eHealth Exchange
Architecture 101

By Eric Heflin, eHealth Exchange CTO
May 22, 2014
Agenda

- eHealth Exchange General Overview
- Guiding Principles
- Use Cases Supported
- High Architectural Components
- Security Overview
- Standards Support
- Testing
- Operational Support
- The Future
- Q&A
EHEALTH EXCHANGE OVERVIEW
2 Defining the NHIN
This section of the document describes the NHIN and provides context for its role within the broader national healthcare agenda.

2.1 Introduction to the NHIN
The Nationwide Health Information Network (NHIN) is a collection of standards, protocols, legal agreements, specifications, and services that enables the secure exchange of health information over the internet. The NHIN is a key component of the nationwide health information technology strategy and will provide a common platform for health information exchange across diverse entities, within communities and across the country, helping to achieve the goals of the Health Information Technology for Economic and Clinical Health (HITECH) Act. This critical part of the national health IT agenda will enable health information to follow the consumer, be available for clinical decision making, and support appropriate use of healthcare information beyond direct patient care, such as to improve public health.
The HITECH Act calls for the Office of the National Coordinator for Health Information Technology (ONC) to develop "a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that...promotes a more effective marketplace, greater competition...[and] increased consumer choice" among other goals. (Section 3001(b)). The NHIN is a critical part of that technology infrastructure and plays an important role in the National health agenda.
Special Deemed Status

• Meaningful Use regulations and guidelines designate the eHealth Exchange as one method of achieving certain measures. See 170.314(b)(2) – Transitions of Care Measure #2
• [http://ehealthexchange.wikispaces.com/Webinars](http://ehealthexchange.wikispaces.com/Webinars)
An eHealth Exchange Participant does not have to be certified in order for Provider A’s transmissions to count for MU. However, Provider A must still use CEHRT to generate a standard summary record in accordance with the CCDA.
eHealth Exchange

Shared trust framework and rules of the road

The Internet

Common standards, specifications and policies enforced through Data Use & Reciprocal Support Agreement (DURSA)
eHealth Exchange Anchor Participants

- etHIN
- SCHEx
- Social Security Administration
- MEDVIRGINIA
- East Tennessee Health Information Network
- OCHIN
- Department of Veterans Affairs
- San Diego Beacon Health Community
- MUSC Medical University of South Carolina
- Dignity Health
- EHRDOCTORS
- Wright State University
- CMS Centers for Medicare & Medicaid Services
- SEMHIE
- United States Department of Veterans Affairs
- Health eWay
- UHIN Connecting the Community
Healtheway

eHealth Exchange network participants currently include:

- 41 Participants live in production with presence in all 50 states (representing four federal agencies, six state HIEs, and more than a dozen health systems and nearly 20 Health Information Organizations)
- 69 organizations in test status
- Together this represents:
  - 1,600 hospitals
  - 10,000 medical groups
  - 850 pharmacies
  - Nearly 800 dialysis centers
  - Targeting 100 million patients
- In 2013:
  - 26 million transactions pushed
  - 250,000 transactions pulled
Participants live in production with presence in all 50 states (representing four federal agencies, six state HIEs, and more than a dozen health systems and nearly 20 Health Information Organizations)

- 69 organizations in test status
- Together this represents:
  - 1,600 hospitals
  - 10,000 medical groups
  - 850 pharmacies
  - Nearly 800 dialysis centers
  - Targeting 100 million patients
- In 2013:
  - 26 million transactions pushed
  - 250,000 transactions pulled
eHealth Exchange Growth

- **2009**: ONC Initiative: NwHIN Exchange
  - Total Participants: 4
  - Operations supported by ONC

- **2010**:
  - Total Participants: 16
  - Non-Federal Participants transacting in connection with federal contract

- **2011**:
  - Total Participants: 23
  - Transitioned to public-private initiative: eHealth Exchange

