LONG 80

A GAVS & PREMIER, INC. JV

PoV

EHR Modernization towards Value Based Healthcare

Srinivasan Sundararajan has been in the technology industry for the last 28 years and has been continuously leveraging emerging technologies for business imperatives across various industries.

He has been considered as one of the early evangelists of Cloud Computing and has been part of the Cloud thought leadership series as featured in the MSDN Block along with the likes of CTO of NASA at the time. He had also been recognized as one of the top 100 bloggers worldwide due to his though leadership on Cloud.

Srinivasan has made immense contributions in the field of AI for IT Operations. He has been a key member of the team that conceptualized ZIF™, GAVS' flagship AIOps product recognized by Gartner and other industry analysts.

Presently, Srinivasan is focused on how distributed databases like Blockchain along with the Graph-based Semantic databases can help enterprises to get deeper insights while ensuring the data sharing related digital ethics are adhered to.

He is focused on Healthcare and has created a patent-pending Healthcare Master Data Management framework. It combines the best of multi-modal databases with the power of Blockchain to provide patient insights and electronic health record interoperability while ensuring patient consent rights are protected.

Srinivasan has been a regular speaker at academic events in Chennai, India, mainly promoting Blockchain especially for healthcare innovation. He has also spoken at various NASSCOM events in the past.

Srinivasan holds a master's degree in Computer Applications from Madras University and has various information technology certifications from major vendors like Microsoft, IBM, Oracle, R3, IFPUG and Oracle.
He has worked in other geographies like USA and Middle East apart from India.

Srinivasan Sundararajan

Technology Advisor

Healthcare Data Sharing

Patient Care Redefined

The fight against the novel coronavirus has witnessed transformational changes in the way patient care is defined and managed. Proliferation of telemedicine has enabled consultations across geographies. In the current scenario, access to patients' medical records has also assumed more importance.

The journey towards a solution also taught us that research on patient data is equally important. More the sample data about the infected patients, the better the vaccine/remedy. However, the growing concern about the privacy of patient data cannot be ignored. Moreover, patients who provide their data for medical research should also benefit from a monetary perspective, for their contributions.

The above facts basically point to the need for being able to share vital healthcare data efficiently so that patient care is improved, and more lives are saved.

The healthcare industry needs a data-sharing framework, which shares patient data but also provides much-needed controls on data ownership for various stakeholders, including the patients.

Types of Healthcare Data

- **PHR (Personal Health Record):** An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being man aged, shared, and controlled by the individual.

- **EMR (Electronic Medical Record):** Health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one healthcare organization.

- **EHR (Electronic Health Record):** Health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed and consulted by authorized clinicians and staff **across more than one healthcare organization.**

In the context of large multi-specialty hospitals, EMR could also be specific to one specialist department and EHR could be the combination of information from various specialist departments in a single unified record.

Together these 3 forms of healthcare data provide a comprehensive view of a patient (patient 360), thus resulting in quicker diagnoses and personalized quality care.

Current Challenges in Sharing Healthcare Data

- Lack of unique identity for patients prevents a single version of truth. Though there are government-issued IDs like SSN, their usage is not consistent across systems.

- High cost and error-prone integration options with provider controlled EMR/EHR systems. While there is standardization with respect to healthcare interoperability API specifications, the effort needed for integration is high.

- Conflict of interest in ensuring patient privacy and data integrity, while allowing data sharing. Digital ethics dictate that patient consent management take precedence while sharing their data.

- Monetary benefits of medical research on patient data are not passed on to patients. As mentioned earlier, in today's context analyzing existing patient information is critical to finding a cure for diseases, but there are no incentives for these patients.

- Data stewardship, consent management, compliance needs like HIPAA, GDPR. Let's assume a hospital specializing in heart-related issues shares a patient record with a hospital that specializes in eye care. How do we decide which portions of the patient information is owned by which hospital and how the governance is managed?

- Lack of real-time information attributing to data quality issues and causing incorrect diagnoses.

The above list is not comprehensive but points to some of the issues that are plaguing the current healthcare data-sharing initiatives.

Blockchain for Healthcare Data Sharing

Some of the basic attributes of blockchain are mentioned below:

- Blockchain is a distributed database, whereby each node of the database can be owned by a different stakeholder (say hospital departments) and yet all updates to the database eventually converge resulting in a distributed single version of truth.
- Blockchain databases utilize a cryptography-based transaction processing mechanism, such that each object stored inside the database (say a patient record) can be distinctly owned by a public/private key pair and the ownership rights carry throughout the life cycle of the object (say from patient admission to discharge).
- Blockchain transactions are carried out using smart contracts which basically attach the business rules to the underlying data, ensuring that the data is always compliant with the underlying business rules, making it even more reliable than the data available in traditional database systems.

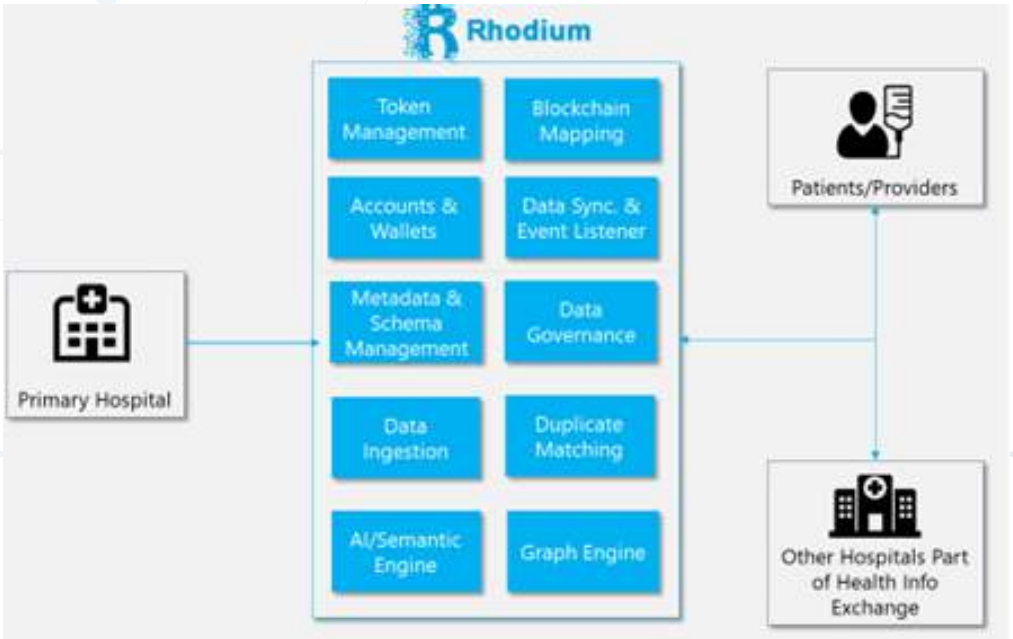
These underlying properties of Blockchain make it a viable technology platform for healthcare data sharing, as well as to ensure data stewardship and patient privacy rights.

Rhodium Framework for Healthcare Data Sharing

This framework combines the best features of multi-modal databases (relational, nosql, graph) along with the viability of data sharing facilitated by Blockchain, to come up with a unified framework for healthcare data sharing.

The following are the high-level components (in a healthcare context) of the Rhodium framework. As you can see, each of the individual components of Rhodium play a role in healthcare information exchange at various levels.

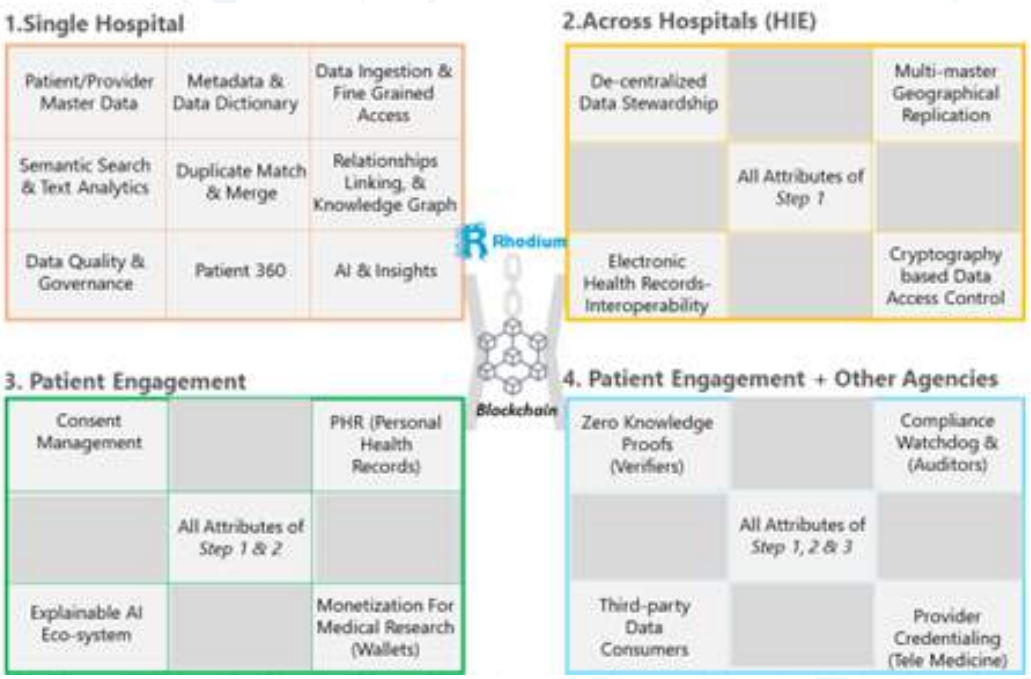
Rhodium Framework for Healthcare



We have also defined a maturity model for healthcare organizations for utilizing the framework towards healthcare data sharing. This model defines 4 stages of healthcare data sharing:

- Within a Hospital
- Across Hospitals
- Between Hospitals & Patients
- Between Hospitals, Patients & Other Agencies

The below progression diagram illustrates how the framework can be extended for various stages of the life cycle, and typical use cases that are realized in each phase. Detailed explanations of various components of the Rhodium framework, and how it realizes use cases mentioned in the different stages will be covered in subsequent articles in this space.



