

ZERO KNOWLEDGE PROOFS



5.1 Actors

- **Patient:** Provides raw cardiac data; identity stays local.
- **Clinic/Data Owner:** Holds raw data, signs consent, runs Cardinex prover.
- **Cardinex ZK Prover:** Creates proofs from encrypted cardiac data; operates locally.
- **Cardano Blockchain:** Verifies zero-knowledge proofs and logs dataset commitments.
- **AI Provider / Researcher:** Receives encrypted or pseudonymized data for analysis.

5.2 Data Flow

1. **Patient → Clinic**
   Raw ECG/PPG/MRI data collected; consent signed.
2. **Clinic → Local Prover**
   - dataset hashed & encrypted
   - metadata extracted
   - ZKP created
3. **Prover → Cardano**

    - upload ZKP
    - upload dataset and consent hashes
    - Cardano verifies proof without seeing data

4. **Researcher / AI Provider**
    - receives encrypted dataset only after on-chain proof acceptance
    - Sapient’s AI analyzes encrypted or feature-level representations

---

6. Why Cardano?

Cardano’s eUTxO model is ideal for verifiable, deterministic workflows required for medical data auditing.

Cardanex benefits from:

- predictable, deterministic verification
- strong formal foundations
- Aiken smart contracts optimized for predictable execution
- growing ZK tooling within the IOG community
- future synergy with **Midnight**, Cardano’s confidential-computation chain.

Midnight can later handle selective disclosure, private queries, and shielded smart contracts—Cardinex is designed to integrate directly once Midnight matures.

---

7. Zero-Knowledge Proof Design

(Diagram Placeholder: “ZK Consent & Data Integrity Pipeline”)

7.1 Public Inputs

- dataset hash
- metadata hash
- consent policy hash

7.2 Private Inputs

- patient consent signature
- raw dataset

- anonymized metadata
- clinic identity keys

7.3 Proof Guarantees

Cardinex proves:

1. **Consent:**
   The patient (or clinic) signed the correct consent template.
2. **Integrity:**
   The encrypted dataset matches the commitment.
3. **Consistency:**
   The metadata summary was derived from the encrypted dataset.

None of these steps reveal patient identity or cardiac data.

8. AI Integration

Sapient's cardiology AI models—ensemble-based, clinically aligned, and optimized through our financial ML research roots—are designed to analyze:

- encrypted ECG/PPG features,
- MRI-derived volumetrics,
- ECHO structural markers.

Our ensemble methods, inspired by the Condorcet Jury Theorem, allow multiple independent models to vote on predictions, boosting accuracy without requiring access to sensitive raw data.

9. Use Cases

Hospitals

Contribute cardiac datasets securely while maintaining compliance.

Research Institutions

Access diverse data for training models without patient exposure.

AI Companies

Evaluate encrypted clinical datasets and train models under strict privacy guarantees.

Cardano Ecosystem

Gain a flagship real-world ZK application with clear medical value and Midnight synergy.

---

10. Roadmap & Milestones

Milestone 1

Milestone Title: Clinical Data Workflow, Privacy Architecture & Initial ZK Pipeline Specification

Milestone Outputs:

- Open-source repository with Cardinex project overview, dataflow diagrams, and initial privacy architecture.
- Defined clinical workflow for ECG/PPG and imaging modalities (MRI/echo) with structured metadata extraction requirements.
- Zero-knowledge validation framework specification (circuit constraints, public/private inputs, verification boundaries).
- Prototype preprocessing scripts for anonymised metadata extraction.
- Draft Aiken smart-contract interface for dataset registration and verification logic.

Acceptance Criteria:

- Repository contains clear documentation describing how clinical datasets will be processed, committed, and validated.
- ZK pipeline specification outlines core constraints without binding the project to a single proving system.
- Preprocessing scripts successfully generate example metadata commitments using public cardiac datasets.
- Contract interfaces provide enough structure for future implementation and testnet deployment.

Evidence of Completion:

- Public GitHub repository URL with architecture docs, workflow diagrams, and preprocessing code.
- Example metadata commitments and anonymised dataset summaries.
- Short video walkthrough of repository structure and design rationale.

