Direct, CONNECT, and RESTful Exchanges: Completing the Interoperability Ecosystem
26 February 2014

Rick Cagle, Lead Information Systems Engineer, The MITRE Corporation
Dr. Suzette Stoutenburg, Principal Engineer, The MITRE Corporation
Conflict of Interest Disclosure

Rick Cagle, MS

Has no real or apparent conflicts of interest to report.

Suzette Stoutenburg, PhD

Has no real or apparent conflicts of interest to report.

Approved for Public Release; Distribution Unlimited. 13-4397

The authors’ affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE’s concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.
Learning Objectives

• Identify the existing protocols, architecture styles, and use cases that make up the ecosystem for health information exchange, and draw analogy to the primary exchanges of information on the internet today

• Illustrate how an important missing piece of the proposed ecosystem can be fully supported by associated technologies and standards

• Characterize the work that needs to be done to integrate a missing component fully into this ecosystem, and propose a strategy for realizing development
Benefits Realized

Value Steps

Health IT creates five kinds of value of benefit to patients, healthcare providers and communities.

TOP STORY
Rural Independent Practice Named 2013 Davies Recipient
White River Family Practice located in White River Junction, Vermont has been named a 2013 Davies recipient! by HIMSS

Read More

- Overall increased data sharing
- Improved care coordination
- Timely remote record access
- Lower barrier-of-entry for small practices

http://www.himss.org/ValueSuite
Outline

• Starting a user story…
• Current information exchange ecosystem – what do we have today?
• Opportunities to enhance the capabilities of the ecosystem
• Pulling it all together
• Use cases and benefits
• Next steps: integrating CONNECT and REST – how do we do it?
• Summary and conclusions
Starting a User Story…

• “Radiological services are not available at the local Air Force Base clinic, so our patient, a Service Member, has been referred to a third-party radiologist in town. The patient has an MRI series performed at the radiology center and we need access to those images in the Military Health System…”

• “Our patient, a Veteran, needs home healthcare but he lives in a rural area far from a VA facility. We need to be able to share patient health information between the VA and Home Healthcare Agency systems…”

How can patient health data be shared with out of network providers?

• As a small, independent provider, we cannot afford an IT staff. How can we participate in the state HIE, offering our patients the benefit of HIE membership? Is there a lightweight, low cost approach that could be administered by the state HIE for us?”

• “As a state just starting to consider an HIE, is there a lightweight low-cost approach to standing up an HIE and integrating with other HIEs in our region?”

Is there a lightweight, low-cost alternative to integrating HIEs?
What We Mean by “Ecosystem”

• Ecosystem – participants and their interactions
• Multiple approaches are employed for health information exchange among parties or resources:
  – Person-to-person
    • **Synchronous Communication**: Face-to-face, instant messaging, and telephone conversations
    • **Asynchronous Communication**: Email, paper, and FAX transmission
  – Machine-to-Machine
    • **Enterprise**: Information volume, speed
    • **Light-weight**: Information that is nimble, browsable
  – Person-to-Machine
    • Limited authorized access to information on a remote system
# eHealth Exchange (Ecosystem)

## NwHIN Building Blocks

<table>
<thead>
<tr>
<th>Vocabulary &amp; Code Sets</th>
<th>SNOMED-CT</th>
<th>LOINC</th>
<th>ICD-10</th>
<th>RxNorm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Structure</td>
<td>Consolidated CDA Care Summaries</td>
<td>Quality Reporting</td>
<td>Lab Results IG Lab Results</td>
<td>HL7 v.2.5.1 Public Health Reporting</td>
</tr>
<tr>
<td>Transport</td>
<td>SMTP-Direct Based Exchange</td>
<td>SOAP-Secure Web Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>X.509 - Digital Certificates</td>
<td>SAML</td>
<td>Consent\ Authorization</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Certificate Authority</td>
<td>DNS, LDAP-Certificate Discovery</td>
<td>UDDI-Certificate &amp; Service Discovery</td>
<td>Provider Directories</td>
</tr>
</tbody>
</table>

NwHIN Components for Transport

**Direct**: Secure Email
- Supports email exchange between people
- Simple text – no real message protocol
- SMTP for transport protocol
- TLS for security protocol

**CONNECT**: Secure services on the Health Information Exchanges
- Open Source
- Supports transactional, stateful exchanges between systems
- SOAP for message protocol
- Transport protocol neutral
  - HTTP is the most popular
  - Also supports SMTP, TCP, JMS, and others
- SAML for security protocol

Exchanges can be grouped into a set of twelve transactions” “Circle of trust” – exchange information with other NwHIN Exchange participants
NwHIN Circle-of-Trust has set the bar for CONNECT

Identifying Ecosystem Data Gaps

• Do We Have Granular and Addressable Data?
  – Breaking healthcare information into small pieces and giving each piece its own URL
  – Enables secure, efficient access
  – Allows data to be combined in many useful ways

