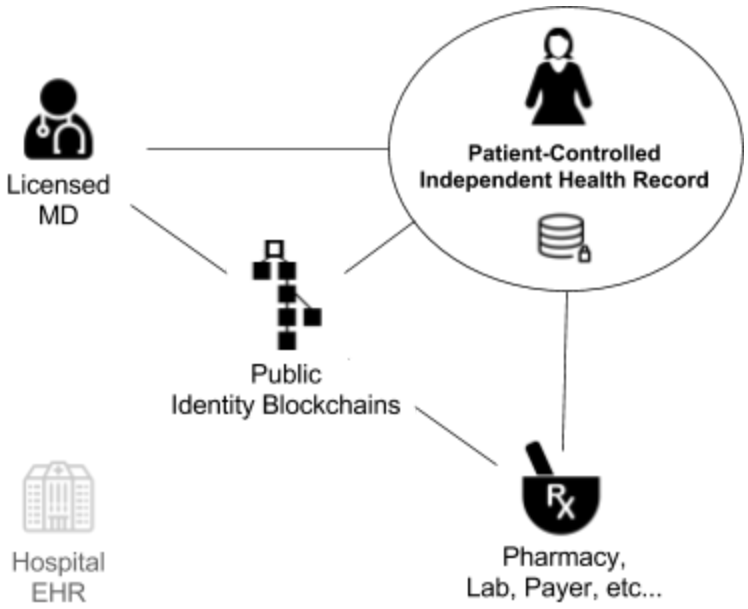
HIE of One Loop: A Patient-Controlled Independent Health Record

Adrian Gropper, MD and the Loop Project Team

September 2017

A patient-controlled independent health record can solve a wide array of problems in health care including delayed diagnosis and treatment, increased risk and cost, and significant provider and patient dissatisfaction with current electronic health records. These are just a few of the many problems caused by current approaches, which give total control to hospitals, corporations, and third-party data brokers. A new patient-centered design will solve many of the problems that frustrate us today, while opening opportunities for physicians, researchers, and governments.

This white paper describes a proof-of-concept demonstration using self-sovereign technology, made practical for the first time by blockchains, that gives power to physicians and patients while taking control away from the institutions that currently hold a monopoly on health data.



Public Blockchains Enable a Patient-Controlled Independent Health Record

Potential Benefits

Privacy and accountability

The benefits of distributing control of health records to patients derive from the many valuable uses of a complete yet private digital dossier. No government or private institution can be trusted with total comprehensive information about us. Even subsets of our aggregated personal data have been demonstrated to be honeypots or single points of failure across millions of

people. Hospital databases leak millions of records each year and Equifax just announced the loss of 145 million records in one incident. When institutional databases cover 10 million people in a regional hospital system or 230 million people in the national Surescripts data brokerage it becomes difficult to hold these institutions accountable because the choice to opt-out is no longer practical.

Adaptability

Current institutional databases are also poorly suited to work with new tools coming from the fields of machine learning and artificial intelligence. We need to interact with AI in a manner similar to how people currently interact with trusted human advisors such as physicians, lawyers, and accountants. Only self-sovereign technology under individual control can have access to sensitive policies such as sexual orientation or who our real friends are, in order to protect our open future and our independence from government and corporate actors.

Glossary

Self-sovereign technology - Technology that is not under the control of any institution

Public blockchain - A distributed public ledger that is not under the control of any specified entity

Identity Container - One person's automated, always-on online presence

Federation - A collection of institutions that share governance and exclude non-members

Cryptocurrency - Like digital gold, a currency that does not require trust in any authority

Authorization server - A digital gatekeeper that controls the flow of personal data held by others

Reputation - An asset associated with a person's identity derived from interactions over time

Mobile wallet - A secure personal device that assists in managing valuable private assets

HIE of One - Health Information Exchange of One, a Delaware public benefits corporation

Interoperability

Interoperability is yet another benefit of individually-controlled (self-sovereign) technology. Health data uses span clinical, research, and community applications. And within each of these application classes, the range of participants in health care is broad. For example, important clinical users may range from highly regulated VA and Medicare, to hospitals and clinics, nursing homes, and individual clinicians around the world.

