Patient-Centric Health Information Exchange

Session #20, February 12th, 2019

Thyge Knuhtsen, Director of Healthcare Solutions, AT&T

Shahryar Sedghi, Blockchain Solutions Architect, IBM

Conflict of Interest

- **Thyge Sullivan Knuhtsen**

  Has no real or apparent conflicts of interest to report.

- **Shahryar Sedghi**

  Has no real or apparent conflicts of interest to report.

Agenda

- **Brief history of HIE**
- **Business / Technical issues that exist**
- **Solution**
  - Introduction to Self-Sovereign Identity (SSI)
  - MyData Model
    - Delegation
    - Repurposing
    - Personal Data Storage (PDS)
- **Conclusion**

Learning Objectives

- Discuss the adverse impact on the American health system and consumer caused by disparate health information systems
- Define a patient-centric architecture that utilizes technologies including Private Blockchain and FHIR resources to liberate PHI
- Recognize state and federal regulatory considerations pertinent to standing-up the solution and promoting mass adoptions
- Recognize future state of health information exchange, new stakeholder dynamic and economic incentivization to reallocate profit-pools

HIE – How did we get here?

- **1999 –** Institute of Medicine Report, “To Err is Human”, identifies medical errors as a significant addressable threat to health of Americans[1]
- **2004 –** ONC and HHS derived from bipartisan initiatives under President George W. Bush.[2]
  - $166M in grants, including State and Regional Demonstration (SRD) to support state and regional HIE[3]
- **2009 – HITECH passes in February. In August, ONC announces the agency will distribute $564 million to states and territories to enable HIE within their jurisdiction.**

Enter: Interoperability

- "The primary function of an HIE is to permit access to clinical information on demand at the point of care"[4]
- The global Health Information Exchange (HIE) market is expected to reach $2.21B by 2024 – Grand View Research
  - **Query-Based Exchange –** Ability for providers to find and/or request information on a patient from other providers, often used for unplanned care
  - **Directed Exchange –** Ability to send and receive secure information electronically between care providers to support coordinated care
  - **Consumer-Mediated Exchange –** Ability for patients to aggregate and control the use of their health information among providers

https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie

HIE Business Model Challenges

Data Blocking

- Sharing PHI out-of-network goes against capitalistic interests
  - Patients stay in-network, where medical record is
  - ONC's report details detriments of data blocking in healthcare ecosystem (2015)

Data-as-an-Asset

- Data sold without patient consent is big business:
  - From: Providers, payers, pharmacies
  - To: Biotech, medical-device and pharmaceutical companies; medical researchers; government agencies; payers and others
  - Why: Determine investments; Decide how to target clinical trials; and Refine marketing strategies

Legalities

- "…healthcare providers like physicians and hospitals usually own the medical records in their custody…" (5)

HIE Technical Challenges

- Personal Health Records are expansive and complex
- Insufficiencies in standards for electronic health information exchange
- State privacy rules and lack of clarity about requirements
- Difficult to accurately matching patients to their health records
- Security concerns for PHI data at-rest and in-motion

The Solution

"On the Internet, nobody knows you're a dog."

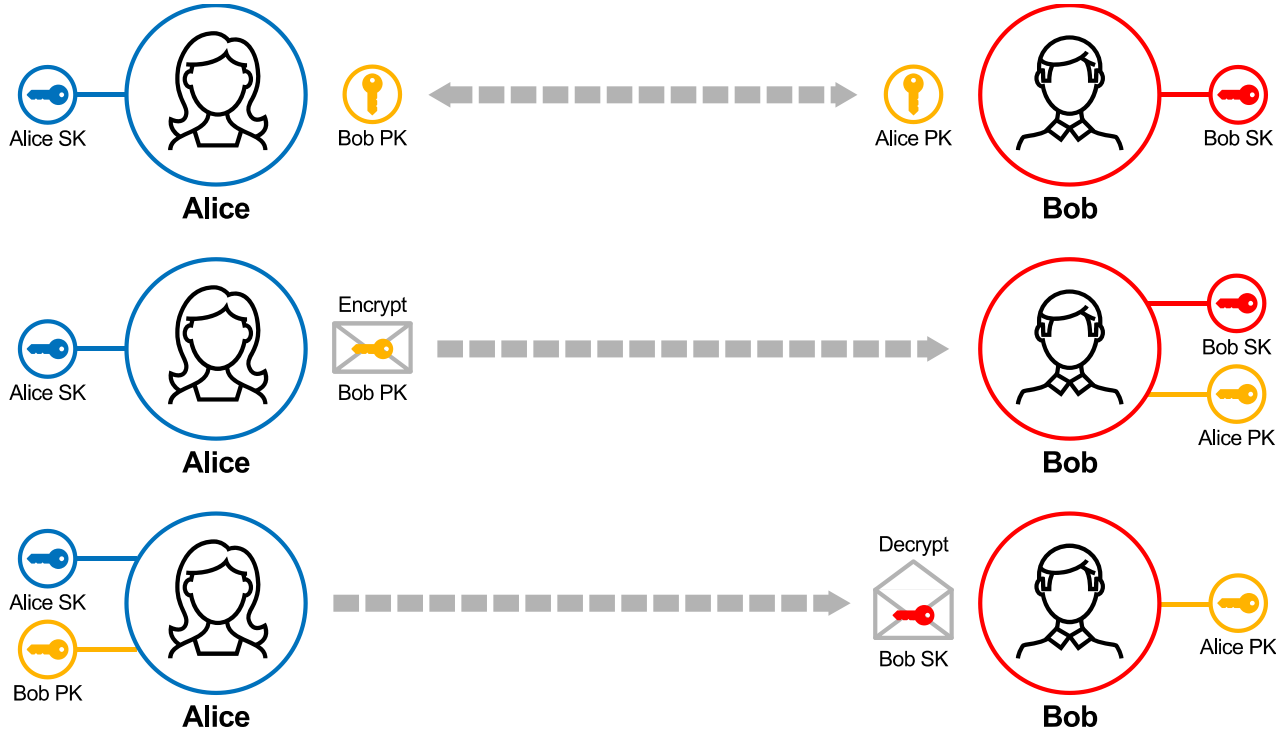
New Yorker 1993

"On the Internet, nobody knows you're a dog."

