dHealth Protocol: A Trustless Healthcare Network for Humans, Providers, and Machines

dHealth DAO
www.dhealth.com

Abstract. The dHealth Protocol links real-world events to digital proof, anchoring trust in cryptographic verification, not centralised systems. It is a trustless coordination layer that proves what happened, who acted, and under what authority, without storing raw health data on the chain. It rests on three primitives. Credentials comprise identity credentials for actors and mandate credentials that delegate revocable authority. Schemas define what attestations mean. Attestations are signed claims about actions or states. Together, they give portable, audit-ready proof across institutional boundaries. Two primitives are the protocol's major applications. The first is the mandate credential, delegating revocable authority to humans, AI agents, and robots. The second is attestation, in particular QR-code attestation, which disseminates AI system prompts. Both share one economic mechanism. Creating either carries a fee in SOL, and the issuer contributes an equal amount to buy DHP on the market for the Community Fund. DHP holders vote to fund projects and actions that bring new users, or to burn the DHP. Primitives define accountability; payments and reimbursements rely on stable-value assets. DHP is an asset for participation, accountability, and governance. Its inflation is 2% annually, and the Community Fund adds a usage-linked counterweight through buybacks and optional burns.

Version: 0.3 (living draft), parameters may change via governance.

1. Introduction

Healthcare is delivered through networks of patients, clinicians, insurers, laboratories, AI systems, and connected devices. Coordination among these actors still depends on trust-intensive artefacts such as portals, PDFs, and vendor-controlled logs. These artefacts do not carry verifiable integrity across institutional boundaries. Proving that an action occurred, who performed it, and under what authority remains slow, fragmented, and fragile. The problem is sharpest in continuous and machine-assisted care.

The dHealth Protocol addresses this coordination gap with a credential-based framework for verifiable healthcare actions that does not require the centralisation of sensitive health data. The protocol defines three primitives. The first is cryptographic credentials, comprising identity credentials for individuals, organisations, and machines, and mandate credentials that delegate authority to act or attest under defined conditions. The second is shared schemas that define the meaning and validation rules of attestations. The third is attestations, which are signed claims that an action or a state occurred. Together, these primitives enable audit-ready proof of action for both humans and machines, and create portable and privacy-preserving evidence of a person's health journey that can be verified independently across systems, organisations, and time.

2. Motivation and Problem Definition

Healthcare has shifted from episodic encounters to continuous, multi-actor workflows. The bottleneck is no longer generating information, but proving that actions were taken **with valid authority**, while preserving privacy and keeping responsibility attributable to humans. The protocol replaces document-centric trust with verifiable, portable evidence of care-relevant actions.

The protocol is designed to address four structural problems in modern healthcare coordination. First, it replaces trust-based artefacts such as PDFs, portals, and unverifiable logs with cryptographic proof that an action actually occurred. Second, it enforces explicit authority by ensuring that every action is attributable to a verifiable credential and, where required, a clearly defined mandate. Third, privacy is guaranteed by architecture: no personal or medical data is stored on-chain, only cryptographic proofs, references, and revocation states. Finally, the protocol enables human-first machine participation, allowing AI systems and robots to act and attest only under explicit, revocable mandates issued by accountable humans or institutions.

3. dHealth Network Legacy

dHealth has migrated its architecture to ensure its primitives, such as credentials, authorisation, and verifiable actions, can be enforced natively. Before Cosmos, the network used Symbol, but its limited smart-contract support constrained programmable authorisation. Cosmos enabled flexibility via an app chain, but continuous-care workloads exposed the costs of running a standalone chain: operational risk and resource diversion. The recent transition retired the Cosmos app chain and migrated DHP, along with attestation/mandate services, to **Solana** for high-frequency, low-latency execution. DHP is defined as a protocol-layer accountability asset, while fees are settled in SOL, and payments should be made using stablecoins.

4. Objectives

Using the protocol, any verifier can independently confirm that an action occurred, who claimed it occurred, and, where applicable, who verified it. The protocol builds on the Solana Attestation Service. It relies on attestations and identity credentials rather than on vendors, portals, bilateral trust, or proprietary databases.

4.1 Identity credentials for all actors

The protocol provides a unified identity and credential layer for all actors in healthcare workflows. An identity credential represents a participant in the network. It anchors the identities of those authorised to act, to issue attestations, and to delegate authority to others. Credentials apply equally to individuals such as patients, caregivers, and researchers, to organisations such as hospitals, laboratories, NGOs, and insurers, and to machines such as AI agents, robots, and connected devices. Creating a credential incurs a small fee to cover network rent and execution, and is accompanied by a locked DHP commitment that represents long-term accountability.