• Can We Link Data?
  – When data is addressable, it can be linked on the web
  – Allows clinical contexts to be built by linking data together
  – Humans and software can browse the web of links to get the information they need
Identifying Ecosystem Protocol Gaps

• How Do We Leverage HTTP?
  – The protocol that drives the web offers many features that can be used to make health information exchange more robust, flexible and scalable
  – Clients can indicate whether they prefer their data in XML, JSON or HTML
  – Servers can indicate how long a large image file should be cached
  – Full utilization of HTTP can lead to powerful, scalable system interfaces

• Can We Achieve Internet Scale Access Management?
  – Standards such as OAuth and OpenID have demonstrated distributed, scalable approaches to authentication and authorization on the web
  – Healthcare data exchanges can use these technologies to provide strong, scalable security at low cost
ONC/HITSC recognize Ecosystem Gaps

• Vol. 77, No. 45 of the Federal Register (March 7, 2012) – ONC “Proposed Rules” on REST in the context of existing accepted protocols of SOAP and SMTP:

  “While we would only permit EHR technology to be certified to these two transport standards, we intend to monitor innovation around transport and would consider including additional transport standards, such as a RESTful implementation, in this certification criterion. The inclusion of additional standards in this certification criterion would permit EHR technology to be certified to added transport standard(s) and could ultimately enable EPs, EHs, and CAHs to meet MU using EHR technology certified with the added transport standard(s).”

• At the Health Information Technology Standards Committee (HITSC) meeting 19 June, 2013, the NwHIN Power Team stated:

  – Secured RESTful transport (HTTPS) +
  OpenID Connect authentication +
  OAuth2 authorization +
  FHIR healthcare content

= a safe and appropriate set of standards to use as building blocks for more complicated healthcare applications
REST and the Web

- Links web-documents together for granular information exchange
- Supports multiple devices
- Uses smaller bandwidth – client may specify formats for exchange
- Has low barrier to entry technically and economically
- Composable – supports “mash-ups”
REST Transport: HTTP

- REST was used to design HTTP 1.1 and Uniform Resource Identifiers (URI)
- HTTP specifies the rules by which Web browsers and servers exchange information

REST Security, Authentication, and Authorization

- TLS: Securing HTTP in motion
- OpenID Connect: Authentication via a trusted 3rd party
  - Google, Facebook, …
- OAuth: Authorization via trusted tokens
Transport Layer Security (TLS)

- Transport Layer Security (data in motion)
- Adds encryption and authentication on top of TCP socket communications
- SSL – Secure Sockets Layer
  - Predecessor to TLS
- Both are protocols to allow secure communication between client and server
  - Mitigates “Man-in-the-Middle” – a third party from eavesdropping on the information exchange
- Widely used on the web today
  - Sites secured have URLs prefixed with “https://”
Security: OpenID Connect Authentication
OAuth

• A method for a website or rich-client app (the *requestor*) to request access to a user's private data stored at another website, along with a standard for the *requestor* to send the user to the second website to grant approval
  – Allows a user to share private data between services without sharing credentials
  – Requesting service does not need to know user’s password to act on their behalf
  – A shared secret, or “token”, is used in place of a username/password combination

• A site determines what a token can be used for
  – Can restrict read/write permissions
  – Can be revoked to end access to the service

• **Web Services Specifications (WS-*)** is not leveraged by most REST based APIs, but the REST community is building standards like OAuth on top of REST APIs which provide similar functionality
REST for Healthcare: Putting It All Together

• Documents contain HTTP links to information
• Clients (web browsers) fetch them separately
• Arbitrary granularity with a well-designed API
• Security and privacy to be applied atomically
  – Each request can be to a different security domain
  – Each request can have its own authentication parameters
  – Supports privacy and security practices of existing deployments
• Availability of information can be hidden where appropriate
  – Presence of a URL in one document does not indicate presence of information at that URL
  – Knowledge of a URL does not automatically grant permission to view content at that URL
Integrating CONNECT & Direct: Initiating Gateway

* Communicates with the Gateway via adapters or email client
Integrating CONNECT & Direct: Responding Gateway

CONNECT as a Responding Gateway

Direct Sender (Part of Trust Framework) → S/MIME encrypted (SMTP/RFC-5332+ (MIME or XDM) → CONNECT Integrated Solution (Responding Gateway) → HIE/HISP

CONNECT Adapter/Recipient*

* Communicates with the Gateway via adapters or email client
But what about our users...

- Share health data with out of network providers
- Share diagnostic images in a scalable fashion
- Enable sharing of home health information for patients in rural areas
- Enable small independent providers to participate in benefits of state HIE
- Enable integration of HIEs
Improving the Consultation/Referral Process – Integrating Direct & REST

PCM and Consulting Physician can access and retrieve current, relevant portions of their respective records when they need them.

