Cardinex: Privacy-Preserving Medical Data Marketplace Using Zero-Knowledge Proofs on Cardano

A Lightpaper

A Lightpaper

Authors: Sapient Predictive Analytics Pte Ltd

Date: November 2025

Version: 0.1.0

Status: Pre-Alpha Technical Proposal

Abstract

This lightpaper presents a novel architecture for a privacy-preserving medical data marketplace built on the Cardano blockchain, utilizing zero-knowledge proof technology to enable secure, compliant sharing of electrocardiogram (ECG) data for machine learning applications. The Cardinex system allows healthcare institutions to monetize anonymized patient data while maintaining strict privacy guarantees through cryptographic proofs, ensuring that patient identities and sensitive information remain protected throughout the data lifecycle. Our approach leverages the recently deployed Halo2-Plutus verifier on Cardano mainnet, combined with Aiken smart contracts, to create a marketplace where data properties can be verified without exposing underlying patient records. The initial deployment targets hospitals in Singapore, Japan, Korea, and various centers at the state university level in the United States, with a pilot program designed to train internal machine learning models for cardiac anomaly detection while demonstrating the system's privacy guarantees to our own engineering teams.

1. Introduction

1.1 Problem Statement

The development of accurate medical artificial intelligence systems requires access to large, diverse datasets of patient records. However, the sensitive nature of medical data creates fundamental tensions between three competing requirements:

First, patients have a fundamental right to privacy, codified in regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. These frameworks restrict the collection, storage, and sharing of Protected Health Information (PHI).

Second, medical researchers and artificial intelligence developers require access to substantial quantities of labeled medical data to train accurate predictive models. Current approaches to obtaining such data involve lengthy institutional review board approvals, complex data use agreements, and significant financial overhead.

Third, healthcare institutions possess valuable data assets that could generate revenue to offset the costs of patient care, but lack mechanisms to monetize these assets without violating patient privacy or regulatory requirements.

Traditional approaches to this problem have relied on de-identification techniques, where identifying information is removed from datasets. However, numerous studies have demonstrated that supposedly anonymized medical records can often be re-identified through linkage attacks, particularly when combined with auxiliary information sources.

1.2 Proposed Solution

We propose a cryptographic approach to this challenge using zero-knowledge proofs (ZKPs), which enable one party to prove statements about private data without revealing the underlying information. Specifically, the Cardinex system allows healthcare providers to prove that a patient's ECG data exhibits certain medically relevant characteristics (such as arrhythmia or tachycardia) and satisfies specific demographic criteria (such as age range and comorbidities) without disclosing the patient's identity, exact measurements, or raw ECG signals.

The Cardinex platform is implemented on the Cardano blockchain, leveraging its Extended Unspent Transaction Output (EUTXO) model and recently deployed zero-knowledge proof verification capabilities. Smart contracts written in Aiken, a modern functional programming language for Cardano, orchestrate the marketplace logic, while Halo2 cryptographic circuits generate and verify the zero-knowledge proofs off-chain and on-chain respectively.

1.3 Deployment Context

The initial Cardinex deployment targets a specific use case that demonstrates both the technical feasibility and privacy guarantees of the system: internal machine learning model training. Our organization operates partnerships with cardiac care facilities in the following regions:

• **East Asia**: Hospital networks in Singapore, Japan, and South Korea

• **United States**: Various centers at the state university level

For the pilot program, we serve as both data provider and data consumer. Hospital partners provide encrypted ECG data with zero-knowledge proofs, which our machine learning engineering teams then purchase through the Cardinex marketplace without gaining access to patient identities or the ability to link records back to specific healthcare facilities. This arrangement allows us to demonstrate the privacy properties of the system to our own technical teams, who can verify that they receive useful training data without compromising patient privacy.

2. Architecture Overview

2.1 System Components

The Cardinex system comprises three primary architectural layers:

Layer 1: Data Generation and Proof Creation (Off-Chain) Healthcare facilities collect ECG data through standard monitoring equipment. The raw signals, along with relevant patient metadata, are processed through a local proof generation system that creates zero-knowledge proofs attesting to specific medical and demographic properties without exposing the underlying data.

Layer 2: On-Chain Verification and Marketplace (Cardano Blockchain) Proof commitments are submitted to smart contracts deployed on the Cardano mainnet. The Halo2-Plutus verifier validates the cryptographic correctness of submitted proofs, while Aiken smart contracts manage the marketplace logic, including dataset listing, purchase transactions, and access token issuance.

