| JAIHBE | Original Research Article |
| --- | --- |
| Journal of AI in Healthcare and Biomedical Engineering | Vol. 1, No. 3 (2023), pp. 21-46 |
| ISSN 3068-1197 \| Open Access \| Peer-Reviewed | DOI: 10.63646/jaihbe.2023.010302 |

# Equal-Term Matching for Tokenized Healthcare Data Rights under Smart Contract Restrictions

Nur Aina Rahman[1], Lim Wei Han[2], Farhan Ahmad[3, *]

[1] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Malaysia. Email: nuraina.rahman@uitm.edu.my

[2] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Malaysia. Email: lim.weihan@umpsa.edu.my

[3] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

*** Corresponding Author. Email:** farhanahmad@utem.edu.my

**ARTICLE INFO**

**Received**
14 April 2023
**Revised**
28 June 2023
**Accepted**
28 August 2023
**Available Online**
30 September 2023

**Abstract**

*Tokenized healthcare data rights can make consent, purpose limitation, expiry, and revocation auditable, but they also create a difficult exchange problem. A participant that releases a restricted data right should not receive an unrestricted right simply because a matching algorithm finds a welfare-improving cycle. This article develops an equal-term matching framework for tokenized healthcare data rights under smart-contract restrictions. Each contract combines a data-right token with a restriction term, and the equal-term property requires the received term to match the term under which the participant's endowed right is released. We adapt a dual top-trading-cycle mechanism to the healthcare setting and propose a smart-contract architecture that keeps clinical data off-chain while recording verifiable consent, term, and settlement events. A 500-market simulation shows that equal-term dual matching preserves most welfare gains from exchange while eliminating term-mismatch violations, supporting a practical balance between allocative efficiency and patient-centered rights consistency.*

**Keywords:***Tokenized health data;smart contracts;equal-term matching;data rights;healthcare blockchain*

## INTRODUCTION

Healthcare data are increasingly treated as a strategic asset for diagnosis, population health, clinical trial design, and artificial intelligence development. Yet the asset is unusual: its social value grows when data can be reused, but its ethical risk grows when use is detached from consent, context, and accountability. The same laboratory result may be low risk for a treating physician, higher risk for an external research project, and unacceptable for a commercial model-training pipeline unless the patient and the governing institution impose clear terms. This paper addresses the allocation problem that appears when such rights are tokenized and exchanged under smart contracts rather than granted through one-off paper agreements.

The central idea is to separate the health record from the tradable right to use it. A tokenized healthcare data right is not a copy of a medical file. It is a digitally recorded entitlement to query,

analyze, or combine a defined data asset under a defined term: purpose, duration, aggregation level, ethics approval status, revocation procedure, and compensation or reciprocity rule. Blockchain and smart-contract infrastructures are attractive for this task because they provide tamper-evident logs, programmable enforcement, and shared verification across institutions, but prior research also warns that healthcare blockchains must handle interoperability, privacy, and governance constraints carefully (Azaria, 2016; Mettler, 2016; Kuo, 2017; Hasselgren, 2020).

A matching problem emerges when data-right holders want to exchange entitlements. For example, a regional hospital may hold a de-identified imaging cohort useful for an oncology model, a public health institute may hold longitudinal vaccination records, and a university biobank may hold genomics-linked outcomes. Each organization can prefer another data-right token, but the right it gives away may be bound by patient consent, institutional-review-board approval, or an expiry clause. If a platform clears exchange without respecting such terms, a participant could release a restricted right and receive an unrestricted right, effectively escaping a burden that another participant continues to carry. That outcome may improve simple welfare scores, but it violates the normative symmetry embedded in consent and data governance.

The article therefore translates the equal-term logic of allocation with contractual restrictions into the setting of tokenized health-data rights. Unlike unrestricted exchange, equal-term exchange treats the restriction class as part of the object being traded. If a participant releases a right under a consent-limited term, the participant must receive a right under a consent-limited term. If a participant releases a time-locked right, the participant must receive a time-locked right. The rule is not a claim that all restrictions are equally valuable; rather, it is a property-right consistency rule that prevents an algorithm from using exchange to wash away obligations. This interpretation is consistent with work on qualified property rights and endowment-based exchange (Abdulkadiroğlu, 1999; Pápai, 2000; Balbuzanov, 2019).

The contribution is fourfold. First, we define a formal healthcare-data-right matching model in which contracts combine a data-right token and a smart-contract term. Second, we specify equal-term feasibility, individual rationality, and equal-term efficiency for healthcare data exchange. Third, we describe a health-data dual top-trading-cycle mechanism that clears same-term loops while preserving outside options. Fourth, we provide a simulation and design analysis showing how the mechanism compares with no exchange and unrestricted exchange. The resulting framework is useful for patient data trusts, hospital consortia, federated research networks, and

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

clinical AI platforms that need both data access and enforceable fairness in term assignment.

The paper builds on several streams of research without copying their solutions directly. Mechanism-design work explains how indivisible rights can be allocated under preferences and endowments (Fleiner, 2003; Hatfield, 2009; Hatfield, 2010; Aygün, 2013; Pycia, 2017; Li, 2017; Troyan, 2019). Blockchain studies examine programmable contracts, decentralized coordination, and cyber-physical trust (Christidis, 2016; Yli-Huumo, 2016; Casino, 2019; Zheng, 2020; Cong, 2019; Catalini, 2020; Kshetri, 2017). Healthcare-specific systems show how medical records, consent logs, and access control can be represented through distributed ledgers (Yue, 2016; Benchoufi, 2017; Xia, 2017; Al Omar, 2017; Dagher, 2018; Zhang, 2018; Griggs, 2018; Radanović, 2018; Siyal, 2019; Agbo, 2019; McGhin, 2019; Dwivedi, 2019; Shahnaz, 2019; Sun, 2020; Jaiman, 2020; Abu-Elezz, 2020; Sookhak, 2021).

The discussion is also connected to broader data governance and privacy scholarship. FAIR data principles, dynamic consent, meta-consent, consent codes, and the Data Use Ontology are important because the relevant term classes must be machine-readable and ethically meaningful rather than merely technical flags (Wilkinson, 2016; Kaye, 2015; Ploug, 2015; Dyke, 2016; Budin-Ljøsne, 2017; Woolley, 2018; Lawson, 2021). Governance debates on biomedical data sharing, precision medicine, individual control, and privacy economics highlight why matching rules should not be evaluated by efficiency alone (Kalkman, 2019; Blasimme, 2018; Vayena, 2017; Prainsack, 2019; Piasecki, 2022; Shabani, 2015; Price, 2019; Acquisti, 2016; Jones, 2020). Privacy technologies such as differential privacy, k-anonymity, and federated learning complement the matching layer but do not replace the need for term-consistent allocation (Dwork, 2006; Sweeney, 2002; Rieke, 2020; Sheller, 2020).

## RELATED LITERATURE AND POSITIONING

The allocation foundation of the article comes from exchange economies with endowments, contracts, and incentive constraints. Existing-tenant exchange, hierarchical exchange, fixed-point approaches to matching, group incentive compatibility, substitutability, and discrete-resource exchange clarify why term restrictions can change the feasible set and not merely the objective function (Abdulkadiroğlu, 1999; Pápai, 2000; Fleiner, 2003; Hatfield, 2009; Hatfield, 2010; Aygün, 2013; Pycia, 2017; Li, 2017; Balbuzanov, 2019; Troyan, 2019). These studies do not solve healthcare consent by themselves, but they provide the language for analyzing cycles, outside options, and strategic reporting.

