NoID: A Novel Approach

By
Amir Abrams, HarmonIQ Health Systems Corp.
Mark A. Schroeder, Ubiquitous Solutions LLC.

BLOCKCHAIN AND ITS EMERGING ROLE IN HEALTHCARE AND HEALTH-RELATED RESEARCH CHALLENGE

ABSTRACT

Achieving true interoperability and trust relationships between disparate healthcare systems which manage patient data is arguably the number one issue facing healthcare IT today. To that end, there are several existing protocols and standards such as HL7 FHIR, HL7 CDA, HL7 2.x, and Direct Messaging which enables the sharing of clinical data among healthcare providers. However, the inability to accurately and securely identify patients across environments has put barriers in place which prohibit the potential of the existing standards. In order to overcome this major hurdle, we have developed the NoID protocol. This is a protocol for uniquely identifying any patient in the United States, in any environment, in a secure, scalable and accurate manner. The NoID protocol uses a RESTful services oriented architecture (SOA) API, existing industry standards (HL7) for data exchange, encryption and a collection of hashed patient demographic and biometric data (NoID Profile) to perform patient matching. NoID accomplishes all of this without PHI leaving the requesting organization's network. The NoID protocol heavily leverages blockchain technology, and its cryptographically secured public ledger, to register healthcare provider participants, build trust relationships, authenticate users, authorize access, audit access across a large distributed network of NoID Healthcare Organizations, and return record location pointers that facilitate data exchange (See Appendix B). NoID changes the clinical data sharing paradigm by putting the patient (or their delegate) in control of protected data and therefore alleviating the healthcare organization's responsibility and risk when engaging in clinical data exchange. NoID creates a self governing ecosystem that lowers the overhead and complexity of the current HIE interoperability model by eliminating the need for complex interorganizational legal data use and sharing agreements.

BLOCKCHAIN USE

NoID is a protocol that provides simple enrollment and identification of patients at the point of care (See Appendix B). Enrollment can occur at any location which chooses to implement the NoID protocol (laboratories, clinics, pharmacies, schools, etc). Locations which can enroll a patient are referred to as "Healthcare Organization Nodes" (or "HealthOrg Nodes", or simply "Nodes"), and the logical nodes which facilitate patient matching and HealthOrg node communication are referred to as "Patient Hubs" (or "PtHub", or simply "Hubs") (See Appendix A). The healthcare nodes on the NoID

network are registered in an immutable public ledger called the blockchain, and the ability to communicate across the NoID protocol is dictated by trust relationships and sharing profiles maintained and audited by PtHubs (See Appendix B). Thus, blockchain technology acts as an anonymous forge proof public audit, trust registry, and provides the public/private key infrastructure (PKI) needed to securely encrypt and digitally sign healthcare data across wide area networks (See Appendix B**)** without costly firewall and VPN configurations, administrators, maintenance and support**.**

Because of the decentralized and distributed architecture, NoID will maintain its high speed, reliability, low cost and accuracy as it expands from the initial implementation enrollment level to full implementation of the entire US population and its visitors. It will do so by leveraging a peer-2-peer (P2P) decentralized cryptocurrency architecture which is highly available and reliable without single points of failure (See Appendix B). Further, NoID Patient Hubs aggregate by region increasing its ability to extend to a global level. The blockchain enrollment of nodes is also highly adoptable and secure. The NoID blockchain is secured by hashing much like Bitcoin (bitcoin.org), and the patient hubs make up a decentralized second tier that are paid to manage trust, sharing preferences, persist patient hash collections, perform matching and provide record location services. Patient hubs need a fixed amount of collateral per patient to operate in the network. As the hub serves more patients, more collateral is needed, and in turn, the P2P cryptocurrency protocol rewards patient hubs for good behavior like timely responses, high availability, good trust relationship management, and high patient ratings, thereby generating economic incentives to perform according to the protocol consensus rules. Periodic patient and healthcare node ratings make up the majority of the reimbursement rate. The system is a Decentralized Autonomous Organization (DAO) that self regulates based on standard decentralized patient satisfaction ratings/votes, cryptographic hash and signature proofs, network consensus and open source algorithms that govern the protocol's operations. NoID includes budget blocks to continuously fund projects that enhance the protocol, reward exploit bounty programs, continuous security penetration testing and other foundation projects like marketing and education. The budget proposals are selected by monthly network stakeholder voting which include the patient hubs, healthcare organization nodes and patient advocate delegates. Dash (dash.org), an open source cryptocurrency and Bitcoin fork, has implemented a DAO like the one described in NoID that enables voting and budgets for foundation projects. The decentralized name registration on a block or DDNS was first implemented in 2011 by Namecoin (namecoin.info) and is another open source Bitcoin fork. The DDNS functionality was further enhanced and developed by Emercoin from 2013-present (emercoin.com).

