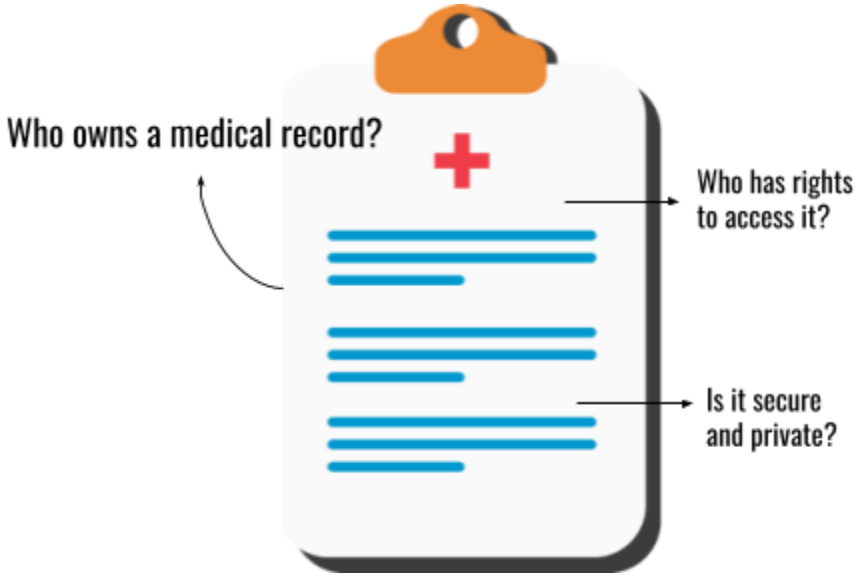
Hippr - “The Hippocrades Protocol”

White Paper: User-Centric Decentralized Health Exchange System

David, D.; Tubig, J.
www.hippocrades.org



Abstract

Who owns a Medical Record? Who has the rights to access it? How does it remain secure and private? The **Hippocrades Protocol (Hippr)** addresses these. It allows users - patients, health providers, and health facilities to manage and audit their medical records while making them shareable and interoperable in a decentralized, secure, private, and permissionless health information exchange (HIE). This framework of interoperability without compromising privacy and security set in smart contracts allows execution of major use cases which were previously very difficult to resolve. Ultimately, Hippr protects users’ access rights to data, promotes transparency, and even creates opportunities and rewards that benefit everyone in the healthcare ecosystem.

Hippr operates with other Hippocrades components that provide healthcare infrastructure, applications, and health APIs utilizing zero knowledge techniques for a truly comprehensive approach. A separate white paper on Hippocrades platform can be read here.

About Hippr

Hippr (Hippocrades Protocol in Blockchain) is a permissionless, autonomous system of smart contracts that allows users to have control of their medical records to be shared and be interoperable in a decentralized health exchange.

Having a consent to share their data not only provides complete privacy, but it also gives them discretion to share their anonymized data to participate in different research studies (and other data-driven activities) to contribute and even profit from it.

Hippr would be open sourced and would be running along with Hippocrades[1] health infrastructure (see About Hippocrades below) that provides healthcare applications and APIs allowing any players in the healthcare ecosystem to easily participate in the protocol.

The meat of the protocol is powered by BerryPied, a generalized IAM layer developed alongside Hippr, which also offers authentication, authorization, access control, delegation services, verifiable credentials, and generic resource access management.

About BerryPied

BerryPied is an Identity and Access Management (IAM) platform optimized for blockchain. It is also being built by the same team from House of Hippocrades (HOH) but will be run independently. Hippr will be utilizing BerryPied's identity framework and processes. It will be published as open source.

[1] Hippocrades website - www.hippocrades.org

About Hippocrades

Hippocrades is the Web 3.0 infrastructure for health information. Its primary purpose is to be a platform for interoperability and health data exchange among different information systems in a secure and decentralized setup, made private by zero-knowledge proofs.

Inside Hippocrades is (1) Curie - a set of health applications and (2) Fleming - a comprehensive set of secured APIs + zero knowledge. Hippr is designed and built with these two modules in mind.

Hippocrades' intention is to be a Decentralized Autonomous Organization (DAO). It will be managed by people around the world who hold its governance token, HIP. A certain percentage will be specifically allotted for people from healthcare. HIP holders, through a system of scientific governance, will manage Hippr to ensure its security, privacy, auditability, and interoperability. Holders can stake their tokens in order to vote, the number of which is proportional to their voting weight.

About the House of Hippocrades

The House of Hippocrades (HOH) is the same team that built the Hippocrades health infrastructure and is currently working on Hippr.

The team will be working with outside partners and the Hippocrades community to bootstrap the decentralized governance. It will ultimately be driven towards complete decentralization.

I. Introduction

A patient goes to a clinic for a check up. A doctor looks at her, provides a diagnosis and issues a prescription. This information, a medical record of the patient, is inputted in the health information system of the clinic.

In this scenario, which happens millions of times, many questions arise.

Who owns this medical record? The patient? The doctor? Or the clinic? If there are other doctors in the clinic, do they have the right to access the record? What about the medical staff, up to what extent do they have access to the information? If the sensitive health data is shared accidentally, or has been accessed by another without permission, how does the patient know about it? Can a patient have an audit trail of all those who accessed her medical records? What if a patient needs the record to be shared with another health facility? How can it remain private and secure?

These are just a few of the many ongoing concerns and issues with regard to rights to medical record access. For a long time now, despite the availability of health systems and information exchanges, even in developed countries, there have been more failures than successes in addressing these.

Fortunately, there have been advances in blockchain and zero-knowledge cryptographic protocols that can help finally resolve these challenges, a major one is the holy grail of healthcare data - on how to make them shareable without compromising its privacy.

Through a permissionless, autonomous system of smart contracts, immutable rules can be set up to give rights and access to certain users while keeping the data private, secure, and auditable. These smart contracts of medical records access and management are what constitute Hippr.

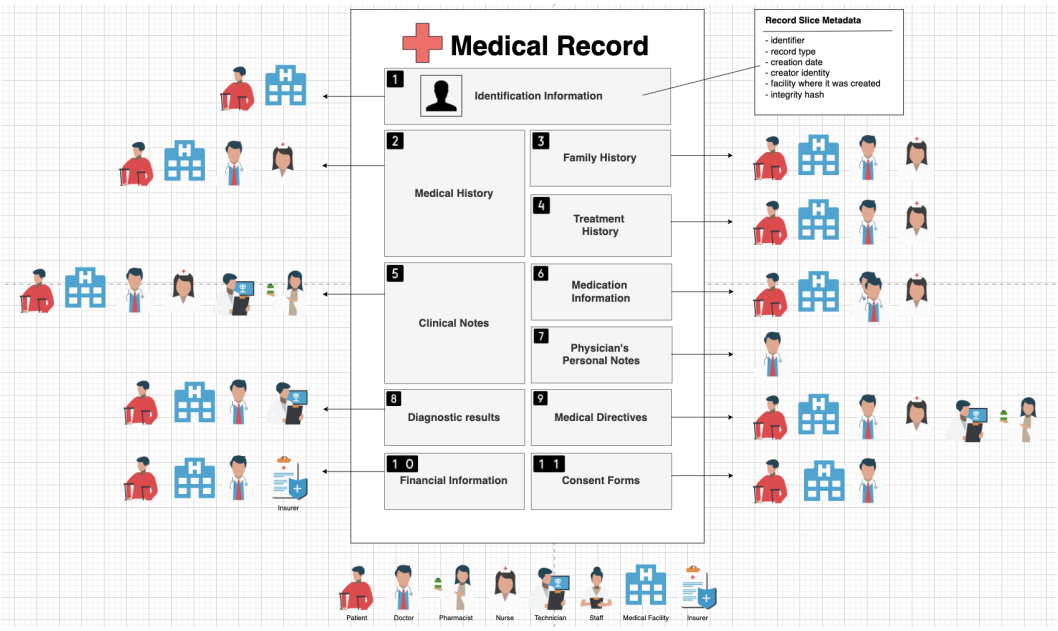
However, Hippr alone would not suffice. Health systems that would integrate with Hippr should be using industry-standard setup. And not all health systems currently being used are utilizing such, many in fact are still using legacy systems and not compliant. Even worse, not all health providers already have health systems in place.

