HIT Standards Committee
NwHIN Power Team
Transport Standards for Consumer Exchanges: Preliminary

Dixie Baker, Chair
David McCallie, Co-Chair

June 19, 2013
NwHIN Power Team

- Dixie Baker (Martin-Blanck and Associates)
- Tim Cromwell (VA)
- Floyd Eisenberg
- Ollie Gray (DOD)
- David Groves (HealthBridge)
- David Kates (Navinet)
- David McCallie (Cerner)
- Nancy Orvis (DOD)
- Marc Overhage (Siemens)
- Wes Rishel (Gartner)
- Cris Ross (Mayo)
- Arien Malec (Relay Health)
★ Supported by Avinash Shanbhag and Jamie Parker (ONC)
## Task Assignment

<table>
<thead>
<tr>
<th>Topic</th>
<th>HITSC Workgroups</th>
<th>Activities</th>
<th>Next Steps</th>
</tr>
</thead>
</table>
| Additional standards to support transport of data to and from patients | • NwHIN Power Team  
• Privacy and Security  
• Consumer team | • Presentation of existing transport standards  
• Presentation of RHEx pilot  
• Presentation of ABBI/Blue button  
• Discussion | • May/June presentation to HITSC |

Further guidance from ONC:

- **Goal:** To recommend whether ONC should consider enhancing the current portfolio of transport standards to support consumer exchanges for Stage 3 (and beyond)
- Consider Automated Blue Button (ABBI), HL7 FHIR, RHEx, etc. to identify industry trends and emerging standards
- Present observations and recommendations to HITSC

*(NB: We have interpreted “transport standards” to cover broad capability to exchange data, and not in the narrow sense of an OSI network stack.)*
## 2014 Patient Empowerment Requirements

<table>
<thead>
<tr>
<th>Certification Criteria</th>
<th>Exchange Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable patient to view EHR data</td>
<td>None specified</td>
</tr>
<tr>
<td>Enable patient to download ambulatory summary, in-patient summary, or transitions-of-care/referral summary</td>
<td>None specified</td>
</tr>
<tr>
<td>Transmit to 3rd party ambulatory summary, in-patient summary, or transitions-of-care/referral summary</td>
<td>ONC Applicability Statement for Secure Health Transport (a.k.a. Direct)</td>
</tr>
<tr>
<td>Generate &amp; enable patient to view activity history log</td>
<td>None specified</td>
</tr>
<tr>
<td>Create customized clinical summary (ambulatory only)</td>
<td>None specified</td>
</tr>
</tbody>
</table>
| Securely send messages to and receive messages from patient (ambulatory only) | • Authentication of patient & EHR technology  
• FIPS 140-2, Annex A for encryption and integrity protection |
Initiatives Asked to Review

• Blue Button Plus (BB+) Initiative
  – S&I Framework Initiative formerly known as Automated Blue Button (ABBI)

• HL7 Fast Healthcare Interoperability Resources (FHIR) specification
  – http://www.hl7.org/implement/standards/fhir/

• RESTful Health Exchange (RHEX) Project
  – Federal Health Architecture + S&I Framework sponsored
  – http://wiki.siframework.org/RHEX
## Notable Commonalities and Key Differences

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Purpose/Scope</th>
<th>Secure Transport</th>
<th>Authentication</th>
<th>Authorization</th>
<th>Healthcare Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>FHIR</td>
<td>Healthcare content standard</td>
<td>HTTPS suggested</td>
<td>Undefined</td>
<td>OAuth2 suggested</td>
<td>FHIR</td>
</tr>
<tr>
<td>BB+ Pull</td>
<td>Consumer transmissions</td>
<td>HTTPS</td>
<td>Undefined</td>
<td>OAuth2 + Registry</td>
<td>FHIR</td>
</tr>
<tr>
<td>RHEx</td>
<td>Working prototypes of RESTful health data exchange</td>
<td>HTTPS</td>
<td>OpenID Connect</td>
<td>OAuth2</td>
<td>hData (likely transition to FHIR)</td>
</tr>
</tbody>
</table>
Two Levels of Specifications Emerged