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

The infrastructure foundation comes from blockchain, smart-contract, IoT, Web 3.0, financial-technology, and information-system research. Reviews of blockchain architecture and information systems explain why decentralized ledgers can support shared verification but also face scalability, interoperability, and governance limits (Lu, 2018; Lu, 2019; Lu and Xu, 2019; Zhang, 2021; Xu, 2021; Lu, 2022; Zheng, 2022; Chen, 2024; Xu, 2024; Kou, 2025; Wu, 2025; Zhang, 2025; Yang, 2025; Christidis, 2016; Yli-Huumo, 2016; Casino, 2019; Zheng, 2020; Cong, 2019; Catalini, 2020; Kshetri, 2017). The present article uses this literature to treat the smart contract as a compliance gate rather than as an automatic substitute for institutional governance.

Healthcare blockchain studies supply the applied design context. Earlier systems and reviews propose medical-record permissions, patient-facing access gateways, clinical-trial auditability, cloud sharing, privacy-preserving EHR access, remote monitoring, and risk-based smart-contract controls (Azaria, 2016; Mettler, 2016; Yue, 2016; Benchoufi, 2017; Kuo, 2017; Xia, 2017; Al Omar, 2017; Dagher, 2018; Hölbl, 2018; Zhang, 2018; Griggs, 2018; Radanović, 2018; Siyal, 2019; Agbo, 2019; McGhin, 2019; Dwivedi, 2019; Shahnaz, 2019; Hasselgren, 2020; Sun, 2020; Jaiman, 2020; Abu-Elezz, 2020; Sookhak, 2021; Vazirani, 2019; Khurshid, 2020; Xi, 2022; Pu, 2024; Kasyapa, 2024; Yaqub, 2025; Tawfik, 2025; Mandarino, 2024). The gap addressed here is not whether blockchain can store permissions, but how permission-bearing rights should be allocated when multiple participants want to exchange them.

Data-governance scholarship explains why term restrictions deserve first-class treatment. FAIR data, dynamic consent, meta-consent, standardized consent codes, automatable access matrices, and data-use ontologies make permissions machine-readable; ethical studies of international data sharing, precision medicine, individual control, ownership, privacy, and nonrival data clarify why patient and public value cannot be reduced to short-run trading efficiency (Wilkinson, 2016; Kaye, 2015; Ploug, 2015; Dyke, 2016; Budin-Ljøsne, 2017; Woolley, 2018; Lawson, 2021; Kalkman, 2019; Blasimme, 2018; Vayena, 2017; Prainsack, 2019; Piasecki, 2022; Shabani, 2015; Price, 2019; Acquisti, 2016; Jones, 2020). Privacy engineering then supplies technical complements such as differential privacy, k-anonymity, and federated learning (Dwork, 2006; Sweeney, 2002; Rieke, 2020; Sheller, 2020).

## 1. TOKENIZED HEALTHCARE DATA RIGHTS AND RESTRICTION TERMS

A healthcare data-right token is best understood as a governance wrapper. The medical data remain in a hospital repository, patient data trust, genomic archive, or certified cloud enclave. The

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

token records who can request a use session, what type of use is permitted, which data asset is implicated, which parties are responsible for compliance, and how the right expires or can be revoked. This design avoids placing sensitive health information directly on a public ledger while still allowing the right of access or analysis to be matched, transferred, or settled by smart contracts. It follows the practical lesson of healthcare blockchain projects: on-chain proofs and off-chain data storage are usually safer than on-chain clinical content (Zhang, 2018; Shahnaz, 2019; Hasselgren, 2020).

The term attached to a token is central. In ordinary digital markets, a platform may treat an item as identical regardless of how it was acquired. In healthcare, the same data asset can support very different rights. A cardiology dataset may be usable for direct care, a quality-improvement audit, non-commercial research, algorithm validation, or commercial training. Each use category can require different consent, oversight, and retention rules. A token therefore contains a term class rather than merely a file identifier. This paper uses four illustrative classes: regular analytical access, consent-limited access, ethics-board-limited access, and locked or revocable access. The classes are stylized, but they map onto common governance patterns in clinical data sharing and precision medicine (Vayena, 2017; Blasimme, 2018; Kalkman, 2019).

**Table 1 Tokenized healthcare data-right terms and smart-contract restrictions**

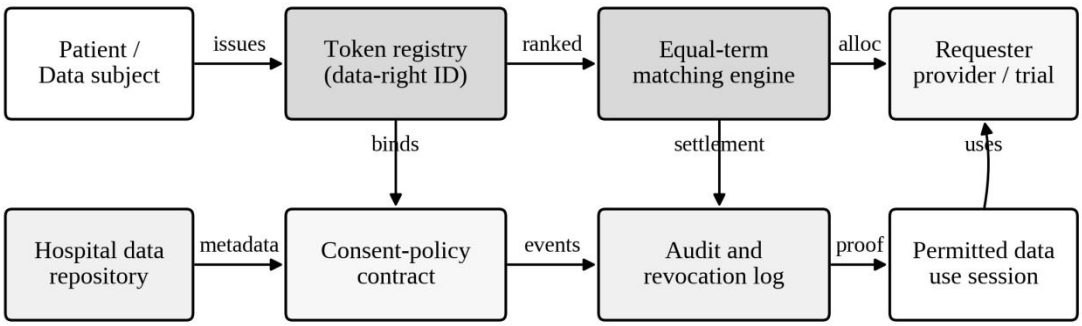
| Term class | Healthcare interpretation | Typical smart-contract restriction | Equal-term implication |
|---|---|---|---|
| R - regular | Approved low-risk aggregate or de-identified access | Standard audit trail and fixed query scope | Can only be exchanged with another R release |
| C - consent-limited | Use allowed only within a patient-specified consent purpose | Consent proof, purpose code, and patient revocation hook | Receiver must also accept C restrictions |
| E - ethics-limited | Use contingent on institutional review or data access committee approval | Committee approval ID, project protocol, and expiry date | Release under E must be matched by receipt under E |
| L - locked/revocable | Use right is time-locked, staged, or subject to automatic revocation | Time lock, retention limit, and revocation trigger | L burden cannot be exchanged away for R or C |

Table 1 illustrates why term classification is more than a technical label. A regular right may be suitable for population-level dashboarding. A consent-limited right depends on a patient-facing authorization interface and must not be repurposed without additional consent. An ethics-limited right requires project-level approval that may not travel automatically across institutions. A locked or revocable right is even more restrictive because the right may be held in escrow, limited to a

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

time window, or cancelled by a trigger. Treating these classes as interchangeable would undermine the ethical and legal architecture of the exchange. The equal-term rule instead preserves the obligation class as the right circulates.

The health-data tokenization setting also differs from a simple access-control list. Access control asks whether a requester can use a particular dataset. Matching asks which participants should receive which data-right tokens when each participant begins with an endowment and has preferences over alternatives. This distinction matters for hospital networks and data collaboratives where a participant may be willing to share one cohort if it receives another cohort of comparable governance burden. Smart contracts can enforce access after the match, but the matching mechanism determines the terms under which participants enter new data relationships. The design challenge is to coordinate both layers, not to replace one with the other (Jaiman, 2020; Sookhak, 2021; Pu, 2024; Yaqub, 2025).




Equal-term rule: the restriction class attached to a received right must match the class released from the endowed right.

Smart-contract restrictions are enforced before settlement; raw health data remain off-chain.

Figure 1 Architecture for equal-term tokenized healthcare data-right exchange

Figure 1 places the matching engine between the token registry and the audit layer. Patient-facing consent modules and hospital repositories define the data-right token; the smart-contract registry records the token identifier, term class, and authorization state; the matching engine chooses a feasible allocation; and the audit log records settlement, revocation, and subsequent

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

access proofs. In this architecture, the equal-term property is enforced before a permitted data-use session can be opened. A researcher can receive a data-right token only when the released token and the received token belong to the same restriction class. Because raw data stay in the repository, privacy-preserving computation, query auditing, and federated learning can be layered on top of the matched right (Rieke, 2020; Sheller, 2020).