- **2012**:
  - Total Participants: 39
  - Operations supported by HealtheWay

- **2013**:
  - Total Participants: 44
  - Maturation of connectivity
  - Non-Federal Participants transacting to achieve MU2 credit for TOC 2 measures

- **2014**:
  - Projected Total: 102
  - Q1: 50
  - Q2: 72
  - Q3: 93

**Operations supported by HealtheWay**

**Transitioned to public-private initiative: eHealth Exchange**

**Maturation of connectivity**

**Non-Federal Participants transacting to achieve MU2 credit for TOC 2 measures**
Healtheway Participants

- Alabama One Health Record
- **Centers for Medicare and Medicaid Services (CMS)**
- Children's Medical Center of Dallas
- Cleveland Clinic Foundation
- Community Health Information Collaborative (CHIC)
- Conemaugh Health System (CHS)
- **Department of Defense (DOD)**
- **Department of Veterans Affairs (VA)**
- Dignity Health
- Douglas County Individual Practice Association (DCIPA)
- Eastern Tennessee Health Information Network (etHIN)
- **EHR Doctors**
- Geisinger Health System
- Gundersen Health System
- The Guthrie Clinic
- Hawaii Pacific Health (HPH)
- HealthBridge
- HealtheConnections RHIO (Central NY)
- *Idaho Health Data Exchange (IHDE)*
- *Indiana Health Information Exchange*
- Inland Northwest Health Services
- Kaiser Permanente
- Lancaster General Health
- Marshfield Clinic
- Medical University of South Carolina (MUSC)
- *MedVirginia*
- The MetroHealth System
- *Michigan Health Information Network (MiHIN)*
- MultiCare Health System
- National Renal Administrators Association (NRAA)
- New Mexico Health Information Collaborative
- North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)
- **OCHIN**
- Providence-Swedish Health System
- Quality Health Network (QHN)
- Redwood MedNet
- San Diego Beacon
- Strategic Health Intelligence
- **Social Security Administration (SSA)**
- South Carolina Health Information Partners, Inc. (SC-HIP)
- South East Michigan Health Information Exchange (SEMHIE)
- Texas Health Resources
- UC Davis Health System
- Utah Health Information Network (UHIN)
- Walgreens
- Western New York HEALTHeLINK
- Wright State University
- Yale New Haven Health
eHealth Exchange Overview

- eHealth Exchange Provides
  - Legal/Trust Framework
  - Operating Policies and Procedures
  - Operational Support (via Healtheway)
- Technical Services
  - UDDI (phone book of other eHEX Participants)
  - Security (x.509 Managed CA)
  - Testing with our partner organization
The DURSA limits treatment, payment and operations beyond what HIPAA permits.
Uses Cases Supported

- Care Summary Focused
- Treatment
- Disability Claims
- MU
- Quality
- Biosurveillance
- Push and Pull
- Audit
- Process for Adopting New Use Cases
Principles

- Security
- Patient Privacy
- Decentralization
- Local Autonomy
- Local Accountability
- Vendor & Technology Neutral
- Based On Open Standards
- Scalable
DURSA-Established Common Trust Framework

DURSA

- Participant (HIE/Intermediary)
- Participant (Governmental Entity)
- Participant (IDN)

End User License Agreement/ Terms of Use

User

Developed by Troutman Sanders
DURSA Architectural Implications

• Establishes common operating, trust, and legal requirements including:
  • Multi-layer security framework
  • Enablement of autonomous operation; thus requires key transaction data elements such as purpose for the request, the role of the user/system making the request
  • Symmetrical audit logging
  • Patient privacy enforcement
  • Formal change control process
Architectural Requirements

• Ability to discover and exchange healthcare information amongst participant entities
• Ability to match patients to their data without a universal or national patient identifier
• Ability to support patient preferences regarding their data exchange
• Support secure data exchange
• Support harmonized standards
• Support diverse set of organizations, technologies, and approaches
• Support a common trust agreement
• Meaningful Use
• Reliability
• Scalability
• Non-repudiation
Specification Development Process

