2025 M Street NW, Suite 800
Washington, DC 20036
(202) 367-1196 • (202) 367-2196
info@namss.org • www.namss.org

NAMSS 2017 Roundtable

Building Blocks for the Future

May 18, 2017

Background

The NAMSS Roundtable Series began in 2014 after a decision by the NAMSS Board to collaborate with other healthcare industry stakeholders on moving toward a more streamlined, more efficient, and less burdensome credentialing process.

The first Roundtable – held in May 2014 – focused on a set of Ideal Credentialing Standards (ICS) for facility provider credentialing. These standards are meant to serve as best practices for all facilities and to promote greater uniformity on the information and primary sources necessary for credentialing.

The following year, Roundtable participants worked together to create a similar list of best practices for the credentialing of providers by payer organizations. This set is called the Essential Common Data Elements for Payer Credentialing.

In 2016, NAMSS presented a draft of the Model Credentialing Application and the Verification of Graduate Medical Education Training Form. These documents – like the sets of best practices developed in previous years – were meant to eliminate inefficiencies in provider credentialing.

2017 Roundtable

This year, NAMSS took the Roundtable Series in a somewhat different direction, focusing on blockchain technology. This idea was brought to NAMSS during a meeting with the Federation of State Medical Boards (FSMB) in early 2017.

NAMSS and Hashed Health – a blockchain technology consortium focused on healthcare applications – presented the potential application of blockchain technology for provider credentialing.

Blockchain technology is a decentralized peer-to-peer system through which digital transactions are created, shared, verified, and stored. This technology consists of three main components: a distributed network, a shared ledger, and digital transactions.

A distributed network is essentially the decentralized architecture for the blockchain. It is a web of individual network members who both generate and verify data generated by others. However, rather than sharing data into a centralized repository, each network member stores an identical copy of the entire blockchain and contributes to the process of verifying digital transactions in the digital network. In the case of credentialing, the individual members in the

distributed network would include training programs, licensing boards, certification boards, Medical Services Professionals at hospital and managed care organizations, etc. Essentially, anyone involved in the generation or verification of provider data necessary for credentialing would play a role in this distributed network.

A shared ledger is the mechanism by which information is shared and verified by members in the distributed network. Data is generated by a member and is recorded in the shared ledger. If the majority of the network members verify the transaction is legitimate, the data is included in the shared ledger. For credentialing purposes, the shared ledger could be a provider's credentialing profile, which would contain all of the information currently necessary for verification. As the provider completes each phase of his or her career – training, licensure, board certification, a change in employment, etc. – the shared ledger would be updated by the individual or organization responsible for that information and then pushed instantaneously to every other member in the distributed network.

A digital transaction in a blockchain is the actual act of generating or verifying data. Data is encrypted and certified to ensure it is both accurate and from an appropriate source. Transactions are structured into blocks, and linked to the existing blocks in a linear, chronological chain. These blocks are immutable. In the example of credentialing, each new credentialing element that is generated by any member and is then verified by other members would be the digital transaction. For instance, when a provider completed their residency training program, the program director would document ***and provide the primary source verification*** in the blockchain. This information would then be available to others that need to view this verified information in the blockchain.

The participants discussed this potential, as well as the potential pros and cons of adoption. Below are the main points raised during the roundtable:

1. Questions about the security of the network and how to assure only appropriate individuals and organizations would be able to input and verify provider data.

2. Questions about how organizations who currently derive financial profits from data and data exchange could continue to do so under a blockchain provider credentialing system.

3. The desirability of creating a minimally viable network demonstration, in which interested stakeholder organizations could pilot a blockchain credentialing system around static provider data.

4. Pursuing a lobbying strategy – either with Congress (through the Blockchain Caucus) or the Center for Medicare and Medicaid Innovation (CMMI) – for federal dollars to support a pilot blockchain provider credentialing system. Such a system could generate significant savings for the Medicare system through the elimination of administrative costs.

5. Development of an ongoing working group to continue discussions around implementing a blockchain provider credentialing system.

Next Steps

NAMSS will organize a Working Group of stakeholders to flesh out the five points raised and address other concerns and opportunities with the goal of developing a proof of concept. The proof of concept should not be overly ambitious but work to address a few pain points within the credentialing process.

The project should develop the technology and governance structure for the blockchain simultaneously. The ultimate goal would be to create a credentialing blockchain that is secure, transparent, and efficient that reduces credentialing costs.

Attached is a report by Hashed Health outlining two potential blockchain structures in greater detail.

Appendix: Blockchain Enabled Provider Identity Management Prototype Summary

Current State

Providers must be credentialed and approved to treat patients, write prescriptions and receive payment. The process of synchronizing which providers are credentialed for certain payers and patients is a mess. Oftentimes, over 20 percent of the data in a payer's directory is incorrect. What would it be like if that same percentage of addresses in Google Maps was incorrect?

The reason the credentialing process can be inefficient and inaccurate is largely because the current process of confirming provider credentials, granting physician privileges and enrolling physicians in payer networks is managed through many different systems and many different times. When compounded across thousands of physicians for a payer or a large provider network, it leads to big headaches and wasted dollars that are eventually passed along to the consumer.