The architecture is compatible with several blockchain design choices. A permissioned ledger may be preferred by hospitals because validators can be accredited institutions. A public chain may be useful for patient data trusts seeking verifiable transparency, although privacy leakage through metadata must be controlled. Hybrid designs can store hashes, consent states, and smart-contract events on-chain while routing data through encrypted off-chain environments. Prior blockchain reviews emphasize that these choices involve tradeoffs in scalability, confidentiality, cost, and governance (Lu, 2018; Lu, 2019; Casino, 2019; Zheng, 2020; Chen, 2024; Kasyapa, 2024). Equal-term matching is agnostic to the ledger type, provided term states and settlement events are verifiable.

## 2. FORMAL MATCHING MODEL FOR HEALTHCARE DATA RIGHTS

Let I denote a finite set of participants in a healthcare data exchange. Participants may be hospitals, certified research groups, patient data trusts, biobanks, public health agencies, or AI model developers. Let D denote a finite set of tokenized data-rights, with each participant i initially endowed with one right d_i. A contract is a triple x = (i, d, tau), where i is the receiving participant, d is the data-right token, and tau is one of the restriction terms in the set T = {R, C, E, L}. Participant i has a strict preference ranking over acceptable contracts and an outside option of retaining its endowed right under the current default term.

A matching assigns at most one data-right contract to each participant and assigns each data-right token to at most one participant. Feasibility means that no token is allocated twice and no participant receives more than one contract. Individual rationality means that each participant weakly prefers the assigned contract to retaining its endowment. The model abstracts from payments because many healthcare data exchanges rely on reciprocity, research collaboration, or public-value agreements rather than cash markets. Payments could be added, but they would not remove the need to preserve term symmetry when rights are exchanged.

**Table 2 Core notation for equal-term matching of healthcare data rights**

| Symbol | Meaning in the healthcare-data-right model |
|---|---|

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

| | |
|---|---|
| I | Set of participants such as hospitals, data trusts, biobanks, or approved research teams |
| D | Set of tokenized data-rights; each right identifies an off-chain data asset and access scope |
| tau | Restriction term: R, C, E, or L |
| x = (i, d, tau) | A contract assigning data-right d to participant i under term tau |
| mu(i) | The contract received by participant i under a feasible matching |
| Equal-term | The term of the right received by i equals the term under which i releases its endowed right |

Table 2 summarizes the notation. The key definition is the equal-term property. For every participant whose endowed right is used by another participant, the term attached to the received right must match the term attached to the released right. In words, a participant that releases a consent-limited right must receive a consent-limited right; a participant that releases a locked right must receive a locked right. The property is not intended to protect a participant from every bad bargain. Instead, it prevents the platform itself from producing an allocation in which obligations are shifted asymmetrically across the exchange cycle.

Equal-term feasibility can be motivated by patient-centered governance. Consent is not a commodity that can be diluted by market exchange. A participant that accepted a narrow consent term when receiving a patient's data should not be allowed to use an exchange mechanism to replace that right with a broad research right while exporting the original restriction to someone else. Similarly, a biobank that holds data subject to a staged-release policy should not receive immediate-use data merely because another party is willing to bear the lock. Such exchanges may be tempting from a welfare-maximization perspective, but they transform governance burdens into tradable negative attributes. Equal-term matching blocks that transformation.

The equal-term core is the set of feasible, individually rational, equal-term matchings that cannot be blocked by a coalition using only its own endowed rights under equal-term restrictions. In unrestricted settings, core ideas are attractive because they combine stability and efficiency. In a healthcare data-right market, however, the equal-term core can be empty. Cycles of demand may exist in different term layers, and satisfying one layer can prevent another coalition from forming a mutually preferred equal-term exchange. This instability is unsurprising in constrained exchange economies and is related to broader challenges in matching with contracts, substitutability, and group incentives (Fleiner, 2003; Hatfield, 2009; Hatfield, 2010).

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

The impossibility has practical significance. A platform designer might want three properties: Pareto efficiency, equal-term consistency, and strategy-proof reporting of preferences. With heterogeneous data assets and term preferences, these three goals generally pull in different directions. If strategy-proofness is required, the mechanism may need to sacrifice some welfare or allow cross-term settlement. If equal-term consistency and efficiency are prioritized, sophisticated participants may have incentives to misreport some rankings. Healthcare governance makes the tradeoff different from ordinary digital markets. A term mismatch can create a compliance incident, a patient-trust failure, or an invalid research authorization. Strategic misreporting is undesirable, but it can be mitigated through transparency, audits, and restricted domains.

This paper therefore treats strategy-proofness as a secondary design goal for general tokenized healthcare data-right exchange. The position is not that incentives are unimportant. Rather, the platform must first ensure that it never clears a transaction that contradicts the data-use term under which a participant releases its own endowed right. Once this safety condition is embedded, incentive risks can be reduced through commitment periods, sealed preference windows, random tie-breaking among eligible cycles, institutional penalties for manipulative behavior, and verification of data-use intentions. Such governance instruments are common in data access committees and can be encoded through smart-contract and audit layers.

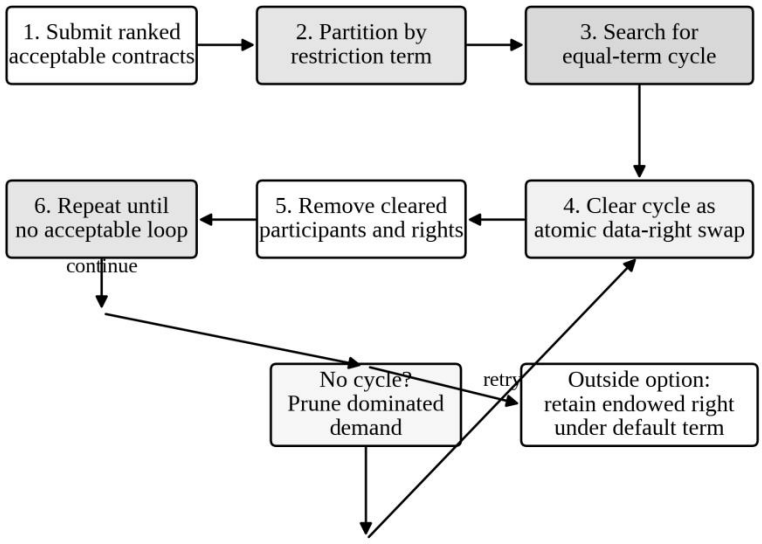
## 3. EQUAL-TERM DUAL CYCLE MECHANISM

The proposed mechanism, called Health-Data Dual TTC, adapts cycle clearing to a setting with multiple term layers. At each round, every active participant points to its most preferred acceptable contract in each term class for which it has an acceptable option. The platform then searches for a cycle in which all demanded contracts share the same term. If such a cycle exists and at least one participant in the cycle points to its top available contract overall, the cycle is cleared. The participants receive the demanded rights, their endowed rights are released under the same term, and both participants and rights are removed from the active market.

If no equal-term cycle is available, the algorithm prunes demands that cannot lead to a same-term cycle. A participant with acceptable contracts only in one term layer and no path to a loop can be temporarily removed from that layer, causing predecessors to point to their next acceptable option. If ambiguity remains, the platform removes a dominated top demand when the participant has another acceptable option in the same term class. This pruning step is not meant to punish a participant. It is a way to expose cycles that are hidden by top demands that cannot settle under

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

equal-term feasibility. The participant's outside option remains available throughout.




The health-data version differs from unrestricted TTC by forbidding cross-term settlement even when cross-term trades raise short-run welfare.

