Decentralized Identity and Healthcare

Part 1

The Importance of Strong Governance

Lumedic

Contents

Introduction **3**

An Introduction to Lumedic Connect **5**

Current Problem 5

Current System Architecture 5

The Opportunity for a Patient-Centered Solution 6

Overcoming Current Challenges to Patient-Centric Health Information. 6

The Enabling Technology and Governance Stack 6

Technical Trust vs. Human Trust. 9

The Trust Over IP Stack 9

A Patient-Centered Model Realized 15

Conclusion **16**

Introduction

Lumedic Connect software, combined with the Lumedic Exchange community, creates a 4-layer ecosystem which makes it possible to, for the first time, allow an individual to be the source of their own data within the healthcare system and beyond. This structure changes the way in which we exchange healthcare information that prioritizes individual privacy and autonomy, creates new efficiencies for healthcare organizations, and allows non-healthcare organizations to leverage individual health data simply. While such a system is a dramatic restructuring of today's methods of health data exchange, Lumedic Connect also maintains adherence to HIPAA as required and, in several key areas, extends it beyond the capabilities of current systems.

The Lumedic Connect Platform provides a set of technologies, patterns, and interfaces for organizations and individuals to exchange health information. By fundamentally rethinking today's assumptions on how healthcare information must be exchanged to and from healthcare systems, health plans, businesses, and individuals, Lumedic has created a solution and ecosystem that is more secure, more patient-centric, more effective at preserving patient privacy, and less costly and resource intensive for institutions managing and utilizing individual health data.

This is accomplished by using modern, distributed ledger technologies to introduce the concept of an immutable public identity for organizations wishing to exchange healthcare information, while also introducing an immutable and private identity for individuals themselves. Using this identity system as the foundation for Lumedic Connect, the network can facilitate the transfer of individual health information in the form of portable, trusted, verifiable digital credentials.

The network prioritizes the individual as the controller of their own data using personal digital devices, improving privacy preservation. Additionally, organizations receiving information from individuals are able to validate the source of the information using cryptography anchored on a public, immutable ledger, ensuring that the information shared by the individual is authentic. In doing so, organizations can rely on the individual and their personal digital devices as the medium of exchange, and not on legacy institutions and 3rd parties that require costly technology integration efforts, hindered by non-standardized technology interfaces.

The result is a "trust" system that prioritizes individual privacy, grants individuals autonomy with respect to their own health data, and makes it possible for organizations within and outside of the healthcare system to seamlessly verify and utilize the precise individual health information they need, when they need it.

This document is the first of two papers that describe how modern technologies, using decentralized systems, provide practical approaches to improving the exchange of patient health information.

The second document (titled Decentralized Identity and Healthcare Part 2: Patient-centricity Fulfills HIPAA) details a step-by-step workflow of Lumedic Connect and why each step does not implicate or violate HIPAA.

This document presents Lumedic Connect as a superior means of exchanging health data—specifically:

- Lumedic Connect presents an alternative means of exchanging health data that improves individual privacy and autonomy, creates greater efficiency within the healthcare system, and minimizes the disclosure of protected health information
- Lumedic Connect gives individuals greater access to and control of their personal health information
- Lumedic Connect enables verification of the authenticity of information shared with individuals and other network participants
- Lumedic Exchange provides the community-driven governance frameworks necessary to ensure accountability and trust in a decentralized model.

An Introduction to Lumedic Connect

Current Problem

Recent studies estimate the amount of waste in the US Healthcare system to be between $760 billion and $935 billion per year. Of that total, administrative complexity leads to the highest amount at roughly $265 billion per year.[1] Much of the administrative waste is related to billing and insurance related (BIR) communication, which is often the result of incompatible and antiquated technology systems, standards, and mechanisms for exchanging information. Because of this, healthcare organizations must often default to manual processes and non-technical means of communication to conduct regular operations, compounding the complexity of the overall system. The result is interoperability challenges that channel money into administration rather than patient care.

Current System Architecture

Currently, the healthcare industry must abide by the regulatory requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) when managing protected health information (PHI). Written before the widespread adoption of the Internet, HIPAA sought to mandate that institutions protect the health information they collected from their patients or members. Because of this, throughout any individual's journey in the healthcare system, from registration to the final bill, most individual financial and health information is passed between institutions, with the individual playing a facilitating role only if needed. The result is that the individual cannot act as a controller of their own health experience from the standpoint of their own data, but only as a passive observer who retroactively receives results and, of course, bills.