As such, a healthcare tech infrastructure is also needed that could provide the needed health applications and health APIs. This is what the Hippocrades infrastructure is for, it has Curie apps and Fleming APIs. For those who do not have a health information system in place yet, Curie has ready-made solutions available. While Fleming’s APIs are provided for

those who already have systems and just wish to utilize Hippr via the provided endpoints. Details can be seen in the Hippocrades white paper.

Thus, the Hippocrades infrastructure is a critical component prior to building Hippr. This infrastructure is now built and in continuous optimizations since 2016. Building Hippr will finally address the medical record access concerns and unlock data privacy and interoperability challenges.

II. Medical Record Anatomy



*click here for an enlarged image

A medical record is potentially generated from numerous sources—doctors, clinics, diagnostic centers, hospitals and so on. With this happening on a daily basis, confusion can easily arise about who has the right to access and share a medical record, among others.

Legislation regarding data privacy continues to be enacted worldwide. For example, GDPR revolves around a person's right to be informed, right of access, right to rectification, right to erasure/to be forgotten, right to restrict processing, right to data portability, right to object and rights in relation to automated decision making and profiling[2].

[2] GDPR = https://gdpr.eu/what-is-gdpr/

Naturally, these laws significantly impact how data should be handled in the medical sector which has been leaning towards a common direction: empowering the patient to exercise their rights over their records.

To define these rights, it is best to dissect a medical record in detail.

Rights

Who owns a Medical Record? A doctor creates one, but the sensitive information is personal to the patient. Other players such as the hospital nurse can also add more data in the record and so on.

So a simple answer is that no single entity owns it. Depending on the case, different players can have varied rights and privileges to access, edit, delete, and share. There are a myriad number of rights that should be determined and managed. Based on existing standards and practices, Hippr attempts to define each player, their roles, and corresponding rights which will then be concretized as smart contracts in the blockchain as the Hippocrades Protocol, or Hippr.

The following are the defined Rights:

- **Create**. User can create a record.
- **Read**. User can request a record.
- **Edit**. User can update a record. *The resulting integrity hash from the updates will be posted and accepted in the blockchain.*
- **Delete**. User can delete a record. *All stakeholders that have delete access must agree to delete before action is executed.*
- **Share: Grant access**. User can provide access to a record. *Either temporarily or permanently.*
- **Share: Revoke access**. User can remove access granted to another user.
- **Share: Sell access** User can share to contribute or for profit purposes. *All stakeholders must agree to sell before a record could be posted for sale in the marketplace.*

Stakeholders

Patient and Healthcare Providers

- **Patient**. As medical records are ultimately about the patient, she should naturally have the rights to access to her medical records. This is also supported by regulations like HIPAA which gives a

person the right to inspect, review, and receive a copy of your medical records[3].

- **Patient Representatives**. When a patient cannot, by herself, manage her medical records, she can give representative/s partial or full rights to handle her data.
- **Doctor**. As the primary producer of medical records' information, a doctor has rights to access to said information.
- **Pharmacist**. A pharmacist needs to know and verify a patient's medication in order to properly manage and dispense medications.
- **Medical Facility (clinic, hospital, etc.).** A facility where records are created can have access to a medical record. In addition, the staff within the facility can be given access as well (which can also be revoked) to certain components of the medical records.
- **Medical Facility Staff**. These users would have access to certain medical record components if they are employed within a facility and were given authorization to do so.
    - **Nurses**
    - **Technicians (Lab and Imaging)**

Managers and Healthcare Purchasers

- **Insurer (HMO)**. Health facilities need to prove to an insurance company that a patient had indeed availed of its services for reimbursement purposes and other insurance-related activities.

Healthcare Data Purchasers

Researchers and similar groups may need to collect useful data and analytics for certain purposes.

- **Insurance Companies**.
- **Pharmaceutical Companies**
- **Research Institutions**

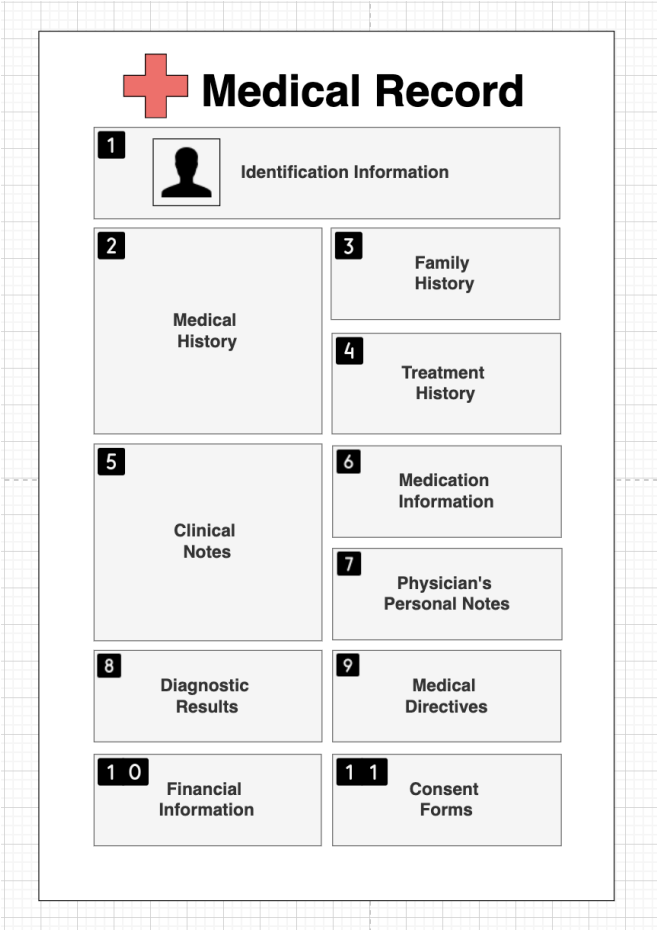
Government Regulators

Government units need data and analytics for better management, monitoring, and policymaking.

- **Government health organizations**

[3] Health Information Privacy - https://bit.ly/3rWAgIE

Components[4] of a Medical Record[5]



1. Identification Information

A medical record needs to have information to help identify who the health data belongs to. This identification information can include:

- Name
- Date of birth
- Marital status
- Social security number.

[4] The 10 Components Of Medical Records In A Hospital - https://bit.ly/3OIGohx
[5] The Medical Record - https://bit.ly/3vVWPOG

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x		x		x	x	x
Doctor	x				x	x	
Technician	x						
Nurse	x						
Medical Facility	x				x	x	

2. Medical History

A medical history is considered for everyone, even those who have never been to a doctor or hospital. This helps doctors understand whether an illness is chronic or acute, seasonal or situational. The history can include:

- Allergies
- Treatments
- Medical Care
- Present and past diagnosis

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x		x	x	x	x	x
Doctor	x	x	x		x	x	
Nurse	x	x	x				
Medical Facility	x			x	x	x	

3. Family History

A patient's family medical history may play an important role in their health as many health concerns are genetic. Some health problems of family members may not be worrisome, however, some hereditary diseases and cancers that may be passed down should be documented.