4.2 Mandate credentials

The protocol separates the ability to act from the authority to act through mandate credentials. A mandate credential delegates authority by defining who is allowed to act, on whose behalf, for which actions, for what duration, and under which constraints. The principal is the individual or organisation that grants the delegation. The principal issues the mandate credential and designates one or more

authorised signers. Those signers may then issue attestations within the scope defined by the credential. Each such attestation is anchored to the mandate credential, so the chain of authority from the action to the delegated signer to the responsible principal can be verified in a single lookup.

4.3 Schemas

To ensure that attestations are interpretable across systems, organisations, and applications, the protocol introduces schemas. A schema defines the meaning of an attestation by specifying the type of action or state being claimed, the required and optional fields, the references to supporting evidence, and the verification expectations. Schemas act as shared and public definitions that make attestations reusable and comparable across contexts, such as vaccination records, weekly outcome reports, or device-generated measurements.

4.4 Attestations

At the core of the protocol is the ability to issue attestations, which are signed statements that an action or a state occurred. Each attestation answers three questions. What happened. Who claims it happened. Where applicable, who verified it. An attestation can reference a schema, a subject identity, optional off-chain evidence, and, where the action is delegated, the mandate credential under which it was performed. Attestations are immutable once issued, and they are revocation-aware, which means they can be invalidated without being erased. Attestations reference evidence through cryptographic commitments, while access control is handled off-chain. Raw healthcare data is never stored on the chain.

5. Major Applications of the dHealth Protocol

The protocol is domain-agnostic and supports many uses. Two applications are central to its current deployment and to its economics. The first is the mandate credential, which delegates revocable authority to humans, AI agents, and robots. The second is the attestation, with a focus on the QR-code attestation used to disseminate AI system prompts. Both applications share one economic mechanism, the Community Fund, described in Section 7.

5.1 Application One: Mandate Credentials

A mandate credential is the protocol's instrument for delegated and revocable authority. It records who may act, on whose behalf, for which actions, for what duration, and under which constraints. The credential is explicit, time-bound, revocable, and independently verifiable by any third party. Revoking the credential or removing an authorised signer immediately invalidates the delegated authority, so principals retain continuous control over actions performed in their name.

Mandate credentials apply across all actor classes. Individuals can delegate to caregivers, family members, or researchers acting on their behalf. Organisations can delegate to staff roles, partner institutions, or contracted providers. Machines, including AI agents, robots, and connected devices, may act and attest only under an explicit mandate credential issued by an accountable human or institution. The mandate credential is therefore the mechanism that lets an AI agent act on behalf of a patient, lets a robot perform a care or rehabilitation task, and lets an organisation operate under regulatory or contractual authority. By making authority a verifiable credential rather than an implicit property of key custody, the protocol keeps machine and institutional actions traceable to responsible human principals.

Creating a mandate credential is a Solana transaction and carries a fee in SOL. Additionally, the issuer contributes an equal amount of SOL to buy DHP on the open market for the Community Fund. The Community Fund mechanism is described in Section 7.

5.2 Application Two: Attestations and QR-Code System Prompt Dissemination

An attestation is a signed claim that an action or a state occurred. The application highlighted here is the dissemination of AI system prompts through a QR-code attestation. A healthcare provider or a sponsor configures an AI agent with a system prompt for one patient or for a defined cohort. The system prompt is hashed. An attestation records that hash. The attestation references a schema that defines the configuration type, the identity of the issuer, and the mandate credential under which the agent operates.

The QR code encodes the address of the agent, not the prompt itself. When a patient scans the QR code, the agent loads, and the system prompt that is served can be checked against the hash recorded in the attestation. A match shows that the prompt was the one the provider approved. The attestation, therefore, makes the configuration tamper-evident and independently verifiable. External parties such as the patient, the sponsor, an auditor, or a regulator can confirm the configuration without access to private data. This supports the position that the prompt is a configuration of a general tool rather than a separate device.

The attestation is immutable and revocation-aware. The provider can let the attestation expire, or can close it to recover the account rent once the QR code is retired. While a QR code is in service, the attestation should be retained so that scans can continue to verify the prompt hash against a live record.