Layer 3: Data Access and Decryption (Off-Chain) After successful purchase verification on-chain, authorized machine learning researchers receive decryption keys that grant access to encrypted ECG data stored on decentralized storage systems. The data remains anonymized, with all identifying

information removed and demographic information binned into ranges.

2.2 Information Flow

The complete data flow through the Cardinex system proceeds as follows:

```
[Healthcare Facility] | | 1. ECG data collection | 2. Patient consent | 3. Local
anonymization | v [Cardinex Proof Generator] | | 4. Analyze ECG signals | 5. Bin
demographic data | 6. Generate ZK proof | 7. Encrypt data | v [Cardano Blockchain] | | 8.
Verify proof via Halo2 | 9. Store commitment in UTxO | 10. List in Cardinex marketplace | v
[ML Research Team] | | 11. Query available datasets | 12. Purchase access | 13. Receive
decryption key | v [Training Pipeline] | | 14. Download encrypted data | 15. Decrypt with
key | 16. Train ML models
```

This architecture ensures that at no point does the machine learning team gain access to patient identities, exact demographic information, or data that can be linked back to specific healthcare facilities.

3. Privacy Model

3.1 Data Classification

The Cardinex system distinguishes between three categories of information:

Private Witness Data (Never Revealed)

• Patient identifiers (names, medical record numbers, national identification numbers)

• Exact age, date of birth, or precise geographic location

• Raw ECG signal data (voltage measurements over time)

• Healthcare facility identifiers

• Treating physician information

• Timestamps that could enable temporal correlation attacks

Binned Metadata (Selectively Disclosed)

• Gender categories: Male, Female, Other

• Age ranges: 0-20, 20-40, 40-60, 60-80, 80+ years

• Geographic regions: Singapore, Japan, Korea, United States (state university centers)

• Medical condition flags (boolean): has_diabetes, has_hypertension, has_heart_disease, has_obesity, smoking_status

Verified Properties (Public Inputs)

• ECG analysis results: has_arrhythmia, has_tachycardia, has_bradycardia, has_abnormal_qrs

• Signal quality score: 0-100 rating

• Data availability commitment: cryptographic hash of encrypted dataset

3.2 Customizable Medical Tags

Recognizing that medical expertise varies and different research projects require different levels of granularity, the Cardinex platform supports a two-tier tagging architecture:

Tier 1: Standard Flags (Boolean) High-level medical conditions that can be represented as binary present/absent indicators:

• Cardiovascular: has_hypertension, has_arrhythmia, has_tachycardia, has_bradycardia, has_atrial_fibrillation

• Metabolic: has_diabetes, has_obesity, has_hyperlipidemia

• Lifestyle: smoking_status, alcohol_consumption

• PLACEHOLDER: Additional standard flags to be defined with medical advisory board

Tier 2: Custom Parameters (Extensible) Domain experts such as cardiologists may require more specific categorizations:

• Arrhythmia subtypes: specific classification of irregular rhythms

• QRS complex morphology: detailed waveform characteristics

• Medication status: current cardiovascular medications

• Ejection fraction ranges: for patients with concurrent imaging data

• PLACEHOLDER: Mechanism for healthcare providers to define custom parameters through governance process

The zero-knowledge proof circuits in Cardinex are designed to accommodate these custom parameters without requiring changes to the core smart contract logic, enabling domain specialists to enhance data richness while maintaining privacy guarantees.

3.3 Proof Construction

The zero-knowledge proof in Cardinex cryptographically establishes the following statement:

"There exists a triple (ECG_data, Patient_ID, Encryption_key) such that: 1. The claimed ECG analysis results (arrhythmia detection, quality score, etc.) are correctly computed from ECG_data using validated algorithms 2. The binned demographic information (age range, region, condition flags) correctly corresponds to Patient_ID when appropriately bucketed 3. The on-chain data commitment equals Hash(ECG_data || Encryption_key) 4. All custom medical parameters, if present, are correctly derived from Patient_ID and ECG_data

WITHOUT revealing the values of (ECG_data, Patient_ID, Encryption_key) or any information that would allow reconstruction of these private values."

This construction ensures that machine learning researchers can verify they are purchasing data meeting their requirements without gaining any information that could compromise patient privacy.