Federation and legal trust agreements across such diverse organizations have limited interoperability in the privatized US model, and have not proven effective in countries with nationalized health systems. The diversity of health data users (as compared with the uniformity of credit cards or ATMs systems) makes federation unworkable as the basis of interoperability in healthcare. Self-sovereign technology, including non-repudiable blockchain-secured identities

when appropriate, does not depend on institutional federation yet retains compatibility with federated systems to the extent they are white-listed by a particular individual.

HIE of One Loop

The Loop independent health record is based on self-sovereign technology linked across individuals via public blockchains. Our approach is novel in that no institutions or federations are needed to mediate between any licensed clinician and the patient's health record. Loop uses standards and open source software to create a health record that is independent of any vendor or institution. Loop health records are as decentralized and self-sovereign as interoperable cryptocurrency wallets.

Extending the cryptocurrency analogy, Loop introduces a personal exchange server component as the online service endpoint associated with a patient's digital identity. This identity container is more than just a database server; it includes an authorization server that can control access to information about us that is managed by labs, hospitals, or other institutions. The standardized authorization server extends patient control to service providers, maintains provenance, and enables query and streaming of data directly from the source.

The combination of a mobile secure app (the identity wallet) and the online identity container (the information exchange) linked via public blockchains maintains control with the patient. No privacy policy is required because there's no counterparty to have a privacy policy with.

From a physician's perspective, the key benefits are:

- Access to a health record that's current across all institutions and has all relevant data
- Access to social determinants of health
- Enhanced communications and engagement across the patient's real-world care team
- Confidence in using a peer-reviewed, customizable, open source tool

Patient control over access means that the data can include social determinants of health and other privacy-intensive components that patients would not trust to an institutional database. A patient-controlled health record places no federation barriers to communications among providers and avoids institutional censorship of apps and decision support services that a physician might want to connect to the patient's record.

From a professional perspective, as software and information technology become integral to clinical medicine, only open source technology can maintain the tradition of peer review, teaching, and local adaptation that are essential to the trust we expect of the physician-patient relationship. When patients consult a physician they expect that physician to be responsible for and in control of her tools rather than mere proxies for a black box process. Loop keeps physicians in the loop as well as the patients.

Independence is yet another benefit of designing health records to be patient-controlled. Health records need to last a lifetime and beyond. They must make the transition from child to adult gracefully, without carrying over prejudice or potential for discrimination on the basis of adolescent behavior or resolved mental health issues. Health records should survive vendor failures, family relocation, and political upheavals. People are not defined by a particular institution or jurisdiction and our health information should not become a barrier to our independence.

Implementation

Loop creates a patient-controlled independent health record by securing health transactions without reliance on institutional controls. This is relatively easy in healthcare because transactions such as prescriptions, referrals, laboratory orders, or consultations are regulated, trusted, and paid on the basis of an individual provider's personal license. This contrasts with banking, commerce, or education where important transactions have to be executed with institutions. We adapt newly developed blockchain identity systems to securely manage physician credentials without the involvement of a hospital or vendor in the trust chain.

To demonstrate self-sovereign interaction between the patient and physicians, Loop implements transactions typical of any health record:

- Writing a prescription represents other orders, referrals, and notes by a licensed clinician
- Decision support around the prescription represents cost, eligibility, and appropriateness
- A signature on the prescription must be legally binding and non-repudiable
- Regulatory requirements on the prescription include records retention, audit, public health, and licensed practitioner reputation

To maintain the independence of both the patient and the practitioner, Loop implements existing and emerging standards and uses public blockchains for all four of these aspects of a transaction.

Blockchain Identity

Blockchains are a distributed trust mechanism that can be as useful for securing identity as they are useful for securing assets. Loop implements three essential aspects of identity using existing public blockchains:

- Authentication and Single Sign-On
- Verified Credentials
- Reputation and Audit

Authentication and single-sign-on

User authentication via local credentials (such as a username and password) is not practical for an independent health record because it would require the clinicians to have as many passwords as they have patients. This means that a single sign-on mechanism is required.