Creating the attestation is a Solana transaction and carries a fee in SOL. The issuer also contributes an equal amount of SOL. That contribution is used to buy DHP on the open market for the Community Fund (see Section 7).

6. Participation Deposits and Fee Model

The dHealth Protocol requires all participants, i.e. humans, organisations, AI agents, and robots, to make a time-limited DHP deposit to participate. This deposit serves as a participation bond: it commits the participant to the protocol, anchors accountability, and creates an economic footprint behind every protocol action. Deposits are denominated directly in DHP, fully reclaimable after the lock period, and adjustable through governance. Sybil and spam resistance are reinforced not by the deposit alone but by Proof-of-Humanity verification, issuer-tier reputation, and the mandate-based authority chains described elsewhere in this paper.

Separately from the DHP deposit, every protocol action, such as onboarding, attestation, mandate, and schema registration, is executed as a Solana transaction and therefore requires SOL to cover the network fee. The smart contract additionally collects a fixed SOL surcharge routed to the dHealth operations pool, which funds account rent, ongoing protocol operations, and treasury-governed public goods.

6.1 Individual Participation

Individuals participate by locking 100 DHP for a minimum of 90 days. The locked DHP remains the individual's property and can be fully reclaimed once the lock period elapses, with a seven-day unlock

notice period. Withdrawing the lock immediately terminates the individual's participation. Maintaining the lock enables credential creation, receipt of attestations, and access to protocol workflows.

6.2 Sponsored Participation by Organisations

As an alternative to direct participation, an organisation may lock 100 DHP on behalf of an individual user. The DHP remains owned and reclaimable by the organisation, allowing the individual to participate without directly holding tokens. The sponsoring organisation also covers the SOL transaction fees and surcharges for the individuals' onboarding and ongoing actions. This model is intended for research studies, care programmes, NGO initiatives, and institutional onboarding, shifting both token and SOL costs upstream while keeping the friction of individual participation low.

6.3 AI Agents and Robots

AI agents and robots participate under a locked deposit of 50 DHP, maintained for at least 90 days. The deposit is locked by the responsible operator — typically a manufacturer, service provider, or owner — and ensures that machine actors operate under accountable economic constraints. The locked DHP is reclaimable after the lock period; unlocking terminates the machine's participation in the protocol. Operators are responsible for the SOL costs of their machine actors' transactions.

6.4 Organisational Participation

Organisations lock 10,000 DHP to participate in the protocol. This deposit enables organisations to:

- issue and receive attestations,
- sponsor individual users,
- operate AI agents and robots, and
- earn from protocol-mediated transactions.

The organisational deposit reflects the higher accountability and impact of institutional participation while remaining modest relative to real-world operating costs. This lock must be maintained for at least 180 days, and withdrawing it immediately terminates the organisation's participation.

6.5 Onboarding Fees in SOL

At the time of onboarding, the smart contract collects SOL to cover Solana account rent and setup transactions, together with a dHealth surcharge that funds the operations pool. Indicative onboarding fees are:

- Individual: 0.010 SOL
- AI agent / Robot: 0.010 SOL
- Organisation: 0.030 SOL

These amounts are governance parameters and may be adjusted in response to changes in Solana network costs or SOL price. Sponsoring organisations may pay these fees on behalf of individual users (see 6.2).

6.6 Design Rationale

The model achieves several objectives simultaneously:

- It introduces mandatory demand for DHP without creating large financial barriers.
- It creates time-bound economic commitment that reinforces accountability.
- It allows organisations to sponsor individuals, keeping the system accessible.
- It ensures that operational and infrastructure costs are covered in kind: SOL is collected to pay for SOL-denominated expenses, with no conversion or oracle dependency.
- It cleanly separates participation collateral (DHP) from operational costs (SOL).

Participation in the dHealth Protocol requires a reclaimable DHP deposit that scales by actor type. Humans, organisations, AI systems, and robots all participate under the same principle: commit DHP to act, reclaim it after participation. Fees are collected in SOL to cover Solana network costs and to fund the dHealth operations pool. In addition, creating a mandate credential or an attestation carries an equal SOL contribution from the issuer, which buys DHP on the open market for the Community Fund. All deposit amounts, surcharge levels, contribution ratios, and lock durations are governance variables and may be updated by community vote.

7. *The Community Fund*

The Community Fund is the shared economic mechanism behind the two major applications. It converts protocol usage into demand for DHP, and it puts the resulting value under community control.