Benefits of the Rhodium Framework for Healthcare Data Sharing

The following are the general foreseeable benefits of using the Rhodium framework for healthcare data sharing.

For Patients	For Hospitals
• Prevents unauthorized monetization of their health data without their consent • Enables a unique identity across providers and clinical facilities • Better and quicker access to healthcare due to the full picture of unified EHR • Lower cost of healthcare services due to the reduced cost of operations • Anytime, anywhere, any device access to data leading to improved patient engagement	• Reduces diagnosis costs and avoids costly duplicate testing efforts • Provides a path to cloud for health data to start with • Enables better care for patients with unified data • More scope for advanced research on healthcare data within the boundaries of privacy • Quicker enrolment of both doctors and patients due to trust-based eco system

Healthcare Industry Trends with Respect to Data Sharing

The following are some of the trends we are seeing in Healthcare Data Sharing:

- Interoperability will drive privacy and security improvements
- New privacy regulations will continue to come up, in addition to HIPAA
- The ethical and legal use of AI will empower healthcare data security and privacy
- The rest of 2020 and 2021 will be defined by the duality of data security and data integration, and providers' ability to execute on these priorities. That, in turn, will, in many ways, determine their effectiveness
- In addition to industry regulations like HIPAA, national data privacy standards including Europe's GDPR, California's Consumer Privacy Act, and New York's SHIELD Act will further increase the impetus for providers to prioritize privacy as a critical component of quality patient care

The below documentation from the HIMSS site talks about maturity levels with respect to healthcare interoperability, which is addressed by the Rhodium framework.

Source: https://www.himss.org/what-interoperability

This framework is in its early stages of experimentation and is a prototype of how a Blockchain + Multi-Modal Database powered solution could be utilized for sharing healthcare data, that would be hugely beneficial to patients as well as healthcare providers.

Zero Knowledge Proofs in Healthcare Data Sharing

Recap of Healthcare Data Sharing

In my previous article **(https://long-80.com/blog/healthcare-data-sharing/)**, I had elaborated on the challenges of Patient Master Data Management, Patient 360, and associated Patient Data Sharing. I had also outlined how our Rhodium framework is positioned to address the challenges of Patient Data Management and data sharing using a combination of multi-modal databases and Blockchain.

In this context, I have highlighted our maturity levels and the journey of Patient Data Sharing as follows:

- Single Hospital
- Between Hospitals part of HIE (Health Information Exchange)
- Between Hospitals and Patients
- Between Hospitals, Patients, and Other External Stakeholders

In each of the stages of the journey, I have highlighted various use cases. For example, in the third level of health data sharing between Hospitals and Patients, the use cases of consent management involving patients as well as monetization of personal data by patients themselves are mentioned.

In the fourth level of the journey, you must've read about the use case **"Zero Knowledge Proofs".** In this article, I would be elaborating on:

- What is Zero Knowledge Proof (ZKP)?
- What is its role and importance in Healthcare Data Sharing?
- How Blockchain Powered GAVS Rhodium Platform helps address the needs of ZKP?

Introduction to Zero Knowledge Proof

As the name suggests, Zero Knowledge Proof is about proving something without revealing the data behind that proof. Each transaction has a 'verifier' and a 'prover'. In a transaction using ZKPs, the prover attempts to prove something to the verifier without revealing any other details to the verifier.

Zero Knowledge Proofs in Healthcare

In today's healthcare industry, a lot of time-consuming due diligence is done based on a lack of trust.

- Insurance companies are always wary of fraudulent claims (which is anyhow a major issue), hence a lot of documentation and details are obtained and analyzed.
- Hospitals, at the time of patient admission, need to know more about the patient, their insurance status, payment options, etc., hence they do detailed checks.
- Pharmacists may have to verify that the Patient is indeed advised to take the medicines and give the same to the patients.
- Patients most times also want to make sure that the diagnosis and treatment given to them are indeed proper and no wrong diagnosis is done.
- Patients also want to ensure that doctors have legitimate licenses with no history of malpractice or any other wrongdoing.
- In a healthcare scenario, either of the parties, i.e. patient, hospital, pharmacy, insurance companies, can take on the role of a verifier, and typically patients and sometimes hospitals are the provers.

While the ZKP can be applied to any of the transactions involving the above parties, currently the research in the industry is mostly focused on patient privacy rights and ZKP initiatives target more on how much or less of information a patient (prover) can share to a verifier before getting the required service based on the assertion of that proof.

Blockchain & Zero Knowledge Proof

While I am not getting into the fundamentals of Blockchain, but the readers should understand that one of the fundamental backbones of Blockchain is trust within the context of pseudo anonymity. In other words, some of the earlier uses of Blockchain, like cryptocurrency, aim to promote trust between unknown individuals without revealing any of their personal identities, yet allowing participation in a transaction.

Some of the characteristics of the Blockchain transaction that makes it conducive for Zero Knowledge Proofs are as follows:

- Each transaction is initiated in the form of a smart contract.
- Smart contract instance (i.e. the particular invocation of that smart contract) has an owner i.e. the public key of the account holder who creates the same, for example, a patient's medical record can be created and owned by the patient themselves.
- The other party can trust that transaction as long the other party knows the public key of the initiator.
- Some of the important aspects of an approval life cycle like validation, approval, rejection, can be delegated to other stakeholders by delegating that task to the respective public key of that stakeholder.
- For example, if a doctor needs to approve a medical condition of a patient, the same can be delegated to the doctor and only that particular doctor can approve it.
- The anonymity of a person can be maintained, as everyone will see only the public key and other details can be hidden.
- Some of the approval documents can be transferred using off-chain means (outside of the blockchain), such that participants of the blockchain will only see the proof of a claim but not the details behind it.
- Further extending the data transfer with encryption of the sender's private/public keys can lead to more advanced use cases.

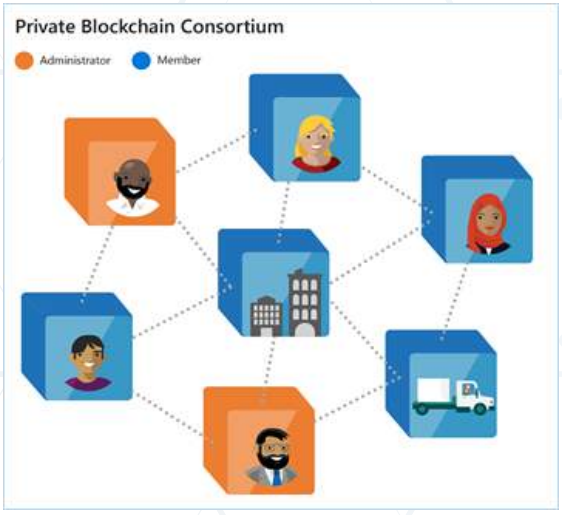
Role of Blockchain Consortium

While Zero Knowledge Proofs can be implemented in any Blockchain platform including totally uncontrolled public blockchain platforms, their usage is best realized in private Blockchain consortiums. Here the identity of all participants is known, and each participant trusts the other, but the due diligence that is needed with the actual submission of proof is avoided.

Organizations that are part of similar domains and business processes form a Blockchain Network to get business benefits of their own processes. Such a Controlled Network among the known and identified organizations is known as a Consortium Blockchain.

Illustrated view of a Consortium Blockchain Involving Multiple Other Organizations, whose access rights differ. Each member controls their own access to Blockchain Network with Cryptographic Keys.

Members typically interact with the Blockchain Network by deploying Smart Contracts (i.e. Creating) as well as accessing the existing contracts.



