

The DEPH chain

Technical Whitepaper · Version v0.5.7 · Oct 9, 2026

Draft. Architecture as intended, subject to independent audit and change.

Abstract

DEPH is infrastructure for consented human biological data. Each member holds a HealthID, a key bound to an encrypted vault. The vault is the member's: they own it, and they control who may use it. The vault contains the member's personal data records, stored encrypted, off the chain. The chain does not store that data. Permission to use that data is a programmable grant, evaluated only inside DEPH. The member uses that grant to admit a researcher's request, or to run a calculation on their own vault for their own use, such as a report. Computation runs on admitted DEPH nodes: confidential virtual machines that prove they are running a named, auditable image. Raw records never leave those nodes. What leaves a job is an aggregate or other attested result. Those nodes checkpoint a public head, the latest published hash of DEPH state, so history cannot be silently rolled back.

1 Why this exists

Health AI has three inputs: compute, models, and data. Compute can be rented by the hour. Anyone who can pay can get more of it. Models are becoming available the same way. A trained model can be copied, licensed, or published. A new one can be trained on that same rented compute. Compute and models are commoditising: they are widely available, and having them is no longer the hard part. Data is the hard part.

What is scarce is consented biological data measured on the same people over time. A single test is a snapshot. A useful record is a timeline: the same person, measured again, with permission at every step. That kind of data is usually held as a platform hoard. The people it describes hold no meaningful rights over it. When a large consumer genomics company entered bankruptcy, the genetic database was treated as an asset of the estate. The people described by that data had no say and no claim.

DEPH replaces the hoard with a vault. Each member holds a HealthID, a key bound to an encrypted vault. They own it, and they control who may use it. A member's permission is a grant, and DEPH's own program is what checks it. A record is unlocked only when that grant is live, and only into an admitted DEPH node: a confidential virtual machine that has

proven it is running the named, auditable image. The record is meant to survive the operator. A public head, the latest published hash of DEPH state, makes silent rewrite of DEPH history visible. A member's data is never stored on the chain.

Applications that write into a HealthID vault are clients of this layer.

2 The DEPH chain

The DEPH chain is a confidential application with a public head. It is not a general-purpose public smart-contract chain. Each DEPH node is a confidential virtual machine (CVM) on Secret Network, the shape that stack uses for apps, dapps, and chains. Consent, unlock, and jobs run on those nodes. DEPH checkpoints to the Secret L1 by posting a public head, the way a layer 2 checkpoints to Ethereum. The head is a hash of DEPH state, posted so history cannot be silently rewritten.

The chain is the control plane. It does not store a member's data. Records are stored encrypted, off the chain. The member controls the access list and delegates by grant: who may use which data, for what, and for how long. The public head is a hash of that control-plane state, checkpointed to the Secret L1. DEPH holds grants, job control, and the unlock path. It does not hold the records.

2.1 The path

Follow one use. A member holds a HealthID key and a vault bound to it. They set a grant: who may use the vault, for what, on which data, and for how long. A party posts a job. The DEPH image checks the grant. The job runs on a node, a CVM, and only while that grant is live. Key material reaches only an authorized machine. The party receives a result. The record stays in the vault. The node checkpoints a public head so this history cannot be silently rolled back.

The running node, the release of key material, and the result are attested. They belong to the named image.

Who	What they do
Member	Holds the HealthID key and the vault. Sets grants.
Client	An application that writes into a vault or posts work. It takes a grant, or it does not run.

Who	What they do
Party	Who the grant names. Often an institution. Posts a job and receives a result, not raw records.
DEPH node	A CVM running the measured image. If a node fails, another can take over.
Storage host	Holds ciphertext. Does not decide unlock.
Confidential KMS	On the Secret side. Releases key material only to an authorized machine.
L1	Control plane only. Holds the public head and the measurement hash of the named image. Does not hold user data.

Figure 1. Who takes part in one use. Key release and results are attested to the named image.

2.2 Three places

User data is not on the chain. The records are stored encrypted, off the chain, under an access list the member controls. Plaintext is used inside a DEPH node, for a job, under a live grant. The public head is a hash, not the records.