7.1 Matching contribution at creation

Creating a mandate credential or an attestation carries a dHealth fee in SOL. At the same time, the issuer contributes an equal amount of SOL. The two amounts are equal by design. The contribution is used in full to buy DHP on the open market. The purchased DHP is sent to the Community Fund. Buy-side demand for DHP, therefore, scales directly with the number of mandate credentials and attestations created. The flow has four steps:

- An issuer creates a mandate credential or an attestation, pays the dHealth fee in SOL, and contributes an equal amount of SOL.
- The protocol uses the contribution to buy DHP on the open market.
- The purchased DHP is deposited into the Community Fund.
- DHP holders direct the fund through proposals, as described in Section 7.2.

7.2 Governance of the fund: grow or burn

The Community Fund holds DHP and is governed by DHP holders under the protocol's voting rules. The fund does nothing on its own. Every outflow requires an approved proposal. A proposal falls into one of two categories.

- **Grow.** A proposal can allocate fund DHP to projects and actions that bring new users to the protocol. Eligible uses include onboarding programmes, partner integrations, adoption campaigns, sponsored cohorts, and contributor grants that expand participation.
- **Burn.** A proposal can permanently remove fund DHP from circulation. A burn reduces total supply and returns the captured value to all holders in proportion to their holdings, rather than directing it to a specific initiative.

Both categories use the same process. A holder submits a proposal that names the category, the amount of fund DHP, and the intended use or the burn. The community reviews it during an open period. DHP holders vote. An approved proposal passes through a timelock before execution. The fund then disburses to the approved recipient, or it executes the burn on the chain.

7.3 Interaction with supply

DHP carries 2% annual inflation and no hard cap, as described in Section 10. The Community Fund works in the opposite direction. The matching contributions create continuous buy-side demand, and governance can vote to burn part of the fund. A burn permanently removes supply and offsets inflation. The net effect depends on the volume of mandate credentials and attestations. At low volume, the effect is small and the 2% inflation dominates. As volume grows, the SOL flowing into DHP buys grows with it, and community burns can match or exceed annual inflation. Net supply can then move toward flat or deflationary. The mechanism ties the supply trajectory of DHP to real protocol usage rather than to a fixed schedule.

7.4 Considerations

The mechanism is deliberate, and several constraints apply:

- The matching contribution doubles the SOL cost of creating a mandate credential or an attestation. This is an intentional cost. It converts protocol usage into DHP demand and into community-governed value.
- The protocol matches its own dHealth fee. The base Solana network fee is paid to validators and is not part of the contribution. Account rent is handled separately and is recoverable when an account is closed.
- Market buys must be executed with care. Concentrated buys can incur slippage on thin liquidity. Execution should use batching, time-averaging, or similar methods, all of which are governance parameters.
- The effect scales with use. At low volume, the contribution flow and the fund are small. The mechanism becomes economically meaningful only as adoption grows.

8. Application Areas

Beyond the two major applications, the protocol supports a range of real-world use cases. Insurers can enable outcome-based reimbursement based on verifiable actions rather than reported activity. Donors and NGOs can rely on outcome-linked donations, where funding is released only when agreed milestones are independently verified. Regulators gain tamper-proof audit trails that allow oversight without access to raw or sensitive data. Researchers can produce reproducible and verifiable evidence for transparent studies and cross-institutional validation. Individuals can participate directly through self-attestations, contributing verifiable records of actions or states such as data sharing or study consent. Across all of these areas, the protocol provides evidence of an action, not opinions, interpretations, or raw data.

9. Protocol Token Utility (DHP)

DHP is the protocol asset for participation, accountability, and governance, not day-to-day payments. Stable-value assets handle commerce and reimbursements. Only Solana-native DHP is canonical; wrapped tokens elsewhere do not govern or inflate.

9.1 DHP as access and membership

Locking DHP gates access to protocol-grade capabilities, including credential creation, higher-assurance features, and issuer-tier eligibility. Onboarding may be sponsored by clinics, insurers, or employers, so individuals are not required to buy tokens directly. Healthcare providers can reference a participant's level of accountability, reflected by their locked DHP, when granting access to specific services or workflows.

9.2 DHP and the Community Fund

The two major applications generate demand for DHP through the Community Fund. Each mandate credential and each attestation triggers a market buy of DHP. The community then decides whether that DHP funds user growth or is burned. DHP holders govern this decision, which links token utility directly to the use and the growth of the protocol.