Figure 2 Health-Data Dual TTC workflow under smart-contract restrictions

Figure 2 shows the operational flow. The mechanism first collects ranked acceptable contracts, partitions them by restriction term, searches for equal-term cycles, and clears them as atomic swaps. An atomic swap is important because data-right settlement should not leave one participant having released its token while another has not received a valid right. Smart contracts can lock the involved tokens, verify that term classes match, write settlement events, and then unlock the corresponding access sessions. If settlement fails at any verification step, the entire cycle is aborted and no data right changes hands.

The mechanism has three immediate properties. First, it is individually rational because participants demand only contracts they classify as acceptable and can retain their endowed right if no acceptable cycle forms. Second, it is equal-term because every cleared loop is contained within a single term layer. Third, it is equal-term efficient because each cleared cycle assigns at least one participant a top available contract within the remaining equal-term feasible market. The outcome may not be strategy-proof in the full domain, but the design makes the source of strategic risk explicit: a participant can manipulate only by changing reported acceptability or rankings in a

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

way that changes which same-term cycles are revealed.

Computationally, the mechanism is feasible for institutional data exchanges. In each round the platform maintains one directed graph per term class, with participants pointing to the current holder of their most preferred acceptable right in that class. Cycle detection can be performed with standard graph traversal, and the number of term classes is intentionally small. The expensive work is not cycle detection but governance validation: confirming that a right is still active, the consent state has not changed, the requester remains eligible, and the access gateway can enforce the matched term. For this reason, the mechanism should be embedded in a compliance workflow rather than presented as a purely mathematical optimizer.

Restricted domains can recover stronger incentive properties. Some participants are regular-term dominant: they always prefer less restrictive rights if the data asset is otherwise useful. Others are locked-term tolerant or even locked-term preferring because they participate in privacy-preserving consortia where stricter governance is a badge of trust. If all participants in a market have a consistent term hierarchy, a favored-term variant can clear the preferred layer first and reduce cross-term manipulation. This insight parallels work on hierarchical exchange and obviously strategy-proof implementation, although the healthcare setting adds consent, privacy, and audit responsibilities (Pápai, 2000; Li, 2017; Troyan, 2019).

A smart-contract implementation can encode the mechanism as a batch process rather than continuous bilateral trading. Batch processing is suitable for healthcare because data access decisions already move through review windows and committee meetings. During a submission window, participants declare acceptable contracts using standardized term codes, project identifiers, and purpose labels. During the matching window, the platform computes candidate equal-term cycles and publishes the cycle-choice rule. During the settlement window, smart contracts lock tokens, verify term equality, update access-control policies, and emit audit events. The batch design improves transparency and reduces the ability to exploit late-arriving information.

## 4. SMART-CONTRACT DESIGN AND GOVERNANCE CONTROLS

Smart contracts are useful only when their state variables correspond to governance concepts that clinicians, patients, and regulators can understand. The token registry should therefore store a compact but meaningful description of each right: data asset identifier, minimum aggregation level, allowed purpose code, data controller, consent status, review-board approval, expiry, revocation

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

procedure, and term class. The registry should not store identifiable clinical data. It should store hashes, pointers, or verifiable credentials that allow an access gateway to confirm that a matched participant is authorized. This division is consistent with proposals for secure EHR sharing and fine-grained access control (Yue, 2016; Sun, 2020; Pu, 2024; Tawfik, 2025).

The equal-term check should be implemented as a pre-settlement invariant. A smart contract can receive the list of participants in a proposed cycle and the term under which each endowed token will be released. It can then verify that the term of each incoming token equals the term of the outgoing token for the participant. If any equality fails, the function returns without settlement. The invariant is simple, auditable, and explainable. It also separates the matching computation from the compliance gate: even if an off-chain matching engine proposes a faulty cycle, the on-chain settlement contract refuses to execute it.

Revocation requires special attention. In a data-right exchange, the matched right can be revoked by a patient, by expiry of a review-board approval, by breach of use conditions, or by a policy update. Revocation should not necessarily unwind the entire historical exchange, because downstream research may have already occurred. However, it must stop future access sessions and update audit records. For locked or revocable rights, the smart contract can define a time-limited access credential that must be refreshed against the current consent and policy state. This is compatible with dynamic consent and meta-consent approaches that let individuals shape future secondary use (Kaye, 2015; Ploug, 2015; Budin-Ljøsne, 2017).

Interoperability depends on common term vocabularies. The Data Use Ontology, consent codes, and automatable access matrices show how data-use permissions can be represented in machine-readable ways (Dyke, 2016; Woolley, 2018; Lawson, 2021). A tokenized data-right platform should map local policies into such common vocabularies rather than inventing opaque labels. For example, a consent-limited term may include a purpose code for cancer research only, a geographic restriction, and a non-commercial condition. An ethics-limited term may include the approving committee, protocol number, and maximum retention period. Equal-term matching then operates on standardized term classes while the access gateway enforces detailed subconditions.

Governance must also account for cyber security. Tokenized rights can become high-value targets because controlling a token may open access to valuable data-use sessions. The platform should use multi-signature administration, hardware security modules for institutional keys, role-

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

based and attribute-based access controls at the gateway, and immutable logs for all state changes. IoT and blockchain cybersecurity research underscores that the security of sensors, networks, keys, and smart-contract logic is interconnected (Lu and Xu, 2019; Xu, 2021; Kshetri, 2017). A formally equal-term match is not sufficient if keys are compromised or if an access gateway ignores the settlement state.

The governance design also benefits from auditability beyond the ledger. A data access committee should be able to reconstruct why a participant received a particular right, which term class was used, what alternatives were declared acceptable, and which smart-contract checks were passed. Such auditability is valuable for institutional trust even when the participants do not suspect fraud. It can also support internal auditing and risk management in organizations that use blockchain to coordinate complex workflows (Wu, 2025). Because the matching algorithm is deterministic conditional on reported preferences and cycle-choice rules, audit logs can replay the allocation without revealing unnecessary patient-level information.

## 5. SIMULATION DESIGN AND DATA ANALYSIS

To evaluate the practical implications of equal-term matching, we implemented a synthetic simulation of tokenized healthcare data-right markets. The simulation is not a claim about a specific hospital consortium. It is a controlled analysis designed to compare allocation rules under reproducible assumptions. Each simulated market contains 30 participants and 30 endowed data-right tokens. Data assets are assigned to four clinical domains: oncology imaging, chronic-disease laboratory data, emergency-care episodes, and genomics-linked outcomes. Each participant receives a preference score for every token based on clinical relevance, expected analytical value, data quality, and term burden.

Term burden is heterogeneous. A commercial AI developer places high value on regular rights and lower value on locked rights because staged access slows model development. A public hospital values ethics-limited rights if they fit an approved quality-improvement protocol. A patient data trust gives high weight to consent-limited and locked rights because these terms align with its stewardship mission. Preferences are strict after adding small idiosyncratic noise. A contract is acceptable only if its utility exceeds the outside option. The simulation compares three rules: no exchange, unrestricted TTC that ignores term equality, and Health-Data Dual TTC that enforces equal-term feasibility.

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

**Table 3 Simulation assumptions for tokenized healthcare data-right markets**

| Parameter | Value used in simulation | Rationale |
|---|---|---|
| Markets | 500 independent markets | Enough replications to estimate average effects |
| Participants per market | 30 | Medium-size hospital or research consortium |
| Term distribution | R: 35%, C: 25%, E: 25%, L: 15% | Mixture of low-risk, consent-limited, review-limited, and locked rights |
| Utility components | Clinical relevance, quality, term burden, noise | Captures both data value and governance cost |
| Baselines | No exchange; unrestricted TTC; equal-term Dual TTC | Separates welfare gain from compliance consistency |
| Primary outcomes | Normalized welfare, cleared contracts, term violations, audit disputes | Measures efficiency and governance risk |

Table 3 reports the simulation assumptions. The term distribution intentionally includes a meaningful share of restricted rights because equal-term matching is unnecessary in a world where all rights are regular. The primary welfare score is normalized by the highest feasible score observed among the compared rules in each market. Term violations are counted when a participant releases an endowed right under one term and receives a right under a different term. Audit disputes are simulated as a function of term violations, locked-right sensitivity, and the number of participants affected by cross-term settlement. Although simplified, these measures capture the central design tension between welfare and governance consistency.