Prior to the introduction of blockchains, single sign-on required federation through a trusted intermediary such as an OpenID Connect[1] Identity Provider (IdP) in order to secure a person's credentials and deploy them in a trusted manner to each patient. The cost of a federated IdP is significant and the loss of privacy for both the prescriber and the patient are often unacceptable. Aside from security and privacy issues, the federated IdP also represents a single point of failure. Blockchain trust replaces IdP trust for authentication by allowing each prescriber to hold their own authentication credentials and use them to sign into any patient controlled record that chooses to recognize their credentials.

It is important to note that a self-sovereign design like Loop does not preclude any of the advantages of federated identity management or IdPs. Because it's the individual's choice to accept verifiable credentials or to whitelist any number of IdP federations, the self-sovereign approach allows the benefits of both on a patient-by-patient basis.

Verified credentials

Aside from authentication credentials, the prescriber must hold and present their licensing credentials to access the independent health record. These credentials are issued to the prescriber directly by federal drug enforcement agencies, state medical boards, and motor vehicle bureaus. Standards under development at W3C[2] and Rebooting Web of Trust[3] are designed to support verification of credentials managed by self-sovereign technology, including mobile wallets, and do not require an intermediary institution such as a hospital or IdP to secure the link between a self-signed authentication credential and multiple verifiable credentials. Each verifiable credential is independently signed by their separate issuer.

Reputation and audit

Reputation and audit must, by definition, be outside the control of the individual. Therefore the self-sovereign technology must leave an indelible yet privacy-preserving audit trail that can be used in cases of dispute or simply to assist in commerce by allowing for a public reputation. To support legal audit requirements, Loop implements pseudorandom blockchain timestamps together with separate document retention by all parties to a transaction. This protects the privacy of both the licensed prescriber and the patient by avoiding any public link between the blockchain timestamp and the blockchain ID of a participant in the transaction.

[1] http://openid.net/connect/
[2] https://www.w3.org/2017/vc/WG/
[3] http://www.weboftrust.info/

Beyond audit, reputation requires some public disclosure as a consequence engagement in a transaction. Loop uses a novel method to enable reputation registries as third-parties to a transaction in a privacy-preserving manner. Reputation, by its very nature, requires some loss of privacy on the part of the prescriber, and in some cases it also requires some loss of privacy on the part of the patient that is rating the prescriber. Loop allows a transaction document such as a prescription, that is private between one or more self-sovereign blockchain identities, to also specify a reputation registrar that is mutually acceptable to the parties. This is similar to specifying a jurisdiction or arbitrator as part of a contract. Different reputation registrars may offer different authority vs. privacy tradeoffs for the prescriber and the patient. Registrars will compete on the basis of how they manage blockchain identities, blockchain timestamps, and limited information about a particular transaction. With Loop, independent self-sovereign entities that want the benefit of a reputation registry are enabled to choose a registrar based on that institution's privacy policies and reputation.

Identity Container

The core of a Loop patient-controlled independent health record is a standards-based server able to engage in transactions with all aspects of a patient's care team. These transactions could be a licensed physician writing a prescription directly into the self-sovereign health record, a cardiac monitor registering to provide access directly to the patient's ECG stream, a family member checking on the next appointment, or a hospital's EHR announcing the visit of the patient to their emergency department. Loop implements a self-sovereign online presence for the patient using standards-based methods. In Rebooting Web of Trust this server is sometimes referred to as the identity container. Aside from links to self-sovereign identity as discussed above, the components of the identity container and the relevant standards vary among implementers.

Whereas some implementations of the identity container mimic databases with access control lists, the Loop implementation includes a standard UMA[4] authorization server. UMA extends the widely adopted OAuth protocols for access control by making the OAuth authorization server independent of the protected resource, wherever that resource might be. Given that independence, the UMA authorization server can itself be self-sovereign or shared. In Loop, every patient runs her own UMA authorization server. This has the further benefit of giving the patient a convenient unified view of her protected resources and associated consents rather than having to visit the the separate consent portals of dozens of hospitals, labs, or directory institutions holding information about them[5].