4. Technical Implementation

4.1 Zero-Knowledge Proof System

The Cardinex platform employs Halo2, a zero-knowledge proof system based on the PLONK proving framework, chosen for several technical advantages:

Transparent Setup: Unlike earlier systems such as Groth16, Halo2 requires no trusted setup ceremony, eliminating a potential security vulnerability and simplifying deployment.

Recursive Composition: Halo2 supports proof recursion, enabling future optimization where multiple dataset proofs could be aggregated into a single verification, reducing on-chain costs.

Performance: Proof generation completes in approximately 2-5 seconds on standard hardware, making the system practical for high-throughput healthcare environments.

Cardano Integration: Input Output Research deployed a Halo2 proof verifier to Cardano mainnet in November 2024, providing native blockchain support for proof verification.

The proof circuits are implemented in Rust using the halo2_proofs library, with circuit definitions organized into three primary constraint groups:

1. ECG Analysis Constraints: Verify that claimed medical properties (arrhythmia detection, quality metrics) follow from the input signals through validated algorithms 2. Demographic Binning Constraints: Ensure that reported age ranges, geographic regions, and medical flags correctly correspond to the bucketed private data 3. Commitment Constraints: Establish that the on-chain data commitment is computed correctly from the private inputs

4.2 Smart Contract Architecture

The on-chain component of Cardinex consists of Aiken validators deployed to the Cardano blockchain. Aiken was selected over the traditional Plutus framework due to its more accessible syntax (inspired by Rust and Elm), shorter learning curve, and modern development tooling.

The primary validator implements a state machine with three states:

Available: Dataset listing is active and can be purchased **Sold**: Dataset has been purchased and access token issued **Withdrawn**: Provider has withdrawn payment after sale

State transitions are governed by redeemers that encode marketplace actions:

• SubmitProof: Healthcare provider submits new dataset with proof

• PurchaseAccess: Researcher purchases dataset

• WithdrawPayment: Provider withdraws funds after sale

• UpdatePrice: Provider modifies dataset price

Each state transition invokes the Halo2-Plutus verifier to validate cryptographic correctness before accepting the transition. The integration between Aiken and the Halo2 verifier follows a reference input pattern, where the verifier's output serves as a trusted oracle for proof validity.

4.3 Data Storage and Access Control

Encrypted ECG data resides in decentralized storage systems, with only cryptographic references (content identifiers) stored on-chain. Upon successful purchase through the Cardinex marketplace, the smart contract issues an access token containing:

• Commitment reference: Links to the specific dataset

• Researcher credential: Identifies the authorized purchaser

• Encrypted decryption key: Decryption key encrypted with researcher's public key

• Timestamp: Records purchase time for audit trails

The decryption key structure ensures that only the authorized purchaser can decrypt the data, and the on-chain record provides an immutable audit trail of all access grants.

5. Use Case: Internal Machine Learning Model Training

5.1 Operational Context

For the initial Cardinex deployment, our organization functions simultaneously as marketplace operator, data aggregator, and data consumer. This arrangement serves multiple strategic purposes:

First, it enables us to validate the privacy properties of the system before external deployment. Our machine learning engineers operate under the constraint that they cannot access patient identities, providing an internal proof-of-concept for the privacy guarantees.

Second, it establishes operational procedures and best practices for healthcare partner integration, data quality assurance, and marketplace operations that can be documented for future external participants.

Third, it produces trained machine learning models for cardiac anomaly detection while demonstrating regulatory compliance, as the training pipeline never exposes Protected Health Information to the model development team.

5.2 Workflow for Pilot Program

The complete workflow for the Cardinex pilot program proceeds as follows:

Stage 1: Data Collection at Healthcare Facilities

Hospital partners in Singapore, Japan, Korea, and various centers at the state university level in the United States collect ECG data through standard monitoring equipment. Patients provide informed consent for anonymized data sharing, with consent management handled at the facility level according to local regulations. The raw ECG signals and associated medical records remain entirely within the healthcare facility's infrastructure.

Stage 2: Local Proof Generation

Each facility operates a Cardinex proof generation node that: 1. Extracts relevant medical properties from ECG signals through validated analysis algorithms 2. Bins patient demographic and clinical data into predefined ranges 3. Generates Halo2 zero-knowledge proofs attesting to these properties 4. Encrypts the raw ECG data with facility-specific keys 5. Uploads encrypted data to decentralized storage (IPFS or equivalent) 6. Submits proof commitments to the Cardano blockchain

At this stage, the proof generation system has access to private data, but this system remains under the healthcare facility's control and does not transmit private information externally.