• eHealth Exchange specifications
  • Prescribe the technical and security requirements necessary to support information exchange among Participants
  • Developed through a collaborative, multi-stakeholder process
  • Work is carried out by the eHealth Exchange Specifications Factory
  • Formerly ONC-facilitated work group; now facilitated by Healtheway
  • Comprised of representatives from a variety of public and private stakeholders.
  • Guided by the eHealth Exchange governance structure (Policy Technical Committee and Coordinating Committee)

• Updates or enhancements to eHealth Exchange functionality are driven by development requests submitted by Participants.
Exchange Specifications

Official eHealth Exchange Testing Documentation Errata and Change Log

2011 Current Specifications (Production Effective Date 3/1/2012)

These specifications were approved for production use for the eHealth Exchange Coordinating 2012-03-01 and should be used by new eHealth Exchange Participants. Note that Participants with their key Exchange partners to coordinate their adoption of 2010 vs. 2011 specifications.

CAQH CORE X12 Document Submission Service Interface Specification v 1.0 3/6/2012 [PDF - 544 KB]
Electronic Submission of Medical Documentation (esMD) X12 Profile v 1.0 3/6/2012 [PDF - 783 KB]
Web Services Registry Web Service Interface Specification v 3.1 3/6/2012 [PDF - 405 KB]
Messaging Platform v3.0 approved by NTCOn 6/27/2011 [PDF - 232 KB]
HIGH-LEVEL ARCHITECTURE
# eHealth Exchange

## Architectural Layers

### Profiles
Employing exchange patterns to enable clinical data enabled workflows

- Care Summary Exchange
- Quality / Admin Data Push
- Claims Eligibility

### Information Exchange
Employing lower-level layers to enable basic message exchange patterns

- Patient Discovery
- Query for Documents
- Retrieve Documents
- Patient Consent
- Push
- Publish / Subscribe

### Discovery, Message Security and Privacy
Message security, privacy, and interoperable healthcare data exchange

- Web Services Discovery (UDDI)
- Message Platform
- Authorization Framework

### Operational Infrastructure
Runtime systems supporting the eHealth Exchange

- Security Infrastructure (Managed PKI)
- Web Services Discovery (UDDI)
Participant Gateway

• Each eHealth Exchange Participant deploys one or more eHealth Exchange “Gateways”
• The Gateway directly, or indirectly, implements many of the architectural layers on the prior slide
• A Gateway typically consists of:
  • A single organization (e.g., Kaiser Permanente, the Department of Veterans Affairs, the SSA)
  • A Health Information Exchange (HIE) representing multiple organizations (e.g., MedVirginia)
  • A HIE representing multiple HIEs (e.g., MiHIN, several state-wide HIEs onboarding now)
• Gateways typically perform the following functions:
  • authentication, authorization, auditing, policy management, internal clinical data connectivity, and much more
• A gateway can be an EMR, or an HIE, or a “thin” connector
MESSAGE EXCHANGE PATTERNS
Query/Response

- Considered by many to be the “core” eHealth Exchange message exchange pattern
- (But, as you’ll see, it is one of several patterns)
- Allows an Initiating Gateway the ability to discover information the Responding Gateway may possess
- Several flavors of this pattern are in broad use
Publish/Subscribe

• Health Information Event Messaging (HIEM)
• Allows for subscriptions followed by messages pushes
• Primary use case is/was biosurveillance
• Not in use today; but appears to have new use cases such as public/private care coordination
Push

- Not widely known, but is currently the most common transaction type on the eHealth Exchange today
- Allows for an unsolicited secure transmission of a message, using the base eHealth Exchange services
- Leverages several IHE Profiles
Other Patterns

- Other message exchange patterns are possible and will be added when, and if, Participants request such
HIGHER-LEVEL EHEALTH EXCHANGE SERVICES
Patient Discovery