SUPPORTING PUBLIC HEALTH AND RESEARCH

Governmental agencies, educational institutions, payors, and other relevant entities in the research community can participate in NoID in the same manner that all NoID Health Org Nodes participate. Any member of the research community can register as a NoID Node via the blockchain methodology described earlier (See Appendix B). The NoID protocol uses a Sharing Profile managed by the patient or their delegate to enable an "opt in" or "opt out" preferences to share their data with the NoID

research community at large (See Appendix A). The NoID Sharing Profile is granular enough to manage patient data sharing preferences that range from excluding or including a specific node, to globally excluding or including patient data for clinical or research purposes.

PATIENT ENROLLMENT

NoID is a fast, easy to implement, utilize and administer protocol that provides simple enrollment of patients at the point of care (See Appendix B). The NoID protocol is not dependent on age, sex, level of education or nationality and can accommodate all patients equally. All patient enrollment happens at the node level. All patient data stored at the PtHub or transmitted between nodes via the NoID protocol is secure and hashed in order to completely abstract patient data from the process (See Appendix B: Patient Enrollment). A foundation of the NoID protocol is its patient identifying resource known as a NoID Profile (See Appendix A). NoID Profiles are used for all patient enrollments and patient matching in NoID.

The NoID protocol minimizes errors in enrollment by dictating the use of electronic means of information gathering. This includes the capture and use of biometrics for authentication and authorization. Further, the NoID protocol encourages scanning, and Optical Character Recognition (OCR) technology to gather demographics from identification cards. NoID promotes the use of multi factor authentication (MFA) using standard smart cards or smart phones to protect the registration and patient lookup process.

All updates and corrections to identification data are made at the HealthOrg node by facility defined patient intake personnel. The NoID protocol is interfaced with the registration system and any updates to a patient's PHI triggers a resyncing process by the Hubs (an update message contains an updated NoID profile) (See Appendix B). Further, if patient data is compromised anywhere in the NoID network, any or all NoID patient profiles can be run through a modified hash algorithm to generate a new and unique profile(s).

If an unidentified patient presents unconscious or otherwise unable to communicate, the NoID protocol can register and/or validate a patient with a single biometric if appropriate. Through the use of administrative overrides during initial patient registration, the substitution of specific placeholder data (reason, date, etc) would be placed in the relevant NoID profile fields and treated as identifying data at patient registration (See Appendix B). Additionally, flags would be added to manage such things as the prompting for re-registration due to incomplete data, or the "quarantining" of a profile.

A further situation which is likely to appear is a patient presenting at a "non-connected" facility. Although the provider would not be able to register a new patient with a NoID Profile, a patient is capable of requesting and receiving contact information for any node which houses a copy of their profile (See Appendix B: Patient Audit Process). Using this contact information, patient data requests can be made.