Identity

- Unique traits associated with an individual; The owner of Personal Identification Information
- Mundane Identity
  - Social Security Card, Birth Certificate, Passport, Driver's License
- Virtual Identity
  - Email, Facebook, Apple ID,….
- Digital Identity
  - X509 Certificate as an example
- We use digital identity to identify ourselves over the Internet
  - you’re not a dog

PKI (Public Key Infrastructure)



Problem with PKI

- **Rely on Certificate Authorities**
  - Over 1200, some in countries that we may not trust
  - Single Point of Compromise
- **Public Keys are difficult to exchange and manage**
  - Revocation is centralized

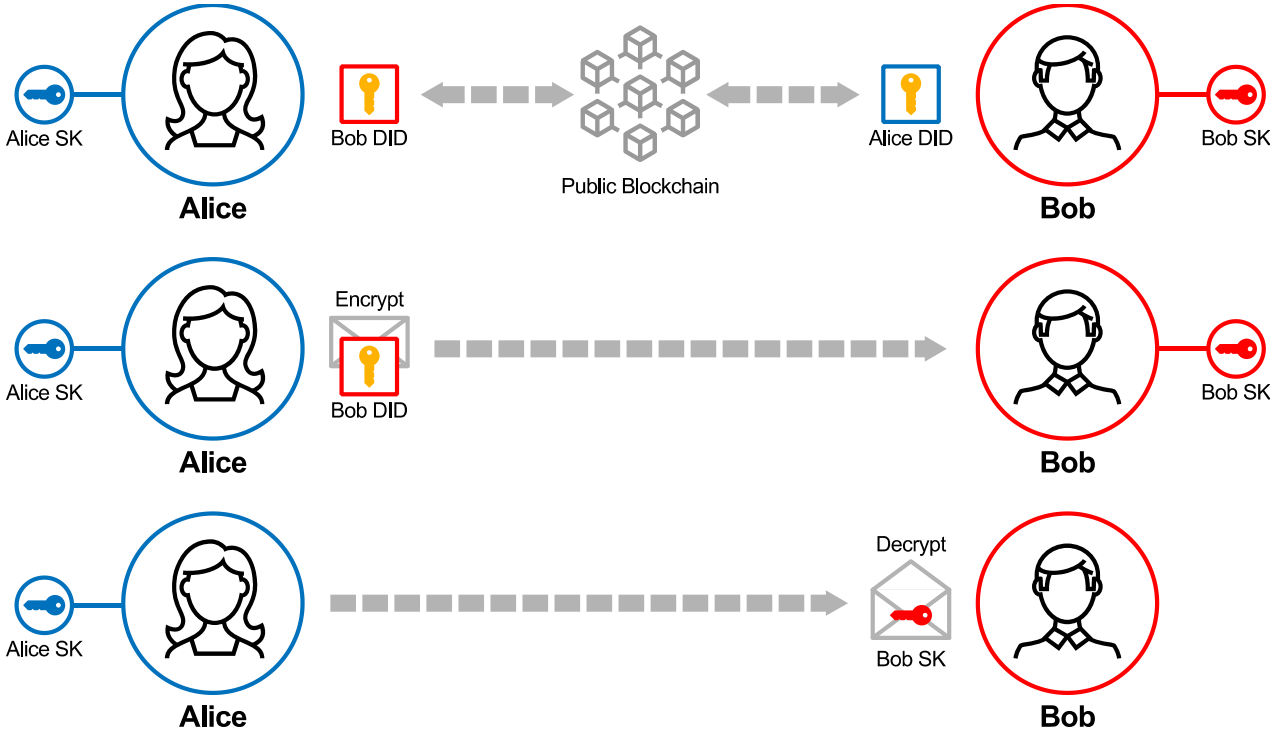
Blockchain in one Slide

- **A Log (ledger) of transactions**
  - Ledger entries cannot be modified or deleted they are Immutable
  - Writing ledger entries requires Consensus in a blockchain network
  - Whatever is written in blockchain can be traced back throughout the time. Blockchain provides Provenance
  - With all these blockchain becomes the single source of truth (Finality)
- **Blockchain can be:**
  - Public or Private
  - Permissioned or Permission less
- **Blockchain Participants can be:** Anonymous, Known or Pseudonymous