Current Industry Research on Zero Knowledge Proof

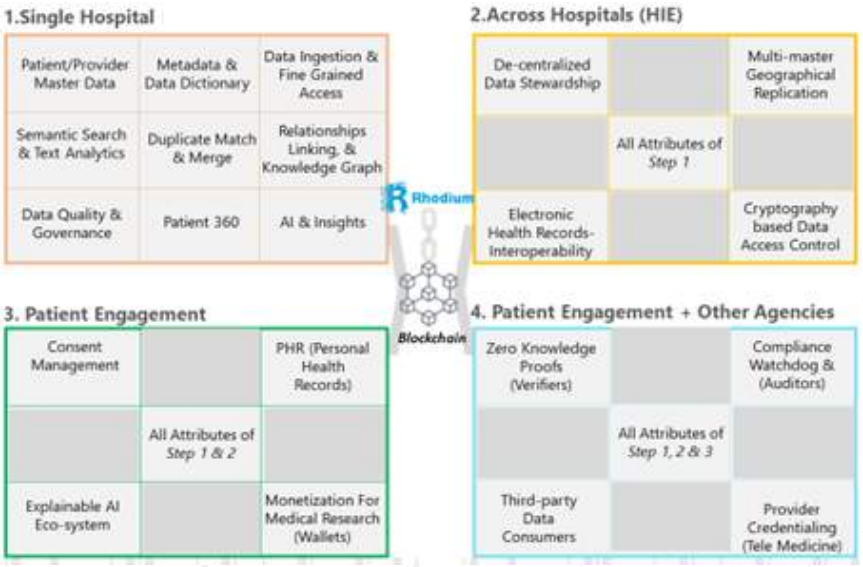
Zero Knowledge Proof is a new but powerful concept in building trust-based networks. While basic Blockchain platform can help to bring the concept in a trust-based manner, a lot of research is being done to come up with a truly algorithmic zero knowledge proof.

A zk-SNARK ("zero-knowledge succinct non-interactive argument of knowledge") utilizes a concept known as a "zero-knowledge proof". Developers have already started integrating zk-SNARKs into Ethereum Blockchain platform. Zether, which was built by a group of academics and financial technology researchers including Dan Boneh from Stanford University, uses zero-knowledge proofs.

ZKP In Rhodium

As mentioned in my previous article about Patient Data Sharing, Rhodium is a futuristic framework that aims to take the Patient Data Sharing as a journey across multiple stages, and at the advanced maturity levels Zero Knowledge Proofs definitely find a place. Healthcare organizations can start experimenting and innovating on this front.

Rhodium Patient Data Sharing Journey



Healthcare Industry today is affected by fraud and lack of trust on one side, and on the other side growing privacy concerns of the patient. In this context, the introduction of a Zero Knowledge Proofs as part of healthcare transactions will help the industry to optimize itself and move towards seamless operations.

Patient 360 & Journey Mapping using Graph Technology

360 Degree View of Patient

With rising demands for quality and cost-effective patient care, healthcare providers are focusing on data-driven diagnostics while continuing to utilize their hard-earned human intelligence. In other words, data-driven healthcare is augmenting human intelligence.

360 Degree View of Patient, as it is called, plays a major role in delivering the required information to the providers. It is a unified view of all the available information about a patient. It could include but is not limited to the following information:

- Appointments made by the patients
- Interaction with different doctors
- Medications prescribed by the doctors
- Patient's relationship to other patients within the eco-systems specially to identify the family history related risks
- Patient's admission to hospitals or other healthcare facilities
- Discharge and ongoing care
- Patient personal wellness activities
- Patient billing and insurance information
- Linkages to the same patient in multiple disparate databases within the same hospital
- Information about a patient's involvement in various seminars, medical-related conferences, and other events

Limitations of Current Methods

As evident in most hospitals, these information are usually scattered across multiple data sources/databases. Hospitals typically create a data warehouse by consolidating information from multiple resources and try to create a unified database. However, this approach is done using relational databases and the relational databases rely on joining tables across entities to arrive at a complete picture. The RDBMS is not meant to handle relationships which extend to multiple hops and require drilling down to many levels.

Role of Graph Technology & Graph Databases

A graph database is a collection of nodes (or entities typically) and edges (or relationships). A node represents an entity (for example, a person or an organization) and an edge represents a relationship between the two nodes that it connects (for example, friends). Both nodes and edges may have properties associated with them.

While there are multiple graph databases in the market today like, Neo4J, JanusGraph, TigerGraph, the following technical discussions pertain to graph database that is part of SQL server 2019. The main advantage of this approach is that it helps utilize the best RDBMS features wherever applicable, while keeping the graph database options for complex relationships like 360 degree view of patients, making it a true polyglot persistence architecture.

As mentioned above, in SQL Server 2019 a graph database is a collection of node tables and edge tables. A node table represents an entity in a graph schema. An edge table represents a relationship in a graph. Edges are always directed and connect two nodes. An edge table enables users to model many-to-many relationships in the graph. Normal SQL Insert statements are used to create records into both node and edge tables.

While the node tables and edge tables represent the storage of graph data there are some specialized commands which act as extension of SQL and help with traversing between the nodes to get the full details like patient 360 degree data.

MATCH statement

MATCH statement links two node tables through a link table, such that complex relationships can be retrieved. An example,

```
-- use MATCH in SELECT to find friends of Alice
SELECT Person2.name AS FriendName
FROM Person Person1, friend, Person Person2
WHERE MATCH(Person1-(friend)->Person2)
AND Person1.name = 'Alice';
```

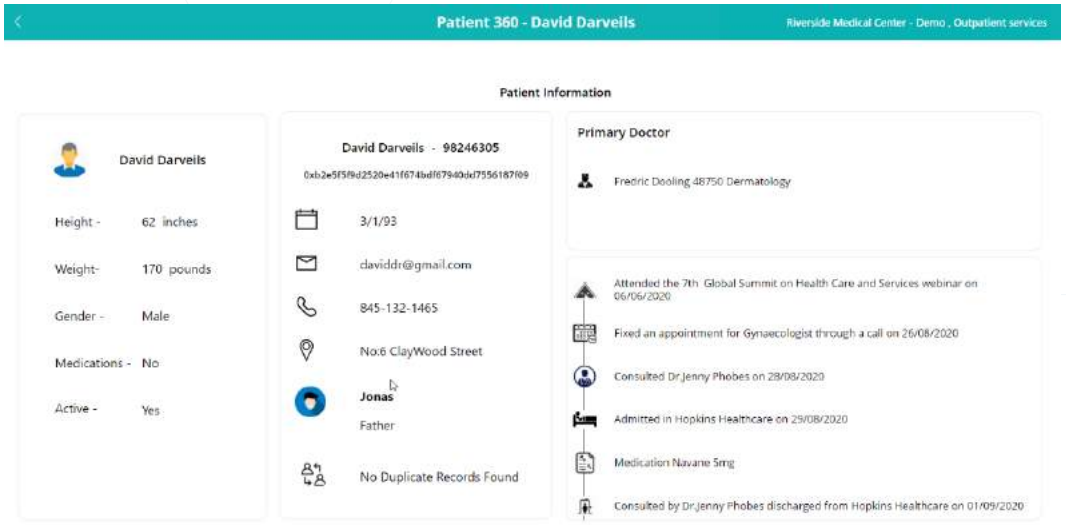
SHORTEST_PATH statement

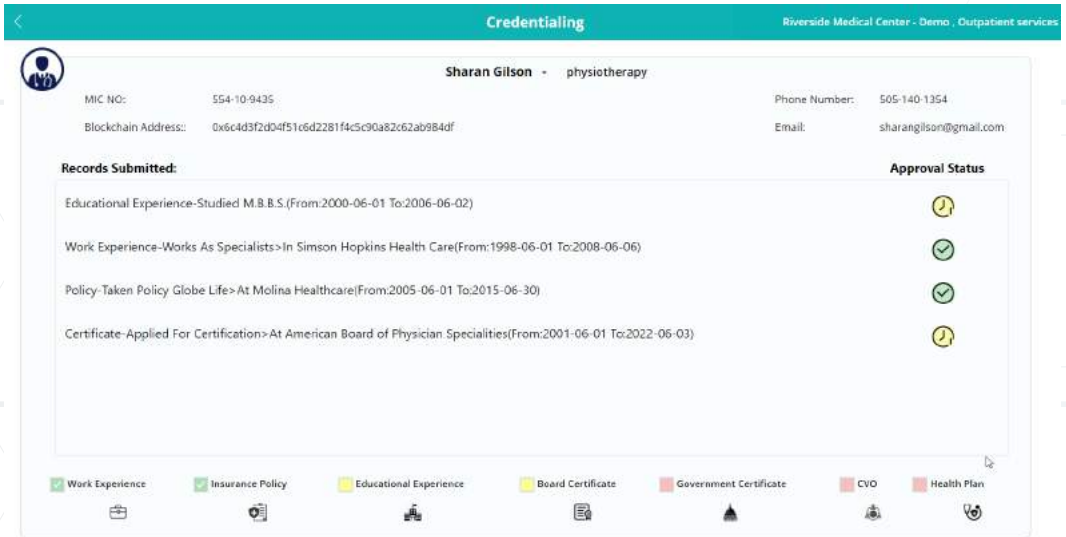
It finds the relationship path between two node tables by performing multiple hops recursively. It is one of the useful statements to find the 360 degree of a patient.