The NoID protocol interfaces with the local HealthOrg node registration systems (via standard HL7 messages). Therefore, the time to complete a standard NoID registration is heavily dependent on the node's internal processes. However, we expect that the NoID process would add an average 3-6 minutes to patient registration in order to gather the appropriate biometrics, request a NoID unlock pattern, and communicate with NoID Hubs. This time estimate is the same regardless of sex, age, or nationality. We would expect that non-standard enrollment, as previously defined, could add another five minutes to this as appropriate overrides are implemented.

ACCURATE IDENTIFICATION

NoID leverages electronic gathering and validation of patient data to provide simple, fast, accurate identification of patients at the "point of care". Hashes of patient data are used for identification ensuring no change in original data. All transmissions are completed using current TCP/IP pipes. NoID reduces transcription errors by mandating biometric input devices and recommending OCR technology for valid forms of ID (See Appendix B).

The NoID protocol leverages complex hashing of all patient data. This in turn will result in a false positive rate (where false positive is equivalent to a patient being matched to the wrong patient) that is exceeding low. False negatives could be higher as the variability of input sources is beyond NoID's tight control, and a match might not return when one exists: potentially 1/1,000,000. Given complete and valid inputs, the potential general error rate could be less than 1 / 10,000,000 or 0.0001%. However, we expect that with valid and complete inputs that correct patient matching and registration could conceivably be 100%.

SECURITY AND FRAUD MANAGEMENT

As previously detailed, the NoID solution provides a web interface and/or standalone kiosks which allow for a patient to retrieve an audit of their NoID Profile updates (See Appendix B: Patient Audit Process). If any part of a patient's data has been compromised in any way, slightly modified hash algorithms can be employed to generate a completely new hashed NoID Profile. This will take place at the HealthOrg node level, and standard node to hub update processes would be employed.

The NoID protocol protects against theft or usage for non-health purposes by 3 key factors: 1. centrally stored profiles are abstracted from their raw data via hashes and have no meaning outside a NoID environment. 2. nodes on the network are members of a blockchain public ledger, and the ability to communicate across the NoID protocol is dictated by the nodes collateral or NoID coins. 3. All communications are digitally signed and fully encrypted using the PKI embedded in the blockchain (See Appendix B).

The NoID protocol protects data integrity and security during the writing and transferring of data by leveraging existing protocols such as TCP for network

communication and package management. Additionally, NoID leverages standard data exchange protocols which check for well-formed and complete data.

SUPPORT FOR PRIVACY AND ANONYMITY

The NoID protocol is fully HIPAA and HITECH compliant with full encryption and hashing of PHI at every layer supporting both privacy and anonymity for patients. As national and state standards change, any changes which require modified functionality will be managed via standard NoID version software updates to the open source reference implementation.

In order to both enable patients to set privacy settings and to allow for more robust auditing capabilities and alerting, the NoID protocol has the ability to put a patient's NoID Profile 'Under Glass". This would allow for a patient to dictate such settings as what Nodes to share their NoID patient resource with, and what geographic regions their data should not leave (See Appendix A: Sharing Profile). Additionally,, the "Under Glass" methodology provides a mechanism for a provider to "break glass" and access the patient's data should an emergency arise.

NoID protocol protects patient's privacy settings by using the same methodology for all NoID communication and data transfer: hashing, network trust, digitally signed and encryption.

Patients can securely store healthcare data using the Sharded Cache Nodes, which encrypt data and break them into small fragments which get distributed to many different nodes with multiple copies for redundancy. The NoID patient profile (biometrics and swipe pattern or other 2FA) acts as the key to find and decrypt all the data when they need to view or update when using their patient hub web portal. This technology is currently implemented in the open source MaidSafe "SAFE" network (maidsafe.net) which utilizes the Bitcoin blockchain.

SCALABILITY

The scalability of the NoID protocol is one of its most robust aspects. Because a NoID Profile of hashed biometrics and demographics is used for patient identification, there is no logical limit on the number of unique NoID patient resources which can be created and managed. We expect this to be true now and well past 120 years from now, and true for 100% of the US population if they are willing to enroll and have access to a HealthOrg Node.