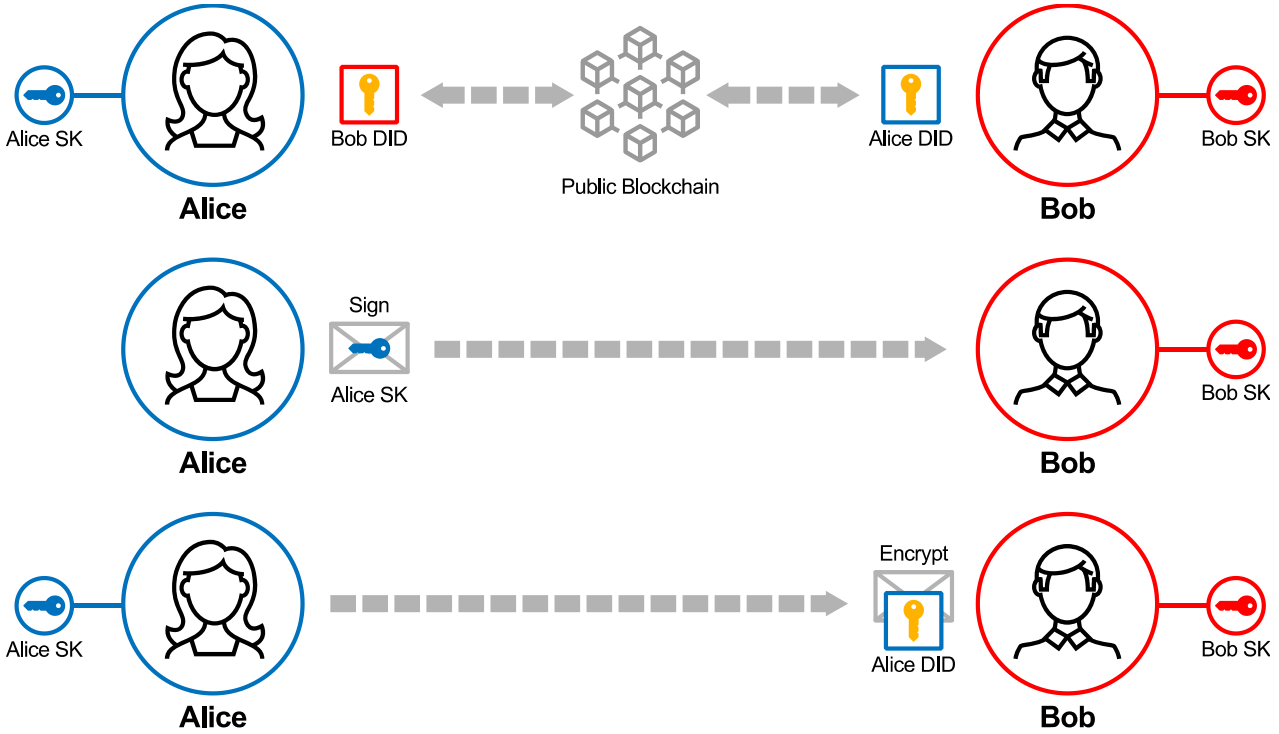
Background – Decentralized Identifier (W3C Draft)

- Based on DPKI concept and created on Web of Trust
- An addressable Public Key on the Internet
  - Like a web address for your public key
- Does not reveal you Identity
- Helps the other to verify your signature
- Every individual or organizations needs to have a DID
- DID is created by Permissioned Actors in a public Blockchain
- You can have more than one DID
- Revocation with Zero Knowledge Proof