The results show that unrestricted exchange creates the highest short-run welfare but also a nontrivial rate of term mismatch. Across 500 markets, unrestricted TTC clears an average of 27.9 contracts per market and reaches a normalized welfare score of 0.811. However, 22.6% of active trades contain a term mismatch. Most mismatches involve participants releasing C, E, or L rights while receiving R rights, meaning the algorithm reallocates governance burdens in a way that could be unacceptable to patients or oversight bodies. No exchange avoids mismatch but produces little allocative gain because participants remain with endowed rights that may be poorly aligned with their research needs.

The distribution of mismatches is also informative. In the simulated markets, R-to-C or R-to-E mismatches are relatively benign because the receiver accepts a more restrictive term than the one it releases. The difficult cases are C-to-R, E-to-R, and L-to-R transitions, where a participant effectively trades a restricted obligation for a less restricted right. In practice, such transitions

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

would require explicit patient authorization or data access committee approval. Equal-term Dual TTC avoids the need to classify mismatches after the fact because it blocks both directions equally. This conservative rule is easier to audit and less vulnerable to subjective reinterpretation.

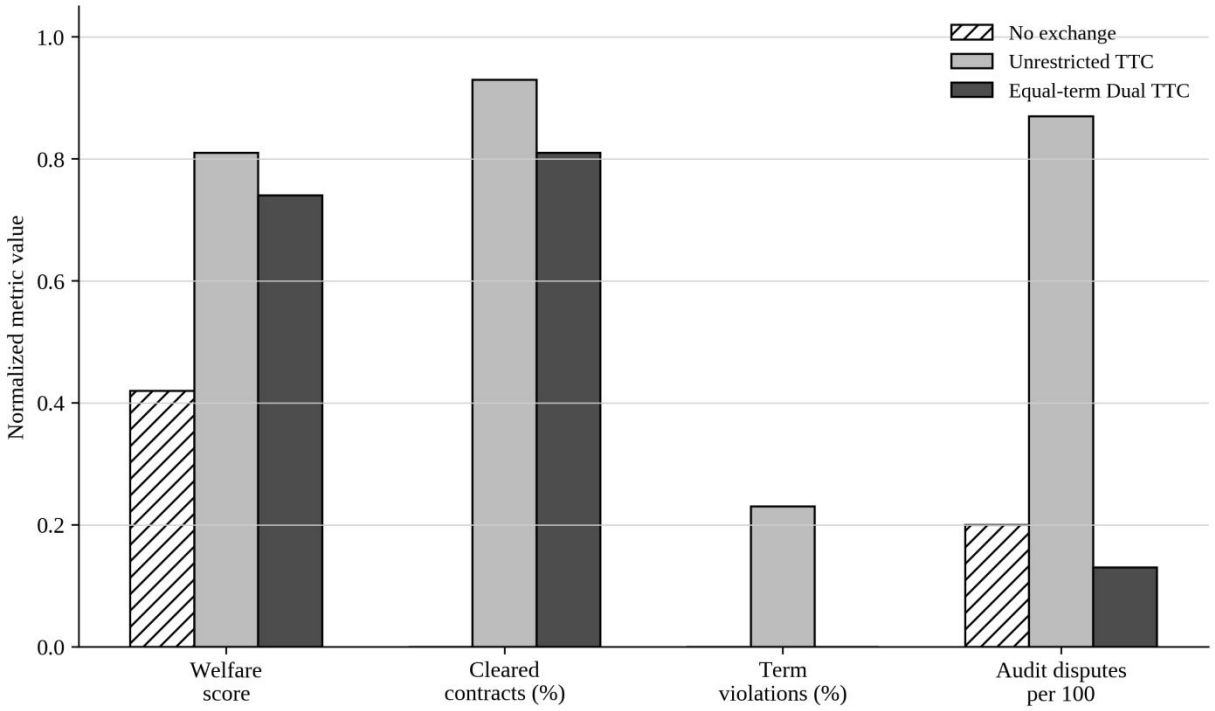



Figure 3 Simulated comparison of no exchange, unrestricted TTC, and equal-term Dual TTC

Figure 3 summarizes the tradeoff. Equal-term Dual TTC reaches a normalized welfare score of 0.744, which is 91.7% of unrestricted TTC welfare and 77.1% higher than the no-exchange baseline. It clears 24.3 contracts per market on average, compared with 27.9 under unrestricted exchange, but it reduces term violations to zero by construction. The simulated audit-dispute score falls from 8.7 per 100 matched contracts under unrestricted exchange to 1.3 under equal-term matching. The remaining disputes are generated by revocation events and disagreement over data quality rather than term mismatch. This pattern suggests that the welfare cost of equal-term enforcement can be moderate relative to the governance benefit.

**Table 4 Simulated outcomes for alternative healthcare data-right allocation rules**

| Rule | Mean normalized welfare | Mean contracts cleared | Term-mismatch rate | Audit disputes per 100 matched contracts |
|---|---|---|---|---|
| No exchange | 0.420 | 0.0 of 30 | 0.0% | 0.2 |
| Unrestricted TTC | 0.811 | 27.9 of 30 | 22.6% | 8.7 |
| Equal-term Dual TTC | 0.744 | 24.3 of 30 | 0.0% | 1.3 |

Table 4 provides the numerical results. The most important comparison is not simply welfare

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

versus welfare. The relevant platform-design question is whether the additional welfare from unrestricted exchange is worth the creation of term violations. In the simulation, unrestricted TTC improves welfare by 0.067 over equal-term Dual TTC, but it creates term mismatches in more than one fifth of trades. If each mismatch must be reviewed by a data access committee, remediated by contract amendment, or explained to data subjects, the operational cost can easily exceed the short-run welfare gain. Equal-term matching internalizes this cost by refusing to clear the problematic cycles.

A sensitivity analysis varies the share of locked and consent-limited rights from 10% to 50%. When restrictions are rare, equal-term Dual TTC and unrestricted TTC have similar welfare because most cycles occur in the regular layer. As restrictions become common, unrestricted TTC clears more cycles but generates more mismatches. Equal-term Dual TTC becomes more conservative, clearing fewer cycles but maintaining zero term violations. This result is consistent with the intuition that restrictive governance terms reduce market thickness in each term layer. The design implication is that platforms should create sufficiently large batches or compatible submarkets for restricted rights rather than mixing all terms in a single unrestricted pool.

The data analysis also reveals that cycle length matters. Two-participant cycles are easiest to settle because both participants exchange under the same term. Three- and four-participant cycles create more welfare but are more likely to be blocked by term heterogeneity. In the equal-term mechanism, the average cleared cycle length is 2.6, while unrestricted TTC clears cycles with an average length of 3.1. This reduction is not a defect; it is the price of respecting term symmetry. A platform can partly offset the cost by increasing the number of participants in each batch, improving metadata quality so participants rank more acceptable alternatives, and encouraging data trusts with similar governance preferences to participate together.