- Patient Discovery (PD)
- Using IHE XCPD
- Targeted vs. broadcast queries
- Uses the eHEX UDDI to identify end points for targets
- Can have demographics and optional an ID in query
Query for Documents

- After Patient Discovery
- Employs the IHE XCA (Cross-Community Access) Profile
- Returns a list of zero or more matching documents
Retrieve Documents

• After Query for Documents
• Leverages the IHE XCA Profile (as does Query for Documents)
• Allows retrieval of zero or more specific documents
Document Submission

- Push profile
- Unsolicited transmission from one Participant to another Participant
- Documents and associate metadata
- Allows automated patient matching
- Accept or Reject status response
Administrative Distribution

• Allows for pushing of administrative batch data
• Accounts for a large amount of eHealth Exchange current transaction volumes
eHealth Exchange Query Workflow

Patient Discovery (IHE XCPD)

Query for Documents (IHE XCA)

Retrieve Documents (IHE XCPD)

Found patient

Searches for patients

Searches for Document(s)

Lists zero or more found documents

Transmits Document(s)

Returns zero or more documents
SECURITY MODEL
NHIN Security Model Overview

Source: ONC
NHIN Security Model Overview

- Is fundamentally a “system level trust model”
- Strong gateway-to-gateway trust
- Heavily leverages Public Key Infrastructure (PKI)
- Employs a secure channel, with SOAP messages + SAML
- Uses a governed Certification Authority (CA)
- Has been reviewed using Threat/Risk Modeling
- A human user is only a “attribute” of Gateway communications
- All activities between gateways are securely logged
- Provides for automation and user-directed activities
Security

• Leverages Public Key Infrastructure
• 2-way-TLS for connections between Participants
• Single Certification Authority creates a trust anchor point
• Certificates are bound to policy
• Revocation is checked for each transaction
Asymmetric Encryption

- Outbound data is encrypted by the sender, using the receiver’s public key.
- The data can only then be decrypted by one with the possession of the corresponding private key.
- Private keys should be carefully protected.
- Optionally the sender can digitally sign the outbound message with the sender’s private key.
- In this case, anyone can validate the signature using the sender’s published public key.

![Encryption and Decryption Diagram]
PKI Use

• PKI is used to:
  • Validate data integrity
  • Protect data from tampering
  • Protect data from being viewed by unauthorized parties
  • Authenticate the identity of each end point
Single Trust Anchor
Other PKI Considerations

• ID proofed to NIST level 3 or 4
• Federal Bridge (FBCA) cross certified
• Publically accessible policy statements
NIST Threat Model

- Requires a mutual authentication encrypted channel
  - NIST: This allows most threats to “fall away” by virtue of this design

Source: NIST
Public Key Infrastructure

- Remaining threats are best solved by other mechanisms
- Replay attacks
  - If a node is compromised, then we have bigger issues of concern such as the validity of the entire document, thus XML-DSig of a timestamp could be forged
  - If a Man In The Middle (MitM) IP-level attack, then it is unlikely that an attacker could form a proper message from low level packets, and perimeter system could mitigate by detecting duplicate package message ID 64-bit serial numbers
- Denial of Service
  - Mitigated by perimeter systems
EHEALTH EXCHANGE MANAGED CERTIFICATE AUTHORITY
eHealth Exchange CA

• The eHealth issues its own x.509 certificates
• Participants are required to use either CRLs or OCSP to frequently determine if a given certificate, that is intact and within its validity period, has been revoked
• Common revocation reasons include
  • CA has been compromised
  • Certificate private key has been compromised
  • Affiliation changed
  • Superseded
  • Others
UDDI
eHealth Exchange UDDI Use

• Universal Description and Discovery Interface
• UDDI OASIS Standard
• Specifies the use of 3.0.2
• Can be thought of as a single, secure, and authoritative directory of key eHealth Exchange Gateway information
• Will likely be decommissioned by the end of 2015 and replaced by ModSpec Federated HPD during 2014 (my estimate)
NHIN UDDI Use/Support (Cont.)