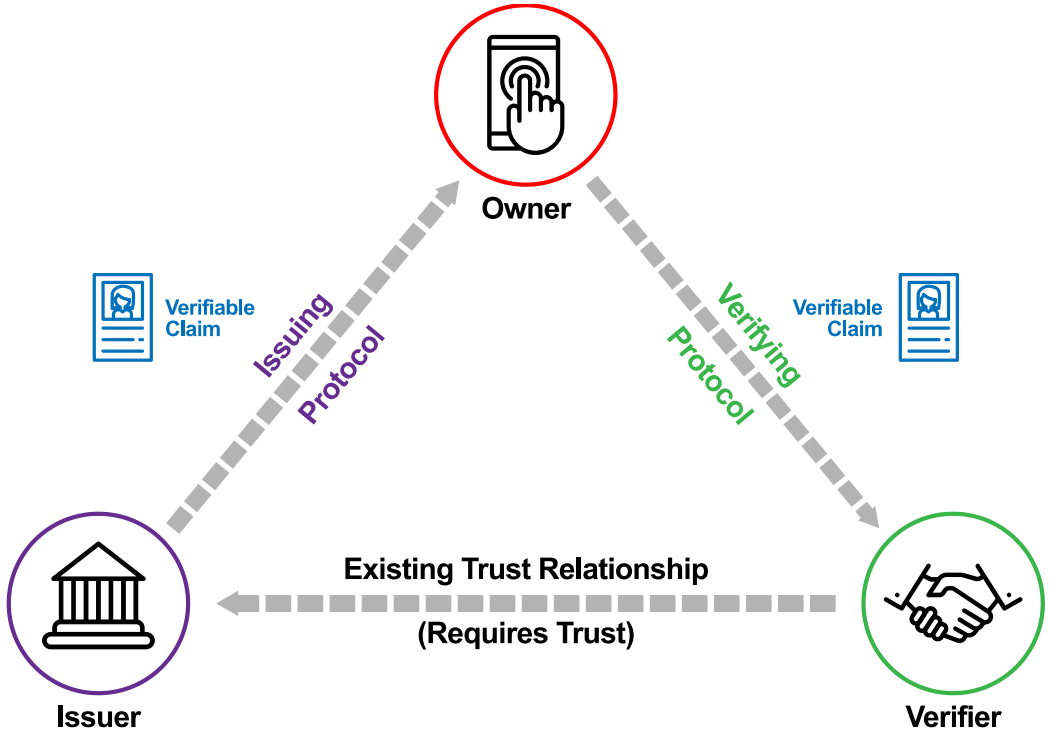
Distributed PKI (DPKI) – Decryption



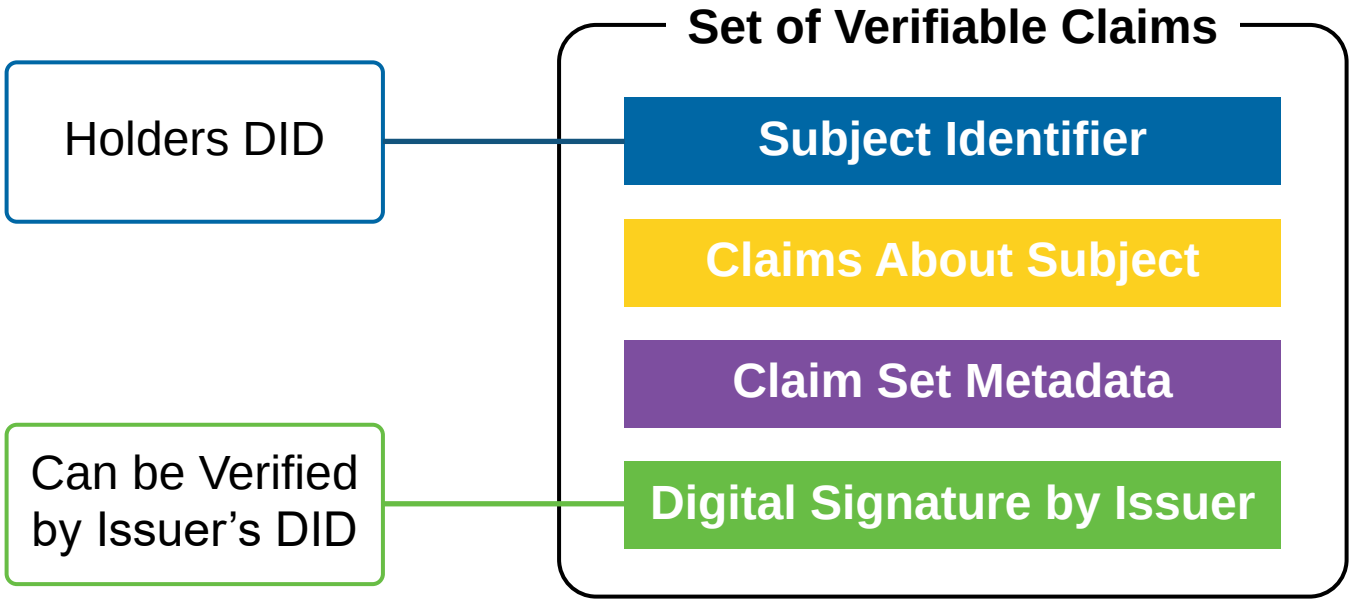
Distributed PKI (DPKI) - Verification



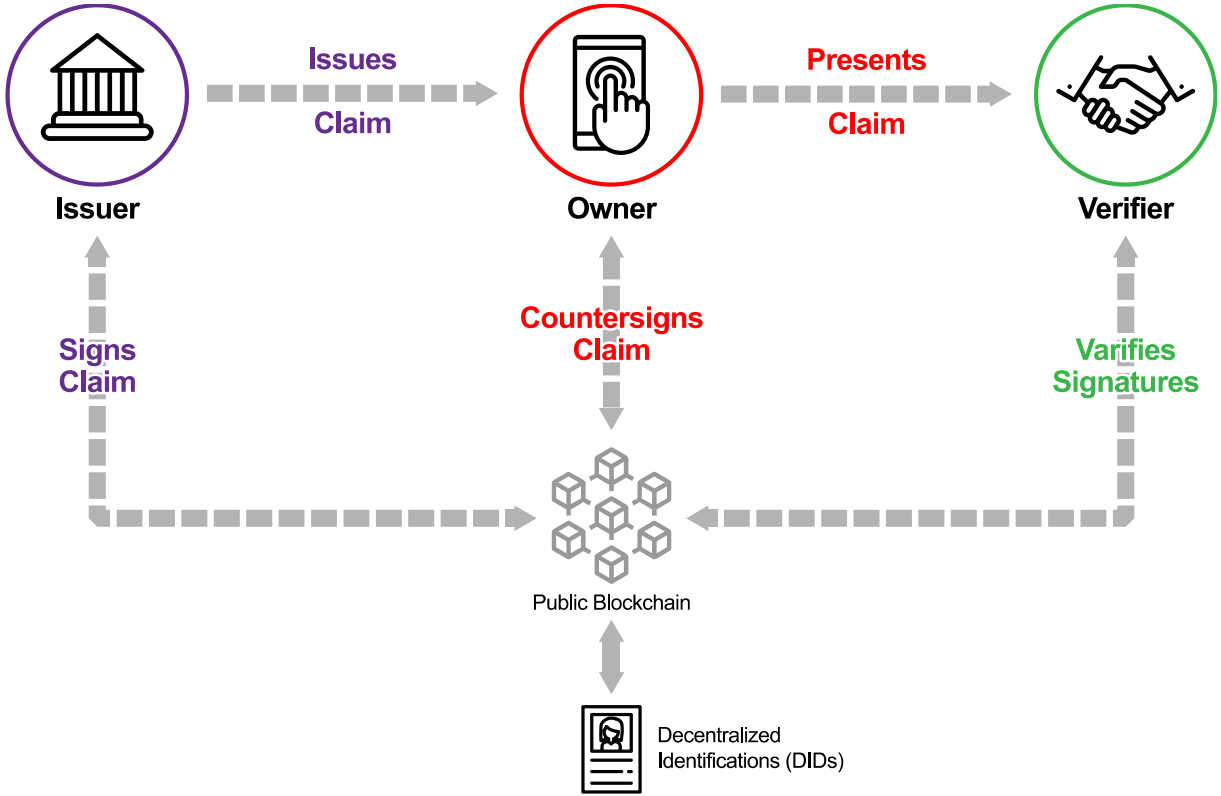
Claim Verification without SSI



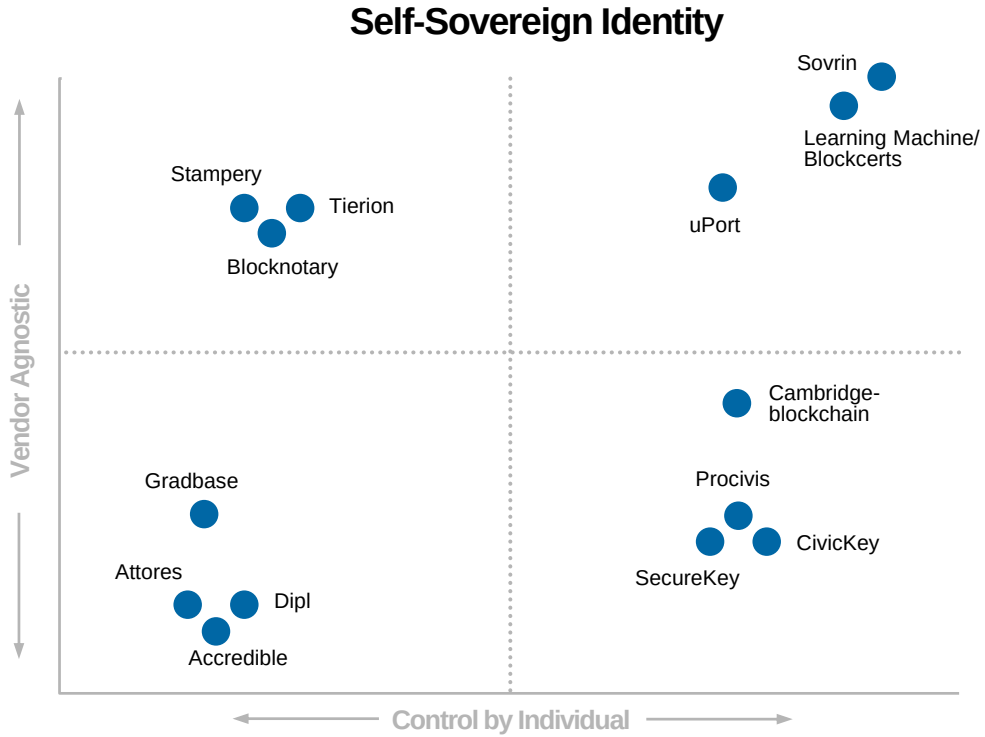
Verifiable Claim – W3C Draft



Claim Verification Based on DID



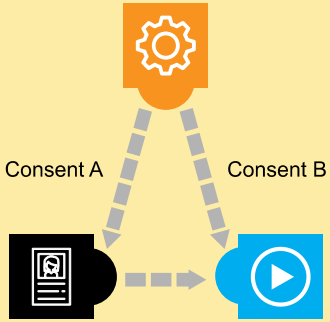
World Economic Forum – The Known Traveler



#HIMSS19

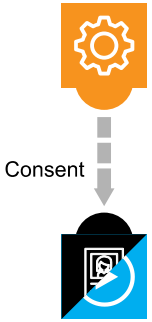
The MyData Model – Human-centered personal data management and processing

Delegation



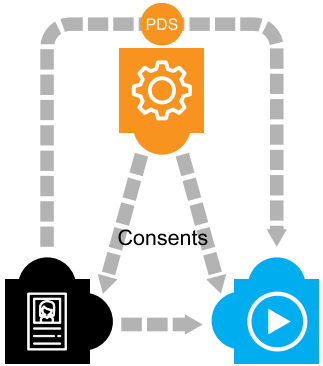
The Data Source provides with Account Owners Consent A personal data to the Data Sink which processes it for a purpose defined in Consent B. In this case both Data Source and The Data Source are in legal terms Data Controllers.

Repurposing