**Improved Coordination of Care ~ Timely Remote Record Access**
Sharing Diagnostic Images using Direct & REST

Out of network providers can access relevant diagnostic images and associated records and metadata when needed securely over the Web.

**Improved Coordination of Care ~ Timely Remote Record Access**
Automating Home Healthcare in Rural Areas with Direct & REST

VA and third-party home healthcare providers can share patient health history and progress toward goals

Enhanced Continuity of Care ~ Timely Remote Record Access ~ Equal Healthcare for All
Demonstrated Direct & CONNECT; Direct & REST...
What about CONNECT & REST?

- Communicate REST endpoint as a SOAP attribute (SOAP Client)
- Proxy REST request (hide REST implementation entirely)
- Translate SAML assertions to OpenID Connect and/or OAuth tokens
Integrating CONNECT & REST: Small Providers

Small, independent providers in rural areas can quickly set up a lightweight transport mechanism to allow participation in the benefits of a Health Information Exchange.

Equal Healthcare for All ~ Lower barrier-of-entry
Integrating CONNECT & REST: New HIEs

New Health Information Exchanges can be set up in a lightweight fashion and integrated with other Health Information Exchanges.

Equal Healthcare for All ~ Lower barrier-of-entry
Integrating SAML & OpenID Connect

• **SAML Web Single Sign-on (SSO)**
  – Security Assertion Markup Language (SAML) is commonly deployed protocol in enterprises to allow users to login once, and automatically authenticate to other systems.
  – SAML is an XML-based framework for identity assertions & protocols, such as Web SSO, but also SOAP web service security tokens.

• **OpenID Connect**: Similar to SAML Web SSO, however with a particular emphasis on
  – Getting the user’s approval to share their identity
  – Allowing an RP & IDP to interact even if they have never previously communicated
  – Avoidance of two IDPs identifying two different people with the same identifier
  – Delegation of IDP functionality as a service
Integrating SAML & OAuth

• OAuth focuses on exchanging user-supplied credentials for an access token
• A SAML assertion can be used as credentials to be exchanged for an OAuth access token
• The OAuth server can set policy to revoke tokens under specific conditions, or expire the token after a preset amount of time
An Integration Approach: Employ an Enterprise Service Bus...

PCP submits request (client)

ESB

IdAM

REST Endpoint
Tooling Example: Open Source ESB Flow

HTTP

CONNECT SOAP Request

Invoke CONNECT SOAP Service

Set SAML Mapping

REST

Invoke REST Request

HTTP

OAuth2 Provider

Profile Lookup

Profile API

OAuth2 Provider

Profile Lookup

OAuth2 Provider

Retrieve Patient Info

OAuth2 Provider

Set Payload

Bookshelf API
Possible Expansion of the eHealth Exchange (Ecosystem)

NwHIN Building Blocks

- **Vocabulary & Code Sets**
  - SNOMED-CT
  - LOINC
  - ICD-10
  - RxNorm

- **Content Structure**
  - Consolidated CDA Care Summaries
  - Quality Reporting
  - Lab Results IG Lab Results
  - FHIR

- **Transport**
  - HTTPS
  - SMTP-Direct Based Exchange
  - SOAP-Secure Web Services

- **Security**
  - OAuth & OpenID
  - X.509 - Digital Certificates
  - SAML
  - Consent\Authorization

- **Services**
  - Certificate Authority
  - DNS, LDAP-Certificate Discovery
  - UDDI-Certificate & Service Discovery
  - Provider Directories

Source: http://www.healthit.gov/sites/default/files/archive/HIT%20Standards%20Committee/2012/2012-01-25/2012-01-25/HITSC%20Jan%2025%202012_UpdateOnVocab.pptx
Small & Disadvantaged Providers using REST with TLS, OpenID Connect and OAuth can clear the bar for Circle-of-Trust

Propose REST as a Stepping Stone to the Complete Ecosystem

• Prototype a REST-based reference architecture
  – Transport protocol
  – Content protocol
  – Authentication & Authorization protocols

• Pilot integration implementation for CONNECT-to-REST exchange
  – SOAP-to-REST mediation
  – SAML-to-OpenID Connect & SAML-to-OAuth brokering
  – Suggest an Enterprise Service Bus to enable integration
Benefits Realized

• Overall increased data sharing
• Improved care coordination
• Timely remote record access
• Lower barrier-of-entry for small practices

Value Steps

Health IT creates five kinds of value of benefit to patients, healthcare providers and communities.

TOP STORY

Rural Independent Practice Named 2013 Davies Recipient
White River Family Practice located in White River Junction, Vermont has been named a 2013 Davies recipient by HIMSS.

Read More

http://www.himss.org/ValueSuite
Questions?

Thank You!

• Rick Cagle
  Email: rcagle@mitre.org
  Twitter: @rcagle_HIT

• Dr. Suzette Stoutenburg
  Email: suzette@mitre.org