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x	x	x	x	x	x	x
Doctor	x	x	x		x	x	
Nurse	x	x	x				
Medical Facility	x			x	x	x	

4. Treatment History

A person's treatment history is another vital part of the patient's medical record. The treatment history encompasses all treatments they have ever undergone, and their results. Some of these include:

- Chief complaints
- History of illness
- Vital signs
- Physical examination
- Surgical history
- Obstetric history
- Medical allergies
- Family history
- Immunization history
- Habits including diet, alcohol intake, exercise, drug use/abuse, smoking etc.
- Developmental history

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x	x	x	x	x	x	x
Doctor	x	x	x		x	x	
Nurse	x	x	x				
Medical Facility	x			x	x	x	

5. Clinical Notes

Progress notes are made by physicians if changes or new information comes up during the course of the treatment. Some information included within these notes are:

- Bowel and bladder functions
- Observation of the mental and physical condition of the patient
- Sudden changes taking place
- Food intake
- Vital signs

Nurses maintain their own clinical notes. Often these are records of the patient's care that includes vital signs, particularly temperature (T), Pulse (P), Respiration (R), and blood pressure (BP).

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x	x	x	x	x	x	x
Doctor	x	x	x		x	x	
Nurse	x	x					
Technician	x	x					
Medical Facility	x			x	x	x	

6. Medication Information

The medicines a patient is ingesting need to be documented in their medical record as it could affect their course of treatment. Whether they have tried herbal remedies, illegal substances or OTC medication, everything should be included.

This information may be gathered through patient testimony or through prescriptions from past doctors already on file.

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x			x	x	x	x
Doctor	x	x	x		x	x	
Nurse	x	x					
Medical Facility	x			x	x	x	

7. Physician's Personal Notes

A physician's personal note regarding the patient's care plan or anything to help give the best care to her patient.

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Doctor	x	x	x	x	x	x	

8. Diagnostic Results

Different diagnostic results that the patient receives are all added to the record. These can be lab results related to cells, tissues or body fluids. Other reports such as X-Ray and imaging tests produced through mammograms, scans, x-rays and ultrasounds are all added as well.

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x			x	x	x	x
Doctor	x	x	x		x	x	
Technician	x	x	x				
Medical Facility	x			x	x	x	

9. Medical Directives

Medical directives are crucial documents to outline directions by the patient regarding what they want or do not want in the case they cannot communicate their medical care. These include the DNR, known as ‘do not resuscitate order, and their will.

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x				x	x	
Doctor	x	x	x		x	x	
Technician	x						
Nurse	x						
Medical Facility	x				x	x	

10. Financial Information

Financial information is also an important part of a patient’s medical records. This can be used to avail of insurance perks for patients as well as the facility be reimbursed by the insurance company.

Stakeholders and their Rights:

	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x						
Doctor	x						
Medical Facility	x	x			x	x	
Insurer	x						

11. Consent Forms

Patients should be able to make informed decisions about their care; thus the physician should let the patient know important information about all medical procedures. These include:

- Diagnosis
- Recovery chances
- Recommended treatment
- Benefits and risks of the treatment
- Risks if the treatment is not taken
- Success probability if treatment is taken
- Length of recovery time and challenges

Stakeholders and their Rights:

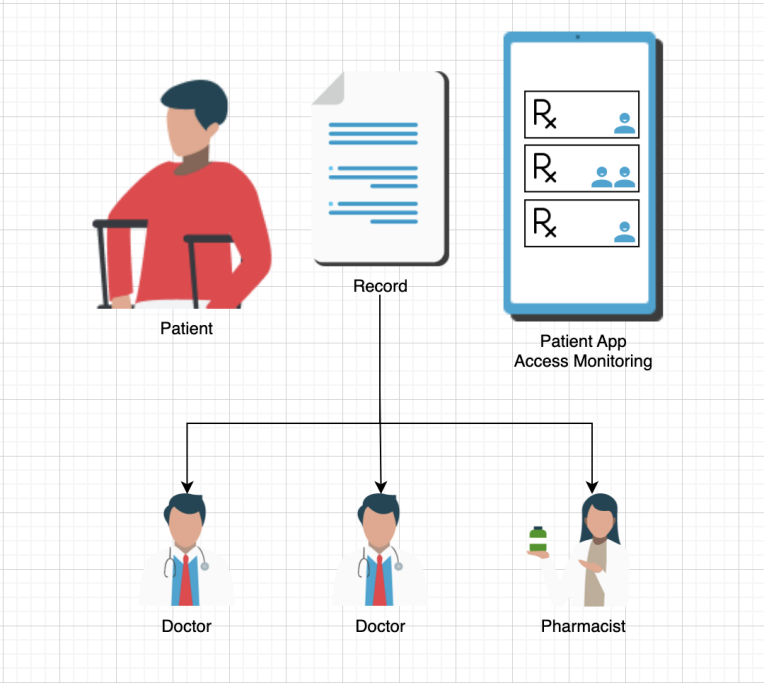
	Read	Create	Edit	Delete	Grant Access	Revoke Access	Sell
Patient	x	x			x	x	
Doctor	x						
Medical Facility	x				x	x	

III. Hippr's User-Centricity

Patient-Centric Model

Because of limitations in existing healthcare systems, current practice does not allow patients to have control of their medical records. Typically, patients' data is stored and managed in the health provider's information system for which patients mostly have zero access. While protected by data privacy laws, patients still have limited capacity to know if their information has been shared intentionally or accidentally.

Simply put, even if a patient has been provided an app to access medical records, the patient still has no idea if her data has been shared elsewhere or been tampered with.

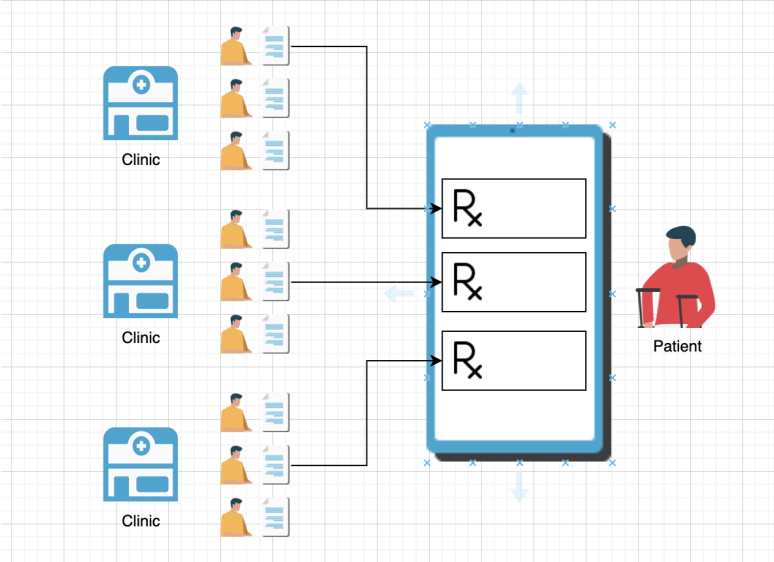


Essentially, as a doctor creates a record for a patient, as it is the patient's own health data, the patient must have rights and privileges over the record. A patient should be able to **AGREE**:

- **A**ccess medical records created by health providers
- **G**rant healthcare providers read access to their records
- **R**evoke healthcare providers' access
- **E**nable Audit if needed
- **E**ngage to Share health data to contribute or profit

Hippr has robust consent management policies to facilitate granting and revoking access via public records in the blockchain, strengthening the integrity, auditability, and trustlessness of the process. This is discussed further in the Records Access Management section below.

However, it must be recognized that the way records are created in practice is health-facility-based: doctors, nurses, and other healthcare providers all contribute to creating medical records for hundreds or even thousands of patients per day, accumulating to millions of records, all under the health facility and stored in the health facility's own information system.