Place	Holds	Does not hold
Public head	A hash binding vault commitments and the grant store. The anchor a replacement node continues from.	Biology, identifiers, grant text, query inputs, results.
DEPH nodes	Grants. Job control. Unlock. Ephemeral working copies while a job runs. The measured DEPH image.	Durable user data. The chain does not hold the records.
Encrypted vaults	Ciphertext of a member's biological record, addressed under their HealthID.	The unlock decision. That decision is DEPH's.

Figure 2. Where state lives. The public head is a hash. Consent is not listed on it.

2.3 What the public head is for

Encrypted storage at rest is confidentiality of bytes, not freshness. A host can restore an earlier valid ciphertext image. The public head is the monotonic anchor against that rollback. A replacement node loads the encrypted vaults and continues from the public head. Failover is that self-heal. History already checkpointed is what it continues from.

The hash binds vault commitments and the grant store. It does not contain biology, grant text, identifiers, or results, and it does not enumerate grants, members, or jobs. An observer of the chain sees the control plane advance. They do not see the member's data, because that data is not on the chain.

2.4 The native token

\$DEPH is the native token. No traditional chain governance is enabled. A member governs their own data through grants.

2.5 Member contributions

Member contributions are tracked in the ledger. That record is stored off the chain, encrypted, with whitelisted partners. The member's reward is the token from the app they contributed to.

3 HealthID and the vault

One person, one HealthID, one encrypted vault. The member holds the HealthID key, and the vault is bound to that key. The vault holds the member's biological record as ciphertext: genomics, methylation, bloods, wearable streams, clinical notes, and whatever else the member contributes.

The chain-level object for a vault is a commitment: evidence that a vault exists and has not been silently substituted, without revealing its contents. The records themselves are not on the chain. They are stored encrypted, off the chain. The member controls who may be delegated access. The public head is a hash.

3.1 A substrate, not a single client

HealthID, the vault, and the grant/unlock path are a substrate. Other confidential applications may request access through the same grant path. They do not get a side door into the vault. They take a grant, or they do not run.

4 DEPH nodes

A DEPH node is a CVM running the DEPH application. It is not a block producer for a public consensus set. A node that has not attested the named image does not receive key material and does not run a job. Several nodes run the same measured image. The set is designed to self-heal if a node fails.

DEPH nodes are run by whitelisted partners. Who may run one is enforced by the protocol. There is no minimum stake to run a node, and nodes are not slashed.

4.1 The bar

- **Measured image.** A node runs a named DEPH image. The measurement of that image is the identity of the program. A different binary is a different image. Stripping audit or key-request capability changes the measurement and fails admission.
- **Attestation.** Before key release, the node proves it is running that image on an admitted CVM. A machine that cannot so prove does not decrypt.
- **Confidential execution.** Plaintext biology exists only inside the node, and only for records covered by a live grant, and only for the life of the job.
- **No durable plaintext.** At rest, vaults are ciphertext. Local disk is a cache, not the history. Working copies are ephemeral and are shredded when the job ends or is killed.
- **No user data on the chain.** Nodes may post a hash. They may not post records, grant text, or identifiers. The blockchain does not store the member's data.
- **Failover.** The system is designed to self-heal. If a node fails, another can take over from the public head. History already checkpointed is not rewritten by that takeover.
- **Grant-gated decrypt.** A node that is admitted but holds no live grant for a record does not receive that record's keys.

4.2 Failover

DEPH is designed to self-heal. If a node fails, another node running the same measured image can take over. It continues from the public head, so history already checkpointed is not rewritten.

4.3 What a node must never hold

Forbidden	Why
Plaintext biology at rest	A disk image of a node must not be a copy of the dataset.
Vault keys on the public head	The head is a hash. Keys are released into admitted nodes under policy, not published.
Decrypt without a live grant	Admission of the image is not permission to read a member. The grant is.
Keep a working copy after job end or kill	Ephemeral decrypt is for the job. Teardown shreds it.

Figure 3. Node prohibitions. These are protocol rules, not operator policy.

4.4 Audit-friendly image

The DEPH image is intended to be independently auditable. Verifying DEPH means verifying that a node is running that named image. The measurement hash is published on the L1 beside the public head. An independent party compares the node's attestation to that hash and can check the code path.

5 Programmable consent

Permission, work, and key release are three objects. The grant is the permission. The job is the work. Unlock is the release of key material that lets that job run.