The primary limits to the number of patients the NoID protocol can handle are centered on patient access to HealthOrg nodes rather than logical scalability. However, the barriers to entry for HealthOrg Nodes are so low that any entity involved in patient care can easily join and participate in NoID. The NoID protocol is designed to use open source software, operate on multiple software platforms, and employ commodity

hardware to help facilitate easy and inexpensive node and hub registration (See Appendix B).

The NoID protocol is capable of handling any patient regardless of socioeconomic or cultural background. For the standard HealthOrg node, such as an ambulatory clinic or pharmacy, facility based protocols for managing non-US citizens would be employed. However, NoID does not require any demographics which are specific to nationality, so any issues relative to non-English speaking or non-US citizens would be relegated to providing meaningful feedback to the patient by the Node. Additionally, we believe that the NoID protocol is ultimately capable of interfacing with other projects which leverage similar biometrics such as the "Aadhaar" project in India[1]. However, this type of interfacing is beyond the scope of this paper.

NoID implements a scalable technical architecture with built in clustering, high availability, fast performance, low maintenance, and easy administration/setup with efficient utilization of computer resources. When data is transmitted over the wire, NoID utilizes protocol buffers (google.com/protocol-buffers) to reduce data packet size and memory utilization. NoID can also integrate with other network protocols like Bittorrent (bittorrent.com) and/or Facebook's warp-speed data transfer (github.com/facebook/wdt) to increase effiencies over high letancy connections.

ADOPTABILITY

The NoID protocol will be adopted by the majority of stakeholders in the US simply because it offers a safe, reliable, scalable, and inexpensive means to uniquely identify all patients in the US. The NoID protocol does not leverage a central repository to house patient PHI, but instead facilitates how Healthcare Organization nodes exchange the PHI that they house and protect (See Appendix B). The framework for this is a standard HL7 messaging protocol. The HL7 Patient Resource serves as a standard which allows for the exchange of patient data with any system which is capable of consuming these standard messages.

IT systems such as Electronic Health Records will also need to adopt the open source protocols to integrate with NoID. However, organizations can use the stand-alone open source reference implementation software without integrating into their HIT system (See Appendix A: Reference Implementation (RI)).

The NoID solution will cause a high percentage of patients of all types to participate due to its adoption by the greater healthcare community. Compared with other possible solutions, NoID is open source (i.e., free), non-proprietary software that runs on commodity (i.e., inexpensive) hardware. Lastly, the solution is cross-platform and capable of running on the vast majority of existing operating systems (See Appendix B: Basic Requirements)

[1] Aadhaar project http://uidai.gov.in/aapka-aadhaar.html

IMPLEMENTATION

The NoID protocol solution will be rolled out across the U.S. by following a typical System Development Life Cycle:

- Planning/Analysis: In-depth analysis of the NoID protocol coupled with environmental analysis.
- Architecture Design, Development and Coding
- Protocol Testing
- Delivery
    - Roll out regional Patient Hub capable of handling 50,000,000 profiles
    - Initial Patient Hub will be administered by the NoID team
    - Registration of HealthOrg nodes within 500 miles of closest functional Patient Hub.
- Maintenance and Support (perpetual)

We expect the hosts of the Hubs to bear the costs for implementation and management of the Hubs. The hosts of these Hubs will likely be parties with a vested interest in patient care (health care organizations, ACO's, pharmacies, laboratories, payers, etc). The reasoning behind the Hub hosts wishing to participate and incur these costs vary by the business model of the host. However, they may include such incentives as NoID acting an Enterprise Master Patient Index across their systems. EMPI costs can be substantial for large organizations. The ability to advertise via the NoID kiosks and web interfaces is another cost savings opportunity for all potential hosts. The ability to gather metadata about patient populations is also a value added capability. Lastly, and beyond the scope of this document, is the potential for NoID to facilitate clinical data exchange across disparate systems.

