HEALTHCARE INTEROPERABILITY USING BLOCKCHAIN TECHNOLOGY
Executive Summary

In the healthcare industry, there is a need for a secure data sharing framework that will consistently apply the right security access and functional controls for every connection and participant. Such a data information exchange framework should allow each participant or provider to manage a patient's records, while the patient retains control over which provider(s) can access the data. The framework should limit data replication within hospital records, and provide direct access to electronic health record (EHR) data wherever needed.

Blockchain technology can revolutionize how protected health information (PHI) is shared, simplifying, enhancing and securing collaboration between partner providers and patients. With the industry's increased focus on quality and continuity of care, access to patient records seamlessly across providers is a significant opportunity space for technologies like blockchain.

Challenges that demand healthcare interoperability and patient consent management include:
- Focus on continuity of care, as patients transition between one or more hospitals or clinics, their homes or post-care facilities.
- The need to know and intervene when a patient appears for service at different member or affiliate facilities.
- Specialized artificial intelligence (AI) and data analytics services that can improve and augment decision-making for providers, helping to improve patient care.
- Standardization of healthcare treatment (aka pathways).
- Creating a single source of truth for coordination of benefits with payers and for health revenue cycle management.
- Demand for specialty care or augmented services.
- Patient consent management in health information exchange (HIE) setting.

A major Midwest medical center together with Sirius conducted a technology proof of concept of blockchain for the representative use case “patient consent management.” This paper reviews the methodology and presents our findings.
Problem Statement

Providing healthcare to a patient population in a geographic region relies heavily upon access to patient records across providers in that region. Yet most providers today are operating independently, and access to medical records is available in a limited manner via point solutions that require heavy lift in terms of code and configuration. There have been formal partnerships across providers that develop into health systems where record access is again dealt with via system integrations. HIEs have achieved a certain level of success; however they introduce a new entity and formality around integration.

Although there are several technologies available to solve the interoperability and patient consent challenges, blockchain offers three distinct features to address the consent management of patients in a consortium setting. They include:

- **Trust**: Blockchain, through its distributed, immutable ledger framework and cryptography, helps to establish trust between patients and the provider consortium network. All participants have an up-to-date copy of the ledger, and it is consistent across consortium participants.

- **Contract governance**: Through Digital Smart Contracts, blockchain unleashes the power of digitalizing the legal contracts that govern the rights in sharing data between consortium providers, and gives patients the ability to grant the appropriate access to providers.

- **Shared control**: Healthcare interoperability between trusted providers requires a shared control responsibility in terms of the data they can access, own and share. At its core, blockchain solves the shared control through smart contracts, distributed ledgers and key infrastructures.

Consent Management With Blockchain

Below is a conceptual view of how patients manage consent for the sharing of their data across providers in a consortium. In this case, a major Midwest healthcare system consisting of three hospitals might enter into a joint venture or joint operating agreement. The primary and secondary organizations are Member Hospitals that have an exclusive Member HIE Contract to share all EHRs across hospitals. The Affiliate Hospital is part of the consortium, but with restricted data-sharing enforced via an “Affiliate HIE Contract.” For the proof of concept, the contract restricts the Affiliate Hospital to limited EHR records such as allergies and medications for a patient.
Patient-Concentric Provider Consortium

Key Elements

**Patient EHRs:** Include patient demographics, medical history, prescriptions, allergies, and other health-related information.

**Master Patient Index:** Patient record index stored in blockchain that is hash-coded and encrypted. Hash code uniquely identifies the patient and enables interoperability across the provider network.

**Member Hospitals:** Members of the health system. Data-sharing contracts are governed through the restrictions of being a Member Hospital; all member hospitals typically share data without restriction.

**Participating Hospitals:** Data-sharing contracts are governed through the restrictions of being Affiliate or Partner Hospitals.

**Third-Party Providers:** Any third-party hospitals that are not typically part of the consortium but would like to access the Master Patient Index on an on-demand basis. Third-party providers are not in scope for proof-of-concept purposes.