At the same time, to the organizations that are transacting this data, HIPAA grants broad authority to use a variety of systems. Organizations can even build their own systems using their own data schemas and definitions. The result is a wide variability in computer systems and data availability from one organization to the next.

[1] https://www.businesswire.com/news/home/20191007005615/en/Journal-American-Medical-Association-JAMA-Publishes-Humana; JAMA Network article here.

At the same time, to the organizations that are transacting this data, HIPAA grants broad authority to use a variety of systems. Organizations can even build their own systems using their own data schemas and definitions. The result is a wide variability in computer systems and data availability from one organization to the next.

When one organization sends data to another, if the two systems are not following the same standards, the information needs to be transformed before it can be properly received and utilized. An entire industry of intermediaries has arisen to address this problem and perform these data transformations at scale. The result is an information exchange that is woefully inefficient, requiring cumbersome, customized technology interfaces and costly services and transaction fees to ensure compatibility and regulatory compliance. With these varied methods and systems comes inherent organizational risks as each healthcare organization must ensure the security of each of these systems and the privacy of the information contained within them in order to maintain HIPAA compliance.

The Opportunity for a Patient-Centered Solution

All these information sharing issues can be addressed by fundamentally shifting the patterns of data exchange in healthcare to focus on the individual as the source and steward of their own data. By architecting a system where all relevant parties look to the individual first for their own health data, coverage information, and any other data directly relevant to the individual's healthcare experience, we can envision a solution where interoperability issues vanish.

Throughout an individual's care journey, there is one constant at every point: the individual themselves. By making that individual the source of their data and by providing a simple, secure, and standardized interface for that individual to exchange that data with the appropriate parties, inter-organizational integration ceases to be a requirement. **Additionally, individuals are now able to take their own healthcare information beyond the healthcare space and can choose to use that data for any number of non-healthcare related reasons.**

Overcoming Current Challenges to Patient-Centric Health Information

Three challenges have traditionally made such a model impossible:

1. If we are going to expect individuals to participate in the healthcare administrative process, we need to ensure **simplicity of use and protections for people against making mistakes.**

2. If we are going to expect organizations to trust the information provided to them from an individual, the data needs to be **completely tamper-proof and verifiable.**
3. If we are going to expect industry adoption, the approach **needs to be compliant with regulations, including HIPAA.**

Modern technologies, and specifically decentralized identity networks built on top of distributed ledger technologies, make it possible to address all three challenges. While Point 3 above is addressed in a second document (Decentralized Identity in Healthcare Part 2: Patient-centricity Fulfills HIPAA), in this document we will explain how:

1. This new patient-centric model radically simplifies the process of exchanging information, resulting in less need for third party intermediaries, lower technology costs for organizations, and fewer delays in care.
2. Lumedic Connect provides a platform over which organizations and individuals can transact health information in a way that is secure and private and prioritizes the individual as the controller of their own data.
3. Relationships and transactions using Lumedic Connect are governed by a common set of standards established by the Lumedic Exchange community, which is a group of organizations aligned around a common governance model for how information is securely exchanged using the Lumedic Connect protocol.
4. Data itself, as well as the originator of the data, can be verified by any other party in a secure and trusted way.
5. This model introduces novel methods for non-healthcare organizations to use individual health information with the individual's direct, auditable consent—a benefit that has never been possible before.

The Enabling Technology and Governance Stack

The patient-centric approach is made possible by building a system that enables the exchange of health information over a decentralized network that enforces security and trust at every point. Such a network is a combination of organizations, governance, and technology—a combination that can produce a complete end-to-end solution for all parties, one that ensures that the provenance, security, privacy, integrity, control, and consent over exchanged information can always be verified.

This new form of decentralized network is achieved by a four-layer stack developed by experts in distributed ledger (blockchain) technology, digital

identity, mobile computing, and trust frameworks. Named the Trust over IP stack, it directly parallels the TCP/IP stack that is the basis for the Internet itself. Both are open standards developed for universal interoperability, and both enable any two peer devices on the Internet to connect and exchange data. The key difference is that the ToIP stack layers on top of the TCP/IP stack in order to address the difficult security, privacy, data protection, and other requirements of trusted data exchange that were not addressed by the TCP/IP stack.