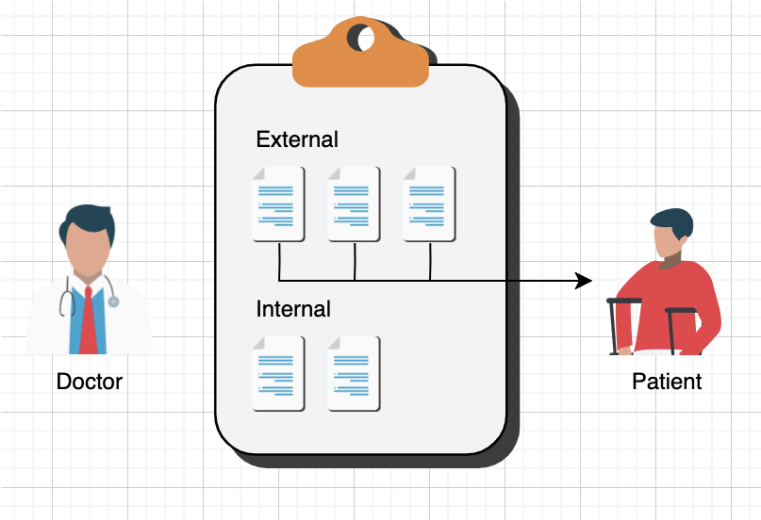
In light of this, it is expected that health providers will be the ones to bring medical records into the system en masse. There must exist a process by which patients prove their identity (via a credential issued by a trusted authority, e.g. a government ID or its decentralized equivalent), so that they may claim access to their records as digitized by the health facilities.\

Hippr addresses this directly by making use of a Decentralized Identifier (DID) for each patient. The credential issued by a trusted authority (in the above example, a government ID or its decentralized equivalent) is saved as a Verifiable Credential on the blockchain to attest to the patient's identity and allow them to claim record access rights.

User-Centric Model: Beyond the Patient

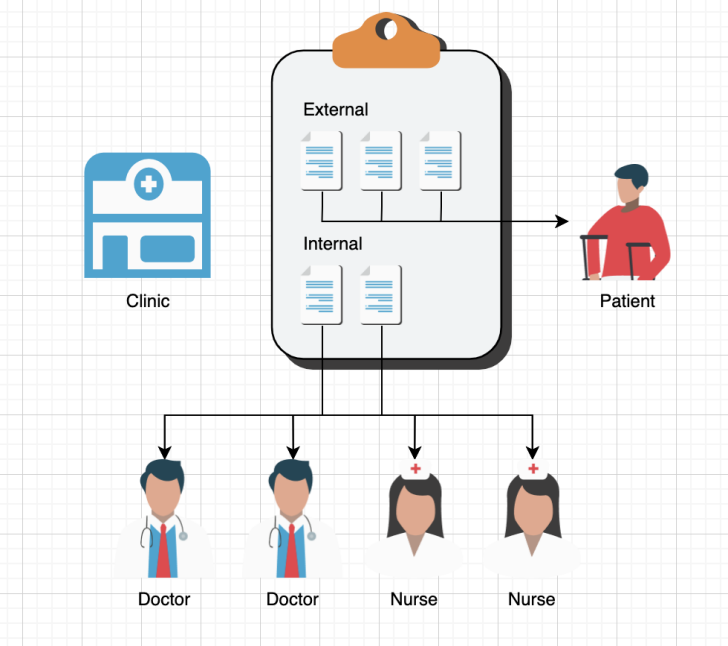
While the patient-centric model has been the long-heeded setup to empower patients with their health data, it must also be likewise recognized that certain records are created by doctors for their own understanding of the patient, and are not meant to be readily shared at the patient's demand.

These may include personal and technical notes that are of use by fellow doctors and providers, but can be dangerously misinterpreted by patients and other laymen (see **Medical Record Anatomy** section).



Because of this, the ideal record access framework must also recognize that doctors and other providers are also Users in this model and can also have rights over certain medical records.

In fact, legislation typically *does* recognize that these providers have rights and privileges for their records up to a certain extent.



In turn, health facilities must also be afforded the ability to acquire rights and privileges to access medical records (that is, to also be represented as its own User), in order to facilitate the generation, management, and

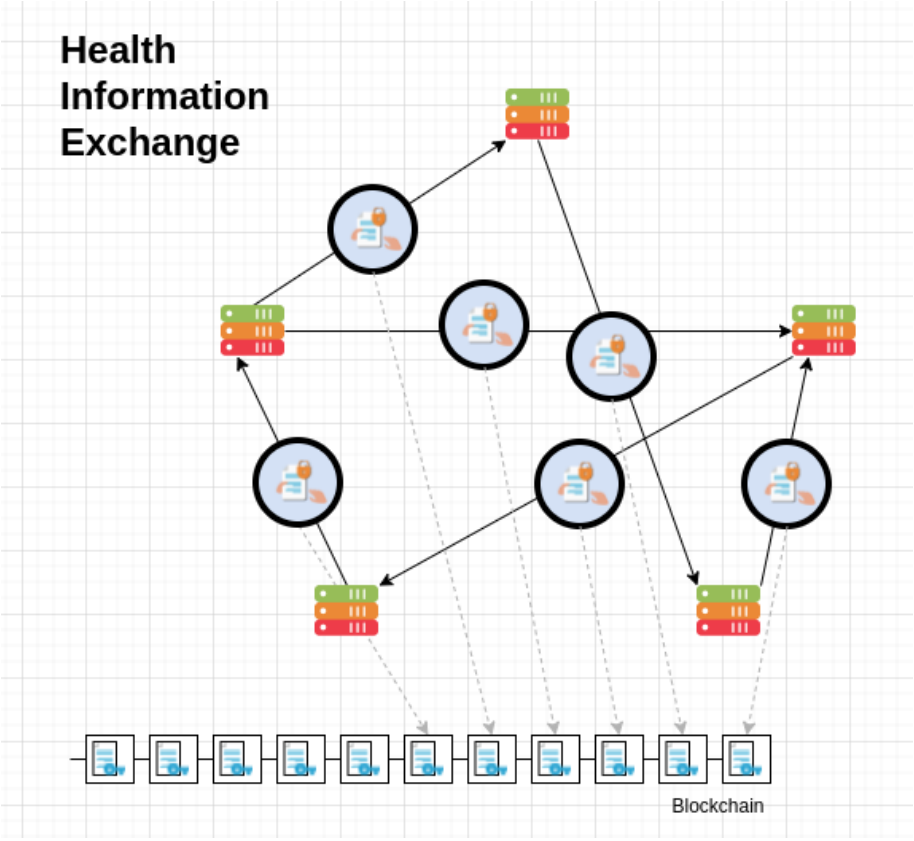
sharing of records within the facility that are needed by its providers in the course of a patient's care.

Imagine a patient admitted to a hospital who is examined by several doctors and nurses as part of bedside care: it is the hospital that ascribes access to different people, with providers being granted access to records by virtue of their being a member of the hospital.

To this end, the record access model of Hippr is ascribed to general Users — be it patient, providers, or health facility — and thus constitutes a User-Centric record access model.

