RegenMed

WHITE PAPER

CIRCLES 4.0: BLOCKCHAIN/TOKENIZATION FOR PATIENT DATA

April 3, 2025

TABLE OF CONTENTS

INTRODUCTION

The Circles platform is a patented system through which correlated, verifiable, and longitudinal healthcare datasets are generated. Because the system is turnkey and closed by design, the datasets which it generates are proprietary to the sources/authors of that data. The primary data sources are physicians, laboratories, and patients (including their remote monitoring devices).

Healthcare data which is attributable to patients enjoys broad legal protection. Legal and ethical policy make clear that individuals are entitled to exclusive ownership of and control over their personal healthcare data. Such protected health information (PHI) can only be viewed and used by others after explicit and informed consent has been given by the patient. Typically, that consent is only given to healthcare providers for the sole purpose of patient care. [1]

Currently, various forms of anonymization and pseudonymization are used to create healthcare datasets which, in theory, are not attributable to individual patients. These so-called anonymized datasets are at the core of the $60+ billion healthcare data analytics market. [2] However, the attempt to dissociate patients' ownership rights from such a valuable datasets is vulnerable on several fronts:

- Many forms of claimed anonymization and pseudonymization are weak. Similarly, databases containing individual healthcare information are regularly accessed by multiple and undisclosed parties, many with poor cybersecurity protection in place. [3]

- Medicine is becoming increasingly "personalized" and "precision". An important part of an individual's health record is her genomic, proteomic, microbiomics, and other "omics" data. [4] Even if an individual's name and other information traditionally defined as personal are removed from this data, omics data is by definition highly specific to an individual.

- As in other fields, consumers are increasingly aware of the value of their data, whether or not it is anonymized. National policies, legislation, class action litigation, patient advocacy, and other trends will inevitably increase the awareness of individuals with respect to such personal healthcare data. [5]

Recognizing these trends, RegenMed is developing blockchain functionality on its Circles platform to provide patients with the option to use public-private key cryptography and distributable ledger technology to secure their PHI. [6] It will further exploit this technology to reward patients with tokens, representing complete longitudinal patient datasets. Those tokens will represent value for their holders in a number of ways, including reduced insurance premiums, access to Circle databases, medical product discounts, etc.

Circles will provide similar token issuance to physicians and other key sources of independent longitudinal healthcare datasets.

CONCEPTUAL MODEL

The idea is to create a token-based system where patients own tokens representing rights or interests in their anonymized health data. These tokens could be monetized, transferred, or managed by the patients themselves.

Key Components

- **Private Blockchain:** Ensures data security, integrity, and traceability.
- **Data Tokens:** Digital representations of ownership or value derived from anonymized health data.
- **Smart Contracts:** Automated contracts governing data usage rights, consent, and revenue-sharing mechanisms.
- **Patient Wallets:** Secure interfaces where patients can hold and manage their tokens.
- **Data Marketplaces (optional):** Platforms where patients can sell or license access to their tokens to authorized entities (e.g., researchers, insurers, providers, product manufacturers).

Technical Implementation

Blockchain Infrastructure

Use a private blockchain (e.g., Hyperledger Fabric, Corda) for better control and security compared to public blockchains. Ensure scalability to handle large volumes of health data tokens.

Token Design

Non-Fungible Tokens (NFTs): Unique tokens representing specific datasets or patient profiles.

Fungible Tokens: Tokens representing a general value derived from aggregated or anonymized data. [7]

Smart Contracts

Automate consent management — ensuring patient consents are recorded and immutable. Enforce revenue-sharing mechanisms — automatically distributing financial rewards to patients when their data is licensed or sold. Provide revocation mechanisms — allowing patients to reclaim ownership or withdraw consent where legally applicable.

Security and Privacy Protocols

Use zero-knowledge proofs to verify data integrity without revealing the actual data. Implement end-to-end encryption for all transactions involving patient data. Ensure robust identity management to prevent unauthorized access.

Legal Considerations

Compliance with Illustrative Data Privacy Laws

HIPAA (U.S.): Ensure that the initial de-identification process complies with HIPAA's de-identification standards. GDPR (EU): If European data is involved, even anonymized data may require consent if it can be reasonably re-identified. CCPA/CPRA (California): Ensure compliance with consumer rights to control, delete, or transfer their data.

Establishing Legal Ownership

Current laws do not clearly define patient ownership of de-identified data. The Circles platform will anticipate the inevitable movement towards recognizing such ownership through the following:

- **Contracts:** Clearly define ownership rights and the value associated with tokens.
- **Data Trusts:** Establish legal entities that hold data on behalf of patients and distribute revenues accordingly.
- **Tokenized Consent Agreements:** Ensure that smart contracts are legally binding and enforceable.

Ethical and Governance Considerations

In dealing with patient healthcare data, ethical considerations are as important as legal ones. Circles functionality will address these considerations as follows:

- <u>Patient Empowerment and Consent.</u> Ensure patients have full control over their tokens and can consent to or revoke data usage. Provide transparent reporting of how their data is being used and monetized.

- <u>Fair Compensation Models.</u> Implement fair revenue-sharing structures that reward patients proportionally based on the value their data generates. Consider differential pricing where patients with rare conditions may earn more due to higher data demand.

- <u>Governance Models.</u> Establish patient advisory boards or token-holder governance structures to ensure ethical use of data. Regularly audit systems and processes for transparency and fairness.

CONCLUSION

In the fast-evolving healthcare data world, adequate security and proof of ownership of — and incentives for consent to use — patient data are becoming pressing societal issues. The patented Circles platform has a strong technical foundation upon which to build efficient and scalable solutions.

Footnotes

1. Another common use case is when a patient is enrolled in a clinical trial. There, the patient typically receives some form of compensation in exchange for his informed consent both to participate in the sponsor's trial, as well as for the sponsor potentially to derive profit from his personal healthcare data.
2. This market is growing at an annual rate in excess of 20%.
3. As of February 2024, approximately 11.6 million individuals had their data exposed due to 79 reported breaches affecting 500 or more individuals. Change Healthcare attack: What to know about cybersecurity. Top 10 healthcare data breaches so far in 2024
4. See for example Multi-Omics Profiling for Health
5. See for example Who Owns Your Health Data? The Fight Between Patients, Big Tech, and Governments
6. This is far superior to current approaches, such as usernames and passwords, even when dual factor authentication is used.
7. Assigning token value should take into consideration the completeness, clinical relevance, longitudinality, and recency of a given data set. For example, token value could be influenced by data accumulation and decay. In such an instance, the value of a dataset (token) over time V(t)V(t) could be modeled by: V(t)=V0e−ktV(t) = V_0 e^{-kt} where V0V_0 = Initial value of the dataset, kk = decay constant (related to how quickly the data becomes outdated), and tt = Time since data was collected.