As shown in Figure 3, the ToIP stack is unique in that it combines both governance (on the left) and technology (on the right). This is how it incorporates both the human elements of digital trust—the legal, regulatory, business, and social requirements—with the technical requirements for trust—cryptography, distributed networking, trusted execution environments, mobile computing, etc. For the Lumedic Connect solution, governance is defined and managed by the Lumedic Exchange, a community of organizations in the healthcare and related spaces whose mission is to transform healthcare by establishing a common set of standards that empowers patients to easily share – and ultimately control - their own health information in a verifiable and trusted way.

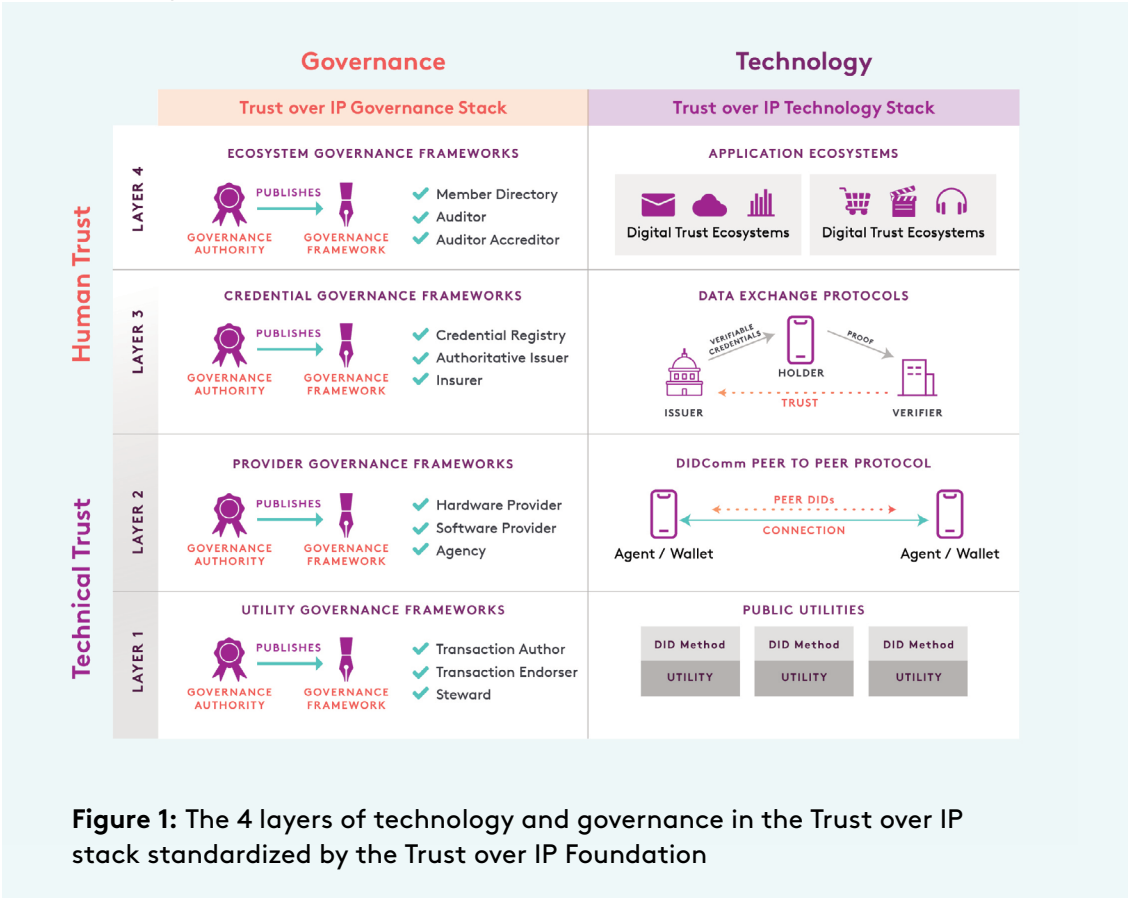

Figure 1: The 4 layers of technology and governance in the Trust over IP stack standardized by the Trust over IP Foundation

Technical Trust vs. Human Trust

As Figure 3 suggests, the bottom two layers of the ToIP stack are designed to provide technical trust—the assurance that any two ToIP-enabled devices can establish a secure, private connection and exchange cryptographically verifiable data. Although these two layers ultimately operate under human governance, trust at these layers is established entirely between machines.