IV. Hippr's Use Cases

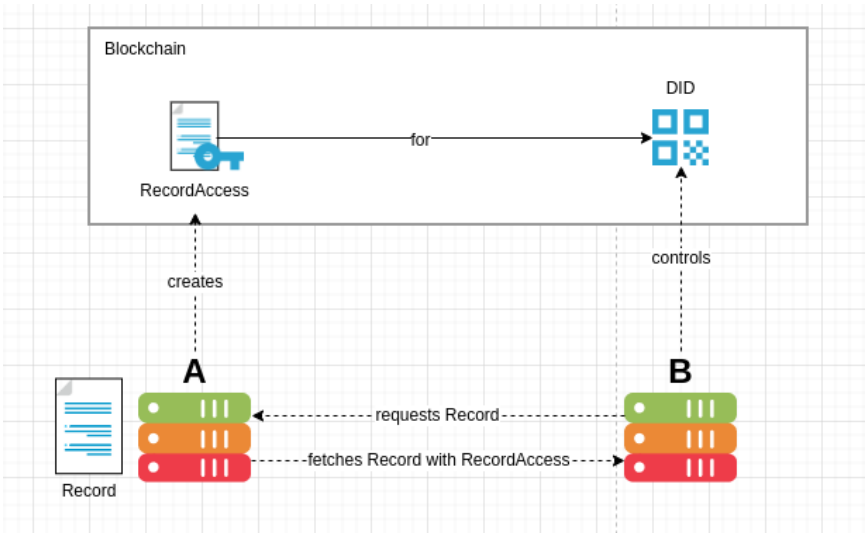
Health Information Exchange (HIE)



HIP's consent model plus Hippocrades' infrastructure setup provides the perfect recipe for a decentralized healthcare information exchange (HIE). The key difference with existing centralized HIEs is the utilization of smart contracts, blockchain, and zero-knowledge allowing safe sharing of health data without compromising privacy (see Hippocrades paper for details on how this works).

The actual medical records are not stored in the blockchain. Only zero-knowledge proofs are stored in the chain to confirm the validity of the medical record (as well as select metadata).

The actual exchange of data happens on the infrastructure level, facilitated by Hippocrades as directed by Hippr's record access consent model in the blockchain.

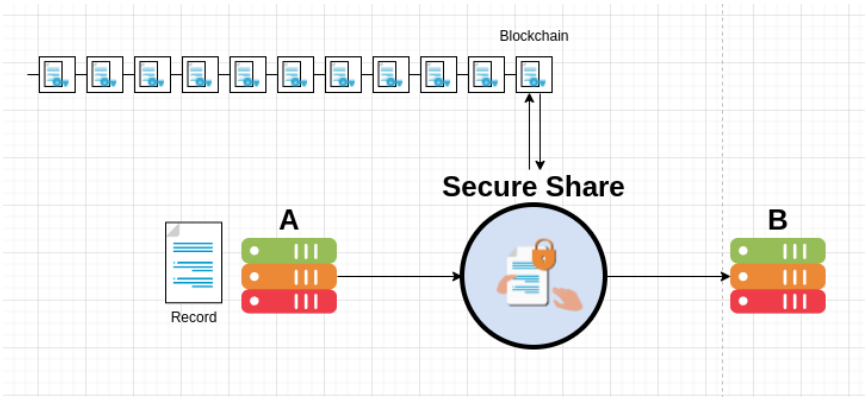


Hippocrades allows for distributed off-chain databases (Fleming instances) in which records are kept. Take two (2) deployments, A and B which are independently managed by two (2) health facilities. To move a record from A to B, a user in B can request a record saved in A. The user in A with the right to grant access then creates a RecordAccess transaction on the blockchain, which:

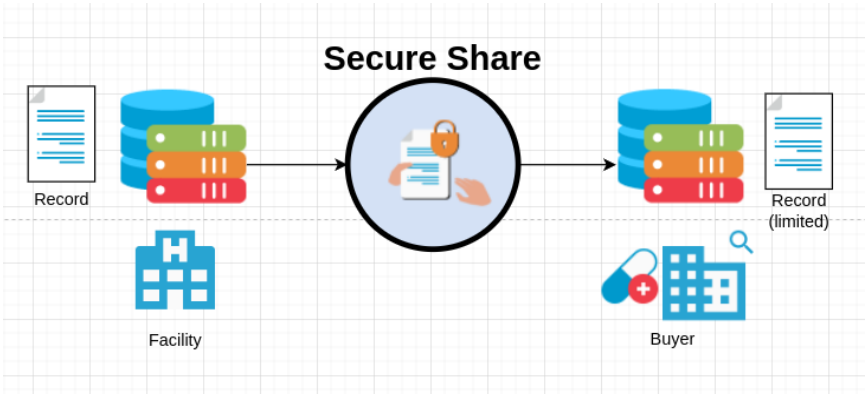
- signifies the consent to grant the user in B access (signed by user in A)
- contains zero-knowledge proof of the validity of the record
- contains access details (Fleming API endpoint URL in A, protected against unauthorized access)

The transaction itself is the blockchain ledger's record that consent has been given. B can then subsequently fetch the record from the off-chain database in A via the provided Fleming API endpoint. No record is shared

without consent explicitly being granted by the authorized entity. All proof of movements are saved in the chain thus all transactions are auditable.



This process is what is known in Hippr as a **Secure Share**. See the **Records Access Management** section below for a more detailed step-by-step.



Secure Share is the mechanism that gives rise to a truly decentralized Health Information Exchange: a persistent, auditable, trustless ledger of each exchange (% Hippr) and a network of decentralized, interoperable Fleming instances performing Secure Shares with each other (% Hippocrades infrastructure).

Medical Record Marketplace

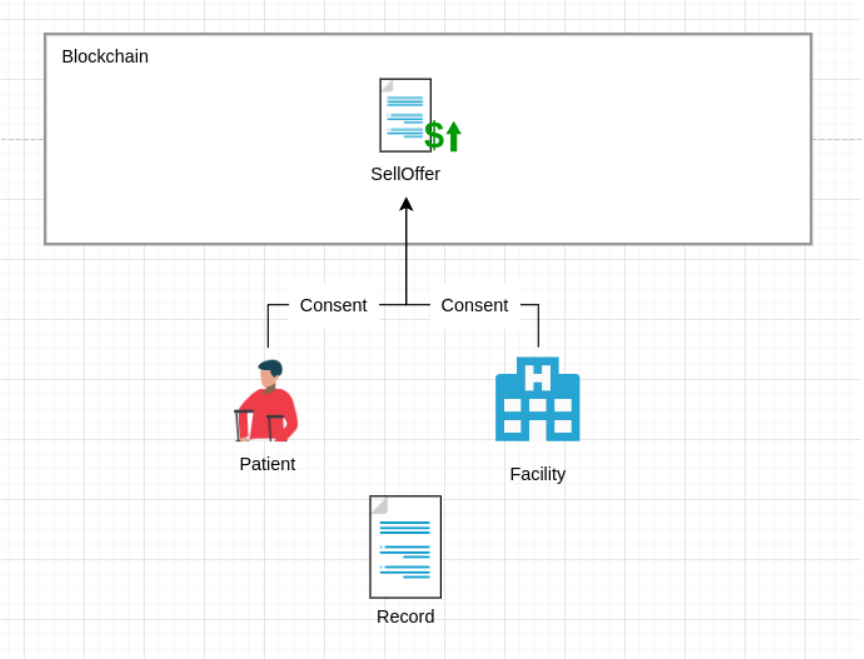
Once a user-centric record ownership and the HIE are in place, there is an opportunity to incentivize users, pharmaceutical companies, and research institutes by establishing a **marketplace for anonymized medical data** for research purposes.

There are important points in every sale on a marketplace for medical data:

a. Consent is required (especially from the patient!) before selling a record on the marketplace
b. The user buying the record must be able to determine the nature of the record being offered (e.g. what type it is, what general demographics the patient falls under, etc) without gaining access to the record prematurely
c. The buyer and the seller must reach an explicit agreement of sale
d. Once a sale is made, the buyer must gain access to the record, but only in an anonymized state

Each of these is addressed in Hippr.