Permission to use a member's data is a grant object inside DEPH. It is not a setting in a consumer application, and it is not a record on the public head. Nothing runs against a vault unless a live grant covers the member, the purpose, the party, the time window, and the data classes the job needs.

Grants are programmable. The fields of a grant are the interface; the product choices that fill those fields — a single study, a standing purpose class, a commercial licence — are applications of the same object.

5.1 The grant

Field	Meaning
Subject	The HealthID whose vault is in scope.
Party	Who may use the data under this grant (the institution or job principal).
Purpose	What the party may do. A grant for one purpose is not a grant for another.
Data classes	Which parts of the vault are in scope.
Window	When the grant is live. Expiry is a protocol event, not a reminder.
Job bind	Optional bind to a named job or class of jobs. Absent bind does not mean unbounded use; purpose and window still constrain.
Status	Live, revoked, expired, or superseded.

Figure 4. Grant fields. Evaluated only inside DEPH nodes.

5.2 Where consent lives

Consent lives in DEPH nodes. It does not live on the public head. The head commits to DEPH state as a hash, so a node cannot silently present a different grant store after the fact without failing the head. An observer who never talks to DEPH still cannot list who consented to what. That is intentional.

Verifying DEPH means verifying the running image. If the image is the audited program, grant evaluation is that program's logic.

6 Encryption and unlock

Vaults are encrypted at rest. Storage hosts see ciphertext. Key material is held apart from that ciphertext. On the Secret side, a confidential key-management service (KMS) releases it only to an authorized machine. Authorized, here, means a DEPH node that has attested the named image, and only for records a live grant covers. A storage host cannot make that release. That is the hinge between ownership and use.

6.1 The unlock sequence

- A job is posted. It names a party, a purpose, a window, and the data classes it needs.
- DEPH selects the cohort: HealthIDs whose live grants cover that job. Cohort membership is not written to the public head.
- The node attests: it is running the named DEPH image on an admitted CVM.
- For each in-scope record, the confidential KMS releases key material into that node. No attestation, no grant, no release.
- The job runs where the data is. Raw records do not copy out.
- Results leave as aggregates or other attested artifacts bound to that job.
- The working copy is shredded when the job ends, expires, or is killed.

If attestation fails, if the image is not the admitted measurement, or if the grant is missing, revoked, or expired, unlock does not happen.

6.2 What encryption does and does not do

Encryption of the vault means a storage host, and an observer of the public head, do not see biology. It does not mean a DEPH node that has justly received keys cannot read the records those keys open. Unlock is deliberate decrypt under a grant. The privacy property for institutions is that they receive results, not that the node is blind to the data it is allowed to compute on.

7 Institutional jobs

An institution does not download a consented dataset. It posts a job. The job runs on DEPH nodes against the cohort whose live grants cover it. What the institution receives is an aggregate or other attested result. Raw records do not copy out. That is how a large consented cohort is used without becoming a bulk export.

7.1 One job

A member's vault holds bloods as ciphertext. They grant an institution a purpose, that data class, and a window. The institution posts a job for that purpose and that class. DEPH selects the HealthIDs whose grants are live. The node attests the named image. The confidential KMS releases key material only to that machine. The job computes inside the node. The institution receives an aggregate. The working copy is shredded. When the window ends, a further job under that grant does not unlock.

7.2 Access at scale

Scale is the size of the covering cohort, not the size of a file transfer. A job over ten thousand consented vaults hydrates and computes inside DEPH. The institution sees the result of that computation. It does not see ten thousand records.

Cohort selection happens inside DEPH, where grants live. The public head does not publish who matched. An institution learns that a result was produced under grants, not the HealthIDs of the cohort, unless a result type that the grant allows is itself identifying — in which case the grant must have allowed that result type. The default result is aggregate.

7.3 When the contract ends

A research contract ends in protocol when its grants expire or are revoked. Then:

- Further key release for that party and purpose fails.
- Any in-flight job under those grants is killed.
- Working copies in the node are shredded.
- The institution cannot start a new job on that cohort under the dead grant.

Already-emitted results remain. A model already trained under the grant remains. The protocol ends access to the vaults. It does not unsay a published aggregate or a model that has already left.