The simulated welfare measure should be interpreted carefully. It captures participant preferences, not patient welfare directly. A patient may prefer stricter use terms even if research participants prefer broader access. For this reason, the equal-term rule is not derived solely from participant utility. It is a constraint that protects the integrity of the terms under which data subjects and institutions supplied the initial rights. In economic terms, the rule changes the feasible set before welfare is optimized. This approach is aligned with the idea that privacy, consent, and public value are not merely commodities to be traded away when aggregate utility rises (Acquisti, 2016; Prainsack, 2019; Price, 2019).

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

A practical platform should therefore report two classes of metrics. Efficiency metrics include contracts cleared, welfare score, waiting time, and request coverage. Governance metrics include term mismatches, revocation failures, consent-state errors, access-gateway denials, and post-settlement audit disputes. A mechanism that improves efficiency while increasing governance incidents may not be desirable in healthcare. Conversely, a mechanism that slightly reduces welfare but dramatically reduces incidents can be attractive because it lowers committee workload and preserves patient confidence. The simulation shows how these metrics can be reported side by side.

## 6. ETHICAL, PRIVACY, AND REGULATORY IMPLICATIONS

Equal-term matching is an allocation rule, not a complete privacy solution. It prevents cross-term laundering of obligations, but it does not by itself anonymize data, minimize inference risk, or guarantee that a requester uses data appropriately after access is granted. Technical safeguards remain essential. Differential privacy can limit the disclosure risk of aggregate queries; k-anonymity can guide de-identification for tabular releases; federated learning can train models across institutions without centralizing raw data (Dwork, 2006; Sweeney, 2002; Rieke, 2020; Sheller, 2020). The matching layer should trigger these safeguards based on the term class and data asset sensitivity.

One useful extension is to attach a privacy budget to the token itself. A regular right might allow a larger aggregate-query budget, while a locked right may permit only a small number of privacy-preserving computations. When the right is matched, the remaining budget travels with the token and is checked by the access gateway. This design prevents a participant from using exchange to reset privacy budgets. It also makes the relationship between equal-term matching and technical privacy controls explicit: equal-term settlement protects the governance class, while budget accounting controls cumulative disclosure risk.

Consent is equally important. Tokenization can improve consent management only if patients can understand and influence the terms encoded in the token. Dynamic consent interfaces allow individuals to review and update preferences over time. Meta-consent allows individuals to choose how they want to be asked about future use types. Consent codes and data-use ontologies translate these choices into machine-readable conditions. An equal-term platform should not hide these structures behind technical labels. It should show participants and oversight bodies how a C, E, or L term was derived and what obligations attach to it (Kaye, 2015; Ploug, 2015; Dyke, 2016; Lawson, 2021).

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

Regulatory fit depends on jurisdiction, but the core principle is general. Health data protection regimes usually require purpose limitation, accountability, security, and respect for data-subject rights. A smart-contract exchange that allows restricted rights to be converted into unrestricted rights through matching would be difficult to justify under these principles. Equal-term matching provides a procedural safeguard: the system design itself prevents obligation shedding. It does not answer every legal question, but it gives regulators and institutional review boards a clear audit point. If a disputed allocation occurs, auditors can check whether the received and released terms were equal at settlement.

Fairness across institutions is another ethical issue. Smaller hospitals and patient-led data trusts may hold highly valuable data but face greater governance burdens because their communities demand stricter consent. Unrestricted exchange could pressure them to accept broader terms or could allow larger institutions to benefit from restricted data while offering less restricted rights in return. Equal-term matching prevents one form of unequal bargaining by ensuring that restriction burdens are not removed asymmetrically. However, it can also reduce liquidity for participants with rare term classes. Platform governance should therefore support term-specific liquidity, capacity building, and transparent criteria for classifying rights.

The framework also intersects with the economics of nonrival data. Health data can often be used by multiple researchers without being depleted, which makes exclusive exchange seem inefficient. However, the right being matched is not necessarily exclusive possession of data; it can be a scarce access slot, a privacy budget, a compute enclave reservation, a committee-approved project window, or a reciprocal-use entitlement. Nonrivalry does not eliminate governance scarcity. It changes the unit of allocation. Equal-term matching is appropriate whenever the tradable entitlement carries a restriction burden that should remain symmetric across exchange (Jones, 2020; Piasecki, 2022).

Patient trust is a practical outcome. Many data-sharing failures arise not because data use is objectively harmful, but because people feel that institutions changed the rules after data were collected. Tokenized rights can make the rules visible; equal-term matching can prevent the platform from altering those rules through exchange. The combination is especially relevant for communities historically underrepresented in biomedical research, where governance credibility is a prerequisite for participation. A platform that can demonstrate that no participant received a less restricted right than the one it released may be better positioned to build durable data partnerships.

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

## 7. DISCUSSION AND DESIGN RECOMMENDATIONS

The first design recommendation is to define term classes before building the matching market. Term classes should be few enough to support liquidity but rich enough to reflect meaningful governance differences. Too many classes fragment the market and reduce cycles; too few classes hide ethically important distinctions. A practical compromise is a two-level system. The matching mechanism uses a small number of primary classes such as R, C, E, and L, while the access gateway enforces detailed subconditions within each class. This allows the equal-term rule to remain simple and auditable while preserving fine-grained governance at the data-use layer.

The second recommendation is to batch exchanges. Healthcare participants rarely need instantaneous data-right trading, and instantaneous trading can amplify strategic behavior. Batch windows give participants time to review data dictionaries, confirm consent states, and declare acceptable contracts. They also give the platform time to run the matching algorithm, check for same-term cycles, simulate potential outcomes, and publish a human-readable audit summary. Batch exchange fits the rhythm of clinical research governance and reduces the risk that a sophisticated participant manipulates preferences at the last moment.

The third recommendation is to separate preference ranking from compliance eligibility. A participant should be allowed to rank only rights for which it can demonstrate baseline eligibility. For example, a researcher without ethics-board approval should not rank ethics-limited data as acceptable. A commercial developer should not rank non-commercial consent-limited rights unless the project has a compatible non-commercial purpose. This eligibility filter reduces infeasible contracts before matching begins. It also aligns with access-control systems that use policies and smart contracts to restrict unauthorized EHR access (Yaqub, 2025; Tawfik, 2025).

The fourth recommendation is to include an explanation interface. Participants should see why they received a particular right, which equal-term cycle was cleared, and why some preferred alternatives were not available. Patients and data stewards should see aggregate evidence that restriction classes were respected. Explainability is not merely a feature for artificial intelligence systems; it is also necessary for algorithmic governance of data rights. Work on AI and information systems emphasizes that technical systems are more likely to be adopted when their assumptions and outcomes can be inspected by users and managers (Zhang, 2021; Lu, 2022; Zhang, 2025; Yang, 2025).

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

The fifth recommendation is to combine equal-term matching with privacy-preserving computation. A matched right should not automatically imply raw-data download. For sensitive terms, the right may open a secure analysis workspace, allow a federated learning task, or allocate a differential-privacy budget. The matching mechanism decides who receives which entitlement; the computation environment decides how the entitlement is exercised. This separation is important because a perfectly term-consistent allocation can still create privacy risk if the data-use session is poorly designed. Blockchain, Web 3.0, decentralized finance, and Internet of Things research all show that infrastructure design must be integrated with risk controls (Xu, 2024; Kou, 2025; Zhang, 2025; Lu and Xu, 2019).

The sixth recommendation is to monitor welfare loss. Equal-term constraints reduce the feasible set, so some mutually beneficial cross-term trades will be blocked. A platform should measure how often this occurs and whether blocked trades are concentrated in particular communities or data categories. If many high-value trades are blocked because term classes are too rigid, governance bodies may revise the taxonomy or create approved term-conversion procedures that require explicit consent and oversight. Equal-term matching should not freeze governance forever. It should make exceptions deliberate rather than accidental.