For physician practices, networks and health systems, the process of provider credentialing is lengthy and costly. A majority of credentialing processes take in excess of 120 days. This process has a direct financial impact, impeding the ability of a physician to provide services and receive payment for those services. Provider credentialing is the first step and is directly related to revenue cycle processes.

For health plans, the process of enrollment is likewise lengthy and cumbersome, varying from as little as 60 days to over 180 days. Beyond enrollment, health plans face significant regulatory risk over the quality and accuracy of the provider data contained in their directories. It is estimated that 12 to 18 percent of directories are incorrect or out-of-date. Over 20 states have regulatory requirements for health plans to frequently maintain accurate physician directory information under penalty of fines and other levies. In addition, CMS similarly requires directory maintenance. Beyond regulatory penalties, bad provider data can cause delay in

claims processing and inaccurate payment denials. The scale of this problem is not insignificant, as it is estimated that 30 to 40 percent of all provider files have inaccuracies.

To compound the problem, these processes are rife with inconsistent data formats and workflows. These manual processes are largely duplicative, requiring providers and payers to submit largely the same data to multiple entities and to resubmit to maintain their credentials and enrollment status in many systems. It's a messy, cumbersome and ultimately costly process that has real consequences for billings, regulatory enforcement, physician engagement and, ultimately, patient care.

Distributed Provider Data Assets

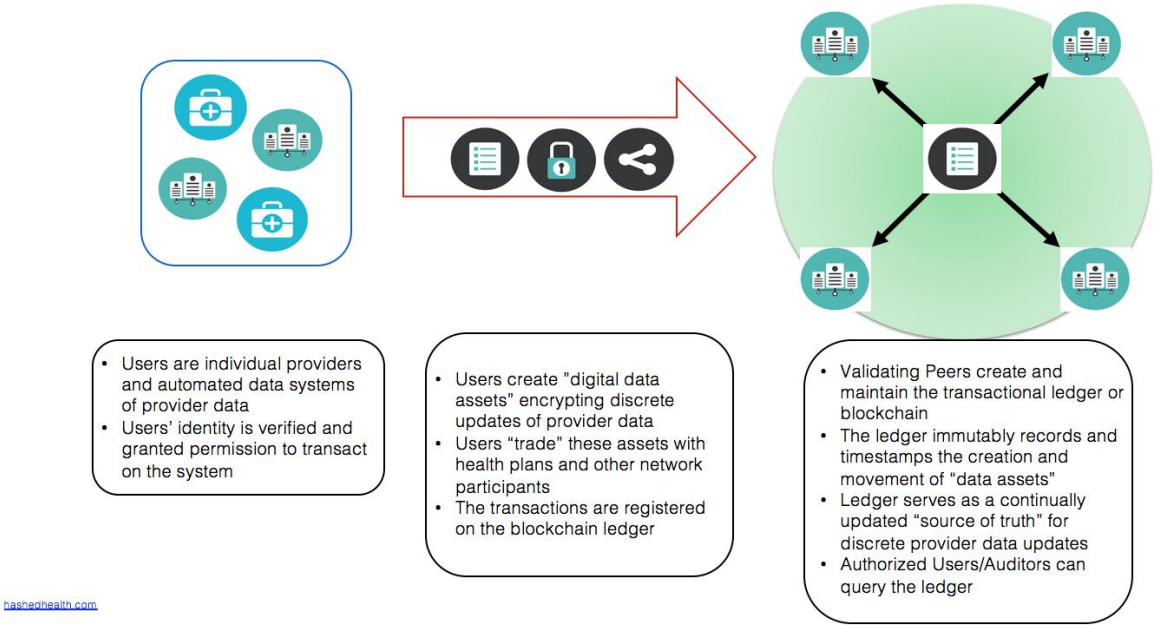
Hashed Health's Provider Data Management project moves beyond the current trend of "digitizing" the collection and management of provider data. From electronic forms to centralized data stores, current efforts are streamlining the manual process of provider data collection by replacing them with digital interfaces. However, centralized approaches fail to cope with the fractured nature of the U.S. health system with a dizzying array of health plans, provider practices and health systems. What is required is not another centralized, universal data store but rather a decentralized transactional layer allowing providers, health systems and health plans to share updates and corrections of provider data files.

Hashed Health has built a test chain to demonstrate the essential benefits of a decentralized transactional layer.

The core function enables plans and individual providers to create and exchange "digital data assets" which can be securely distributed to network members via a permissioned, distributed ledger system. By "tokenizing" provider updates, the system creates trackable data assets which can be distributed to multiple network participants. The reporting of the all asset changes to the distributed ledger ensures that provider data is up-to-date and consistent across multiple entities as well as internal, siloed data systems. The proposed solution architecture builds upon the current "data store" model, introducing a "transactional" model that enables greater liquidity of data.