By contrast, the top two layers are designed to establish human trust—exchange of the data people and organizations need to make real-world trust decisions.

This approach, which achieves a trust framework for a decentralized solution by enabling both machine and human trust, enables Lumedic Connect to fully create a model for trusted, patient-centric interactions in healthcare. To fully appreciate how all four layers of governance and technology make this possible, we will provide a brief explanation of each layer.[2]

The Trust Over IP Stack

Layer 1: Public Utilities

The purpose of Layer 1 is to establish strong cryptographic roots of trust for the security needed at the higher layers. This is the layer that takes advantage of the unique security and availability capabilities of blockchains and distributed ledgers. In the case of the ToIP stack, these capabilities have nothing to do with cryptocurrencies (the best-known use of blockchains). Rather, the primary advantage of immutable public ledgers—that they are all-but-impossible to tamper with, even for the largest nation states—are harnessed for a simple purpose: to store the public keys and other cryptographic metadata needed to support public key infrastructure (PKI).

This new layer of PKI is referred to as *decentralized public key infrastructure* (DPKI). DPKI uses the same fundamental cryptography as the current centralized PKI that powers trust on the World Wide Web, i.e., the X.509 digital certificates used by the secure SSL/TLS connections managed by any internet browser, indicated by the lock icon in a browser. The difference is that public keys no longer need to be registered with a small number of certificate authorities (CAs) whose own public keys must be built directly into our browsers and other software (long recognized as a single point of failure in PKI).

[2]To explore the ToIP stack in more detail, see the ToIP Foundation white paper or review the Hyperledger RFC.

Instead, public keys can now be registered directly by their owners on a blockchain, distributed ledger, or other *verifiable data registry* using a new open standard from the World Wide Web Consortium (W3C) called Decentralized Identifiers (DIDs).[3] With DIDs, the ability to register and verify public keys and other cryptographic metadata not only becomes dramatically easier and less expensive, but the underlying infrastructure is less vulnerable to attacks or lapses in availability.

DPKI has the flexibility to rely on a variety of Layer 1 blockchains or distributed ledgers (what the ToIP stack refers to as a public utility). Each of these utilities use the governance model or framework best suited to the needs of its trust community (see the Sovrin Governance Framework for an example). Lumedic Connect will use only the Layer 1 public utilities that meet the strict security, privacy, availability, and data protection requirements of the Lumedic Exchange Governance Framework (see Layer 4: Application Ecosystems).

Layer 2: DIDComm Peer-to-Peer Protocol

While Layer 1 is all about publicly accessible cryptographic infrastructure, Layer 2 is all about private, peer-to-peer communications. This is the layer of digital agents and digital wallets that people and organizations need to store cryptographic keys and establish private, peer-to-peer connections using an open standard secure messaging protocol. For the ToIP stack, this is the DIDComm protocol that originated in the Hyperledger Indy project and is now being standardized in the DIDComm Working Group at the Decentralized Identity Foundation (DIF).

All interactions at Layer 2 take place over private, secure, peer-to-peer connections directly between the two parties to a data exchange relationship—doctor-to-patient, patient-to-hospital, patient-to-payer, and so on—with no intermediaries. These connections use a special type of DID called a peer DID. Every new ToIP relationship made using Lumedic Connect generates peer DIDs that are exchanged directly, peer-to-peer, every time. Each peer DID is a **pairwise pseudonym** given to the other party and stored in the digital agents and wallets. The result is that no personal data is stored on a public blockchain or other immutable distributed ledger.

The DIDComm protocol used to communicate between all agents and wallets uses end-to-end encryption by default. This means cloud agents—Layer 2 agents that are hosted in the cloud so they can send and receive messages 24x7 just like email servers—are not in a position to "leak" any of the data in

[3]The DID specification is currently in the final stage of standardization at W3C. Lumedic's implementation partner Evernym co-chairs this Working Group. See https://www.w3.org/TR/did-core/

DIDComm messages. They simply do not have access to the data. They only have the ability deliver it to the next agent along the "technical trust tunnel" connecting the ultimate sender and receiver of the message.