Appendix A: NoID Protocol Definitions:

- NoID Blockchain: A decentralized, consensus driven immutable public ledger that securely stores monetary inputs/outputs (wallet balance), NoID fees, node registration, hub registration, budget proposals, budget votes and hub quality votes. This blockchain is implemented and based on the Bitcoin protocol.
- Reference Implementation (RI): The NoID open source protocol reference implementation software is hosted on github.com. The core implementation supports all protocol node types and all functions of the system.
- NoID P2P Network: A peer to peer network of nodes running the NoID RI software. The P2P network enables nodes to securely communicate and share the public NoID blockchain.
- Healthcare Organization Node (HeatlhOrg or Node): A registered name/public key pair that represents a healthcare organization on the NoID blockchain. Decentralized name registration or DDNS will be implemented much like Emercoin.
- Sharing Profile: A hashed patient resource used to store and transmit patient privacy and security settings.

- Patient Hub (PtHub or Hub): The patient hub is a specialized second tier node responsible for patient record location and patient security profile services. Stores biometric and demographic hashes for match verification. Patient HUBs maintain a list of trusted healthcare organization nodes. Patient Hubs must maintain a collateral wallet address and the balance dictates how many patients they can host on the NoID network. These nodes will be implemented much like Dash's masternodes and also use DDNS name registration on the Blockchain.
- Node Trust Template: List of nodes trusted by a PtHub used in a patient's default privacy and security settings.
- NoID Profile: A resource containing hashes that represent a patient's demographic and biometric information used for matching.
- NoID Coins: The integrated cryptocurrency used to pay for patient matching queries, collateral, PtHub & Node name registration fees, storage, and patient location services.
- Hub Quality Votes: Each match fee paid by a Node entitles them to 1 quality vote in the next monthly quality budget superblock cycle.
- Budget Proposal Votes: Patient Hubs can vote on foundational project budgets that are paid monthly with a superblock cycle. Project budgets are used to fund protocol and foundation development.
- Sharded Cache Nodes: Specialized decentralized NoID nodes used to store shards of encrypted patient hub cache data. These nodes work much like the MaidSafe's SAFE network to protect from decryption, unauthorized access and data loss.
- NoID Certificates: These certificates are created during the hub and node registration process and contain all the information and keys needed to run a registered NoID node or cluster.

NoID Appendix B: Protocol Setup and Configuration Workflows:

- Basic Requirements: Internet connected NoID approved biometric device running the NoID RI software. All major Smartphone, Kiosk, and Desktop platforms supported.
- NoID blockchain: Uses the Argon2d password hash algorithm which is ASIC resistant for a healthy GPU ecosystem. Protocol & chain parameters:

TCP/IP ports: 39600 for protocol & 39601 for RPC	**Block Time Interval**: 4 minutes or 360 blocks/day.
Block Rewards (Every 4 Minutes)* Patient Hub: (300 coins + fees)/total patients x your patients per block. Halves every 2 years. PoW Miner: 80 coins per block, halves every 2 years.	**Collateral*** Budget Proposals: 100 coins Patient Hub Collateral: 1 coin per 100 active patients with a min of 10,000 coins (1 million patients) and a max of 1,000,000 (100 million patients).
Superblocks* First block: 10 million coin seed.	**Fees*** HealthOrg Name Registration: 100 coins per year.