The Data Source is also Data Sink processing personal data for a specified purpose – at some point they may suggest for the individual a new purpose or means of processing data and individual may give new repurposing Consent. In this case the Data Source is in legal terms the Data Controller

MyData Account as PDS



Personal Data Storage can be integrated into the individual's MyData account. This is a complementary feature that provides certain benefits, but it is not expected to be the primary tool for data flow management.

MyData Terminology

Individual / data subject / account owner/ Patient: person who created and is using the account to link new services and authorize data flows with consents. Has relationship with the source, the sink and the operator

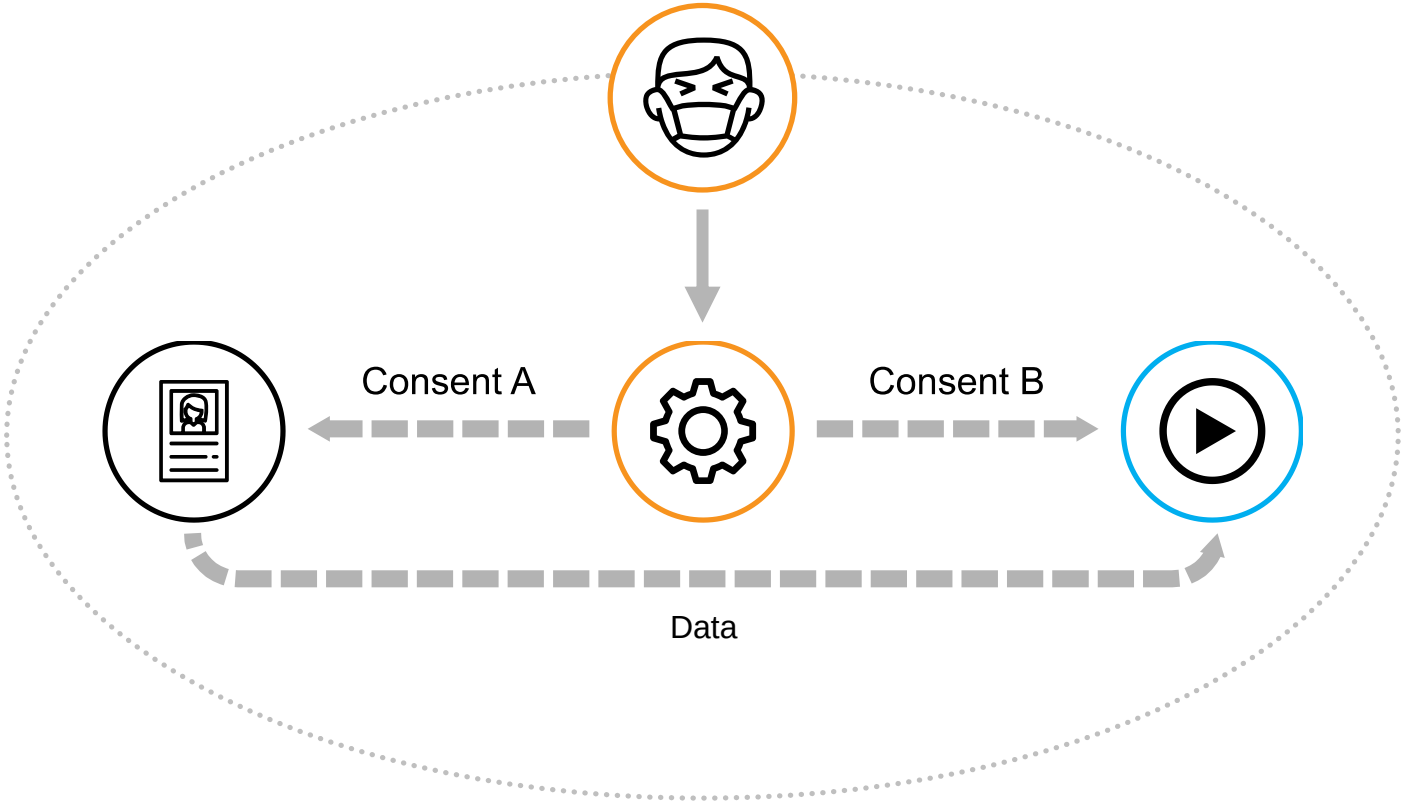
My Data Operator: Provides My Data Accounts and related services. Account enables digital consent management – Authorization as a Service.