• In 2009 the NHIN Spec Factory completed the UDDI client specification

• Specifies the optional use of the ONC-governed UDDI for:
  • Determining end points
  • Obtaining additional organization info (such as versioning)
  • Organization scope of coverage (states)
  • Contacts

• Goal is to provide for automation of some aspects of provisioning

• Status: Technical implementation is ready for internal ONC testing; expected to be ready within a few months for external testing
<businessEntity businessKey="udi:ABCHealthGWPRD01:1.2.840..." xmlns="urn:udi-org:api_v3">
  <name xml:lang="en">ABC Health GWPRD01</name>
  <description xml:lang="en">OID:1.2.840... GWPRD01 Integrated health system.</description>
  <contacts>
    <identifierBag>
    </identifierBag>
    <categoryBag>
    </categoryBag>
  </contacts>
</businessEntity>
UDDI Demo

```xml
<contacts>
  <contact>
    <personName xml:lang="en">Eric Heflin</personName>
    <phone>+1-512-555-1212</phone>
    <email>eheflin@abc.com</email>
    <address xml:lang="en" useType="" sortCode="">
      <addressLine>ABC Health</addressLine>
      <addressLine>123 Main Street, City, State, Zip 12345</addressLine>
    </address>
  </contact>
</contacts>
```
UDDI Demo

```xml
<businessServices>
  <businessService serviceKey="uddi:ABCHalthGWPRD01:PatientDiscovery" businessKey="uddi:
  <businessService serviceKey="uddi:ABCHalthGWPRD01:QueryForDocuments" businessKey="udd
  <businessService serviceKey="uddi:ABCHalthGWPRD01:RetrieveDocuments" businessKey="udd
</businessServices>
```
<businessService serviceKey="uddi:ABCHealthGWRD01:PatientDiscovery" businessKey="uddi:ABCHealthGWRD01:PatientDiscovery">
  <name xml:lang="en">Patient Discovery</name>
  <description xml:lang="en">This is an implementation of the eHealth Exchange Patient Discovery service. It provides a method for discovering patient information based on the eHealth Exchange standards.

  <bindingTemplates>
    <bindingTemplate bindingKey="uddi:e6db8080-dd1a-11e3-9a77-086c5e8199dd" serviceKey="uddi:ABCHealthGWRD01:PatientDiscovery">
      <accessPoint useType="endPoint">https://ehealthexchange.ABChealth.org/xcdpresp</accessPoint>
      <categoryBag>
        <keyedReference tModelKey="uddi:nhin:versionofservice" keyName="" keyValue=""/></keyedReference>
      </categoryBag>
    </bindingTemplate>
  </bindingTemplates>
</businessService>
UDDI Live Query Demo

Request

```xml
  <soapenv:Header/>
  <soapenv:Body>
    <urn:find_business>
      <!-- Zero or more repetitions: -->
      <urn:name xml:lang="EN">SSA</urn:name>
      <urn:name xml:lang="EN">Yale New Haven Health GW01</urn:name>
    </urn:find_business>
  </soapenv:Body>
</soapenv:Envelope>
```
UDDI Live Query Demo