Stage 3: Marketplace Listing

The Cardinex smart contract receives the proof commitment and invokes the Halo2-Plutus verifier. Upon successful verification, the commitment is recorded in a UTxO (Unspent Transaction Output) on the Cardano blockchain, making it queryable by potential purchasers. The listing includes:

• Verified medical properties (arrhythmia type, quality score, etc.)

• Binned demographics (region, age range, condition flags)

• Price in ADA (Cardano's native cryptocurrency)

• Geographic region tag: Singapore, Japan, Korea, or United States

Critically, the listing does not include any information that could identify the specific healthcare facility or individual patient.

Stage 4: Dataset Query and Purchase

Our machine learning team operates as a customer of the Cardinex marketplace. Using a client application, they specify search criteria such as:

• "ECG datasets with confirmed arrhythmia"

• "From patients aged 40-60 with diabetes"

• "Minimum signal quality score of 80"

• "From any East Asian facility or United States facility"

The query returns matching datasets without revealing which specific facility provided each dataset. This ensures that our ML engineers cannot infer patterns based on facility characteristics or correlate datasets from the same institution.

The purchase transaction transfers ADA payment to the healthcare facility's address and triggers access token issuance through the Cardinex smart contract.

Stage 5: Data Decryption and Model Training

Upon successful purchase, the ML team receives:

• Decryption keys for the specific datasets

• Download links to encrypted data on decentralized storage

• On-chain receipts proving authorized access

The team downloads the encrypted ECG signals, decrypts them locally, and incorporates them into training pipelines for cardiac anomaly detection models. Throughout this process, the team works only with:

• ECG signal data (voltage measurements over time)

• Known medical labels (has_arrhythmia, etc.)

• Binned demographic information (age range, region, flags)

They cannot determine which facility provided each dataset, which patient the data corresponds to, or any identifying information beyond the binned categories.

Stage 6: Validation and Audit

The on-chain transaction history in Cardinex provides a complete audit trail showing:

• When each dataset was submitted (block height and timestamp)

• Which proofs were verified successfully

• Which datasets were purchased by our ML team

• Payment flows to healthcare facilities

This transparency enables regulatory compliance verification and internal auditing while maintaining patient privacy through the zero-knowledge proof construction.

5.3 Privacy Demonstration

This pilot program provides a concrete demonstration of the Cardinex system's privacy guarantees. Our ML engineers—technically sophisticated individuals with strong incentives to extract maximum information from available data—operate under the constraint that they cannot:

1. Identify individual patients 2. Determine which facility provided specific datasets 3. Correlate multiple datasets from the same patient (each dataset receives a unique anonymous identifier in Cardinex) 4. Reconstruct exact demographics from binned information 5. Link ECG data to external databases through auxiliary information

If the Cardinex system successfully prevents our own engineering team from compromising privacy despite their technical capabilities and data access, it provides strong evidence for the viability of external deployment where data consumers have less sophisticated capabilities and fewer resources.

6. Deployment Roadmap

6.1 Phase 1: Integration and Testing (Weeks 1-4)

The initial phase focuses on completing technical integration of the Cardinex platform:

Week 1-2: Halo2-Plutus Verifier Integration Implement the connection between Aiken smart contracts and the deployed Halo2-Plutus verifier on Cardano mainnet. This involves defining the reference input pattern, encoding public inputs in the format expected by the verifier, and handling verification results.

Week 3-4: Testnet Deployment Deploy the complete Cardinex system to Cardano's preprod testnet environment. Conduct integration testing with simulated ECG data and validate all state transitions, proof verifications, and payment flows.

6.2 Phase 2: Pilot Program (Weeks 5-12)

Week 5-6: Healthcare Partner Onboarding Establish technical infrastructure at partner facilities in target regions. Install Cardinex proof generation nodes, configure encryption systems, and train facility staff on system operation.

Week 7-8: Initial Data Submission Begin collecting and submitting anonymized ECG datasets through Cardinex. Target initial corpus of 1,000-2,000 datasets across all partner facilities to ensure diversity.

Week 9-12: ML Model Training Machine learning team queries the Cardinex marketplace, purchases datasets meeting research criteria, and initiates training for cardiac anomaly detection models. Concurrent documentation of privacy preservation throughout the process.