Data Source

Data Sink

Data sources and data using services: Data source provides data about the Individual to the services that use this data (Data Sinks). Same actor can be working as both Data Source and Data Sink.

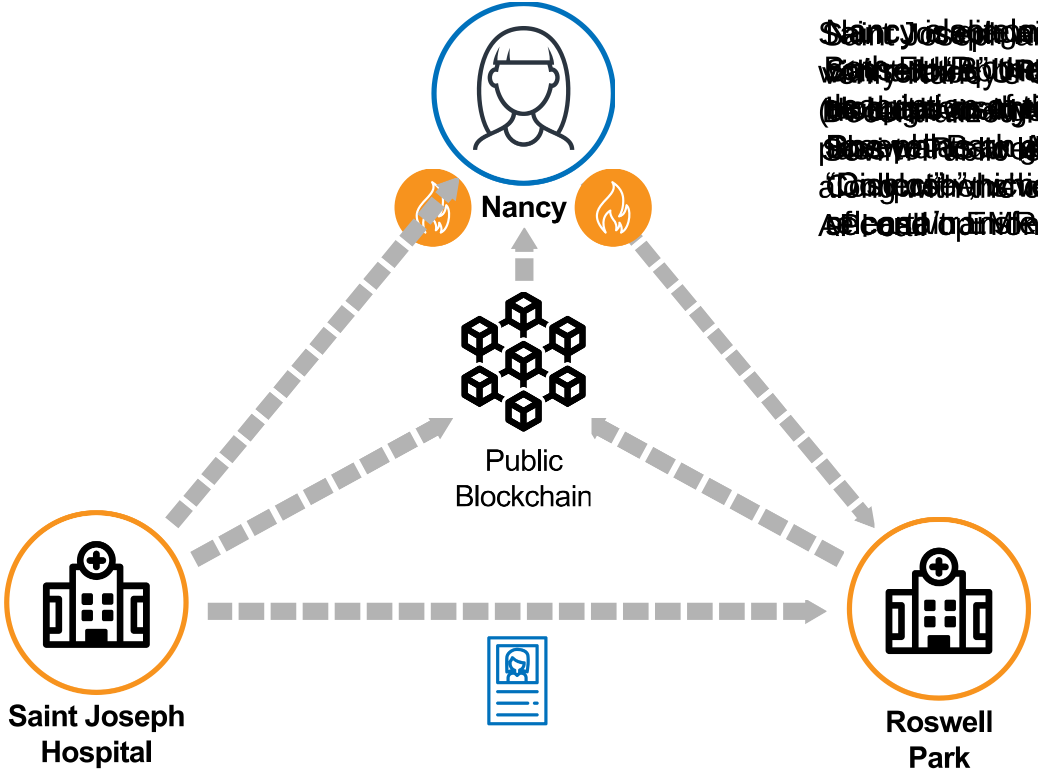
#1 Delegation



Nancy's Story – Background

- A public Blockchain is already created by **Sovirn Foundation as an example**. This public Blockchain is **Permissioned**
- Nancy Lives in a REAL ID compliant state. State DMV can be a member (Steward) of Sovirn foundation or can be onboarded by another Steward of the foundation.
- DMV issued a Decentralized Identity when she renewed her Driver's License and applied for REAL-ID.
- As an example, Saint Joseph is onboarded by Steward A as a trust anchor and Roswell Park is onboarded by Cisco another member of Sovirn foundation
- Nancy and both providers have verified self-sovereign identity. All three can provide enough verifiable claims for their identity. Their Identity can be verified by Decentralized Identity (DID)stored in Sovirn public ledger.
- Regardless of different EMR systems both providers Saint Joseph and Roswell Park are able to generate and consume FHIR Resources, and able to provide APIs to access these resources

Nancy's Story

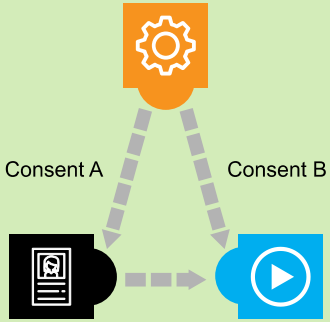


Nancy's Story

- Nancy is diagnosed with Cancer in Saint Joseph Hospital. Her EMR includes many visits, tests and MRI. She wants to go to Roswell Park Comprehensive Cancer Center for a second opinion.
- Nancy electronically signs a FHIR consent "A" that assigns Saint Joseph Hospital as the consenting party and Roswell Park as an Actor with Action "Disclose", which allows release/transfer of certain EMRs
- Nancy also electronically signs FHIR consent "B" that assigns Roswell Park as the consenting party and Saint Joseph as an Actor with action "Collect" which allows gather/acquire of certain EMRs
- Both FHIR consents contain enough description of the EMRs to be shared
- Saint Joseph and Roswell Park can verify Nancy's Consent with Nancy's Decentralized Identity stored in the Sovirn Public ledger
- Saint Joseph will deliver an API Key with related URL securely to Nancy' (through an Agent) which Nacy will pass to Roswell Pack for retrieval along with the consent or in a separate API call.
- Roswell Park accesses Saint Joseph system through API to retrieve Nancy's EMRs