Response

```xml
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
  <Body>
    <businessList xmlns="urn:uddi-org:api_v3">
      <listDescription>
        <includeCount>1</includeCount>
        <actualCount>1</actualCount>
        <listHead>1</listHead>
      </listDescription>
      <businessInfos>
        <businessInfo businessKey="uddi:YaleNewHavenHealthGW01:1.2.840.114350.1.13.301.3.7.3.688884.100">
          <name xml:lang="en">Yale New Haven Health GW01</name>
          <description xml:lang="en">OID:1.2.840.114350.1.13.301.3.7.3.688884.100 Multi-Regional Health Care Organization</description>
          <serviceInfos>
            <serviceInfo serviceKey="uddi:YaleNewHavenHealthGW01:PatientDiscovery" businessKey="uddi:YaleNewHavenHealthGW01:1.2.840.114350.1.13.301.3.7.3.688884.100">
              <name xml:lang="en">Patient Discovery</name>
            </serviceInfo>
            <serviceInfo serviceKey="uddi:YaleNewHavenHealthGW01:QueryForDocuments" businessKey="uddi:YaleNewHavenHealthGW01:1.2.840.114350.1.13.301.3.7.3.688884.100">
              <name xml:lang="en">Query for Documents</name>
            </serviceInfo>
            <serviceInfo serviceKey="uddi:YaleNewHavenHealthGW01:RetrieveDocuments" businessKey="uddi:YaleNewHavenHealthGW01:1.2.840.114350.1.13.301.3.7.3.688884.100">
              <name xml:lang="en">Retrieve Documents</name>
            </serviceInfo>
          </serviceInfos>
        </businessInfo>
      </businessInfos>
    </businessList>
  </Body>
</Envelope>
```
ANATOMY OF A EHEALTH EXCHANGE MESSAGE
eHealth Exchange XML SOAP Message
Sample Test Message
(Patient Discovery)
STANDARDS
eHealth Exchange - Use of Standards

• EVERY aspect is based on standards
• Transport (2-way-TLS)
• Encryption (PKI)
• Transactions (IHE XCPD, XCA, XDS)
• Containers (SOAP/XML)
• Clinical Data (CDA)
• And more
TESTING
Testing

• The community has developed a large body of test cases, data, and conformity assessment tools
• Designed to ensure interoperability and assure compliance and minimal implementation
• Healtheway has developed and now operates a validation program to implement these tests
• Battle-hardened by years of operations
Validation Programs

- Participant Testing
  - Required of all Participants before they enter into production

- Product Testing
  - Optional program designed to provide more assurance than the Participant Testing program
  - Allows for reduced effort, times, and testing costs
  - Will evolve as new interoperability issues arise
  - Intent to publish a multi-year roadmap
EHEALTH EXCHANGE OPERATIONS
Environments

- We maintain four distinct environments
  - Testing – The Developers Integration Lab
  - Validation – Facilitates peer-to-peer testing
  - Staging – Reserved for future use
  - Production – Live operations
Clinical Data

- No clinical data flows through the eHealth Exchange
  - We are not a party to the clinical data exchange
  - We have no CDR or repository
  - We have no MPI
  - We are not a HIPAA Business Associate even under Omnibus rules since we are not even a conduit
- Data flows between eHEX Participants ONLY
- The eHEX offers no services that accept any clinical data
THE FUTURE
Technical Strategic Roadmap

- Via our consensus based process, we’ll likely consider the following for 2014-2015:
  - Replacing the UDDI with Federated (ModSpec) HPD
  - Adding more testing scope, tools, and transparency (ACP, content, etc.)
  - Adding bridges for other healthcare information exchanges
  - Simpler methods of exchange
  - Automated consent / patient preferences
  - More use cases
Support

• Help desk
  • Normal hours 9am to 5pm Eastern time
  • Email / web portal support via a support system
  • Telephone support for production emergencies
  • On call for after hours scheduled maintenance

• Operations
  • Tech Ops mailing list

• Change log
For More Information

• Exchange specifications

• DURSA

• Meaningful Use

• Onboarding

• Testing program
  • [http://healthewayinc.org/index.php/resources/testing-program-resources](http://healthewayinc.org/index.php/resources/testing-program-resources)

• Weekly meetings
Getting Help

• Business issues
  • admin@healthewayinc.org

• Testing
  • testing@healthewayinc.org

• Spec/UDDI/X.509 certificates
  • techsupport@healthewayinc.org
Please Join the Community!

- Weekly Spec Factory technical calls
  - Specs
  - Testing
  - Operations
  - General technical
- Bi-weekly Policy/Technical
- Monthly Communications
- Monthly Coordinating Committee
Q&A

• Is the eHealth Exchange a “network of networks”?
• Does data flow through the eHealth Exchange?