6.3 Phase 3: Validation and Audit (Weeks 13-16)

Week 13-14: Privacy Audit External security firm conducts penetration testing focused on privacy preservation in the Cardinex system. Attempts to re-identify patients or link datasets to facilities using all available information.

Week 15: Regulatory Review Legal team reviews Cardinex system compliance with HIPAA, GDPR, and local healthcare data regulations in Singapore, Japan, and Korea.

Week 16: Documentation and Reporting Compile results from pilot program, including ML model performance, privacy audit findings, and regulatory assessment. Prepare materials for potential expansion of Cardinex to external data consumers.

6.4 Phase 4: External Expansion (Future)

Subject to successful completion of pilot program:

• Expand Cardinex to additional healthcare facilities in existing regions

• Enable external ML research teams to participate as data consumers

• Implement governance mechanisms for custom medical tag definitions

• Integrate with Midnight Network (Cardano's privacy-focused sidechain) when available in 2026

• Explore cross-chain bridges for broader ecosystem integration

7. Economic Model

7.1 Pricing and Incentives

Healthcare facilities set prices for individual datasets in the Cardinex marketplace denominated in ADA. Suggested initial pricing:

• Standard ECG dataset: 5-10 ADA (approximately $2-10 USD at current exchange rates)

• High-quality datasets (quality score > 90): 10-15 ADA

• Rare conditions or specific demographic combinations: 15-25 ADA

• PLACEHOLDER: Dynamic pricing based on supply and demand metrics

The Cardinex marketplace operator (our organization during the pilot) collects a small transaction fee (0.5-1%) to cover infrastructure costs and smart contract execution fees.

7.2 Cost Structure

On-Chain Costs:

• Proof verification: Approximately 1-2 ADA per dataset submission

• Marketplace operations: Standard Cardano transaction fees (0.17 ADA + size-based fees)

• Smart contract execution: Included in transaction fees

Off-Chain Costs:

• Proof generation: Computational resources at healthcare facilities (amortized cost ~$0.50 per dataset)

• Encrypted storage: Decentralized storage fees (~$0.01 per GB per month)

• Client infrastructure: Standard web hosting and bandwidth

7.3 Revenue Projections

PLACEHOLDER: Detailed financial projections pending pilot program results. Initial estimates suggest:

• 10,000 datasets per year across Cardinex partner facilities

• Average price of 8 ADA per dataset

• Total marketplace volume: 80,000 ADA annually

• Healthcare facility revenue: ~70,000 ADA after fees

• Platform revenue: ~800 ADA from transaction fees

8. Regulatory Considerations

8.1 HIPAA Compliance (United States)

The Cardinex system architecture aligns with HIPAA requirements by ensuring that Protected Health Information (PHI) never resides on-chain. Only cryptographic commitments and binned demographic information are recorded on the blockchain, neither of which constitutes PHI under HIPAA definitions.

The system satisfies HIPAA's de-identification requirements through the Safe Harbor method, as all of the following are removed or binned:

• Names and identifiers

• Dates (except year)

• Geographic subdivisions smaller than state level

• All elements that could identify individuals

8.2 GDPR Compliance (European Union and Singapore)

GDPR's primary principles of data minimization, purpose limitation, and the right to erasure are addressed in the Cardinex architecture as follows:

Data Minimization: Only the minimum necessary information for ML training purposes is collected and shared.

Purpose Limitation: Datasets are explicitly tagged for cardiac anomaly research purposes.

Right to Erasure: Raw encrypted data resides off-chain and can be deleted upon patient request. On-chain commitments (cryptographic hashes) do not constitute personal data under GDPR Article 4.

8.3 Regional Considerations

Singapore: Personal Data Protection Act (PDPA) compliance through anonymization and consent management at healthcare facilities.

Japan: Act on the Protection of Personal Information (APPI) compliance, with particular attention to provisions regarding medical data handling.

Korea: Personal Information Protection Act (PIPA) compliance, including specific healthcare data provisions.

PLACEHOLDER: Detailed jurisdiction-specific compliance documentation to be completed during Phase 3.