There are more options and statements as part of graph processing. Together it will help identify complex relationships across business entities and retrieve them.

GRAPH processing In Rhodium

As mentioned in my earlier articles (Healthcare Data Sharing & Zero Knowledge Proofs in Healthcare Data Sharing), Rhodium framework enables Patient and Data Management and Patient Data Sharing and graph databases play a major part in providing patient 360 as well as for provider (doctor) credentialing data. The below screen shots show the samples from reference implementation.





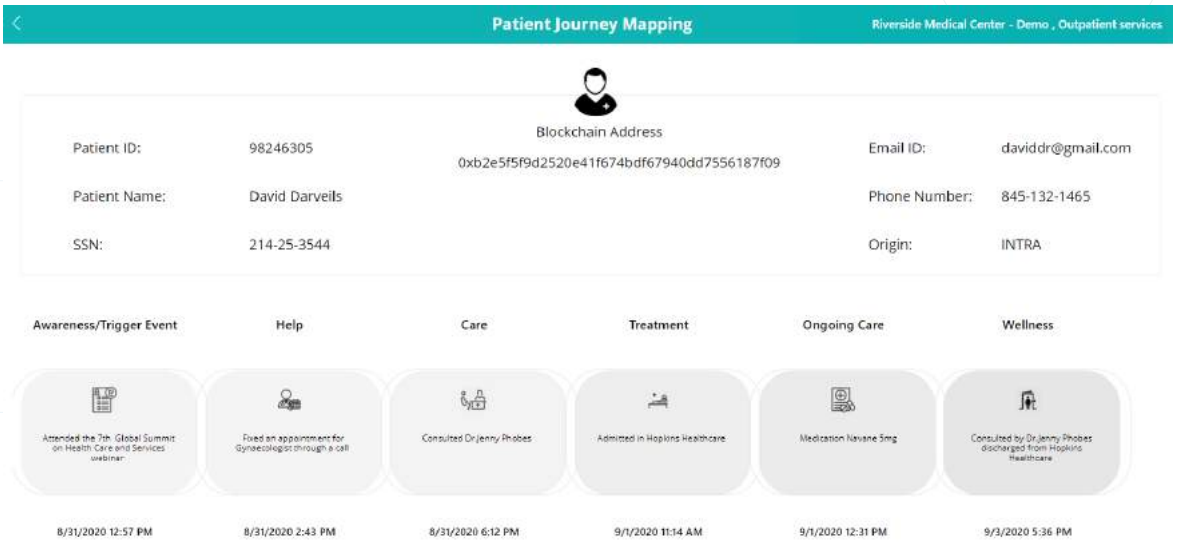
Patient Journey Mapping

Typically, a patient's interaction with the healthcare service provider goes through a cycle of events. The goal of the provider organization is to make this journey smooth and provide the best care to the patients. It should be noted that not all patients go through this journey in a sequential manner, some may start the journey at a particular point and may skip some intermediate journey points. Proper data collection of events behind patient journey mapping will also help with the future prediction of events which will ultimately help with patient care.

Patient 360 data collection plays a major role in building the patient journey mapping. While there could be multiple definitions, the following is one of the examples of mapping between patient 360-degree events and patient journey mapping.

Patient 360 Degree Event	Patient Journey Mapping
Registration	Awareness/Trigger Event
Appointment	Help
Physician Interaction	Care
Admission	Treatment
Prescriptions	Ongoing Care
Discharge	Wellness

The below diagram shows an example of a patient journey mapping information.



Understanding patients better is essential for improving patient outcomes. 360 degree of patients and patient journey mapping are key components for providing such insights. While traditional technologies lack the need of providing those links, graph databases and graph processing will play a major role in patient data management.

Patient Segmentation Using Data Mining Techniques

Patient Segmentation & Quality Patient Care

As the need for quality and cost-effective patient care increases, healthcare providers are increasingly focusing on data-driven diagnostics while continuing to utilize their hard-earned human intelligence. Simply put, data-driven healthcare is augmenting the human intelligence based on experience and knowledge.

Segmentation is the standard technique used in Retail, Banking, Manufacturing, and other industries that needs to understand their customers to provide better customer service. Customer segmentation defines the behavioral and descriptive profiles of customers. These profiles are then used to provide personalized marketing programs and strategies for each group.

In a way, patients are like customers to healthcare providers. Though the element of quality of care takes precedence than profit-making intention, a similar segmentation of patients will immensely benefit the healthcare providers, mainly for the following reasons:

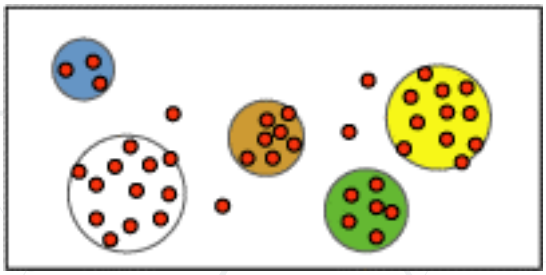
- Customizing the patient care based on their behavior profiles
- Enabling a stronger patient engagement
- Providing the backbone for data-driven decisions on patient profile
- Performing advanced medical research like launching a new vaccine or trial

The benefits are obvious and individual hospitals may add more points to the above list; the rest of the article is about how to perform the patient segmentation using data mining techniques.

Data Mining for Patient Segmentation

In Data Mining a, segmentation or clustering algorithm will iterate over cases in a dataset to group them into clusters that contain similar characteristics. These groupings are useful for exploring data, identifying anomalies in the data, and creating predictions. Clustering is an unsupervised data mining (machine learning) technique used for grouping the data elements without advance knowledge of the group definitions.

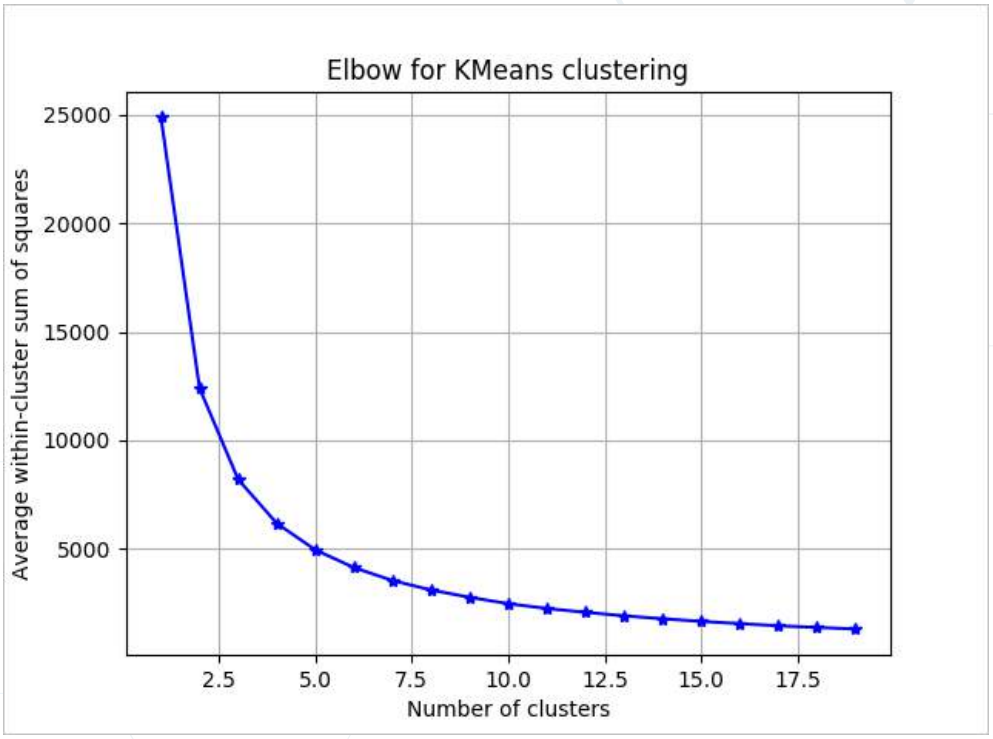
K-means clustering is a well-known method of assigning cluster membership by minimizing the differences among items in a cluster while maximizing the distance between clusters. Clustering algorithm first identifies relationships in a dataset and generates a series of clusters based on those relationships. A scatter plot is a useful way to visually represent how the algorithm groups data, as shown in the following diagram. The scatter plot represents all the cases in the dataset, and each case is a point on the graph. The cluster points on the graph illustrate the relationships that the algorithm identifies.



