Global patient identifiers are dangerous and when compromised, could provide access to Protected Health Information. We believe a better approach is to create HL7 FHIR resources containing hashed patient demographic and biometric data, which in its entirety, acts as the means for patient identification. The methodology to achieve this goal uses a decentralized blockchain and public ledger technology to manage participants, encryption, and advanced cryptography to protect communication and patient data, HL7 FHIR protocols for interoperability, and hardware such as smartphones to gather and validate biometric data. This is the NoID protocol.

* NoID provides simple and fast patient enrollment
  + Enrollment occurs at Healthcare Organization Nodes
  + Nodes communicate with Patient Hubs which provide identification verification
  + All communication between Nodes and Hubs is secure
  + Protocol is not dependent on age, sex, nationality, health condition, etc
  + NoID Profile is a shared data set used to store hashed patient data. NoID Profile are stored/transported as FHIR resources
  + Biometrics used to minimize errors in enrollment and increase accuracy
  + Data is meaningless outside of NoID. However, if a NoID profile was compromised, it can be changed by applying a modified hash algorithm
  + The setup of NoID functionally at a node is highly automated
  + The protocol handles exceptions to typical biometric gathering by providing alternative pathways to populate NoID Profiles
  + Hubs provide a secure web interface which allows patients access to privacy/anonymity settings and audit metadata. No PHI is stored on hubs
  + Enrollment adds 3-6 minutes to the patient registration processes (biometric gathering) but saves time on subsequent registration
* NoID provides fast, accurate identification
  + Reduces transcription errors by mandating biometric input devices and recommending OCR technology
  + A single biometric is enough to positively identify an existing patient
  + If a match is found, the Patient Hub returns a FHIR location resource to the calling node with pointers to other nodes which have a copy of that profile. The calling node then requests a FHIR Patient Resource to update their systems. Any new data added to the NoID profile triggers a cascade of node-to-node updates to sync profiles
  + Should remove 30 seconds from standard facility registration
  + All queries should complete in under 10 seconds
  + False positive rates would be extremely low: 1/10,000,000,000. Expected false negative rates are higher at 1/1,000,000. This is due to the variability of data inputs
* NoID provides security and fraud management
  + Protects data by 3 key factors.
    1. Centrally stored profiles are abstracted from their raw data
    2. Nodes ability to communicate across the NoID protocol is dictated by the node’s collateral or NoID coins
    3. Communication is fully encrypted
  + Uses the latest asymmetric cryptography standards
* NoID provides support for privacy and anonymity
  + HIPAA and HITECH compliant through encryption and hashing
  + Provides patient ability to set privacy and anonymity settings
* NoID is scalable
  + Software is free, open source, and available via MIT license
  + Uses commodity hardware
  + Supports all major platforms (Android, iOS, Windows, Linux, etc)
  + Uses peer-2-peer (P2P) decentralized cryptocurrency architecture
  + Profiles are completely unique and can scale to handle the US population
  + Potential interoperability with other systems such as India’s “Aahaar”
* NoID high adoptability
  + Offers a safe, reliable, scalable, and inexpensive means to uniquely identify all US patients
  + Patient participation will be driven by healthcare providers
* NoID will follow standard implementation using SDLC
  + Planning/Analysis : 100-200 man-hours
  + Design: 1500 man-hours total
  + Implementation: 32 man-hours per hub. 8 man-hours per node
  + Maintenance: perpetual
  + Total annual costs for all US population is approximately $4,500,000
  + Initial patient Hub will be hosted by NoID team. Subsequent hubs to be hosted by payers, large healthcare organizations, etc