Layer 2 also has its own dedicated type of governance framework—one designed explicitly to establish the privacy, security, and data protection standards against which ToIP-compatible hardware, software, and cloud hosting providers for digital agents and wallets can be certified. Again, Lumedic Connect will only use Layer 2 digital agents and wallets that meet the stringent security, privacy, and data protection requirements of the Lumedic Exchange Governance Framework.

Layer 3: Data Exchange Protocols

The machine trust established and supported in Layer 1 and Layer 2 are the foundation of what make it possible to have distributed, trusted human interactions (the exchange of healthcare information) using Layer 3 and Layer 4. At Layer 3 we shift from technical trust to human trust—and to the digital trust model at the very core of the patient-centric paradigm of Lumedic Connect. This model can be summarized in a single diagram (Figure 4) from the W3C Verifiable Credentials standard called the *trust triangle*.[4]

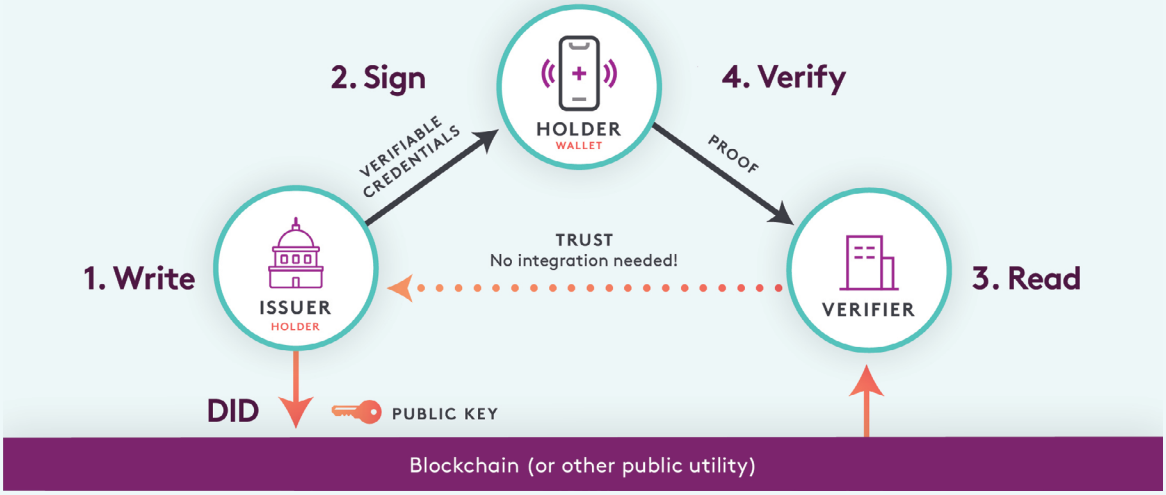

Figure 2: The W3C Verifiable Credentials Trust Triangle

[4]The W3C Verifiable Credentials Data Model was approved as a full W3C Recommendation in September 2019. https://www.w3.org/TR/vc-data-model/

What the trust triangle illustrates is the same trust model that applies to how we establish identity and trust in the real-world today—using credentials that we obtain from trusted authorities, store in our wallets, and present to verifiers when they need us to prove some aspect of our identities—can be adapted to the digital world. And not only is it decentralized, *but none of the roles or relationships need to change*. The only difference is that the credentials are in digital form; they are obtained, stored, and shared using digital protocols; and they are verified using cryptography instead of manually by humans.