One of the important parameters for a K-Means algorithm is the number of clusters or the cluster count. We need to set this to a value that is meaningful to the business problem that needs to be solved. However, there is good support in the algorithm to find the optimal number of clusters for a given data set, as explained next.

To determine the number of clusters for the algorithm to use, we can use a plot of the within cluster's sum of squares, by the number of clusters extracted. The appropriate number of clusters to use is at the bend or 'elbow' of the plot. The Elbow Method is one of the most popular methods to determine this optimal value of k i.e. the number of clusters. The following code creates a curve.

```
from sklearn.cluster import KMeans
wcss = []
for i in range(1, 20):
  kmeans = KMeans(n_clusters = i, init = 'k-means++', random_state = 42)
  kmeans.fit(customer_data[columns])
  wcss.append(kmeans.inertia_)
plt.plot(range(1, 20), wcss)
plt.title('The Elbow Method')
plt.xlabel('Number of clusters')
plt.ylabel('WCSS')
plt.show()
```



In this example, based on the graph, it looks like k = 4 would be a good value to try.

Reference Patient Segmentation Using K-Means Algorithm in Rhodium Platform

In Rhodium Platform, which helps healthcare providers with Patient Data Management and Patient Data Sharing, there is a reference implementation of Patient Segmentation using K-Means algorithm. The following are the attributes that are used based on a publicly available Patient admit data (no personal information used in this data set). Again in the reference implementation sample attributes are used and in a real scenario consulting with healthcare practitioners will help to identify the correct attributes that is used for clustering.

To prepare the data for clustering patients, patients must be separated along the following dimensions:

- HbA1c: Measuring the glycated form of hemoglobin to obtain the three-month average of blood sugar.
- Triglycerides: Triglycerides are the main constituents of natural fats and oils. This test indicates the amount of fat or lipid found in the blood.
- FBG: Fasting Plasma Glucose test measures the amount of glucose levels present in the blood.
- Systolic: Blood Pressure is the pressure of circulating blood against the walls of Blood Vessels. This test relates to the phase of the heartbeat when the heart muscle contracts and pumps blood from the chambers into the arteries.

- Diastolic: The diastolic reading is the pressure in the arteries when the heart rests between beats.
- Insulin: Insulin is a hormone that helps move blood sugar, known as glucose, from your bloodstream into your cells. This test measures the amount of insulin in your blood.
- HDL-C: Cholesterol is a fat-like substance that the body uses as a building block to produce hormones. HDL-C or good cholesterol consists primarily of protein with a small amount of cholesterol. It is considered to be beneficial because it removes excess cholesterol from tissues and carries it to the liver for disposal. The test for HDL cholesterol measures the amount of HDL-C in blood.
- LDL-C: LDL-C or bad cholesterol present in the blood as low-density lipoprotein, a relatively high proportion of which is associated with a higher risk of coronary heart disease. This test measures the LDL-C present in the blood.
- Weight: This test indicates the heaviness of the patient.

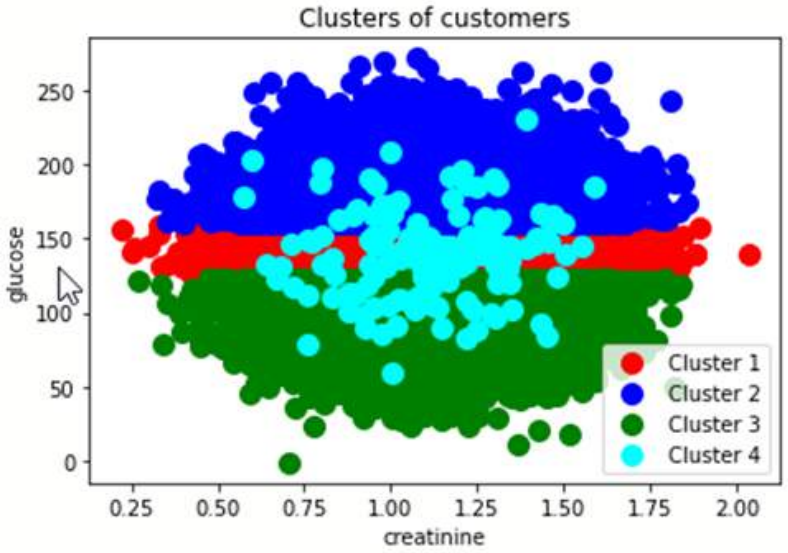
The above tests are taken for the patients during the admission process.

The following is the code snippet behind the scenes which create the patient clustering.

```
columns = [ "creatinine",
"glucose",
"sodium",
"hematocrit",
"respiration",
"pulse",
"bloodureanitro",
"neutrophils",
"lengthofstay"]

n_clusters = 4
means_cluster = sk_cluster.KMeans(n_clusters=n_clusters, random_state=111)
kmeans = KMeans(n_clusters = 4, init = 'k-means++', random_state = 42)
```

The below is the output cluster created from the above algorithm.



Just from this sample, healthcare providers can infer the patient behavior and patterns based on their creatinine and glucose levels, in real-life situations other different attributes can be used.

AI will play a major role in future healthcare data management and decision making and data mining algorithms like K-Means provide an option to segment the patients based on the attributes which will improve the quality of patient care.

Health Information Exchanges in Post-Pandemic Healthcare

IElectronic Health Information Exchange (HIE) allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically - improving the speed, quality, safety and cost of patient care.

HIE enables electronical movement of clinical information among different healthcare information systems. The goal is to facilitate access to and retrieval of clinical data to provide safer and more timely, efficient, effective, and equitable patient-centered care.

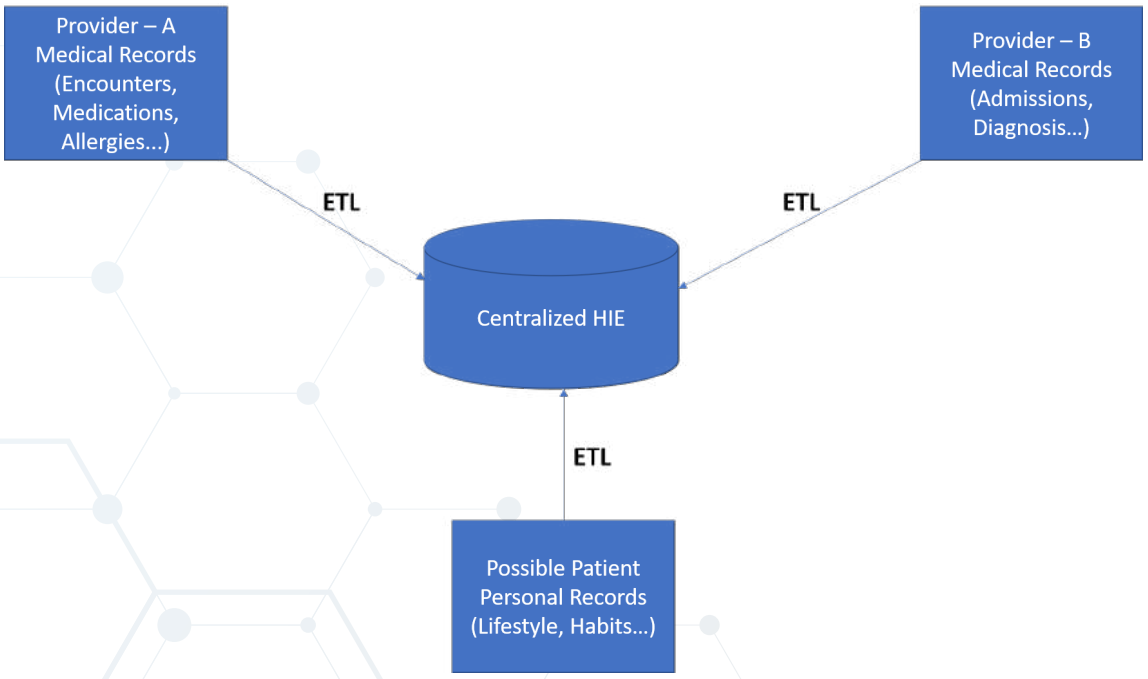
While the importance of HIE is clearly visible, now the important question is how hospitals can collaborate to form a HIE and how the HIE will consolidate data from disparate patient information sources. This brings us to the important discussion of HIE data models.

HIE Data Models

There are multiple ways in which a HIE can get its data, each influencing the way in which the interoperability goals are achieved, how easily a HIE platform is built and how to sustain in the long run especially if the number of hospitals in the ecosystem increases. The two models are

- Centralized
- De-centralized

Centralized HIE Data Model



This is a pictorial representation of centralized HIE data model.