The authorization server component of the identity container is "in the loop" for how a personal resource is used even when the source and the destination share data directly without the data itself touching the identity container at all. This capability, for example, enables the patient-controlled independent health record to manage streaming data from a heart monitor

[4] https://kantarainitiative.org/confluence/display/uma/Home
[5] http://openid.net/wg/heart/

without the cost, risk, and loss of provenance that would be incurred if the ECG had to be continuously proxied through the patient's identity container.

The authorization server is the outward-facing aspect of the identity container. It controls authentication and authorization of would-be users of the health record and issues secure tokens to them for access to local or remote attributes by consulting the secret policies of the individual patient. Secret policies are analogous to the secret keys in public key infrastructure - they are secured in the identity container and not shared with anyone, by design. The analogy continues if you consider that access tokens are derived from policies by the authorization server just as public keys are derived from private keys by a secure element. Just as you cannot go backward and derive a private key from a public key, you cannot derive the patient's policies from the scope of authorizations that are issued. This ability to protect one's policies from scrutiny by others is essential to independence and human dignity. It is at the core of Loop's self-sovereign design.

The self-sovereign identity container goes one step further to empower the individual by incorporating unique machine learning and artificial intelligence capability that cannot be provided in an external or institutional context. Given that our personal policies represent our deepest secrets and the essence of our individuality, the only place a learning system can be located so that it can have the benefit of both external interactions with would-be users of our authorization server and with secret policies is in the identity container itself. The learning and policy modification aspects of our independent selves has to be hosted in a self-sovereign manner.

More mundane aspects of the Loop identity container are also worth noting. The hardware or hosting environment for the identity container is self-sovereign to the extent it's standards-based for portability and fungibility, open source for inspection and modification, and offers a secure execution environment for apps and services.

Mobile Identity Wallet

The self-sovereign identity container is controlled by the individual through self-sovereign components of a mobile device. The mobile device itself need not be self-sovereign--it's hard to own your connection to the Internet or to open-source the hardware in your smartphone. It is practical, however to control a secure element linked to local biometrics and to an app or wallet functionality that helps manage private keys and key recovery processes linked to blockchains. The mobile device, local biometrics, secure element, and trusted apps work together to enable:

- Secure single sign-on without passwords
- Data minimization around managed credentials to protect privacy
- Review of transactions and documents that are about to be signed
- Application of non-repudiable signatures
- A good user experience in key rotation or device recovery

- Payment and replenishment of payment caches in the identity container

Loop currently implements the ConsenSys uPort[6] identity wallet that is linked to Ethereum and compatible blockchains. uPort is also a participant in the self-sovereign identity standards[7] in Rebooting Web of Trust. Although blockchain ID can be built on different public and permissioned blockchains, self-sovereign account recovery and other features of the uPort wallet benefit from smart contract capability built into Ethereum. It is also worth noting the complementary relationship between smart contracts, which are very public code out of anyone's control, and identity containers which execute totally private code. This complementary relationship makes Loop implementation of a patient-controlled independent health record more cost-effective and more likely to achieve a mass-market network effect.

Trust among self-sovereign entities is another implementation aspect to be considered when removing the hospital or other institutional intermediaries from the relationship between independent patients and independent physicians. Trust enters the implementation as:

- Credentials verified as directly signed by the issuing authority
- Software subject to certification by authorities that do not themselves have access to private data or metadata in the transactions
- Patient data that retains its provenance or can prove its authenticity
- Auditor confidence in the authenticity of signatures and the integrity of logs
- Reputation that can be made as fair and as accessible as privacy constraints allow

The Loop implementation of these trust essentials is ongoing. Our approach is incremental as we support use-cases with different trust requirements one patient at a time. An enterprise adoption model would have required us to solve for most or all of the trust issues before real world use.