9. Technical Specifications Summary

9.1 System Requirements

Healthcare Facility Infrastructure:

• Cardinex proof generation node: 8-core CPU, 16GB RAM, 500GB storage

• Network connectivity: Minimum 10 Mbps upload bandwidth

• Operating system: Linux (Ubuntu 24.04 LTS recommended) or containerized deployment

Blockchain Requirements:

• Cardano node access: Full node or API provider (Blockfrost recommended for pilot)

• Wallet infrastructure: Support for payment key management and transaction signing

• Minimum ADA balance: 10 ADA per facility for transaction fees and minimum UTxO requirements

Machine Learning Team Requirements:

• Cardano wallet with ADA for purchases on Cardinex

• Decentralized storage client (IPFS or equivalent)

• Standard ML infrastructure (Python, PyTorch/TensorFlow, GPU resources for training)

9.2 Performance Characteristics

Throughput:

• Proof generation: 2-5 seconds per dataset

• On-chain verification: 5-10 seconds per transaction (Cardano block time)

• Dataset query: <1 second (indexed blockchain data)

• Maximum sustained throughput: ~200-300 dataset submissions per hour per facility

Scalability:

• Current Cardinex architecture supports 10-20 participating facilities

• Future Layer 2 integration (Hydra) could increase throughput by 100x

• Midnight Network integration (2026) may reduce verification costs by 50-80%

Storage:

• On-chain: ~2 KB per dataset commitment

• Off-chain: Variable based on ECG duration (typical: 5-50 MB per dataset)

10. Conclusion

This lightpaper presents a technically feasible architecture for privacy-preserving medical data marketplaces that addresses the fundamental tension between data utility and patient privacy. By leveraging zero-knowledge proofs, blockchain infrastructure, and modern cryptographic techniques, the Cardinex system enables valuable medical research while maintaining strict privacy guarantees.

The pilot program design—wherein our organization serves as both data aggregator and consumer—provides a concrete demonstration of the Cardinex system's privacy properties. If our own machine learning engineers cannot compromise patient privacy despite their technical sophistication and data access, the system demonstrates robustness suitable for broader deployment.

Key innovations in Cardinex include:

1. **Cryptographic Privacy**: Zero-knowledge proofs provide mathematical guarantees rather than relying on trust or procedural controls 2. **Verifiable Properties**: Researchers can verify data characteristics before purchase without accessing the underlying information 3. **Economic Incentives**: Healthcare facilities gain revenue streams from data assets while maintaining patient privacy 4. **Regulatory Alignment**: Architecture designed for HIPAA, GDPR, and regional compliance from inception 5. **Extensible Framework**: Custom medical tags and parameters enable domain expert input without compromising privacy

The 16-week deployment roadmap provides a practical path from current prototype to production system, with clear milestones for validation and regulatory compliance. Success in the pilot program would establish both technical feasibility and regulatory viability, positioning the Cardinex platform for broader adoption across healthcare institutions and research organizations.

Future work will focus on integration with emerging Cardano ecosystem technologies, particularly the Midnight Network privacy sidechain, which may significantly reduce verification costs and enhance privacy guarantees when it becomes available in 2026. Additionally, exploration of Layer 2 scaling solutions such as Hydra could increase throughput for high-volume healthcare environments.

The convergence of blockchain technology, zero-knowledge cryptography, and healthcare data infrastructure presents an opportunity to fundamentally reimagine how medical data flows through research ecosystems. This lightpaper demonstrates that the Cardinex system is not merely a theoretical possibility, but a technically feasible solution ready for real-world deployment.

References

PLACEHOLDER: Full bibliography to include:

• Halo2 technical specification (Electric Coin Company)

• Cardano protocol documentation (IOG)

• Aiken language reference

• HIPAA and GDPR regulatory texts

• Medical privacy literature

• Zero-knowledge proof foundations

Appendix A: Glossary

ADA: The native cryptocurrency of the Cardano blockchain **Aiken**: A modern programming language for Cardano smart contracts **Cardinex**: Privacy-preserving medical data marketplace system described in this lightpaper **EUTXO**: Extended Unspent Transaction Output model used by Cardano **Halo2**: A zero-knowledge proof system without trusted setup **HIPAA**: Health Insurance Portability and Accountability Act **GDPR**: General Data Protection Regulation **PHI**: Protected Health Information **UTxO**: Unspent Transaction Output **ZKP**: Zero-Knowledge Proof

Appendix B: Contact Information

Sapient Predictive Analytics Pte Ltd

PLACEHOLDER: Contact details for:

• Technical inquiries

• Partnership opportunities

• Regulatory questions

• Press relations

END OF LIGHTPAPER

This document represents a technical proposal and feasibility analysis. Implementation details are subject to change based on pilot program results, regulatory guidance, and technological developments in the Cardano ecosystem.