As evident, in the centralized model all the stakeholders send their data to a centralized location and typically a ETL (Extraction, Transformation and Loading) process ensures that all the data is synced with the centralized server.

Advantages

- From the query performance perspective this model is one of the most efficient, because the DBAs have complete control of the data and with the techniques like partitioning, indexing they could ensure that the query can be done in the best possible manner. Since the hardware is fully owned by a single organization (which is the HIE itself), this can be scaled out or scaled up to meet the demands of the business.
- This model is fairly self-sufficient once the mechanism for the data transfers are established, as the need to connect to individual hospitals are no longer there.
- Smaller hospitals in the ecosystem need not take the burden of maintaining their data and interoperability needs and can just send their data to the centralized repository.
- Better scope for performing population predictive and prescriptive analytics as the data resides in one place and easier to create models based on the historical data.

Limitations

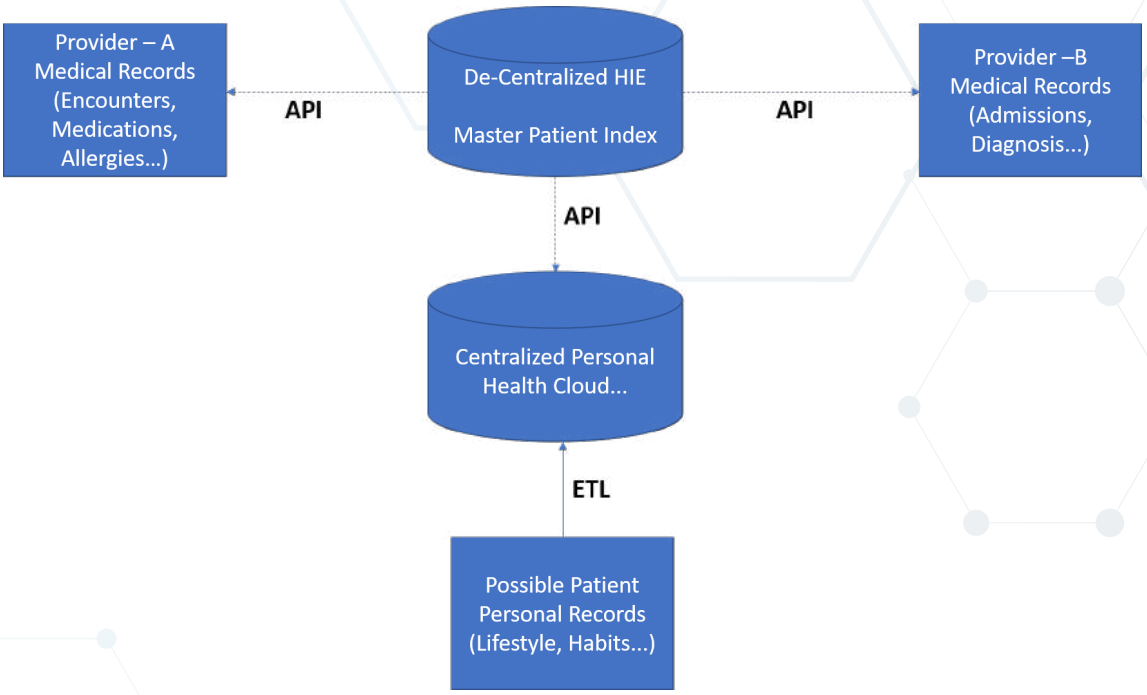
- This model needs to have highest level of security built in, because any breach in the system will compromise the data of entire ecosystem. Also considering that individual hospitals send their data to this model, all the responsibility lies with a single agency (HIE) which is highly prone to lawsuits related to data privacy and confidentiality.
- There is no control for patients in managing their own records and right to provide consent for data access, even though this information can be collected there is no easy way to implement them.
- The system is prone to a single point of failure and hence require efforts for high availability of the platform.
- This model will face scalability challenges as the network grows beyond a point, unless the platform is modernized with latest big data databases, the system will have scalability issues.
- Lot of coordination required to monitor the individual ETL jobs for their success, failure, and record synchronization details, so this model will have a huge allocation of IT resources and will increase the total cost of ownership.
- The model of expense sharing between the HIE, data producers, data consumers will be difficult and needs to have a strong governance model.
- Difficult to match the patient information across hospitals, unless the both the hospitals use deterministic matching attributes like SSN, otherwise it would be difficult to match between patients who have misspelt names, different addresses etc.
- This model may suffer data integrity issues when the participant hospitals merge with each other, such that the IT systems of the two hospitals need to take care the internal details of the ETL jobs.

De-centralized HIE Data Model

There are multiple ways in which a HIE can get its data, each influencing the way in which the interoperability goals are achieved, how easily a HIE platform is built and how to sustain in the long run especially if the number of hospitals in the ecosystem increases. The two models are

- Centralized
- De-centralized

Centralized HIE Data Model



The above is the pictorial representation of decentralized HIE data model.

As evident, in this model individual hospitals continue to own all their data, however the centralized database keeps a pointer - MPI (Master Patient Index), which serves as a unifying factor for consolidating data for that patient. While some books also suggest a variant called Hybrid model which combines centralized and decentralized data models, we believe that pure play decentralized model itself is a hybrid (i.e. centralized + decentralized) because there needs to be a centralized repository to keep the master patient index along with all the access rights and related information.

Advantages

- It is much easier to implement as no huge investment is required from a centralized provider perspective. The HIEs in this model can start low and grow on demand basis
- Less expensive as no single organization owns all the data, but only a pointer to the data and the respective hospitals continue to own the data.
- Much easier to provide patients the control of their own data and patient's consent can be a key in accessing information from the respective hospitals.
- No need to worry about broken ETL jobs and the latency between source and destination. All the data is always current.

- No need to worry about single point of failure, as the individual sub systems will continue to exist even if one link to a particular hospital is broken. Maintaining the high availability of this light-weight platform is much easier than a monolithic large database as part of a centralized data model.

- A data breach into the centralized repository still will not compromise all the data, as the individual hospitals are likely to have some more additional controls which prevent a free flow for hackers. This also prevents one organization from facing all the legal issues resulting from patient data breach.

Limitations

- This model will have a query performance problem when it comes to aggregating a patient information across multiple hospitals, because each has to be obtained with a separate API call and a facade has to group multiple datasets.

- Difficult to establish common standards in terms of data formats and APIs across multiple hospitals, this may result in each hospital having their own methods.

- Bringing all the stakeholders including the patients to agree on a MPI (Master Patient Index) will have governance challenges and needs to be implemented carefully.

- Providing analytics for a large set of population will have challenges due to the difficulties in consolidating the data.

Our Point of View & Role of Blockchain

While no model can be 100% perfect for building a HIE, Our analysis point to that fact decentralized model of building and operating HIE is better than centralized model. The COVID pandemic has changed the world and the boundaries of healthcare no longer exist within a smaller geography or neighbourhood as it used to. More the participants and bigger the network size, the better it is for population health improvement initiatives. Also, in high population countries where there are initiatives like national healthcare for all, these larger initiatives cannot be done using a pure play centralized model.

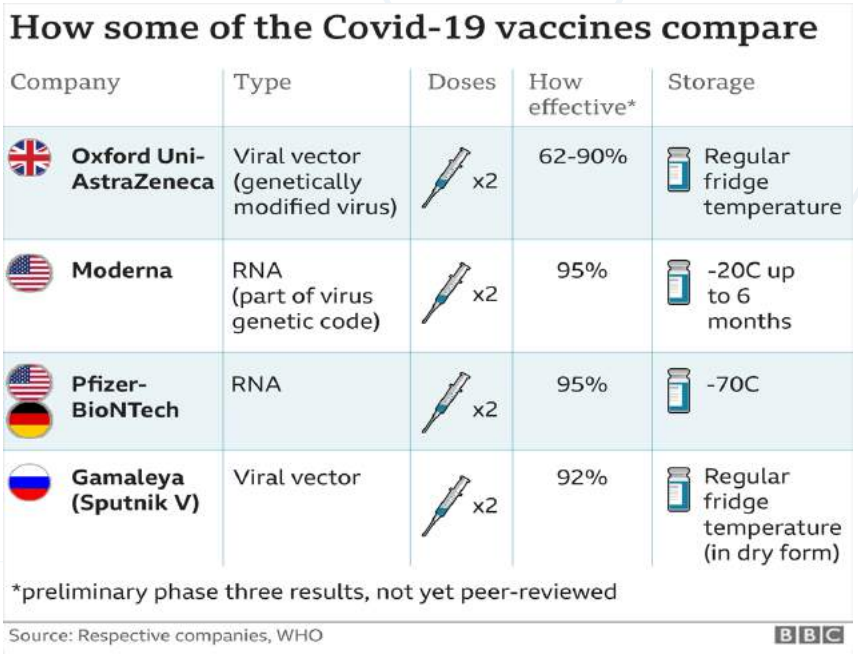
From an implementation perspective the Healthcare IT world has been curiously watching the role of Blockchain in data interoperability and in the implementation of decentralized HIE. Blockchain which is a distributed database has decentralization built in as part of its core architecture. It would be easier to implement decentralized HIE using blockchain.