• Lower Level ("building block") Protocols
  – OAuth2
  – OpenID Connect
  – hData
  – FHIR

• Higher Level ("composite") Protocols
  – Blue Button Plus (BB+) “Pull”
  – RESTful Heath Exchange Project (RHEEx)
Two Levels of Specifications Emerged

- **Lower Level** ("building block") Protocols
  - OAuth2
  - OpenID Connect
  - hData
  - FHIR

- **Higher Level** ("composite") Protocols
  - Blue Button Plus (BB+) “Pull”
  - RESTful Health Exchange Project (RHEX)
OAuth2

- IETF Standard for remote service & third-party authorization (RFC6749)

- Flexible framework that supports numerous options, and thus needs to be profiled for specific use-cases (e.g., healthcare)

- Closely tied to HTTP, and thus assumes browser user-agents

- Used here by both RHEx and BB+

- Status: Balloted standard widely used by major Internet companies (Google, Facebook, eBay, etc.)
OpenID Connect

• IETF Pre-standard for remote authentication
  — http://openid.net/connect/
• Communicates user information from authenticating service to another service, such as for single sign-on
• Analogous to the use of SAML in traditional SOAP web services stacks
• Designed to replace “OpenID”, which has seen significant uptake among major Internet companies
• Layered on top of OAuth2, and thus can be co-deployed
• Status: Emerging standard in limited, but growing, use for passing user authentication assertions; used here by RHEx
hData

• Predecessor to FHIR
• RESTful exposure of healthcare resources
• Status:
  – HL7 DSTU
  – Likely to be superseded by FHIR
FHIR - Fast Healthcare Interoperability Resources

- New HL7 standard in development – strong support by HL7 leadership & rapidly emerging industry interest
- Focuses on “resources” used for exchange; each resource includes:
  - Defined, simple, structured data (mapped to RIM, but need not be computable)
  - Extensions (formally defined & published)
  - Narrative
- Emphasis on simplicity, implementability, and human readability
  - Single syntax for documents, messages, queries, services, etc.
  - Specification includes RESTful transport, but other transports may be used
- No licensing required
FHIR Status

- Base specification is complete and stable
- Currently defining resources; plans for 25 CCDA resources and 6 IHE and DICOM resources
- Targeting ~150 resource definitions, then will shift to profiles
- Anticipated initial use
  - Web-centric, social-media apps
  - HL7 V2 content exposed with FHIR
  - CDA Release 3 likely to be displaced by FHIR
- Used by BB+
- CommonWell using to build record and encounter record locator service – FHIR chosen for simplicity and implementability
Two Levels of Specifications Emerged

• Lower Level ("building block") Protocols
  – OAuth2
  – OpenID Connect
  – hData
  – FHIR

• Higher Level ("composite") Protocols
  – Blue Button Plus (BB+) “Pull”
  – RESTful Health Exchange Project (RHEX)
Blue Button Plus (BB+)

- For structured and secure transmission of personal health data on behalf of an individual consumer
  - BB+ “Push” uses Direct email transport (MU 2 VDT) – implementation guide available at bluebuttonplus.org
  - BB+ current efforts focus on “Pull”

- BB+ “Pull” is an application programming interface (API) that enables an application to “Pull” EHR data on behalf of the consumer
  - Application uses OAuth2 to register with a provider
    - App name, location, permissions it might ask patients for, and how to display an authorization screen to patients
    - OAuth2 Dynamic Client Registration allows “open” registration (no pre-negotiated vetting)
    - “Trusted” registration requires use of BB+ registry (vetted)
  - FHIR for content search and retrieval
  - HTTPS (HTTP + TLS) secure RESTful transport
(1) Consumer uses MyHealthMonitor app to record diet history and blood pressure readings

(2) MHM service requests access to EHR

(3) EHR service asks consumer for authorization to access EHR

(4) MyHealthMonitor pulls cholesterol data from EHR and plots with user-provided data
Authorize a new application

The following application is asking for authorization to access your account:
MyHealthMonitor 2.0

Authorize this application

Request for permission

MyHealthMonitor is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.