At Layer 3, the digital agents and wallets from Layer 2 play the three critical roles in the patient-centric model: The *issuer* of health information, the *holder* (for example, a patient holding their own data), and the *verifier* (any organization the holder chooses to share their information with). Health information is exchanged on this model in the form of verifiable credentials (See sidebar: "Key Concepts in Lumedic Connect). A typical exchange is as follows:

1. By joining the Lumedic Exchange the issuer (for example, an insurance provider) writes a Decentralized Identifier (DID) together with its public key (and any other cryptographic material needed for the issuer's verifiable credentials) to the Layer 1 Network.[5]
2. The issuer uses its private key to digitally sign a verifiable credential (for example, a credential detailing individual insurance coverage information) it issues to a qualified holder (for example, an insured individual), who stores that credential in their own digital wallet. Note that for privacy preservation, this entire issuance process takes place "off-ledger", i.e., the interaction is directly between the issuer's agent and the holder's agent and does not involve any transactions with the Layer 1 public utility.
3. A verifier (for example, a healthcare provider) requests a digital proof of one or more credentials from the holder (for example, insurance eligibility information for registration). If the holder consents, the holder's wallet generates and returns the proofs to the verifier. Since the proofs contain the issuer's DID, the verifier uses it to read the issuer's public key and other cryptographic metadata from Layer 1.
4. In the final step, the verifier uses the issuer's public key to verify that the proofs are valid and that the digital credential has not been tampered with.

A critical aspect of the proof described in Step 3 above is the option to utilize a special branch of cryptography known as zero-knowledge proofs (ZKP). Using a ZKP enables a holder to prove facts about the data in a

[5]This cryptographic material can include *revocation registries*—a powerful way to provide near-real time revocation of previously-issued digital credentials that does not require verifiers to integrate or communicate with issuers in any way.

credential without revealing the underlying data. For example, the holder of a ZKP-based driver's license could prove to a verifier (the bartender) that the holder is older than the legal drinking age without revealing the holder's birthdate—or any other information on the driver's license.

In the context of healthcare and protected health information (PHI), this is a tremendous benefit. An individual is now able to provide organizations with outcomes driven by their own PHI without disclosing that information itself. The benefits here extend to verifiers as well. Not only can an individual maintain absolute privacy as it relates to their own health data, but verifiers—and specifically verifiers outside of the healthcare space—are able to operationalize individual health information in any number of ways (given the individual's consent) without having to take on the burden of needing to manage that data.

Layer 3 is also where the ToIP governance model comes into full bloom through the introduction of a second trust triangle—the governance trust triangle shown in Figure 3.

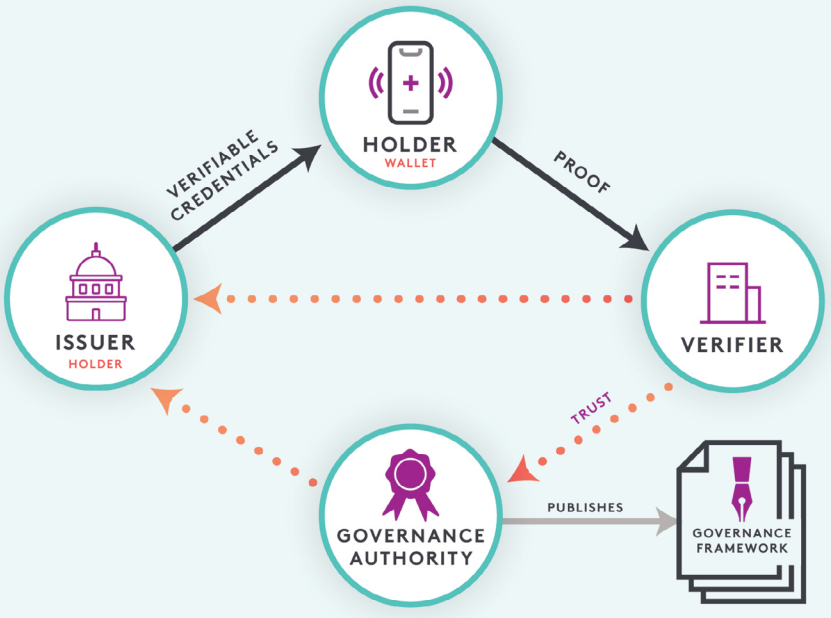

Figure 3: The second trust triangle—how credential governance frameworks work with verifiable credentials

Governance frameworks managed by governance authorities who are widely trusted by verifiers—be they governments, industry consortia, or NGOs—are the way trust networks scale. For example, in the credit card industry, Mastercard and Visa govern two of the largest trust networks in the world. Every digital credential on Lumedic Connect is backed by a governance framework defined and managed by the Lumedic Exchange that outlines the business, technical, and legal rules under which the credential operates.