Hub Quality Votes: 50,000 coins per month split. Budgets: 25,000 coins per month for 10 years.	Patient Match: 0.01 coins. Earns 1 quality vote. Patient Hub Registration: 100,000 coins, and 10,000 coins per year thereafter.
Max coins* = 200 million. **Parameters subject to change before deployment to sustain a healthy ecosystem.*	

- Patient Hub Setup: To register a new patient hub on the blockchain, basic information is entered, a collateral wallet is created and a hub registration fee is paid in NoID Coin. This is a list of the required information:
    - Public Key Address
    - Private Key Associated with Public Key Address.
    - Hub Name Associated with Public Key Address
    - Hub Patient Portal Page
    - Challenge/Response page URL. Verifies your system can decrypt using the public key registered in the blockchain.
    - System Admin Contact group of NoIDs
    - Compliance Office group NoIDs
    - Send coins to collateral wallet address.
  - Each hub node needs access to a Couchbase Server NoSQL cluster (couchbase.com) that securely stores NoID resource hashes for their patient accounts. All PHI required by the hub UI is stored by Sharded Cache Nodes.
- Node Setup:
  - Register name on the blockchain with basic organizational information and a node registration fee.
  - Required Information:
    - Public/Private Key Pair.
    - Healthcare Organization Name
    - Organization Domain URL
    - Node Type (Pharmacy, Hospital, Small Doctor's Office, etc..)
    - Challenge/Response page URL.
    - Facility Address
    - List of primary contact phone and email
  - Optional Information
    - Communication Server URL
- Patient Enrollment: There is no enrollment fee. A patient can enroll using a smartphone, PC or kiosk running the NoID RI software with a fully downloaded blockchain. The device(s) collects demographic and biometric information, downloads the hub hash template and creates hashes to form the NoID Profile used for authentication and matching. To secure the account, the patient selects an unlock pattern on top of a custom image. A patient can only enroll once in the NoID system. The patient can delegate authority to other NoID profiles if they can not manage their own account like in the case of children.
  - Required Demographics Hashes
    - Full Name, Date of birth, Gender, City, State

    - Biometrics Template Hashes
    - Optional Information Hashes
        - Street address, zipcode, phone number, name of parents, name of children, name of siblings, driver's license number, insurance policy numbers, race/ethnicity, blood type, chronic diseases, birth order.
- Patient Hub Access: The patient can access their hub account by using the NoID RI software. At least one biometric reading and the correct unlock pattern is needed to authenticate. Once authenticated, the user can modify default sharing profile, anonymity settings, demographics, and all other settings to manage their hub account. The hub also stores audits collected from node match requests.
- Node to Node Communication: All registered node names/public keys are discoverable using the NoID blockchain. Nodes can securely communicate by sending NoID resources and encrypting them using the recipient's public key.
- Node to Patient Hub Communication: To conduct patient matching, nodes send the captured NoID profile to regional patient hubs. If there is a match, a response is sent back to the node with record location information and the patient's sharing profile.
- Patient Hub to Patient Hub Communication: Hub to hub communication is needed to transfer patient accounts. Hubs can also propagate NoID Profile changes to other Hubs (i.e., due to need to rehash data).
- Patient Verification Process:
    - Patient presents at NoID node, and node captures at least one biometric from the patient and creates a preliminary NoID profile.
    - The NoID software checks for an internal node match
        - If an internal match is found, the user must confirm the match.
        - If a match is not found, the node user selects or enters the patient demographics. Demographics can auto populate a NoID node via a typical registration resource interface. NoID uses a REST RPC API to send and receive NoID patient messages within their intranet.
    - The node sends the patient's full NoID profile to regional patient hubs for matching. A fee is paid to the network to conduct the match.
        - If a match is found, a NoID resource is returned containing record location pointers and the patient's sharing profile.
        - If a match is not found, the fee is refunded and the node user should follow the patient enrollment procedures if possible.
- Patient Audit Process
    - Patient can audit their NoID Profile via a secure website using the unlock pattern created at enrollment. This website provides metadata about the patient's NoID Profile such as which nodes matched on their Profile, what data element may have been updated, date/times of any actions related to their profile, and contact information for HealthOrg nodes. However, no PHI is available for download or viewing via this site. This interface also exposes the NoID privacy and security settings for review and/or modification.