Send me email
famously may email me directly at erzmazor@hotmail.com · Change

Post to my Wall
famously may post status messages, notes, photos and videos to my Wall

Access my data any time
famously may access my data when I'm not using the application

Access my Profile information
Facebook status

Report app

Logged in as Joe Schmo (Not you?)

Allow Leave app
BB+ “Pull” Status

- Draft specification available online at https://github.com/blue-button/blue-button-plus-pull
- Responds to well-defined Internet use-case where consumers control who to expose their data to
  - Especially appealing for mHealth “apps”
- Ongoing debate about the need to “certify” or otherwise control which apps can use the service
- EHR vendors currently underrepresented – very few have committed to implementing
- Server-side tools being developed
RESTful Health Exchange (RHEX)

- Applies open-source, Web technologies to demonstrate uses of RESTful, secure, standards-based approaches to health information movement
  - Responsive to NwHIN Power Team’s September 2011 recommendation for a RESTful transport alternative to (SMTP-based) Direct and (SOAP-based) Exchange

- Layered over core Internet standards
  - HTTPS for secure transport
  - OpenID Connect for authentication
  - OAuth2 for authorization
  - hData for health content
    - Was designed before emergence of FHIR, but could switch to FHIR for resource definitions
RHEx Status

- Completed two pilots
  - TATRC for exchanging data between two people
  - Maine HealthInfoNet for transporting volumes of data to the state repository
- New pilots under way at TATRC
  - Sharing large images between AHLTA and third party provider systems
  - Providing patients access to their medical history in AHLTA using a mobile platform (hReader)
  - Securely migrating health data from AHLTA to VistA
- Maine implementing RHEx statewide to support small, independent providers and FQHCs in underserved areas
- Planned pilot with VHA
Readiness Evaluation

Maturity

Low

 Moderate

High

Adoptability

Low

Moderate

High

HTTPS

OAuth2

RHEX

FHIR

OpenID Connect

Blue Button+

“Pull”

Emerging Standards

National Standards

Pilots

Red Type = building blocks
Overarching Conclusion

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
• Recommend that ONC support and encourage the development and piloting of BB+, FHIR, and RHEX.
  
• BB+ “Pull” focuses on a specific, identified need to enable a consumer to access their own health information or to authorize a third-party application to do so:
  – Emerging standard whose development should be supported and early pilots encouraged
  – Encourage EHR vendor participation
  – No known alternatives that address this need

• FHIR is highly likely to become a key next-generation content standard for healthcare:
  – Need for FHIR CCDA (being developed)
  – Appropriate as content standard for both BB+ and RHEX
Recommendations (2 of 2)

- RHEx is a useful demonstration of how HTTPS, OpenID Connect, OAuth2, and FHIR can be used together to support robust, but simple healthcare exchange
  - Commendable response to NwHIN Power Team’s recommendation for a RESTful complement to Direct and Exchange
  - Responds to industry need for a simple means of transmitting large healthcare data objects (e.g., images) that cannot be accommodated by Direct
  - Encourage replacement of hData with FHIR
  - Given the flexibility of the RHEx architecture and the optionality available from OAuth2, profiles based the RHEx initiative may be more appropriate candidates as national standards than the full body of work
Next Steps

• Present preliminary results to Privacy and Security Workgroup and Consumer Workgroup

• Consider questions such as:
  – BB+ Pull considers “open registration” (i.e., non-vetted) appropriate only for new and experimental apps, and suggests displaying a warning with these apps. For a higher level of assurance, apps can undergo a “trusted registration.” What level of assurance is reasonable and appropriate for BB+ Pull apps?
  – How might OAuth2 apps be authenticated? Is TLS server authentication sufficient?
  – Any other security concerns around the use of OAuth2 for enabling consumers to “pull” their data from certified EHRs?
  – ... Other questions suggested by HITSC…