RegenMed

WHITE PAPER

THE CIRCLES PLATFORM

A CLOSED-SYSTEM ARCHITECTURE FOR SOVEREIGN HEALTHCARE DATA

August 3, 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Systemic Failure of Legacy Architectures

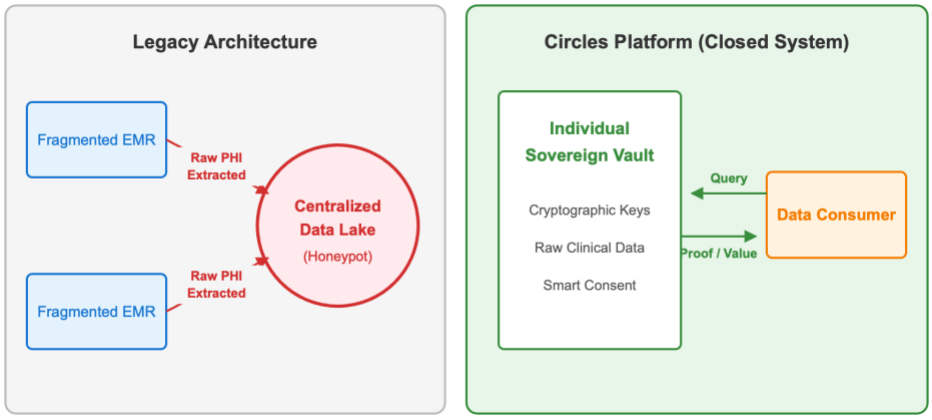
The contemporary healthcare data economy operates on centralized aggregation and third-party brokerage. This legacy architecture relies on enterprise data lakes and extraction methods that structurally separate clinical data from its individual creators – the patient and/or clinician. Intermediaries compile, de-identify, and commercialize health information without returning equitable economic value to the data originators. Beyond the economic misalignment, this model exposes healthcare institutions to cybersecurity vulnerabilities and compounding regulatory liabilities.

The Closed-System Paradigm

Establishing true data sovereignty by attempting to reform fragmented, legacy EMR platforms is an intractable objective. Institutional EMRs are designed for administrative custody, not individual ownership. The Circles Platform bypasses this limitation by operating as a closed, independent architecture. The platform does not attempt to extract or control data residing in legacy hospital systems. Instead, it provides a distinct, secure environment where individuals directly enter, manage, and govern their clinical records under a new operational framework.

The Core Thesis

When an individual enters a medical record into the Circles Platform, it becomes an unambiguously owned asset. The record is cryptographically secured and structurally isolated from competing institutional claims. Through the integration of deterministic lineage metadata, the data is perpetually tracked across all states of use. Unlike legacy models where de-identification severs the patient's legal connection to their data, the Circles Platform ensures the chain of ownership persists regardless of anonymization or aggregation. Because ownership remains clear and uncontested within this closed system, the data can be frictionlessly licensed and exchanged for economic value through automated smart contracts.



Strategic Alignment

This architecture resolves the primary market deficits for both data producers and data consumers. For life science researchers, payers, and artificial intelligence developers, the platform delivers a clean supply chain of high-fidelity, fully consented clinical evidence. For the individual, it establishes absolute economic sovereignty, ensuring that the value generated by authorized evidence uses is automatically and transparently attributed to the data creator.

THE CLOSED SANCTUARY AND CRYPTOGRAPHIC SECURITY

Abandoning Perimeter Security

Traditional network architectures rely on perimeter-based security models. These models assume internal actors and connected systems are trustworthy once inside the firewall, creating centralized "honeypots" highly vulnerable to threat actors and systemic breaches. The Circles Platform replaces this paradigm with a strict Zero-Trust Architecture aligned with NIST SP 800-207 principles. The operational mandate shifts to continuous cryptographic mutual authentication for every interaction, eliminating implicit network trust zones.

Individual Cryptographic Sovereignty

Within this closed system, legacy institutional custodianship ceases. The individual becomes

the absolute sovereign over their data vault. Access is governed not by centralized administrative permissions, but by cryptographic keys controlled exclusively by the individual. This architectural boundary ensures that no external entity—hospital, EMR vendor, or platform operator—can unilaterally access, modify, or extract the record without explicit, mathematically verified authorization.