Our Reference Implementation Rhodium to cater to Healthcare Data Management and Interoperability has positioned Blockchain as a core mechanism for patient data sharing, we will share more of our thoughts and details of reference implementation in the coming articles in this series.

Blockchain-based Platform for COVID-19 Vaccine Traceability

The massive exercise of administering vaccines to billions of people across different geographies poses various challenges. Add to this the fact that different vaccines have strict conditions for storage and handling. Also, the entire history of traceability of the vaccine should be available.

While tracking the supply chain of any commodity in general and pharmaceutical products in particular is always complex, COVID-19 vaccine poses tougher challenges. The following are the current temperature sensitivity needs of various vaccine manufacturers.



How some of the Covid-19 vaccines compare

Company	Type	Doses	How effective*	Storage
Oxford Uni-AstraZeneca	Viral vector (genetically modified virus)	x2	62-90%	Regular fridge temperature
Moderna	RNA (part of virus genetic code)	x2	95%	-20C up to 6 months
Pfizer-BioNTech	RNA	x2	95%	-70C
Gamaleya (Sputnik V)	Viral vector	x2	92%	Regular fridge temperature (in dry form)

*preliminary phase three results, not yet peer-reviewed

Source: Respective companies, WHO BBC

The information is from publicly available sites and should not be treated as a guideline for vaccine storage.

Blockchain to the Rescue

Even before the pandemic, Blockchain with its built-in ability of providing transparency across stakeholders has been a major platform for pharmaceutical traceability. The criticality for providing COVID-19 vaccine traceability has only strengthened the cause of utilizing blockchain for supply chain in the pharma industry.

Blockchain networks with its base attributes like de-centralized ownership of data, single version of truth across stakeholders, the ability to ensure the data ownership based on cryptography-based security and the ability to implement and manage business rules, will be a default platform handling the traceability of COVID-19 vaccines across multiple stakeholders.

Going beyond, Blockchain will also play a major role in Identity and Credentialing of healthcare professionals involved, as well as the Consent Management of the patients who will be administered the vaccine. With futuristic technology needs like Health Passport, Digital Twin of a Person, Blockchain goes a long way in solving the current challenges in healthcare beyond streamlining the supply chain.

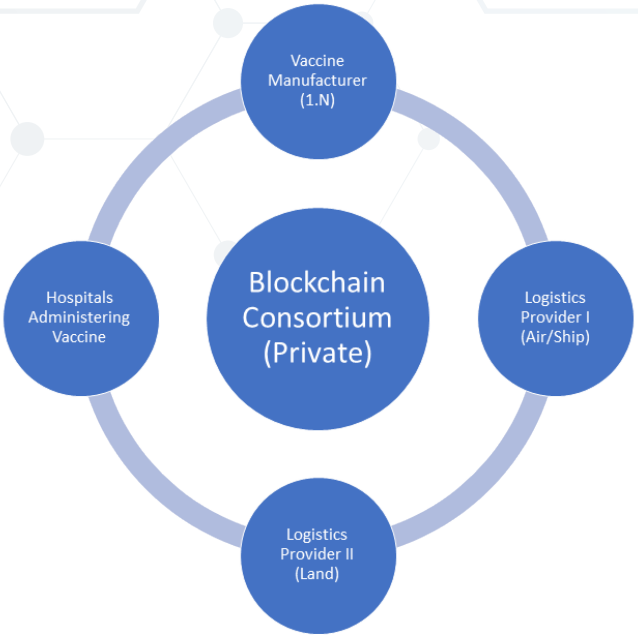
Blockchain Based Prototype for COVID-19 vaccine Traceability

We have created a prototype of Blockchain based network platform for vaccine traceability to demonstrate its usability. This solution has a much larger scope for extending to various healthcare use cases.

The below is the high-level process flow of COVID-19 vaccine trial and various stake holders involved.

Based on the use case and the stake holders involved. The prototype first creates a consortium using a private blockchain network. For the sake of simplicity, Distributors are not mentioned, but in real life every stakeholder will be present. Individuals who receive the vaccine from hospitals are not part of the Network at this stage. But in future their consent can be tracked using Blockchain.

Using Azure Blockchain Service, we can create private consortium blockchain networks where each blockchain network can be limited to specific participants in the network. Only participants in the private consortium blockchain network can view and interact with the blockchain. This ensures that sensitive information about vaccines are not exposed or misused.



The following smart contracts are created as part of the solution with assigned ownership to the individual stake holders.

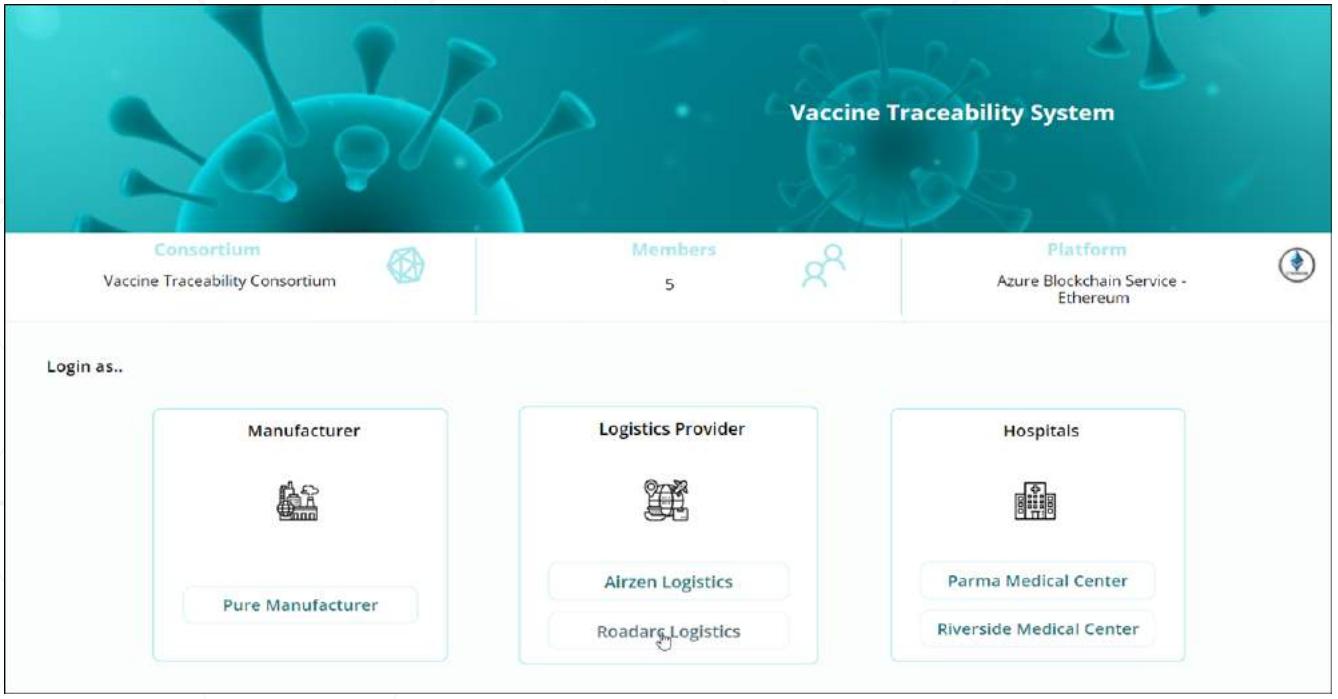
Contract Name	Contract Owner	Purpose
Batch	Vaccine Manufacturer	This contract has all the details of the batch. These details can be updated by the Manufacturer only.
AirLogShippingStatus	Air Logistics	This contract has the current and historic temperature and location details of the batch and it can be updated by air logistics only.
LandLogshippingStatus	Land Logistics	This contract has the current and historic temperature and location details of the batch and it can be updated by land logistics only.
ReceiptNote	Hospital Inventory Admin	This contract has the details of the hospital that received the batch and temperature maintained by the hospital.
Patient Vaccine Administration	Hospital Staff	This contract has the details of the patient who has received the batch of vaccine.

A glimpse of few of the smart contracts are listed for illustration purposes.