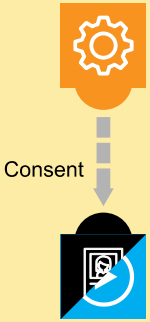
MyData Model – #2 Repurposing #3 Personal Data Storage (PDS)

Delegation



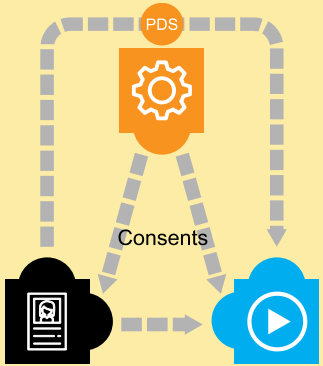
The Data Source provides with Account Owners Consent A personal data to the Data Sink which processes it for a purpose defined in Consent B. In this case both Data Source and The Data Sink are in legal terms Data Controllers.

Repurposing



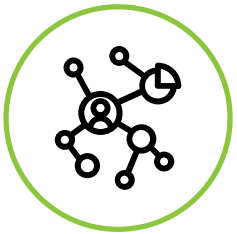
The Data Source is also Data Sink processing personal data for a specified purpose – at some point they may suggest for the individual a new purpose or means of processing data and individual may give new repurposing Consent. In this case the Data Source is in legal terms the Data Controller

MyData Account as PDS



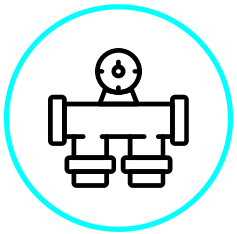
Personal Data Storage can be integrated into the individual's MyData account. This is a complementary feature that provides certain benefits, but it is not expected to be the primary tool for data flow management.

Architectural Overview



Datastore

HL7® FHIR®



Middleware

Self-Sovereign Identity

Datastore

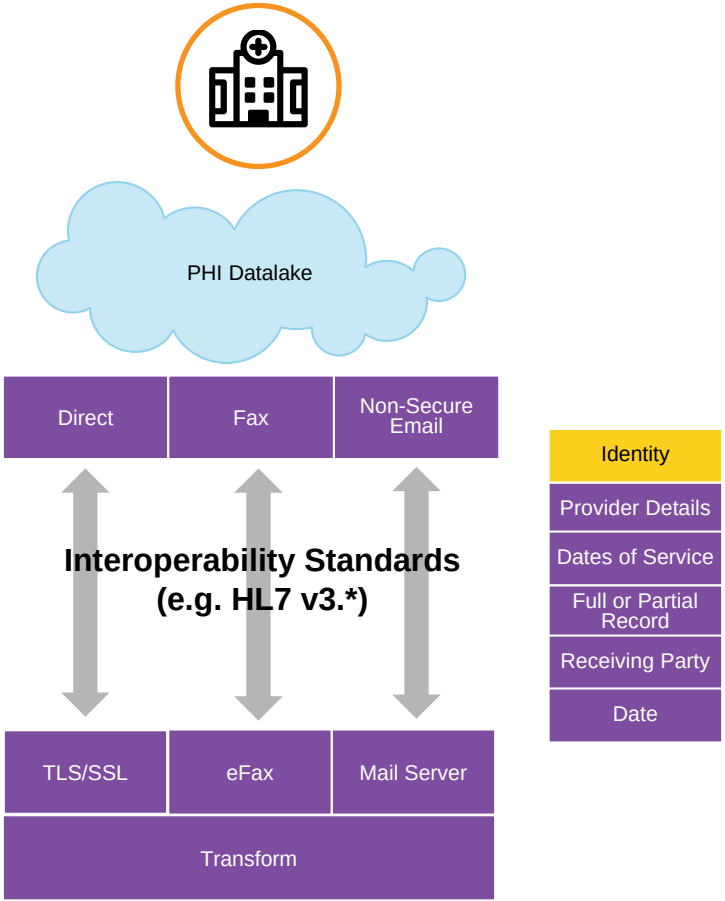
- **Problem:** Lack of productized HIPAA / HITECH cloud storage offerings
  - Microsoft Health Vault, Google Health
- **Cause:** Security controls for PHI data at-rest and in-motion aren't easy
- **Solution:** Encrypt data at-rest, in-motion with NIST 800-53 Infrastructure
  - Consumers: Apple Health
  - Business: IBM OneCloud, AWS HCLS Cloud, Microsoft Azure
- **Benefits:** The ability for consumers to manage their PHI, and for business associates to steward their information.

HL7® FHIR®

- **Problem:**
  - Personal Health Records are expansive and complex
  - Insufficiencies in standards for electronic health information exchange
- **Cause:**
  - Many different underlying data schemas and modes of transport
- **Solution:** HL7 FHIR Resources
  - Crosswalks for all previous HL7 versions before
  - C-CDA
  - Maturity Models
  - OpenEpic, OpenCerner

Middleware

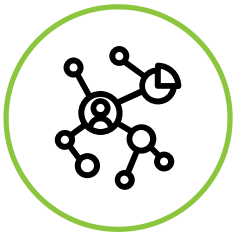
- We're moving in the right direction
- Meaningful Use III
- 80% of unique patients seen by eligible provider must provide timely access to download his or her health information
  - But: That might be a stretch...
- 21st Century Cures Act
- Trusted Exchange Framework and Common Agreement
  - But: Completed by 2021
- MyHealthEData
- Blue Button 2.0
  - But: Only for the nationally insured
- So, we leverage: Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524