Discussion

Loop has been a reference implementation of clinical health records best-practice and interoperability standards as a collaboration, started in 2013, with the New Open Source Health (NOSH) project of Michael Chen, MD. Our source code is at https://github.com/shihjay2/

The current version, as of September 2017, implements all of the key aspects and standards of the identity container except for machine learning. uPort blockchain ID is the primary authentication mechanism and Google ID is used to demonstrate compatibility with federated IdPs. The current second-generation codebase includes a mobile-friendly adaptive design for the independent health record (NOSH2) with separate interfaces for the patient and professional users. The current version of Loop also implements the FHIR standards that enable direct

[6] https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf
[7] https://w3c-ccg.github.io/did-spec/

patient-directed access to live clinical data in Epic EHR systems, already live at 37 hospitals[8] around the US. This capability is mandated for all US Meaningful Use hospitals by 2019.

Nonetheless, widespread adoption of patient-controlled independent health records is still subject to potential blockers and significant delays. Some of these include:

- UMA is an added IT expense on top of FHIR / OAuth as they are currently being deployed. In the absence of privacy regulation such as the European Union's General Data Protection Regulations (GDPR) and Payment Services Directive (PSD2), UMA adoption will be slow since US health care institutions still avoid transparency and digital patient engagement.

- Loop is currently using a dedicated virtual machine for each patient's identity container. This is expensive for all but the sickest of patients. Hosting that charges based on the actual computer cycles used (the duty cycle of a single patient's EHR is exceedingly low) is slowly becoming available. Another cost-effective and self-sovereign solution will be self-hosted identity containers in the home that will become practical as IPv6 eliminates router and server addressing complexities.

- The high cost and maintenance requirements of a personal domain, currently about $1 / month are also a barrier to rapid adoption. We look forward to blockchain ID and more sophisticated cloud services as a lower-cost alternative to ownership of a routable address to one's identity container. Privacy will also benefit from less expensive personal domains as people could afford separate domains for separate digital personas.

- No blockchain or hosting solution can be expected to last a lifetime. Standards and best practices for self-sovereign identity, verifiable credentials, and personal server hosting are essential to decouple the longitudinal health record from the technology infrastructure and from the institutional practices.

Perhaps most important, the fundamental human right to privacy and self-determination has been subsumed by technology. Enormous economic interests are now in control of our personal information and extract substantial economic value by mining our personal data for the benefit of a limited elite (the 5 largest companies are Apple, Alphabet /Google, Microsoft, Facebook, and Amazon). The value of personal health data being sold without patient knowledge and consent is estimated to exceed $100 billion annually in the US. As licensed professionals, parents, and patients, we face formidable barriers to regaining control of our reputation and to avoid discrimination and price manipulation.

Loop has been selected by a million-patient health information exchange (CriticalConnection, Austin, TX) to add patient access and single sign-on to their Community Health Record (CHR)[9]. CriticalConnection is notable for their non-profit physician-centered model and their established

[8] https://open.epic.com/MyApps/Endpoints
[9] https://chr.criticalconnection.com/default.aspx

role within the community. The legacy HIE will continue as an automated data feed into each patient's Loop with Loop acting as a patient portal for the CHR. Labs and imaging centers will have the option of using Loop as their patient engagement portal as well. A key value of Loop in this context is reducing the cost of onboarding a patient to the various practice portals. The user experience will be better as well. Loop is also able to add data from hospitals that are not participating in the CHR by directly connecting to their Meaningful Use interfaces. The physicians look forward to simpler and more secure passwordless single sign-on and access to more information. There is some physician concern about how information flows into their practice management systems. They don't want to have to access information in multiple systems. This problem is currently managed by their staff, and that work-around could continue with Loop. However, the problem of accepting incoming data is common to all institutional health record systems, even the newest ones being installed in large hospitals. We look forward to this collaboration in Austin as a way to improve the experience of physicians with health IT.

Next steps for Loop include piloting the technology with a major national research services supplier. We are also investigating blockchain-based funding (so-called app tokens) as an economic model for avoiding a digital divide in access to Loop and to support a network effect around an open source business model. We continue to engage with leading innovators in privacy preserving services and certification experts such as Patient Privacy Rights Foundation [10]. For now, we are supporting independent deployments of Loop through our GitHub and expect some Loop-supported public access in 2018[11].

---

[10] https://patientprivacyrights.org/
[11] http://hieofone.org/