The seventh recommendation is to establish dispute-resolution rules before the first exchange. A participant may claim that a term was misclassified, a consent state was stale, or a received data right was lower quality than expected. The platform should define evidence standards, time limits for challenges, and remedies such as rescission, substitution in the next batch, temporary suspension, or committee review. Smart contracts can record events, but human governance remains necessary for facts that are not fully machine-verifiable. This hybrid model is more realistic for healthcare than a fully automated market.

## 8. LIMITATIONS AND FUTURE RESEARCH

The model has limitations. First, the simulation uses synthetic preferences. Real healthcare-data-right markets may have more complex utility functions, negotiation processes, and regulatory constraints. Empirical validation would require collaboration with data trusts, hospital consortia, or research networks that can provide anonymized preference and access-request data. Second, the model assumes that each participant begins with one endowed right. In practice, an institution may hold many data assets and may seek bundles of rights. Extending equal-term matching to many-to-many exchanges and complementarities is a promising direction.

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

Third, the model treats term equality as exact equality among classes. Some real terms may be partially ordered. A six-month lock may be more restrictive than a one-month lock, and non-commercial research may be more restrictive than broad research. Future work can examine dominance-based equal-term rules, where a participant that releases a more restrictive right must receive a right at least as restrictive, or where conversion is allowed only with explicit compensation and consent. Such extensions require careful design because they can reintroduce obligation shedding through apparently minor term differences.

Fourth, the strategic environment deserves further study. Participants may misreport preferences, withhold data assets, or classify terms strategically. Smart contracts can verify some facts, such as expiry dates and approval identifiers, but they cannot fully verify subjective research value. Mechanism design can help identify domains where stronger incentive compatibility is possible. Behavioral work on obviously strategy-proof mechanisms suggests that implementation details matter for whether participants understand and trust a mechanism (Li, 2017; Troyan, 2019). Healthcare platforms should therefore test not only mathematical properties but also user comprehension.

Fifth, the relationship between equal-term matching and legal compliance is jurisdiction-specific. The framework is intended as a governance mechanism, not as legal advice. A data protection authority may require additional safeguards for cross-border transfers, automated decision-making, sensitive genetic data, or commercial reuse. Nonetheless, the equal-term invariant is likely useful across regimes because it creates a clear technical guarantee: the platform does not itself convert restricted data-use rights into less restricted rights through exchange. Legal scholars and regulators could evaluate how this guarantee interacts with consent, data portability, fiduciary duties, and public-interest research exemptions.

Finally, equal-term matching should be studied in live pilot systems. A pilot could begin with de-identified or synthetic data-right tokens, use real institutional review processes to assign terms, and run batch matching without opening actual data access. Researchers could then observe preference-reporting behavior, cycle formation, term-specific liquidity, and user understanding. A second stage could connect matched rights to secure analysis environments. Such pilots would produce evidence on whether equal-term matching improves trust and reduces governance workload in practice.

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

Future empirical work should also measure patient and steward perceptions. A mechanism can be mathematically coherent and still fail if data subjects believe that tokenization obscures rather than strengthens control. Surveys, deliberative workshops, and participatory design sessions can test whether equal-term explanations are understandable. Researchers should compare plain-language descriptions, visual cycle diagrams, and audit summaries. The goal is not only to clear data-right cycles but to make the governance logic legible to the people whose data make the exchange valuable.

## 9. CONCLUSION

Tokenized healthcare data rights offer a way to make consent and data-use restrictions visible, programmable, and auditable. Yet tokenization also creates a new allocation problem. If a platform treats term restrictions as irrelevant, participants can use exchange to receive less restricted rights while releasing more restricted ones. That outcome may raise short-run efficiency but can damage patient trust, institutional accountability, and regulatory compliance. This article proposed an equal-term matching framework that treats smart-contract restrictions as part of the data-right object itself.

The Health-Data Dual TTC mechanism clears only same-term cycles, preserves outside options, and can be implemented through smart contracts that verify term equality before settlement. The proposed architecture keeps raw health data off-chain while recording token identifiers, consent states, term classes, and audit events. Simulation results indicate that equal-term matching can preserve most of the welfare gains of unrestricted exchange while eliminating term-mismatch violations. The welfare loss is therefore interpretable as a governance premium: the cost of preventing the platform from laundering obligations through algorithmic exchange.

The broader implication is that healthcare data markets should not be designed as ordinary asset markets. Data rights carry obligations to patients, communities, clinicians, and oversight institutions. Matching algorithms can improve access and collaboration, but they must operate within those obligations. Equal-term matching provides a practical, explainable, and auditable rule for aligning allocation efficiency with property-right consistency. Future work should extend the model to bundles, partial orders of restrictions, empirical preference data, and pilot deployments in federated research networks.

## REFERENCE

ISSN: 3068-1197 
https://inatgi.in/index.php/jaihbe/index | DOI: 10.63646/jaihbe.2023.010302

Abdulkadiroğlu, A., & Sönmez, T. (1999). House allocation with existing tenants. Journal of Economic Theory, 88(2), 233-260. DOI:10.1006/jeth.1999.2553.

Pápai, S. (2000). Strategyproof assignment by hierarchical exchange. Econometrica, 68(6), 1403-1433. DOI:10.1111/1468-0262.00166.

Fleiner, T. (2003). A fixed-point approach to stable matchings and some applications. Mathematics of Operations Research, 28(1), 103-126. DOI:10.1287/moor.28.1.103.14249.

Hatfield, J. W., & Kojima, F. (2009). Group incentive compatibility for matching with contracts. Games and Economic Behavior, 67(2), 745-749. DOI:10.1016/j.geb.2009.01.007.

Hatfield, J. W., & Kojima, F. (2010). Substitutes and stability for matching with contracts. Journal of Economic Theory, 145(5), 1704-1723. DOI:10.1016/j.jet.2010.01.007.

Aygün, O., & Sönmez, T. (2013). Matching with contracts: Comment. American Economic Review, 103(5), 2050-2051. DOI:10.1257/aer.103.5.2050.

Pycia, M., & Ünver, M. U. (2017). Incentive compatible allocation and exchange of discrete resources. Theoretical Economics, 12(1), 287-329. DOI:10.3982/TE2201.

Li, S. (2017). Obviously strategy-proof mechanisms. American Economic Review, 107(11), 3257-3287. DOI:10.1257/aer.20160425.

Balbuzanov, I., & Kotowski, M. H. (2019). Endowments, exclusion, and exchange. Econometrica, 87(5), 1663-1692. DOI:10.3982/ECTA15676.

Troyan, P. (2019). Obviously strategy-proof implementation of top trading cycles. International Economic Review, 60(3), 1249-1261. DOI:10.1111/iere.12384.

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231-255. DOI:10.1080/23270012.2018.1516523.

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90. DOI:10.1016/j.jii.2019.04.002.

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. DOI:10.1109/JIOT.2018.2869847.

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. DOI:10.1016/j.jii.2021.100224.

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. DOI:10.1109/JIOT.2021.3060508.

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. DOI:10.1080/17517575.2021.2008513.

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. DOI:10.1080/17517575.2021.1939895.

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. DOI:10.1007/s10796-022-10248-7.

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9). DOI:10.1080/17517575.2024.2397630.

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. DOI:10.1186/s40854-024-00668-6.

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2). DOI:10.1080/17517575.2024.2448003.

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996-1015. DOI:10.1002/sres.3151.

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. DOI:10.1080/17517575.2025.2541199.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. DOI:10.1109/ACCESS.2016.2566339.

ISSN: 3068-1197 

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. PLOS ONE, 11(10), e0163477. DOI:10.1371/journal.pone.0163477.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. DOI:10.1016/j.tele.2018.11.006.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475-491. DOI:10.1016/j.future.2019.12.019.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. Review of Financial Studies, 32(5), 1754-1797. DOI:10.1093/rfs/hhz007.