Self-Sovereign Identity

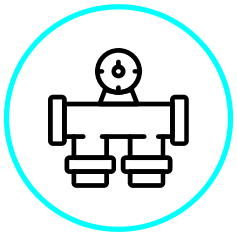
- **Problem:** Unable to prove you're not a dog on the internet
- **Cause:**
  - No acceptable methods for providing identity on the web
  - Difficult to accurately matching patients to their health records
- **Solution:**
  - Leverage Self-Sovereign Identity + EMPI to identify individual
    - W3C + DIF Standards emerge
    - Decentralized PKI's! (Decentralized Identity, or DID)
- **Benefits:** Ability to request PHI, completely electronically, via HIPAA 45 CFR § 164.524

Architectural Overview



Datastore

HL7® FHIR®



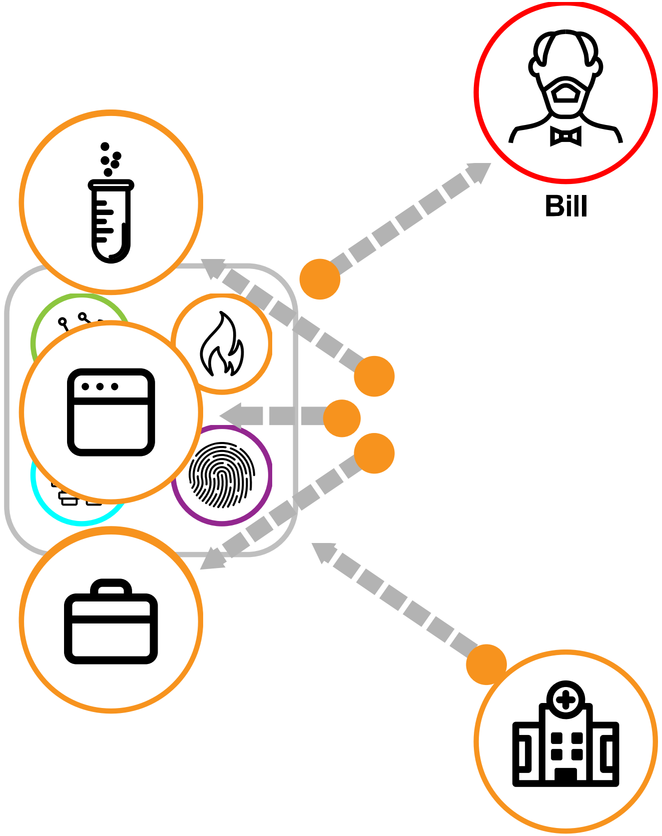
Middleware

Self-Sovereign Identity

Bill's Story – Assumptions

- A Self-Sovereign Identity (SSI) Blockchain will be leveraged to disclose identity electronically (e.g. Sovrin, uPort, etc…)
- Bill who lives in a REAL ID compliant state is onboarded to this blockchain by the state who is a validating peer on the SSI Blockchain (e.g. Sovrin, uPort) when she renewed her Driver's License and applied for REAL-ID.
- Bill will leverage the following additional technologies:
  - A datastore that supports HIPAA / HITECH compliance
    - E.g. IBM Cloud, AWS, Google Cloud
  - FHIR Resources (Implemented)
  - Middleware for the query and interpretation of Healthcare PHI requests and responses

Bill's Story



conform to "data schema" (i.e. FHIR Resources)

Provider communicates partial or full

medium

Bill's Story

- Bill wants to compile a single, longitudinal record of their PHI which they will steward.
- Bill provisions instance of aforementioned "datastore", "data schema" & "middleware".
- Bill instantiates request for either partial (CCDA) or full (all data) PHI from provider under HIPAA Individuals Right to Access their Health Information 45 CFR § 164.524 via "middleware" component
  - Now completely electronically via SSI (issue before was providing electronic identity)
- Provider has 30 days to respond via available electronic mode (e.g. Direct API, Email, Fax).
- Provider communicates partial or full PHI via available electronic medium. "middleware" component interfaces via provider's selected electronic medium (e.g. Direct API = TLS / SSL | Email = iMAP, SMTP, POP3 | Fax = eFax)
- "middleware" performs any transformations for data normalization (e.g. HL7 v2.* → HL7 FHIR) via pre-existing mappings to conform to "data schema" (i.e. FHIR Resources)
- "middleware" then stores personal health information as FHIR resources, physicalized in agent "datastore" that supports HIPAA / HITECH compliance
- Bill is able to move data to covered entities (e.g. New providers) and persona data storage devices (e.g. Apple "Health Records") via FHIR C-CDA
- If Bill would like to send entire medical records to qualified third-parties while maintaining the protections offered by HIPAA / HITECH legislation, Bill is able to extend the Cloud Solution Provider (CSP) Business Associate Agreement (BAA) to ensure his sensitive information maintains civic protections.

Future state of HIE

Business Model: Consumer-Mediated Exchange

- Ability for patients to aggregate and control the use of their health information among providers

Form: Digital Longitudinal Patient Record

- Compile and aggregate all Personal Health Information (PHI), append homogenous data

Key Stakeholder: The Patient

- Patient will own their clinical data and will have the ability to broker their data to covered entities, business associates and ancillary entities

Innovation: Application

- Clinical trials, clinical research, health monitoring, population health management, data monetization

Questions

Thyge Sullivan Knuhtsen

AT&T

https://www.linkedin.com/in/thyge-sullivan-knuhtsen-46b28233/

Shahryar Sedghi

IBM

https://www.linkedin.com/in/shahryarsedghi/

#HIMSS19

References

- Must see, Very Funny, YouTube video about identity by David Birch
  - https://www.youtube.com/watch?time_continue=188&v=hS15p5V3slg
- World Economic Forum, Digital Identity
  - http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf
- MyData
  - https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/
- Decentralized Identity Foundation
  - https://identity.foundation/
- Reference to Verifiable Claims
  - https://www.w3.org/TR/verifiable-claims-data-model/