9.3 Disputes and accountable issuance

Attestations can trigger downstream consequences, so their issuance may require stake-backed commitments. Bonded DHP provides an enforcement mechanism for disputes and penalties, including cases involving machine actors with real-world operational consequences.

9.4 DHP as governance and voting power

DHP governs schema upgrades, protocol parameters such as locks, tiers, and slashing, treasury spending, the Community Fund, and safety procedures. Governance is conservative and anchored to Solana to avoid fragmented legitimacy.

10. Tokenomics and Inflation

After the migration, Solana-native DHP has 2% annual inflation and no hard cap. The intent is predictable long-horizon funding and incentives aligned with productive participation. Inflation is not passive yield. The Community Fund mechanism in Section 7 operates alongside inflation as a usage-linked counterweight.

10.1 Supply policy

The initial supply after migration is 1,850,000,000 DHP. The protocol targets a constant annual growth rate of 0.02. Supply grows as $S(t) = S(0)(1 + r)$ raised to t, with r equal to 0.02. Inflation is emitted quarterly to preserve the same annualised rate. Issuance is controlled and predictable despite the absence of a hard cap. Community Fund burns reduce supply against this baseline.

10.2 Productive distribution

Protocol inflation is distributed quarterly and allocated only to active participants. The annual amount is split into four equal quarterly tranches. Each tranche is divided into two equal parts, one for individuals and machines, and one for organisations. The allocation to individuals and machines is weighted by verified activity during the quarter, measured by the number of attestations associated with the participant. The allocation to organisations is weighted by the number of attestations issued or verified and by the number of individuals onboarded. The precise weightings, the eligibility thresholds, and the lock durations are protocol parameters subject to community governance.

10.3 Canonical inflation and governance on Solana

Solana is the canonical chain for protocol state, governance, and inflation. The Solana-native DHP state defines all authoritative locks, tier bonds, and inflation eligibility. Governance rights derive solely from Solana-native DHP. Any wrapped or bridged representation on other chains is explicitly non-canonical. Such representations may improve access and liquidity, but they remain fully backed by Solana-native DHP and do not fragment supply, governance, or protocol integrity. Inflation is minted only against the Solana-native supply. The Community Fund and its burns are also settled on Solana.

11. Governance

Governance is treated as a safety system. It changes rules that affect privacy, authorisation, dispute procedures, tier definitions, and token parameters. Solana is the single source of truth. Wrapped tokens do not vote or define canonical locks. Governance uses timelocks for review and includes constrained emergency controls for severe vulnerabilities. Issuer tiers and machine constraints are governed to preserve the human-first principle, so machines act only under explicit and traceable authority.

11.1 Governing the Community Fund

The Community Fund is governed by the same token holders and the same voting rules. Each outflow requires an approved proposal that either funds projects and actions that bring new users or burns DHP. The lifecycle is transparent: submission, an open discussion period, a vote by Solana-native DHP holders, a timelock, and execution. Treasury and fund spending support the growth and the maintenance of the protocol, and the community decides the balance between funding growth and reducing supply on a case-by-case basis.

12. Conclusion

The dHealth Protocol is a trustless coordination layer for healthcare. It lets actions be proven without vendor databases, bilateral trust, or unverifiable documents. It reduces cross-institutional coordination to independently verifiable primitives. Identity credentials record who acts. Mandate credentials record under what authority. Schemas record what an attestation means. Attestations record what happened. Privacy is structural, since raw health data remains off the chain and integrity rests on cryptographic commitments and revocation-aware verification.

This version frames two of these primitives as the major applications. Mandate credentials delegate revocable authority to humans, AI agents, and robots. Attestations record verifiable actions, and the QR-code attestation disseminates AI system prompts in a tamper-evident and independently verifiable way. Both applications share one economic mechanism. Creating a mandate credential or an attestation carries a fee in SOL, and the issuer contributes an equal amount of SOL that buys DHP for the Community Fund. The community then votes to fund projects and actions that bring new users, or to burn the DHP and remove it permanently from circulation.

DHP remains the protocol's asset for participation, accountability, and governance, not a payment coin. Inflation is set at 2% annually on Solana-native DHP and is distributed only to active participants. Together, inflation and the Community Fund keep the supply and the incentives of DHP linked to real and verifiable protocol work.