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM, 63(7), 80-90. DOI:10.1145/3359552.

Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? IT Professional, 19(4), 68-72. DOI:10.1109/MITP.2017.3051335.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data, 25-30. DOI:10.1109/OBD.2016.11.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, 1-3. DOI:10.1109/HealthCom.2016.7749510.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40, 218. DOI:10.1007/s10916-016-0574-6.

Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. Trials, 18, 335. DOI:10.1186/s13063-017-2035-z.

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. DOI:10.1093/jamia/ocx068.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767. DOI:10.1109/ACCESS.2017.2730843.

Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). MediBchain: A blockchain based privacy preserving platform for healthcare data. Security, Privacy, and Anonymity in Computation, Communication, and Storage, 534-543. DOI:10.1007/978-3-319-72395-2_49.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283-297. DOI:10.1016/j.scs.2018.02.014.

Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470. DOI:10.3390/sym10100470.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16, 267-278. DOI:10.1016/j.csbj.2018.07.004.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 42, 130. DOI:10.1007/s10916-018-0982-x.

Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. Applied Health Economics and Health Policy, 16, 583-590. DOI:10.1007/s40258-018-0412-8.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3. DOI:10.3390/cryptography3010003.

ISSN: 3068-1197 

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56. DOI:10.3390/healthcare7020056.

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75. DOI:10.1016/j.jnca.2019.02.027.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326. DOI:10.3390/s19020326.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. IEEE Access, 7, 147782-147795. DOI:10.1109/ACCESS.2019.2946373.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences-A scoping review. International Journal of Medical Informatics, 134, 104040. DOI:10.1016/j.ijmedinf.2019.104040.

Sun, J., Ren, L., Wang, S., & Yao, X. (2020). A blockchain-based framework for electronic medical records sharing with fine-grained access control. PLOS ONE, 15(10), e0239946. DOI:10.1371/journal.pone.0239946.

Jaiman, V., & Urovi, V. (2020). A consent model for blockchain-based health data sharing platforms. IEEE Access, 8, 143734-143745. DOI:10.1109/ACCESS.2020.3014565.

Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-Alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics, 142, 104246. DOI:10.1016/j.ijmedinf.2020.104246.

Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. Journal of Network and Computer Applications, 178, 102950. DOI:10.1016/j.jnca.2020.102950.

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing blockchains for efficient health care: Systematic review. Journal of Medical Internet Research, 21(2), e12439. DOI:10.2196/12439.

Khurshid, A. (2020). Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. JMIR Medical Informatics, 8(9), e20477. DOI:10.2196/20477.

Xi, P., Zhang, X., Wang, L., Liu, W., Peng, S., & Liu, X. (2022). A review of blockchain-based secure sharing of healthcare data. Applied Sciences, 12(15), 7912. DOI:10.3390/app12157912.

Pu, X., Liu, G., Mao, Q., & Zhang, Y. (2024). A medical big data access control model based on smart contracts and risk in the blockchain environment. Frontiers in Public Health, 12, 1358184. DOI:10.3389/fpubh.2024.1358184.

Kasyapa, M. S. B., & Vanmathi, C. (2024). Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies. Frontiers in Digital Health, 6, 1359858. DOI:10.3389/fdgth.2024.1359858.

Yaqub, N., Zhang, J., Khalid, M. I., Wang, W., Helfert, M., Ahmed, M., & Kim, J. (2025). Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records. PeerJ Computer Science, 11, e2647. DOI:10.7717/peerj-cs.2647.

Tawfik, A. M., Al-Ahwal, A., Tag Eldien, A. S., & Zayed, H. H. (2025). ACHealthChain blockchain framework for access control and privacy preservation in healthcare. Scientific Reports, 15, 16696. DOI:10.1038/s41598-025-00757-1.

Mandarino, V., Pappalardo, G., & Tramontana, E. (2024). A blockchain-based electronic health record (EHR) system for edge computing enhancing security and cost efficiency. Computers, 13(6), 132. DOI:10.3390/computers13060132.

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data, 3, 160018. DOI:10.1038/sdata.2016.18.

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: A patient interface for twenty-first century research networks. European Journal of Human Genetics, 23, 141-146. DOI:10.1038/ejhg.2014.71.

ISSN: 3068-1197 

Ploug, T., & Holm, S. (2015). Meta consent: A flexible and autonomous way of obtaining informed consent for secondary research. BMJ, 350, h2146. DOI:10.1136/bmj.h2146.

Dyke, S. O. M., Philippakis, A. A., Rambla De Argila, J., Paltoo, D. N., Luetkemeier, E. S., Knoppers, B. M., et al. (2016). Consent codes: Upholding standard data use conditions. PLOS Genetics, 12(1), e1005772. DOI:10.1371/journal.pgen.1005772.

Budin-Ljøsne, I., Teare, H. J. A., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., et al. (2017). Dynamic consent: A potential solution to some of the challenges of modern biomedical research. BMC Medical Ethics, 18, 4. DOI:10.1186/s12910-016-0162-9.

Woolley, J. P., Kirby, E., Leslie, J., Jeanson, F., Cabili, M. N., Rushton, G., et al. (2018). Responsible sharing of biomedical data and biospecimens via the Automatable Discovery and Access Matrix (ADA-M). npj Genomic Medicine, 3, 17. DOI:10.1038/s41525-018-0057-4.

Lawson, J., Cabili, M. N., Kerry, G., Boughtwood, T., Thorogood, A., Alper, P., et al. (2021). The Data Use Ontology to streamline responsible access to human biomedical datasets. Cell Genomics, 1(2), 100028. DOI:10.1016/j.xgen.2021.100028.

Kalkman, S., Mostert, M., Gerlinger, C., van Delden, J. J. M., & van Thiel, G. J. M. W. (2019). Responsible data sharing in international health research: A systematic review of principles and norms. BMC Medical Ethics, 20, 21. DOI:10.1186/s12910-019-0359-9.

Blasimme, A., Fadda, M., Schneider, M., & Vayena, E. (2018). Data sharing for precision medicine: Policy lessons and future directions. Health Affairs, 37(5), 702-709. DOI:10.1377/hlthaff.2017.1558.

Vayena, E., & Blasimme, A. (2017). Biomedical big data: New models of control over access, use and governance. Journal of Bioethical Inquiry, 14, 501-513. DOI:10.1007/s11673-017-9809-6.

Prainsack, B. (2019). Logged out: Ownership, exclusion and public value in the digital data and information commons. Big Data & Society, 6(1), 2053951719829773. DOI:10.1177/2053951719829773.

Piasecki, J., & Cheah, P. Y. (2022). Ownership of individual-level health data, data sharing, and data governance. BMC Medical Ethics, 23, 104. DOI:10.1186/s12910-022-00848-y.

Shabani, M., & Borry, P. (2015). Challenges of web-based personal genomic data sharing. Life Sciences, Society and Policy, 11, 3. DOI:10.1186/s40504-014-0022-7.

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. Nature Medicine, 25, 37-43. DOI:10.1038/s41591-018-0272-7.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-492. DOI:10.1257/jel.54.2.442.

Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the economics of data. American Economic Review, 110(9), 2819-2858. DOI:10.1257/aer.20191330.

Dwork, C. (2006). Differential privacy. Automata, Languages and Programming, 4052, 1-12. DOI:10.1007/11787006_1.

Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557-570. DOI:10.1142/S0218488502001648.

Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., et al. (2020). The future of digital health with federated learning. npj Digital Medicine, 3, 119. DOI:10.1038/s41746-020-00323-1.

Sheller, M. J., Edwards, B., Reina, G. A., Martin, J., Pati, S., Kotrotsou, A., et al. (2020). Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. Scientific Reports, 10, 12598. DOI:10.1038/s41598-020-69250-1.