Layer 4: Application Ecosystems

Layer 4 is the application layer of the ToIP stack—the layer in which the functions of the three lower layers are combined not just into standalone applications, but into entire ecosystems of applications that orchestrate sophisticated workflows that can safely cross trust boundaries of any kind—countries, industries, networks, domains, databases—by speaking a common language and following the policies defined by each governance authority and governance framework involved.

Lumedic Exchange is just such an ecosystem. It uses the unique capabilities of the ToIP stack to enable secure and private patient-centric data exchange between any two members of the Lumedic Exchange - patients, providers, payers, or any other participants in the healthcare system. Lumedic, together with our partners, will serve as the governance authority for this ecosystem via the Lumedic Exchange Governance Framework ("LXGF") —a comprehensive set of policies covering security, privacy, data protection, inclusion, auditing, and regulatory compliance.

Because LXGF is a Layer 4 governance framework, it can set the base level of policies that **must be observed by all applications, services, and participants on the network.** This means participants on the network—as long as they are satisfied with the ecosystem-level privacy policies—do not need to check (or even worry about) the privacy policies of the other participants. They know that the entire ecosystem is collaborating to protect their privacy.

This is one of the most powerful features of Lumedic Connect. By leveraging the Lumedic Exchange Governance Framework shared by all members, it can implement robust privacy preserving policies for 100% of the members 100% of the time.

A Patient-Centered Model Realized

Lumedic Connect software, combined with the Lumedic Exchange community, create a 4-layer ecosystem which makes it possible to, for the first time, allow an individual to be the source of their own data within the healthcare system and beyond. This structure changes the way in which we exchange healthcare information that prioritizes individual privacy and autonomy, creates new efficiencies for healthcare organizations, and allows non-healthcare organizations to leverage individual health data simply. While such a system is a dramatic restructuring of today's methods of health data exchange, Lumedic Connect also maintains adherence to HIPAA as required and, in several key areas, extends it beyond the capabilities of current systems.

Conclusion

Lumedic Connect presents a platform that radically redesigns how information is exchanged in the healthcare system. This new pattern greatly reduces the cost and infrastructure required for health care providers, insurance companies, and other organizations to exchange data critical to healthcare processes. At the same time, Lumedic Connect uses modern technology to prioritize the individual's privacy and control of their own data, including a new ability to dramatically limit disclosure of their protected health information. Lastly, organizations that previously were unable, or unwilling to use individual health information due to regulatory requirements or business risk, can now do so with the individual's consent, operationalizing the information without interacting with the underlying data.

All of this is possible while not only adhering to HIPAA regulations, but creating a pattern that more fully realizes the core intent of HIPAA. Regulatory concerns that previously sought to minimize exposure of data can instead be taken to their logical conclusion, making it possible to limit individual information exposure completely. Individual privacy is cryptographically enforced, and the authenticity of individual identity, individual data, and transacting parties is linked to verifiable identity information attached to an immutable ledger.

Example: A New Model

The following outlines a specific example of how Lumedic Connect can be used today. This example follows an individual through several interactions, and illustrates the value of the network, as well as its adherence to HIPAA regulations.

Individual Onboarding

Our individual begins by downloading the free Lumedic Connect mobile application in the same way they obtain any other mobile application – from the appropriate marketplace. This application serves as their own mobile wallet and establishes their footprint on Layers 2 and 3 of the ecosystem. The individual has not registered in a centralized system and has not revealed any of their own personal identity information to Lumedic. Access to the wallet is controlled with individual biometrics (fingerprint, face recognition), and Layer 2 agents are attached to that wallet.

Coverage Credential

The individual then seeks to receive their own insurance coverage and eligibility information in the form of a digital credential. They begin by interacting with their own insurance benefit provider (a Covered Entity) within some existing trusted context. This could be through a secure member portal, or even face-to-face. The individual uses their mobile wallet to begin the digital interaction, via standard methods such as an NFC communication, by scanning a QR code, or similar means. This establishes a connection between the individual's agents and the agents of the benefits provider (Layer 3). A secure connection is established, peer DIDs are created, and the coverage credential is signed by the insurance company and issued to the individual. The individual can now see that credential in their own mobile wallet, including all the claims within.

