CHIME National Patient ID Challenge

NoID: A Novel Approach

1) TABLE OF CONTENTS

2) SIMPLE, FAST 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). Enrollment can occur at any location which chooses to implement the NoID protocol (laboratories, 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 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 been 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 scanning of two fingers to obtain fingerprints for use as biometrics for authentication. This requirement greatly reduces the potential for future matching errors[1]. The NoID protocol also dictates the use of electronic iris recognition devices to gather additional biometrics (See Appendix B). Further, the NoID protocol encourages scanning and Optical Character Recognition technology to gather demographics from identification cards.

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 an update message to

[1] Frost & Sullivan, 8. https://danishbiometrics.files.wordpress.com/2009/08/a-best-practices-guide-to-fingerprint-biometrics.pdf

be processed 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).

The barriers to entry for our solution for both providers and patients center primarily on access to a HealthOrg node, and the technical requirements to participate in the protocol. However, the setup of the NoID protocol at the node level is highly automated requiring minimal technical skills to accomplish (See Appendix B). Lost network connectivity could provide challenges as well. However, all NoID messages are queued at the node and hubs and are processed immediately upon reconnection.

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 present itself 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 2.x and FHIR 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. Use cases are in the table below (See Appendix B: Patient Enrollment).

Use Case	Scenario	Use Case	Scenario	Use Case	Scenario
Adult male	Standard enrollment	**Adult female**	Standard Enrollment	**Male child**	Guardian standard enrollment.
Newborn	Guardian standard enrollment.	**Twins**	Standard Enrollment	**Surgery**	Preoperative standard enrollment
Foreign citizen	Standard enrollment	**Fully amputated fingers.**	Use alternate biometric sites (iris) and log amputation as biometric.	**Emergency**	Standard enroll after stabilized
Refuses	Can not enroll without informed consent	**Unconscious**	Can not enroll without informed consent	**Psychiatric without guardian**	Can not enroll without informed consent or state mandate

3) SIMPLE, FAST, 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).

When an enrolled patient visits a provider, a single valid biometric (either fingerprint or Iris scan), is enough to positively identify an existing patient. The Hub will process the NoID Profile, query other Hubs for matches, and if found, return a FHIR resource(s) detailing Node data for Node update process (See Appendix B: Patient Verification Process).

We estimate that the NoID protocol will remove 30 seconds from the standard facility based registration processes for existing patients. However, this is highly dependent on the biometric device employed, and could be as little as 10 seconds. We expect all NoID based network calls, NoID database queries, and responses to complete in less than 10 seconds regardless of the NoID patient population.

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: 1/10,000,000,000 or lower. 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%. Uses cases in the table below (See Appendix B:Patient Verification Process).

Use Case	Scenario	Use Case	Scenario	Use Case	Scenario
Primary care	Standard verification	**ED visit**	Standard verification	**Overseas Military Personnel**	Standard verification
Hospital admit	Standard verification	**Outpatient pharmacy**	Standard verification	**Outpatient chemotherapy**	Standard verification
Unconscious	Standard verification	**Commercial laboratory**	Standard verification	**Organization without NoID**	Patient can verify if enrolled.
Ambulance	Standard verification	**Bilateral iris rubeosis**	Use alternate site and log iris rubeosis as biometric.	**Deformed target finger**	Use alternate site and log deformity as biometric.

4) SECURITY AND FRAUD MANAGEMENT

As previously detailed, the NoID solution provides for 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 communication is fully encrypted (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 such as HL7's FHIR which check for well-formed and complete data. Uses case scenarios are depicted in the table below:

Use Case	Scenario	Use Case	Scenario
Unauthorized Hub Access	Hacker will need the swipe pattern or password and a forged biometric to gain unauthorized access. Audits and alerts help react to this unlikely event.	**Impersonate HealthOrg Node on the Network**	Several private keys, system admin NoID profiles and the organization's web site would need to be compromised.
NoID Protocol Security Vulnerabilities	Open source code allows more vetting by the community than proprietary code. NoID protocol has budgets blocks that can fund pen testing and bounties for Vulnerability Reward Programs.	**NoID Blockchain Corruption or Forking**	By controlling >51% of the network hashing power, an attacker can alter the chain to double spend coins. This attack is cost prohibitive and does not breach registration signatures or anything else.
Social Engineer to Imposter Patient	Imposter would need multiple forged biometrics scanned with a PatID Hub agent conducting the scan.	**DDoS PtHub Attack**	PtHubs are resilient to DDoS due to NoID's clustering ability and decentralized architecture. PtHub nodes can run on top of I2P or Tor to obscure their nodes from DDoS attackers.
Fraudulent Enrollment with Fake Demographics	This only hurts themselves but is possible. HealthOrg nodes and PtHubs should develop methods to prevent this.	**DDoS HealthOrg Attack**	HealthOrg nodes are resilient to DDOS due to NoID's clustering ability and decentralized architecture. HealthOrg nodes can run on top of I2P or Tor to obscure their nodes from DDoS attackers.