Sellers: Record Stakeholders (Patients, Health Facilities)



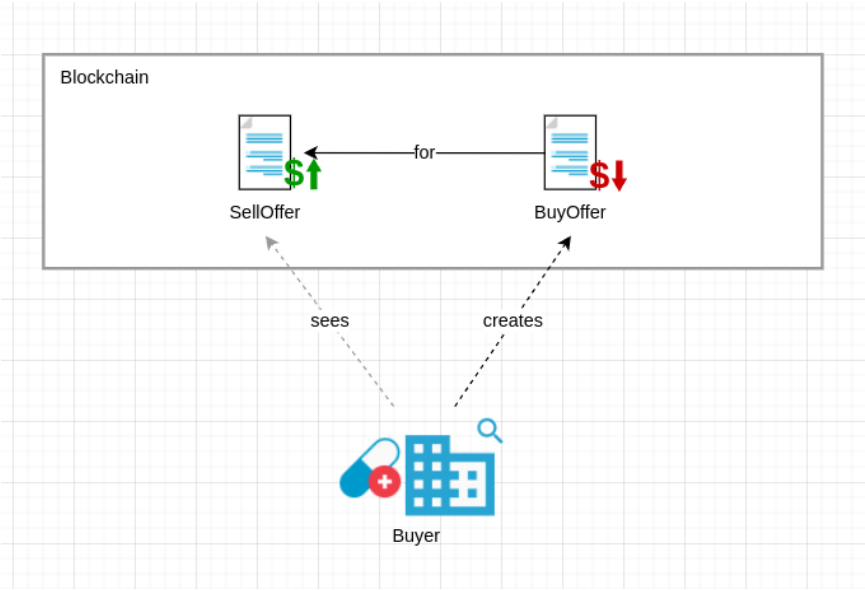
In order to start a sale process, both the patient and the health facility storing the record must consent and sign the sell offer before saving it on the blockchain.

Before Hippr, it is the health facilities that have the capability to sell off data en masse (since they hold the storage for the record), so the process can only be instigated by the facility. However, the sale can only ethically be done with the consent of the patient, which is why both of them must give their consent — in Hippr, this is done using signatures and the public key infrastructure.

The sell offer includes a zero-knowledge proof attesting to the nature of the record (e.g. type, patient age restrictions, etc) without leaking the record itself, so that potential buyers have the opportunity to assess whether the record can be useful for them.

Buyers: Pharmaceutical Companies, Research Institutes

Potential buyers such as pharmaceutical companies and research institutes can peruse sell offers and find records that fit their research profile (based on the limited information they have from the zero-knowledge proof within the sell offer).



Once a buyer identifies a sell offer they would like to buy, they simply create a buy offer that references the sell offer, as well as transfers an amount to cover the price. The price may eventually be regulated by Hippr (the organization, as well as eventually the DAO), as opposed to leaving to market forces due to a need to enforce fair valuation on patient's information.

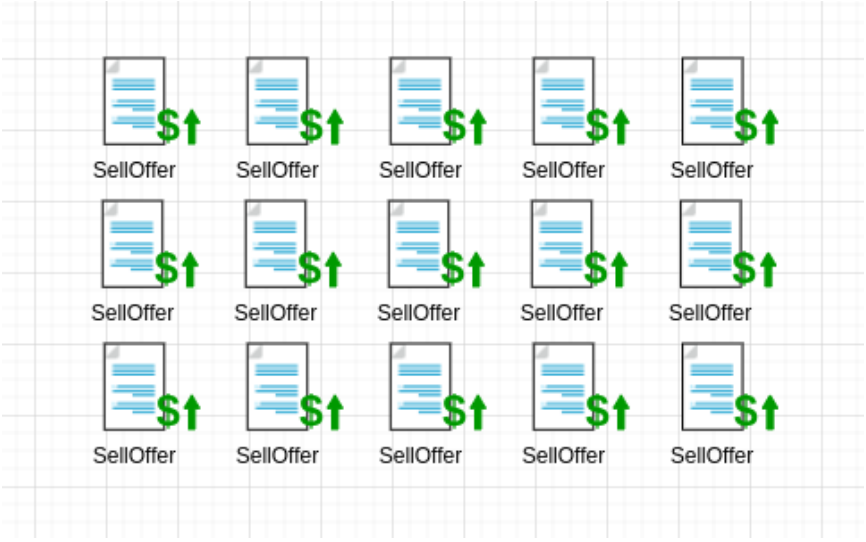
Once a sale has been reached, the transferred amount is split between the patient and the health facility, with a small transaction fee going to Hippr. The buyer then simply transacts a **Secure Share** to receive the record. The record is anonymized and limited in content by the intervening Fleming API.

Marketplace Proper

In practice, buyers and sellers will more likely be dealing with record sell offers in bulk. Hippr still allows for this, as long as each individual sale meets the criteria — most especially the patient's consent.

This marketplace is important because it incentivizes key players to engage with the protocol:

- Patients and health facilities are incentivized to transact with their records via the revenue from their sales
- Pharmaceutical companies and research institutes are incentivized to engage because the marketplace represents an evergreen source of research and business intelligence that is difficult to find elsewhere



Additionally, by charging transaction fees, the marketplace represents a source of additional revenue for Hippr as well (in addition to being a way to incentivize traction).

Medical Loans

Orthogonally, by virtue of Hippr working with tokens on the blockchain, Hippr can also (in the future) support loans for further developing the health industry (such as for the procurement of medical equipment, or the development of further healthtech solutions in the space, or later even for the construction of health facilities).

This is a use case that Hippr will further expound in the next version of this paper, as it requires the DES stablecoin and governance to already be established.

Users can generate DES stablecoins by staking collateral assets (at the discretion of the governing body behind Hippr). These can be used in exchanges to trade for fiat currency (in cases that require it, such as construction of health facilities) or used directly as payment (such as for third-party developers who accept DES).

Loans of this sort are intended to develop the health industry via entrepreneurial ventures – expecting return on investment. The loans will be paid back in DES (the original amount + additional fees) in order to release the collateral assets.

V. Components

Identities

Decentralized Identity (DID) can be used across different roles in the health ecosystem to verify their eligibility to own or be permitted to access medical records, one way or another.

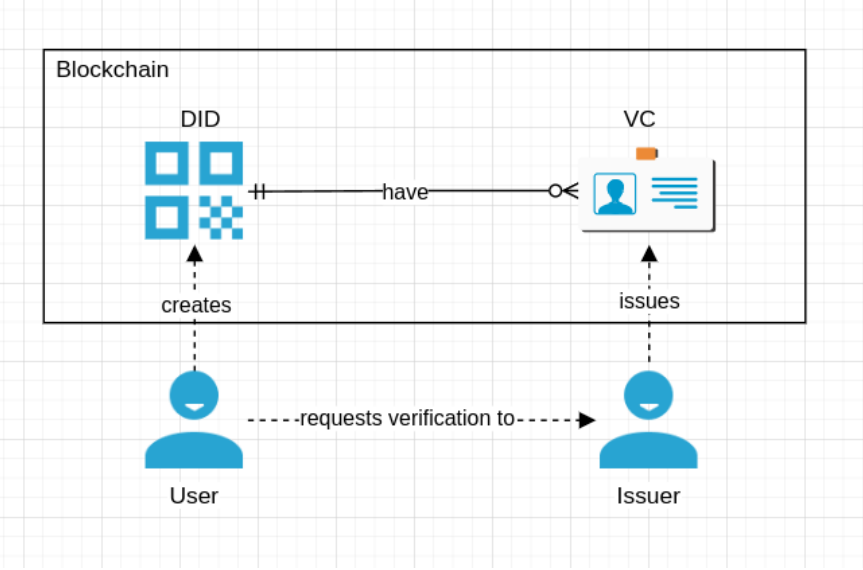
- **Patients:** They prove their own identity, so that they may claim their rights over records created for them by health providers. Verifiable Credential is a government-issued ID (eventually issued by a decentralized Trust Framework).
- **Doctors:** They prove their legitimacy as a doctor, so that they may create and be permitted to access medical records. Verifiable Credential is a license issued by the prevailing regulatory agency.
- **Pharmacists:** They prove their legitimacy as a pharmacist, so that they may be permitted to access prescriptions and other relevant medical records. Verifiable Credential is a license issued by the prevailing regulatory agency .