Registration

The individual now arrives at their healthcare provider (a Covered Entity) and needs to register and provide their coverage information. Again, the interaction is initiated by NFC, QR code scanning, or a similar means to establish the same type of private, secure connection between the individual and provider agents. The Covered Entity is equipped to handle PHI, and via a proof request seeks coverage details from the individual to add to that individual's record in the provider's EMR for eligibility and

billing. The individual sees that request within their mobile wallet and can choose to allow that data to be presented to the provider. The Lumedic Connect solution automatically passes that data from the individual credential to the EMR and completes individual registration.

Personal Health Data

The individual receives a lab test and wishes to receive a record of that test result for later use. Because the individual has already established a secure, private connection with the provider, that same connection can be utilized to issue the test result record to the individual as a new digital credential. The individual sees the credential offer on their mobile wallet and can choose to accept. When they do, a second credential is added to their wallet in the form of the test result.

Health Data Use Without Disclosure

The individual then wishes to use that test result credential to satisfy the requirements of a university at which they are a student. Once more, the individual begins the interaction digitally with the university using their mobile wallet. A private, secure connection is established, and the university makes a proof request of the individual. The university is not a Covered Entity and is not equipped to store PHI. Because of this, the university makes a zero-knowledge proof request that seeks not to access the underlying data, but simply provides the criteria to be applied to the individual's data to prove that they are eligible for classes based on their test results. The individual accepts the request, and once the transaction is complete the university only sees a confirmation that the individual is, in fact, eligible for classes. The individual has not disclosed any PHI to the university.

Key Concepts in Lumedic Connect

Issuers

An issuer is any organization that issues a set of verifiable data, called a credential, to a holder of that credential so the holder is able to present that credential to any party who needs to verify it in order to establish a trust relationship. As shown in step 1 of Figure 4, the issuer first writes a DID and public key to their choice of ToIP Layer 1 public utility. Then the issuer uses the corresponding private key to digitally sign credentials that are issued entirely off-ledger using a private, peer-to-peer connection with the holder established at ToIP Layer 2 (step 2 of Figure 4). On Lumedic Connect, examples of issuers include healthcare providers issuing personal health information to patients, or insurance companies and health plans issuing coverage information to members.

Holders

A holder is the party receiving a digital credential from an issuer. On Lumedic Connect, the holder is most frequently an individual acting either as a patient or guardian. Organizations of any kind may also be holders, as can some types of digital devices (e.g., computer-equipped cars, drones, medical devices). Individuals holders on Lumedic Connect maintain their own Layer 2 digital wallets and do not register public DIDs on a Layer 1 public utility. Instead they establish direct, non-correlatable connections with issuers and verifiers using private, peer DIDs. This means holders always maintain complete control over what is issued to their wallet, and what information they choose to provide to verifiers.

Verifiers

A verifier is any organization that needs proof of some data stored in the credentials belonging to a given holder. On Lumedic Connect, verifiers can include health systems seeking to access individual health or coverage information, employers wishing to access an employee's vaccination history, or businesses wishing to confirm a customer meets specific health and/or safety standards. Verifiers use the issuer's DID (included in the credential) to look up the issuer's public key from a Layer 1 public utility (step 3 in Figure 4) to cryptographically verify the authenticity of the issuer and the integrity of the data within the credential itself (step 4 in Figure 4).

Digital Credentials and Claims

In Lumedic Connect, health information takes the form of a set of claims (a claim being a single piece of information, e.g. date-of-birth) packaged within a digital credential that is digitally signed by the issuer of the credential. Once issued, the credential lives within the wallet of the holder until there is a need to present a proof of some or all of the claims in that credential to a verifier. Examples of digital credentials on Lumedic Connect include individual coverage and eligibility information issued by the individual's own benefits provider, or health information issued by their own healthcare provider, such as a lab test or vaccination record.

Proofs

A proof is a cryptographically secure and verifiable package of information derived from one or more claims contained within one or more digital credentials. A proof is produced as a response to a proof request made by a verifier to a holder. The proof is produced by the holder's digital wallet using a cryptographic process that enables the holder to selectively disclose information in the claims, so the verifier receives only the information actually needed. On Lumedic Connect, an example of such a request would be a health provider requesting specific eligibility information within that individual's own digital coverage credential.