Self-Sovereign Health Identity (SSI)

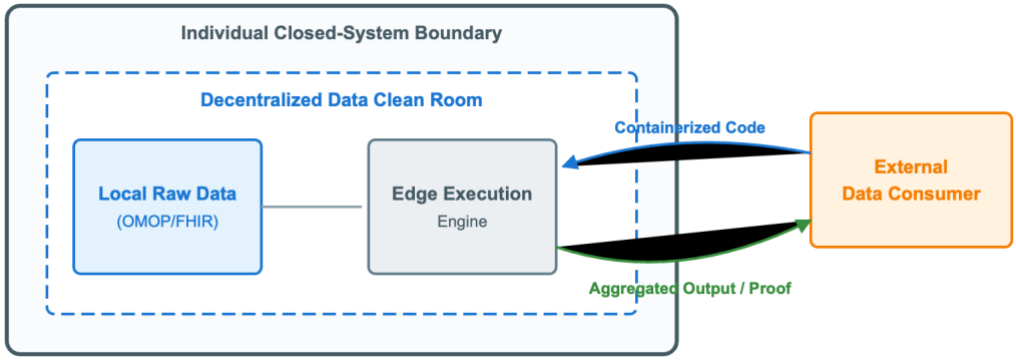
Legacy healthcare identity management relies on centralized enterprise master patient index (MPI) systems and third-party identity providers, introducing single points of failure and tracking vulnerabilities. The platform decouples authentication from corporate directories through a self-sovereign health identity (SSI) framework.

By utilizing World Wide Web Consortium (W3C) Decentralized Identifiers (DIDs) and verifiable credentials (VCs), identity verification occurs peer-to-peer via cryptographic challenge-response protocols. This structure prevents centralized authorities or intermediaries from tracking, correlating, or arbitrarily revoking an individual's network access.

Decentralized Data Clean Rooms

Commercial analytical environments typically require the extraction and pooling of records into centralized repositories, violating data sovereignty and recreating honeypot vulnerabilities. The platform eliminates the risk of unauthorized extraction by deploying decentralized data clean rooms (DCRs).

Rather than moving data to the computation, authorized analytical scripts and queries are containerized, cryptographically signed, and transmitted directly to the data source. Computations execute securely at the network edge against the individual's local data store. Only aggregated, non-re-identifiable mathematical summaries or verified Boolean outputs cross the network boundary, ensuring the raw longitudinal record is never exposed to external actors.



CLOSING THE DE-IDENTIFICATION LOOPHOLE

The Illusion of HIPAA Ownership

The HIPAA Privacy Rule establishes a patient's right to access their medical information, but it does not confer a legal property right. Under current regulatory frameworks, third parties are permitted to strip specified identifiers from a patient's record, claim commercial ownership of the resulting "de-identified" derivative dataset, and monetize it without returning economic value to the data creator.

Unambiguous Custody

Because the Circles Platform operates as an independent, closed system, it avoids the conflicting institutional claims inherent to legacy EMR environments. When an individual enters clinical data into the platform, ownership is established unambiguously at the point of genesis. The architecture structurally recognizes the individual as the sole legal and operational custodian of the asset, removing the legal ambiguities associated with co-created hospital records.

The Immutable Chain of Provenance

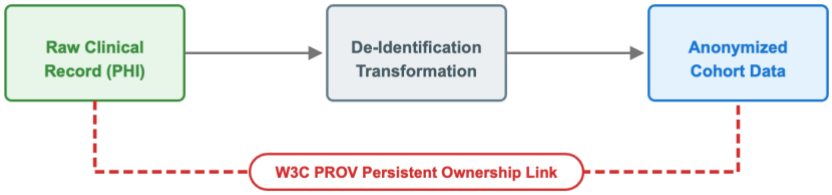
Ownership is enforced through technical architecture rather than administrative policy. The platform utilizes the W3C PROV data model to embed deterministic lineage metadata into every record. This establishes a cryptographically signed, reproducible audit trail documenting the exact origin, transformation, and access history of the data element

without exposing the underlying clinical facts.

Persistent Tracking Beyond Anonymization

In legacy data brokerage models, de-identification severs the legal and operational link between a patient and their medical history. Within the closed architecture of the Circles Platform, anonymization or aggregation does not sever this cryptographic link. Ownership and the right to economic attribution persist through all downstream transformations.

If a consumer derives commercial value from a de-identified cohort, the smart contract routes the corresponding value back to the specific individuals whose data comprised that cohort.