Milestone 2

Milestone Title: ZK Circuit Prototype, Proof-Service Backend & Metadata Validation Logic

Milestone Outputs:

- Prototype ZK circuit implementing core checks: demographic bins, dataset size minima, structural metadata validation.
- Proof-service backend capable of running the circuit, generating proofs, and preparing public inputs.
- Test harness for validating correctness using sample ECG/PPG or MRI datasets.
- Modular design allowing substitution of ZK frameworks (Halo2, Noir/ACIR, Plonky2) without altering external interface.

Acceptance Criteria:

- Circuit prototype generates valid proofs for test datasets with ≥90% success rate.
- Backend exposes proof generation as a reproducible API endpoint.
- Public inputs match the structure defined in Milestone 1.
- Test harness demonstrates proof stability under multiple dataset configurations.

Evidence of Completion:

- Public repository update containing the circuit folder, backend code, and test harness.
- CLI or API demonstration showing proof generation and validation workflow.
- Video demonstration explaining circuit logic and proof-service operation.

Milestone 3

Milestone Title: Aiken Smart Contracts, Testnet Deployment & On-Chain Verification

Milestone Outputs:

- Aiken-based smart contracts for dataset registration, ZK verification, and controlled access logic.
- Integration layer bridging the proof-service outputs with testnet submission scripts.
- PreProd testnet deployment of the dataset registry contract.
- Reference transaction set demonstrating dataset submission, proof verification, and state continuity.

Acceptance Criteria:

- Contract compiles successfully and verifies submitted proofs on testnet with ≥90% acceptance stability.
- End-to-end transaction flow shows registration UTxO creation, proof validation, and consistent on-chain metadata.
- Documentation explains how developers can reproduce the testnet process locally.

Evidence of Completion:

- Public PreProd deployment addresses and example transaction URLs.
- Updated GitHub documentation covering contract usage and verification logic.
- Video demonstration of testnet validation transactions and contract walkthrough.

Milestone 4

Milestone Title: Frontend Integration, Encrypted Access Workflow & AI Benchmarking

Milestone Outputs:

- Minimal frontend enabling dataset submission, proof generation requests, and browsing of verified dataset summaries.

- Encrypted access workflow triggered by successful testnet purchase transaction.
- Benchmark evaluation of Sapient’s cardiology AI on anonymised datasets, demonstrating expected ensemble uplift.
- Public API endpoints enabling external developers to interact with the prototype.

Acceptance Criteria:

- Frontend can submit at least five datasets end-to-end into the testnet pipeline.
- Access workflow securely delivers encrypted bundles or keys following on-chain purchase events.
- AI benchmark demonstrates ≥5% improvement via ensemble comparison on anonymised test datasets.
- API documentation is clear, versioned, and reproducible.

Evidence of Completion:

- Public demo environment URL and GitHub frontend repository.
- Benchmark charts, summary metrics, and anonymised example outputs.
- Video showing full user flow from dataset submission to encrypted access and AI analysis.

Milestone 5 — Final Milestone

Milestone Title: Public Launch, Documentation Finalisation & Close-out Deliverables

Milestone Outputs:

- Public prototype launch on Cardano testnet, including updated contracts, frontend, and proof-service.
- Final technical documentation: architecture, ZK pipeline, API reference, and reproducibility guide.
- Public Project Close-out Report.
- Public Close-out Video.
- Outreach package for developers: integration guides and contract examples.

Acceptance Criteria:

- Prototype accessible publicly with stable testnet endpoints and clear usage instructions.
- Documentation provides enough detail for external developers to fork and extend the system.
- Close-out Report summarises achievements, metrics, risks, and future roadmap.
- Close-out Video presents functionality, lessons learned, and next steps.

Evidence of Completion:

- Public GitHub release tagged as v1.0-testnet.
- Published Close-out Report (PDF or markdown) and Close-out Video link.
- Public announcement post summarising the Cardinex prototype launch.

11. Licensing & Open Source

All core components will be released under the **MIT License**, ensuring:

- maximum developer reusability,
- zero vendor lock-in,
- compatibility with commercial deployment.

12. Conclusion

Cardinex provides a cryptographically secure pathway for hospitals to contribute cardiology data without exposing patient identities. By verifying consent and integrity through zero-knowledge proofs on Cardano, it unlocks a medically crucial dataset flow that was previously impossible to achieve safely.

Cardinex strengthens Cardano’s position in privacy, healthcare, AI, and regulated industries—and brings the ecosystem one step closer to real-world life-saving impact.