Prototype 1 – Health Plan Provider Data Sharing – Hyperledger Fabric v0.6

Figure 1 – Process Flow



Prototype 2 & 3 – Provider Licensing and Third Party Attestations – Hyperledger Fabric (HL) v0.6 & Ethereum

Smart Contract configuration enables Third Party (Primary Source) Attribute **Stakeholders** to securely attest to attributes via digital signature appended to individual **Provider** contracts. This removes the need for middlemen to independently attest to a providers credentials or for providers to coordinate third party communication with credential authorities, i.e., State Medical Licensing Bodies, Health Systems, etc.

The core functionality of the two prototypes are essentially the same, as outlined above. The following are key differences:

- HL allows for full transactional confidentiality at the expense of a cumbersome enrollment or membership services process.
- Ethereum allows to a streamlined and automated enrollment process but requires full transactional transparency.

Figure 1 - HL & Ethereum Process Flow: Utilizing HL Chaincodes and Ethereum Smart Contracts respectively

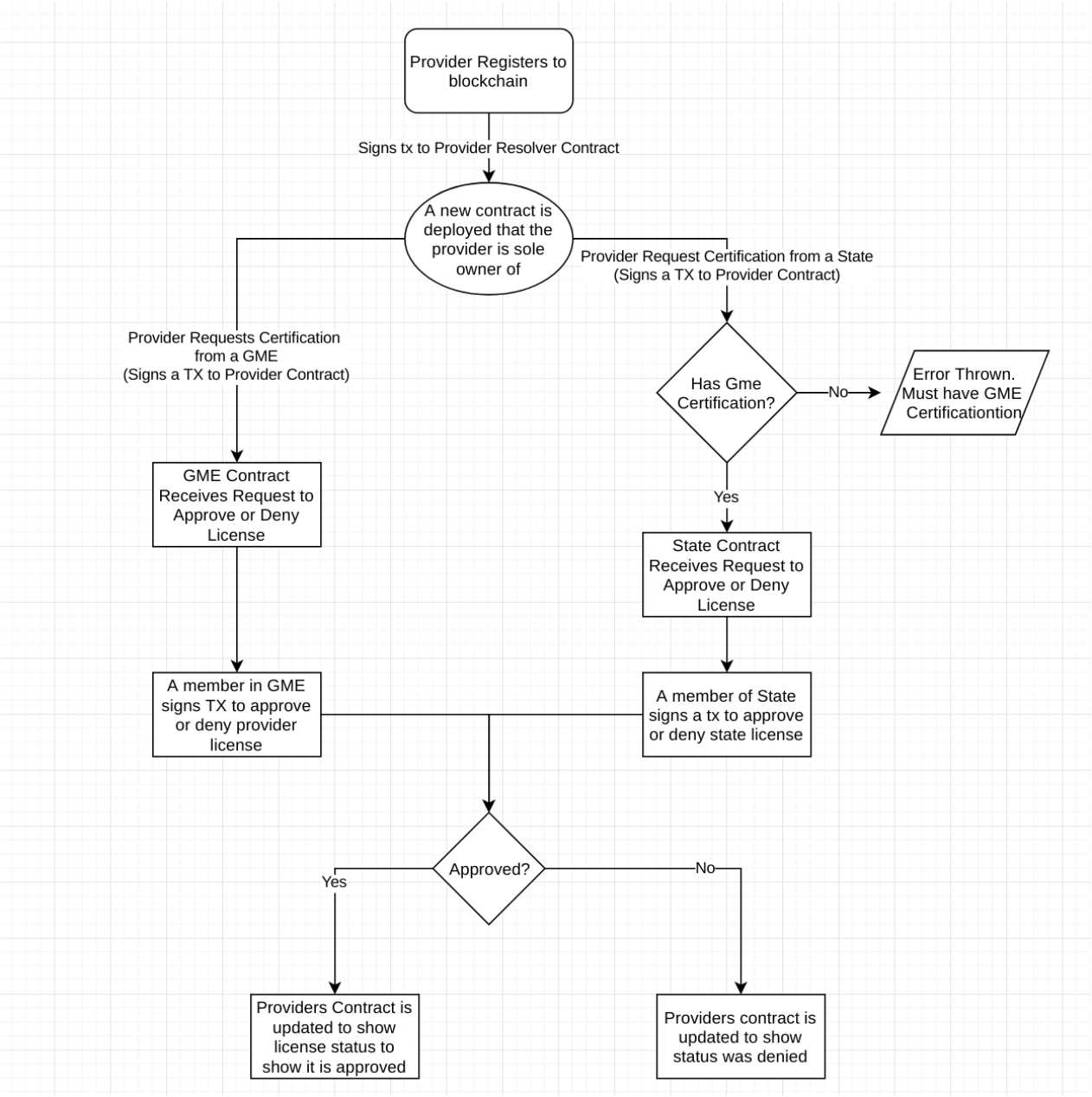


Figure 2 - Ethereum User Enrollment Process: Ethereum prototype utilizes “Resolver” Contracts.

- For the **Provider** (outlined in Fig 1), a Resolver Contract creates a Provider owned and controlled account to which can be added third party attestations.
- For the **Stakeholder**, type specific Resolver Contracts create organizationally owned and controlled accounts and a process to assign “signatory authority” to authorized individuals.