Granular Smart Consent and the Kill Switch

The platform replaces broad, static consent forms with machine-readable smart consent objects bound directly to the transactional metadata. These objects enforce strict boundaries, including explicit purpose limitations and temporal expiration timers. The individual retains dynamic agency, including an enforceable "cryptographic kill switch".

Activating this mechanism instantly invalidates access keys across the distributed registry, purges decrypted local views from active memory, and structurally blocks the network perimeter, guaranteeing absolute compliance with data withdrawal mandates.

FRICTIONLESS VALUE REALIZATION

The Individual as an Economic Actor

The architecture transitions the individual from a passive subject of data extraction into an active economic participant. By establishing a closed system where ownership is absolute and mathematically verifiable, the platform creates the foundation for a liquid healthcare data economy. Individuals receive direct, opt-in compensation for the clinical intelligence they generate and choose to share.

Circle Health Coins as Entitlement Units

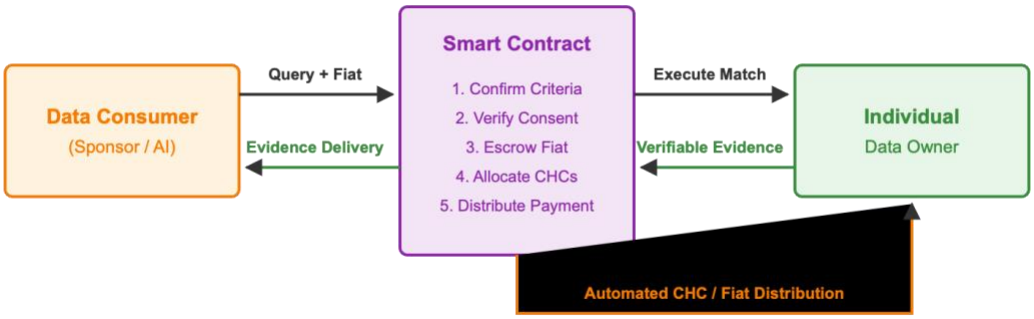
Within this ecosystem, Circle Health Coins (CHCs) function as a digital accounting and allocation mechanism. They do not act as conventional currency. Instead, they measure the individual's validated data contributions and dictate the precise allocation of economic participation rights when commercial transactions occur. This design distinctly separates the structural creation and validation of the data asset from the eventual realization of its market value.

Smart Contract Execution

Because data ownership is uncontested within the closed platform, commercial transactions execute without the friction of multi-party institutional negotiations. Smart contracts automate the transactional workflow. When a data consumer queries the network for a defined cohort, the smart contract automatically confirms participation conditions, verifies the current state of patient consent, enforces execution thresholds, and initiates the payment process.

Automated Settlement Without Intermediaries

The settlement architecture bypasses traditional data brokers and intermediary aggregators. The smart contract calculates revenue allocations based on predefined contribution parameters and distributes fiat currency, approved stablecoins, or other permitted settlement instruments directly to the individual. This mechanism eliminates administrative tolling, institutional payment delays, and the extraction of value by third-party intermediaries.



THE CLEAN SUPPLY CHAIN FOR DATA CONSUMERS

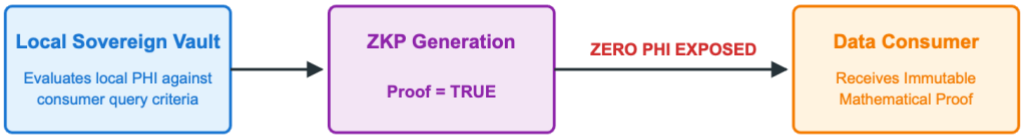
The Value Proposition for Consumers

Life science sponsors, clinical researchers, and artificial intelligence developers face severe operational bottlenecks when utilizing legacy datasets, which frequently contain uncorrected documentation errors and systemic demographic biases. Traditional analytics rely on indirect administrative proxies, such as billing and claims codes, which fail to accurately capture true patient physiology or functional health status.

The Circles Platform resolves this measurement gap by providing a direct pipeline to fully consented, regulatory-grade clinical intelligence without relying on legacy data brokers.

Zero-Knowledge Proofs

Commercial data consumers do not need to extract raw PHI to verify clinical facts. The Circles Platform architecture utilizes ZKPs to establish cryptographic certainty. ZKPs allow a network node to mathematically prove to a purchaser that a specific longitudinal record satisfies defined inclusion criteria, medical necessity parameters, or protocol requirements without revealing the underlying patient record, demographic identifiers, or laboratory values.