**Patients:** Patients of the consortium hospitals who give exclusive consent to view their health records.
For the evaluation, the following data attributes and sharing rules were considered:

<table>
<thead>
<tr>
<th></th>
<th>Patient Demographics</th>
<th>Allergy</th>
<th>Prescription</th>
<th>Order</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Member Hospitals</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2.</td>
<td>Participating Hospital 1</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>3.</td>
<td>Participating Hospital 2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4.</td>
<td>Patient</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Following are the use case steps:
1. Patient submits consent on blockchain to allow providers to view allergies, prescribed medicines, etc.
2. Smart Contract ensures HIPAA compliance
3. Authorized healthcare organizations approve access to data
4. Ledger is updated with approved healthcare organization
5. HIE portal provides real-time, single view of the health data from the approved healthcare organization

Patient Visits Member Hospital

A sample scenario would be a patient who receives care at a Member Hospital of the health system. Behind the scenes, the EHR and back-end infrastructure communicate with blockchain, and data is seamlessly copied across all member ledgers.
Patient Visits Primary Hospital

If the patient then visits the Primary Hospital, the EHR can query the ledger, retrieve the consent, and query the Member Hospital’s services to retrieve their records.

Patient Visits Affiliate

If the same patient visits an Affiliate Hospital or provider that does not have consent, the Affiliate Hospital is able to request consent from the patient and the blockchain can facilitate the process. The request for such a consent would be routed via a patient portal or mobile app.
Blockchain Architecture and Technical Details

The blockchain solution consists of three peer nodes (Primary Hospital, Member Hospital, Affiliate Hospital) built using Hyperledger Fabric technology. The blockchain nodes are containerized and docked using AWS Cloud Platform. Smart Contracts are developed using Golang, and integration is done using the Node.js SDK.

The UI layer is built to add, view and update the blockchain data. Blockchain is visualized using Blockchain Explorer, which is also implemented into AWS S3.

<table>
<thead>
<tr>
<th>Engagement Layer</th>
<th>A view of blockchain data. Visualizing the data of patients who have provided consent for data-sharing between consortia. UI shows patient information along with allergies, medications and events.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Layer</td>
<td>Node.js SDK for Hyperledger Fabric. Web app uses the Node.js SDK to query/update the blockchain.</td>
</tr>
</tbody>
</table>

**Business Network**

<table>
<thead>
<tr>
<th>Primary Hospital Organization</th>
<th>Member Hospital peer that has the ledger data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member Organization</td>
<td>Member Hospital peer that has the ledger data.</td>
</tr>
<tr>
<td>Affiliate Organization</td>
<td>Affiliate Hospital peer that has the ledger data.</td>
</tr>
<tr>
<td><strong>Smart Digital Contracts</strong></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| **Smart Contract (Query, Invoke the Block Chain Data)** | Two Smart Contracts are developed as part of the proof of concept:  
  - Member HIE Contract  
  - Affiliate HIE Contract |
| **Member HIE Contract** | Enables and governs the contractual rules in patient EHR data exchange between Member and Primary Hospitals. |
| **Affiliate HIE Contract** | Enables and governs the contractual rules in patient EHR data exchange between Affiliate and Primary Hospitals. |

<table>
<thead>
<tr>
<th><strong>Technology Selection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hosting Platform</strong></td>
</tr>
<tr>
<td><strong>Blockchain</strong></td>
</tr>
<tr>
<td><strong>Smart Contracts</strong></td>
</tr>
<tr>
<td><strong>Integration APIs</strong></td>
</tr>
</tbody>
</table>

**Data Privacy and Security**

Hyperledger Fabric provides options to encrypt the data as required by the use case. It also provides a channels mechanism that helps to keep the data private between specific participants. Below are few mechanisms that were explored for data privacy and security:

- Cryptography-enabled data encryption
- Data privacy using Hyperledger Fabric Channels
- Certificate authority setup to sign, endorse and validate transactions
- Optional public key infrastructure (PKI) setup for certificate interoperability

**Conclusion**

The proof of concept has successfully demonstrated that blockchain is a good technology fit for interoperability across providers in a region. There are some prerequisites before there can be a plan to implement:

- Implementation of an Enterprise Master Patient Index (EMPI) that maintains a master list of patients across multiple provider EHR systems.
- A framework to expose data from EHR systems with permissions that can be tokenized and encrypted. Only encrypted permissions to data access endpoints (services) are stored in the blockchain.
- Sharing of the patient consent information from the EHRs with the blockchain platform.
We recommend a deliberate process that is implemented in phases:

The steps would be:
- Complete Master Patient/Provider Index
- Expose FHIR services to the ESB
- Automate workflow around MyChart Accessibility
- Get executive buy-in and funding to further invest in the technology
- Strategic alliance with vendor to build the pilot solution

For more information about blockchain solutions for healthcare and other industries, speak to your Sirius representative, call Sirius at 800-460-1237, e-mail info@siriuscom.com, or visit siriuscom.com/blockchain.