DDoS Network Attack	Decentralized P2P systems are resilient to DDoS since there is no central point.	**Hub Cache Breach**	Hacker will need the pattern swipe or password and a copy of a biometric to gain unauthorized access.
Impersonate Patient Hub Node	Several private keys, NoID profiles and the org's web site would need to be compromised.	**PatHub Data Breach**	Biometrics/demographics are hashed and not useful outside NoID. PatID regularly re-set hash parameters so the hashes are eventually replaced.
Unauthorized Hub Registration Updates	Attacker would need to gain access to the hub's system admin NoID profile.	**Breach Sharded Cache Node**	Breaching a cache node doesn't expose cache since it is encrypted and sharded. The attacker would have access to the node's NoID coins and reward.
Unauthorized HealthOrg Registration Updates	Attacker would need to gain access to the node's system admin NoID profile.	**Register a Fake HealthOrg Node**	By default, new registrations are not trusted. The PtHubs verify the authenticity of the HealthOrg using digital and manual methods.
Fraudulent Verification By HealthOrg User	NoID biometric devices used by HealthOrg nodes prevent but are not resistant to forgery. Access activity is audited so the user would likely get caught.	**Fraudulent Reset By Patient Hub User**	The standard NoID biometric devices used by PtHubs prevent forgery. Reset activity is audited so the user would likely get caught. Notifications are sent to the patient and hub administrators.
PtHub Exceeds Patient Collateral Rules	They do not get reimbursed for the extra patients and get penalized in the quality vote blocks.	**Send A Node a Forged Blockchain**	New blocks will not fit in the forged chain so the node will know and ban the misbehaving node.

5) 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.

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, and encryption.

6) 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[2] . However, this type of interfacing is beyond the scope of this paper.

Our solution will maintain high speed, security, 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 scalable (See Appendix B). Further, NoID Patient Hubs aggregate by region increasing its ability to scale to a global level. The blockchain enrollment of nodes is also highly scalable and secure. The blockchain is secured by hashing much like Bitcoin and the patient hubs make up a decentralized second tier much like masternodes in Dash. Patient hubs, or masternodes, need a fixed amount of collateral per patient. 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 and high patient ratings, thereby generating the required collateral. Periodic patient ratings make up the majority of the reimbursement rate. The system is Decentralized Autonomous Organization that self regulates based on standard decentralized patient satisfaction ratings.

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

7) ADOPTABILITY

The NoID protocol will be adopted by the majority of stakeholders in the US simply because if 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 Facility Nodes exchange the PHI that they house (See Appendix B). The framework for this is HL7 FHIR messaging protocol, and crucially the FHIR Patient Resource. The HL7 Patient Resource serves as a standard which allows for the exchange of patient data with any system which has stood up a FHIR server.

State and federal agencies such as Medicare, Medicaid, and the V.A. will need to register as NoID HeatlhOrg nodes and adhere to NoID protocol in order to participate and gain access NoID patient populations. This is required so that Patient Hubs can verify and trust all NoID interfaced agencies.

IT systems such as Electronic Health Records will also need to adopt the open source protocols to integrate with NoID. However, organizations can use 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) 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)

8) 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: 100-200 man-hours
- Design: Architecture design : 200 man-hours, Coding/Programming: 1,200 man-hours, Protocol Testing: 100 man-hours
- Implementation
    - Roll out regional Patient Hub capable of handling 100,000,000 profiles: 32 man-hours per Patient Hub
        - Initial Patient Hub will be administered by the NoID team
    - Registration of HealthOrg nodes within 500 miles of closest functional Patient Hub: 8-32 man-hours
- Maintenance (including updates and upgrades): Perpetual

The total costs for full U.S. implementation over a five year period are limited. Patient Hub implementation costs will be borne by the Patient Hub host and will consist of one-time costs of approximately $1000 for system setup and configuration (32 man-hours at $100 an hour). Hub costs will also consist of recurring annual costs of $10,000 for hardware and $40,000 for system admin. System admin costs are per

5,000,000 profiles, and will need to scale up proportionately as PtHubs host more NoID profiles. There are no costs for the software at either the node or hub levels. We feel that a reasonable number of patient Hubs which would realistically cover the entire U.S. population would be 50 (although, each Patient Hub can hold a max of 100,000,000 NoID Profiles and conceivably, 5 Patient Hubs could cover the U. S. population). Consequently, one time costs for national Patient Hub implementation are estimated at $50,000. Recurring national Patient Hub costs are: ((50 x $10,000 for server infrastructure) + ($40,000 server administration per 5,000,000 patients)), or ($500,000 infrastructure + ($40,000 X (500,000,000/5,000,000)), or $500,000 + $4,000,000 or $4.5 million annually for all Hub hardware and support for the U.S. population.

We expect the hosts of theHubs 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 (healthcare 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 (bitcoin.org).
- 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.
- FHIR Resources: Fast Healthcare Interoperability Resources (hl7.org/fhir). FHIR resources are used to store and transmit healthcare data within the NoID P2P network.
- Healthcare Organization Node (HeatlhOrg or Node): A registered name/public key pair that represents a healthcare organization on the NoID blockchain.
- Sharing Profile: A hashed FHIR 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 (dash.org).

- Node Trust Template: List of Nodes trusted by a PtHub used in a patient's default privacy and security settings.
- NoID Profile: FHIR 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 Storj (storj.io) to protect from decryption 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 hash algorithm which is ASIC resistant for a 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. Hub Quality Votes: 50,000 coins per month split. Budgets: 25,000 coins per month for 10 years.	**Fees*** HealthOrg Name Registration: 100 coins per year. 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 Redis database (redis.io) that stores encrypted NoID and other FHIR resources 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
        - FHIR 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 FHIR 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
- Required Biometrics Template Hashes:
    - Two fingerprint scans where scanners must adhere to Electronic Fingerprint Transmission Specification
    - Iris Scanners: Right and left iris scans.
- 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 FHIR 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 HL7 2.x ADT, CDA or a FHIR registration resource interface. NoID uses a REST RPC API to send and receive FHIR 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 FHIR 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.