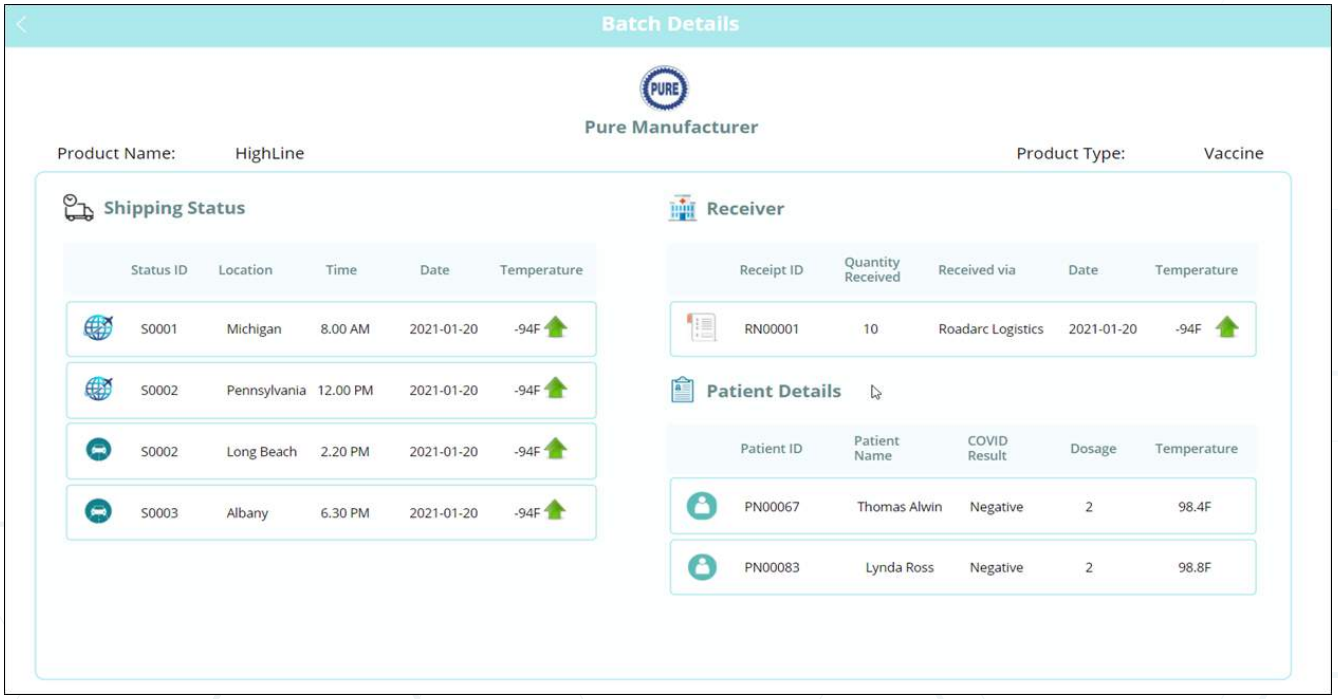
```
pragma solidity ^0.5.3;
pragma experimental ABIEncoderV2;
contract Batch {
    string  public BatchId;
    string  public ProductName;
    string  public ProductType;
    string  public TempratureMaintained;
    string  public Efficacy;
    string  public Cost;
    address public CurrentOwner;
    address public ManufacturerAddr;
    address public AirLogAddr;
    address public LandLogAddr;
    address public HospAdminAddr;
    address public HospStaffAddr;
    string[] public AirTemp = new string[](10);
    string[] public LandTemp = new string[](10);
    string[] public HospTemp = new string[](20);
    string  public receiptNoteaddr;
    constructor  (string memory _batchId, string memory _productName,  string memory _productType,  string
memory _TemperatureMaintained,  string memory _Efficacy,  string memory _Cost) public {
        ManufacturerAddr = msg.sender;
        BatchId = _batchId;
        ProductName = _productName ;
        ProductType = _productType;
        TemperatureMaintained = _TemperatureMaintained;
        Efficacy = _Efficacy;
        Cost = _Cost;
    }
    modifier onlyOwner()    {
        require (msg.sender == CurrentOwner, "Only Current Owner Can Initiate This Action");
        _;
    }
    function updateOwner(address _addr) onlyOwner public{
      CurrentOwner = _addr;
    }
    function retrieveBatchDetails() view  public returns (string memory, string memory, string memory, string
memory, string memory, address, address, address, address, address, string[] memory, string[] memory, string[]
memory, string memory) {
        return (BatchId,ProductName,TemperatureMaintained,Efficacy,Cost,Manu-
facturerAddr,AirLogAddr,LandLogAddr,HospAdminAddr,HospStaffAddr,AirTemp,LandTemp,HospTemp,receiptNot
eaddr);
    }
}
```

The front end (Dapp) through which the traceability of the COVID-19 vaccine can be monitored is also developed and the following screen shots show certain important data flows.

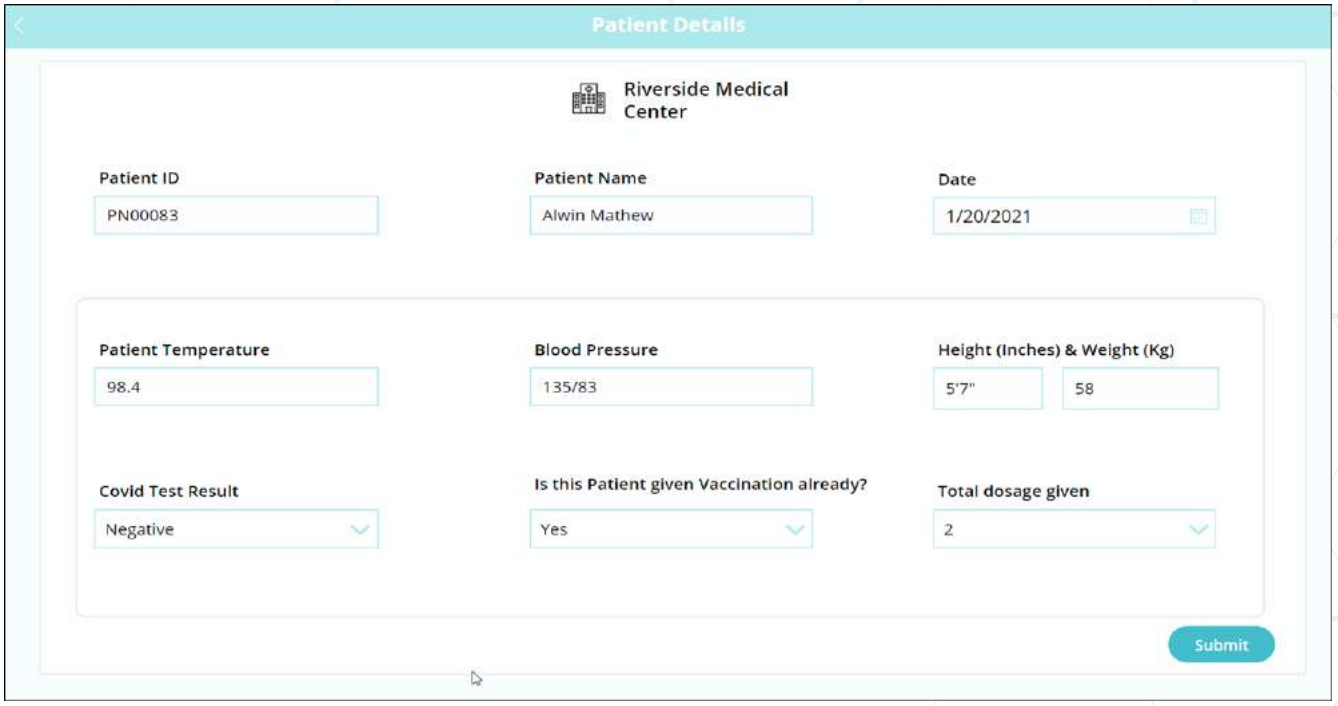
Vaccine Traceability System Login Screen



Traceability view for a particular batch of Vaccine



Details of vaccinated patients entered by hospital



Advantages of The Solution

- With every vaccine monitored over the blockchain, each link along the chain could keep track of the entire process, and health departments could monitor the chain as a whole and intervene, if required, to ensure proper functioning.
- Manufacturers could track whether shipments are delivered on time to their destinations.
- Hospitals and clinics could better manage their stocks, mitigating supply and demand constraints. Furthermore, they would get guarantees concerning vaccine authenticity and proper storage conditions.
- Individuals would have an identical guarantee for the specific vaccine they receive.
- Overall this technology driven approach will help to save the lives in this critical juncture.

Extensibility to Future Needs

Gartner's latest hyper cycle for emerging technologies highlight several new technologies and notably Health Passport. As the travellers used to travel with a physical passport pandemic has created the need for a health passport, which is more like a digital health record that passengers can carry on their phones. Ideally, it should show the passengers past exposure to diseases and the vaccine records. By properly deploying health passports, several industries can revive themselves by allowing free flowing movement of passengers across the globe.

The above blockchain solution though meant for COVID-19 traceability can potentially extended to a health passport once the patient also becomes part of it by a wallet based authentication mechanism, we plan to explore the health passports on Blockchain in the coming months.

LONG 80

A GAVS & PREMIER, INC. JV

www.long-80.com