8 Revoke and erase

8.1 Revoke

A member withdraws a grant. Status becomes revoked. Future unlocks that depended on that grant fail immediately. Any in-flight job that unlocked under it is killed, and its working copy is shredded. Already-emitted results of that job stay.

Revoke is not retroactive against published output. It is retroactive against the running node: the job does not get to finish.

8.2 Erase

A member destroys their vault. The protocol does three things:

- **Crypto-shred.** Keys for that vault are destroyed so remaining ciphertext is unreadable under this design.

- **Tombstone.** The vault is no longer served. Jobs cannot unlock it. The HealthID is retired and is not reused.
- **Deletion request.** Storage hosts are told to garbage-collect the ciphertext. Honest hosts delete. The protocol cannot prove that a hostile host has done so.

The public head still contains hashes from before the erase. Those hashes are not biology. They do not restore the vault once keys are shredded.

8.3 What may remain

Erase and revoke stop future access. They do not undo every consequence of past use:

- **RAM.** A node that already decrypted under a then-live grant had plaintext in working memory. Kill and shred end the job. They do not un-see that interval.
- **Published results.** Aggregates and attested artifacts already emitted remain with the party who received them.
- **Trained models.** A model already produced under a grant remains. DEPH has no kill switch for it.
- **Retained ciphertext.** A hostile storage host may keep bytes. Without the shredded key those bytes should be unreadable. That is a cryptographic claim, not a proof of physical destruction on someone else's disk.
- **Genetic re-identification.** DNA data cannot be fully anonymised. Running the job where the data lives is how DEPH avoids handing over records. It is not a claim that an aggregate can never be identifying if badly specified. Result types must stay aggregate unless the grant says otherwise.

9 Auditability and verification

DEPH is designed to be audit-friendly without putting user data on the chain.

- **Named image.** The program that evaluates grants and runs jobs is a measured image. Independent audit of that image is how the logic is inspected.
- **Attestation.** A live node proves it is running that image. Verifying DEPH is verifying the code that is running. The measurement hash of the named image is published on the L1 beside the public head.
- **Public head.** A hash binding vault commitments and the grant store, so a node cannot silently roll history back. It does not contain biology, grant text, identifiers, or results.

An auditor who verifies the image and the attestation knows which program is evaluating consent. They do not, from the public head, receive a list of grants. They do not receive biology. That is the intended split: inspect the code path in the open; keep the records in the vault.

10 Glossary

Term	Meaning in this paper
DEPH chain	The control plane: consent, grants, jobs, and the public head, run on CVMs. It does not store user data. Not a general-purpose public contract chain.
CVM	A confidential virtual machine. Each DEPH node is one.
Public head	A hash checkpointed to the L1. It binds vault commitments and the grant store. It does not contain biology, grant text, identifiers, or results.
DEPH node	A CVM running the measured DEPH image. Not a public block producer. The set is designed to self-heal.
Measured image	The named DEPH program. Its measurement hash is published on the L1 beside the public head.
HealthID	A key the member holds. One encrypted vault is bound to it. Retired on erase, not reused.
Vault	The member's encrypted biological record, stored off the chain and bound to their HealthID. Not stored on the blockchain.
Grant	The member's access list. They set it and use it to delegate: subject, party, purpose, data classes, window, status.
Unlock	The confidential KMS releases key material into an authorized node for records a live grant covers. No attestation, no grant, no release.

Term	Meaning in this paper
Job	A computation posted by a party, run on DEPH nodes against the covering cohort. Results leave; records do not.
Working copy	Ephemeral plaintext inside a node for the life of a job. Shredded on end, expiry, or kill.
Crypto-shred	Destroy vault keys so remaining ciphertext is unreadable under this design.
Confidential KMS	On the Secret side. Releases key material only to an authorized machine: a node that has attested the named image, under a live grant.
\$DEPH	The native token. No traditional chain governance is enabled. A member governs their own data through grants.
Contribution ledger	The record of a member's contributions: samples, tests, questionnaires, check-ins and lifestyle data, and the use of their data under a grant. Stored off the chain, encrypted, with whitelisted partners. The member's reward is the token from the app they contributed to. Scoring and settlement are specified in the token paper.

Figure 5. Terms of art used in this paper.