- **Health Facility Staff (e.g. Nurses, Technicians):** They prove their membership in a health facility, so that they may create and be permitted to access limited medical records shared across the health facility. Verifiable Credentials are:
    - A license issued by the prevailing regulatory agency — for creating limited medical records.
    - Membership credentials issued by the health facility they are a member of — for being permitted to access limited medical records shared across the health facility.
- **Health Facilities:** They prove their legitimacy as a health facility, so that they may generate and store medical records, as well as employ healthcare professionals who themselves may create and be permitted to access medical records. Verifiable Credential is a license issued by the prevailing regulatory agency.

Identities are one of the two key parts of BerryPied's IAM layer.

Mechanisms and Concepts

Decentralized Identifier (DID) - is a new type of identifier that enables verifiable, decentralized digital identity[6]. It is globally unique, resolvable with high availability, and cryptographically verifiable. DIDs are typically associated with cryptographic material, such as public keys, and service endpoints, for establishing secure communication channels[7]. A DID refers to any subject (a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID



[6] Decentralized Identifier https://en.wikipedia.org/wiki/Decentralized_identifier
[7] A Primer for Decentralized Identifiers https://w3c-ccg.github.io/did-primer/

Verifiable Credentials (VCs) - credentials that are issued by an issuer (trust framework). They can represent information found in physical credentials, such as a passport, as well as new things that have no physical equivalent, such as ownership of a bank account[8]. Other examples are (1) driver's license that is used to assert that a person is capable of operating a motor vehicle (2) university degree that can be used to assert level of education; and (3) government-issued passport that enable a person to travel between countries

User - creates DIDs in the blockchain that she can control effectively identifying her

Issuer - an entity (trust framework) that can issue verifiable credentials to a user's DID.

Records Access Management

Hippr is designed to finally address patient-centric health records and put them in control of their health data without disregarding the rights to access of the health providers who may have been contributory in creating the same information.

There are delicate intricacies in healthcare data access since they are generated from at least two (2) sources - the patient and the doctor. This can get more complex if the medical data becomes part of a clinic, hospital, and an insurance company's records for example.

Hippr addresses these concerns via smart contracts clearly defining the roles, privileges, and rights of each user. Rules, policies, and different use cases are likewise placed in smart contracts. Proofs of the transactions are then saved in a blockchain.

All these are automated, transparent, verifiable, and auditable. This will allow any user, not just the patient, to manage, control, and audit their medical data.

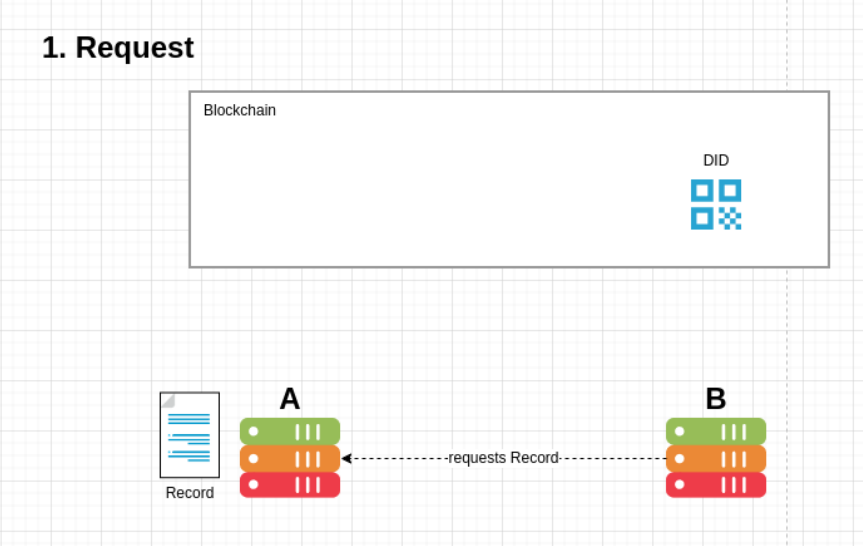
Mechanisms and Concepts

The **Secure Share** process inherently involves both the blockchain (via the RecordAccess transaction) and the implementing Fleming instances.

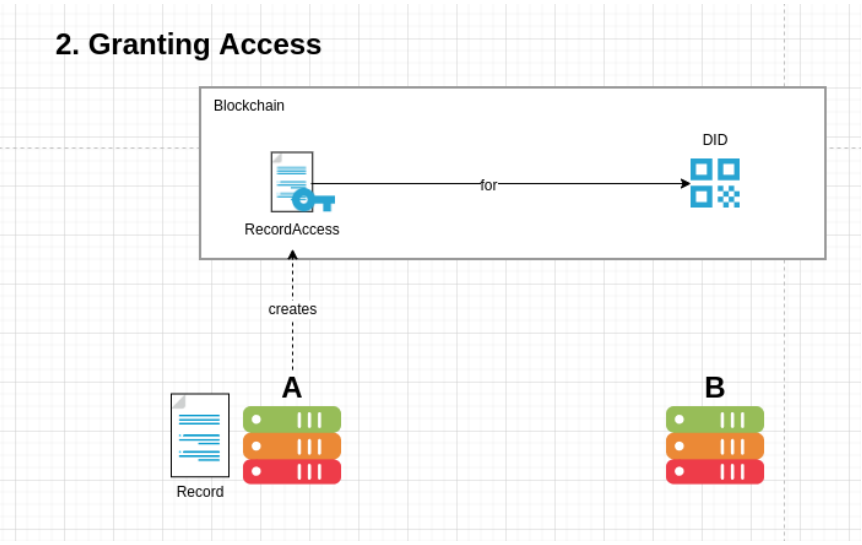
The initial state: two separate Fleming instances (% Hippocrades). A record will be transferred from A to B. B controls a DID.

[8] Verifiable Credentials - https://en.wikipedia.org/wiki/Verifiable_credentials

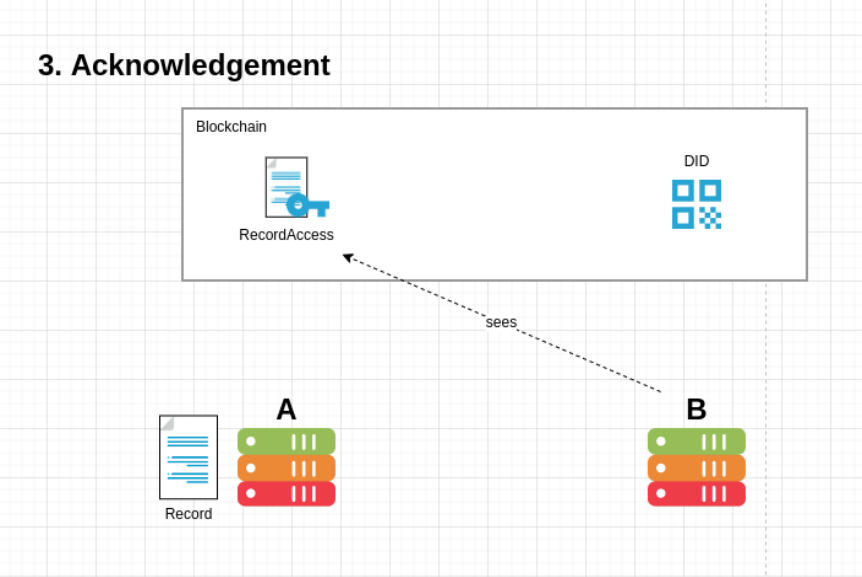
B requests a record from A.