Fueling Medical AI

Medical artificial intelligence models require pristine training data to function safely and satisfy regulatory scrutiny. The closed-system Circles Platform supplies these models with "human ground truth"—primary clinical evidence derived directly from patient physiology, vital signs, and clinician interactions. Because this data is subject to schema-on-capture validation and explicit, smart-contract-governed consent, it prevents the training degradation and regulatory exposure caused by uncurated retrospective EHR dumps.

Quarantining Consumer Liability

Purchasers acquire verified analytical outputs, cryptographic proof packages, or localized query access rather than unredacted patient charts. By structurally eliminating the transmission and storage of raw PHI, the architecture acts as a legal liability sink. This design isolates purchasing organizations from the systemic breach exposure, class-action litigation risks, and acute regulatory penalties inherent in managing centralized data lakes.

CONCLUSION

The Sovereign Standard

The architecture resolves the structural friction between individual privacy mandates and the commercial requirement for large-scale medical research. By establishing a closed system governed by individual cryptographic control, the platform eliminates the need to balance clinical data utility against patient exposure.

The Economic Foundation

By securing the longitudinal record at the individual level, eliminating the de-identification ownership loophole, and automating economic attribution via smart contracts, the Circles Platform creates a new operational baseline.

It transitions the healthcare data economy from a legacy model of opaque, third-party extraction to a direct exchange between verified data producers and authorized commercial consumers. This framework aligns the economic incentives of the individual with the evidentiary requirements of the healthcare ecosystem, providing a functional standard for secure, consented data commercialization.

REFERENCES

Zero-Trust Architecture (ZTA)

- **National Institute of Standards and Technology (NIST)**

  NIST Special Publication 800-207: Zero Trust Architecture establishes the standard for migrating from static, perimeter-based security to a model that eliminates implicit trust and focuses on continuous cryptographic verification of users and assets.
  https://www.nist.gov/publications/zero-trust-architecture

Self-Sovereign Identity and Decentralized Identifiers

- **World Wide Web Consortium (W3C)**

  Decentralized Identifiers (DIDs) v1.0 outlines the core architecture and data model for verifiable, decentralized digital identities that operate independently of centralized registries, identity providers, or certificate authorities. https://www.w3.org/TR/did-1.0/

- **World Wide Web Consortium (W3C)**

  Verifiable Credentials Data Model v2.0 provides the specification for expressing claims on the web in a cryptographically secure, privacy-respecting, and machine-verifiable manner.
  https://www.w3.org/TR/vc-data-model-2.0/

Data Provenance and Lineage

- **World Wide Web Consortium (W3C)**

  PROV-Overview (W3C PROV Data Model) defines the foundational specification for recording immutable provenance information and documenting the core structures of data lineage, transformation, and historical access. https://www.w3.org/TR/prov-overview/

HIPAA Privacy Rule and De-identification

- **U.S. Department of Health and Human Services (HHS)**

  Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule details the statutory frameworks for de-identifying data, specifically outlining the Safe Harbor and Expert Determination methodologies. https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html

- **U.S. Department of Health and Human Services (HHS)**

  What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? clarifies the scope and limitations of an individual's right to access their protected health information (PHI) within designated record sets, distinguishing administrative access rights from legal property ownership. https://www.hhs.gov/hipaa/for-professionals/faq/2042/what-personal-health-information-do-individuals/index.html

Regulatory-Grade Data Integrity

- **U.S. Food and Drug Administration (FDA)**

  Data Integrity and Compliance With Drug CGMP: Questions and Answers establishes the regulatory framework for data integrity (the ALCOA+ standard), mandating that clinical and manufacturing data be Attributable, Legible, Contemporaneous, Original, and Accurate. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers

Zero-Knowledge Proofs in Healthcare Privacy

- **National Institutes of Health (NIH) / National Center for Biotechnology Information (NCBI)**

  Health-zkIDM: A Healthcare Identity System Based on Fabric Blockchain and Zero-Knowledge Proof provides peer-reviewed architectural analysis on utilizing zero-knowledge proofs (ZKPs) to authenticate and verify healthcare identities and clinical statements without exposing the underlying private data. https://pmc.ncbi.nlm.nih.gov/articles/PMC9608194/