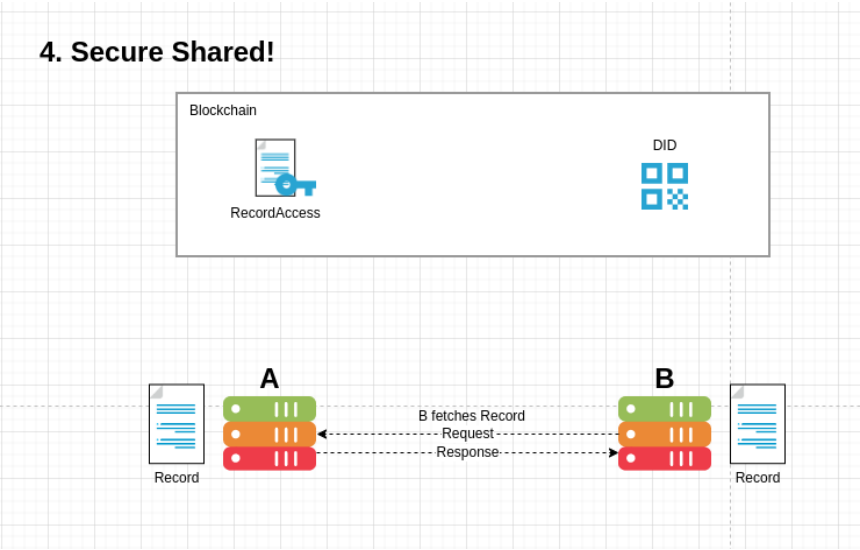
A grants access by creating a RecordAccess transaction for B's DID.



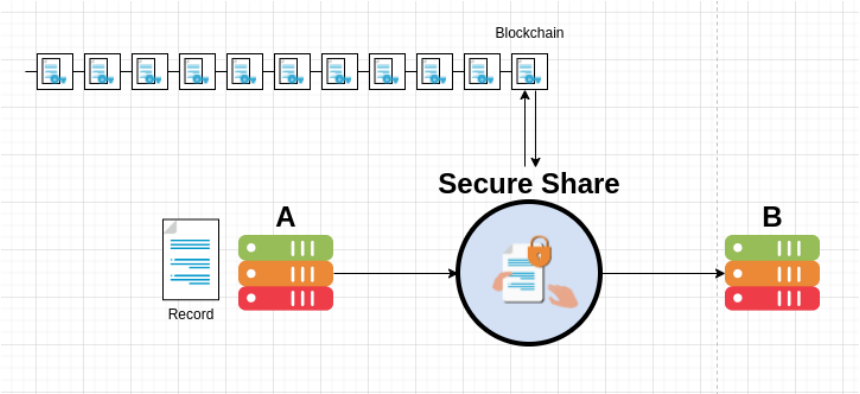
B sees the RecordAccess transaction…



…and uses its metadata to fetch the record from A.



This process is known elsewhere in this white paper as a **Secure Share**.



Key Points

Decentralized Identifier (DID): Users (integrating system in the case of the above diagram) can use DIDs uploaded and verified by the system for authenticating requesting users and deciding if record requests are to be accepted.

Record Access: requested users can then create Record Access transactions in the blockchain to represent sharing and the level of access that the requested user is willing to grant to the requesting user. This Record Access can then be used by the requesting user to finally request the actual data to the system which hosts it.

Record Access (or Resource Access when generalized) are one of the two key parts of BerryPied's IAM layer.

Tokens of Hippocrades

There would be three (3) types of tokens in the Hippocrades ecosystem - HIP, RAD, and DES as briefly described below.

Note: The first version of this paper is focused on the concepts of user-centricity in a decentralized exchange, details of the following tokens will be discussed in the next version of this paper.

The HIP Governance Token

The HIP token has three (3) methods of use within Hippr:

- As a utility token.

- As a governance token. HIP (staked) is used by HIP holders to vote for changes
- As a recapitalization resource.

The total supply of HIP is 500,000,000 tokens. Allocations will be unlocked in a predetermined schedule.

The RAD Rewards Token

To attract a wide range of users to the ecosystem, tokens will be rewarded for key behaviors such as (but not limited to):

- Set number of successful end-to-end transactions
- Championing meaningful proposals
- Using the marketplace system
- Using the ecosystem features/products that haven't been announced yet
- Contribution to the development

The DES Stablecoin

The stablecoin will be developed in the future for the medical loans use case. It will be used in a decentralized credit system for medicine related loans.

VI. Implementation

While the spirit of record access management is encoded into Hippr's blockchain protocol, there are aspects of our vision for robust health information management and exchange that require implementation by the surrounding infrastructure, which is where Hippocrades' Fleming and Curie modules come into the picture.

- **Enforcement of rights:** As steward of the off-chain database, the Fleming API must enforce access management and respect Hippr's designated rights to access
- **Enforcement of audit logs:** Every read or write operation for any medical record must generate the corresponding audit logs, which must also undergo access management
- **Easier interface for blockchain operations:** The creation of the RecordAccess transaction (as well as other blockchain transactions

described by Hippr) is abstracted by Fleming and exposed as REST API calls

- **Interface for identity and credential management of end users:** In the same way, DIDs and VCs are also abstracted and exposed as REST API calls
- **Patient claiming patient records:** While Hippr provides the DIDs, VCs, and RecordAccess transactions to represent which records a patient may claim, it is up to Fleming to implement the process via its access management, who is the one that ultimately guards the records

VII. Staking

Staking is a way to reward Hippocrades' community members in having a long term mindset by locking up their HIP token. By staking their HIP tokens, they will be able to earn rewards.

Note: The first version of this paper is focused on the concepts of user-centricity in a decentralized exchange, details of the Staking Section - voting, development, revenue, and rewards will be discussed in the next version of this paper.

VIII. DAO

Through HIP, Hippr will gradually evolve into a community-owned decentralized organization. This process will occur as HIP is distributed among actors and stakers, with the House of Hippocrades' ownership becoming less concentrated over time.

Note: The first version of this paper is focused on the concepts of user-centricity in a decentralized exchange, details of the DAO section, including its roadmap will be discussed in the next version of this paper.

IX. Conclusion

There are ever-ongoing concerns when it comes to healthcare data: (1) security and privacy, (2) shareability, and (3) ownership. As they are significant concerns on their own, there are numerous attempts to address each, but still falls short on an ideal solution. Moreso, attempting to address all of them at the same time seems like an impossible task, a holy grail in this sector.

Simply, there is no system in place to execute this challenge perfectly without resolving issues on ownership, privacy, security, and auditability altogether in a permissionless environment.

Data is siloed into each individual health facility's information system and generally not easily shareable with other facilities. This is not on purpose, however, but a natural consequence of the limitation of technology, especially so that privacy and interoperability are on the two opposing sides of the equation. Increasing shareability means giving up some privacy and vice versa. In addition, identifying who has access to such data adds to an already complex equation.

The Hippocrades Protocol, or Hippr provides a framework to finally resolve this. Hippr leverages the auditability of the blockchain, the privacy of zero-knowledge proofs, the power of smart contracts with well-defined user-centric record access privileges, and the infrastructure of Hippocrades platform to solve all the above challenges in one go, defining users' rights to access while allowing interoperability and protecting their privacy.