Health IT Standards Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

NwHIN Power Team

Final Recommendations for RESTful Exchange Standards

August 22, 2013

NwHIN Power Team Membership

- Dixie Baker, Chair (Martin-Blanck and Associates)
- David McCallie, Co-Chair (Cerner)
- Jitin Asnaani (AthenaHealth)
- Keith Boone (GE Healthcare)
- Kevin Brady (NIST)
- Keith Figlioli (Premier)
- Ollie Gray (DOD)
- Josh Mandel (Harvard Medical School)
- Wes Rishel (Gartner)
- Cris Ross (Mayo)
- Arien Malec (Relay Health)

★ ONC support: Avinash Shanbhag, Jamie Parker, and Debbie Bucci

Agenda

- Review and update of assigned task
- Review of preliminary recommendations presented to HITSC in June
- Results of coordination with Privacy and Security Workgroup and Consumer Technology Workgroup
- Final recommendations

Acronyms defined on slide 22

Initial Task Assignment

- Recommend whether ONC should consider enhancing the current portfolio of transport standards to support consumer exchanges for Stage 3 meaningful-use (and beyond)
  - Consider Blue Button Plus (BB+), HL7 Fast Healthcare Interoperability Resources (FHIR), and RESTful Health Exchange (RHEx) to identify industry trends and emerging standards
  - NwHIN Power Team lead, with inputs from Privacy and Security Workgroup and Consumer Technology Workgroup

Task Update

- Preliminary recommendations presented to HITSC at June meeting
  - Expanded scope of applicability beyond consumer-provider exchanges to include any health information exchange that can be supported using a RESTful service

Initiatives Reviewed (1 of 2)

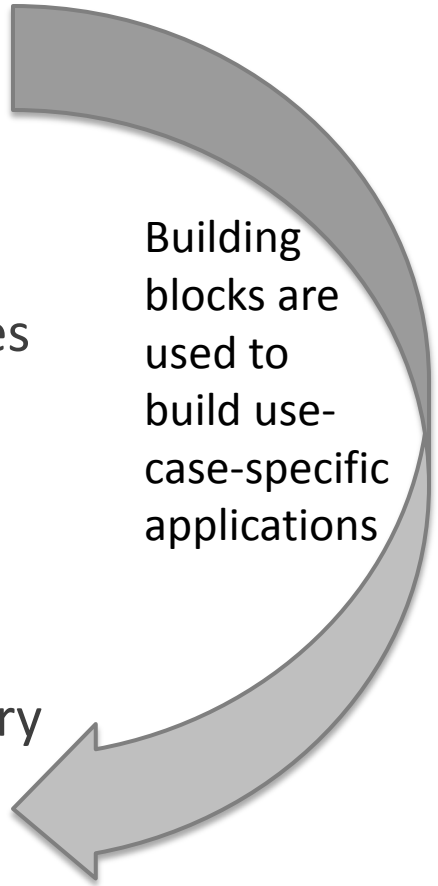
- Blue Button Plus (BB+)
  - Standards and Interoperability (S&I) Framework Initiative formerly known as Automated Blue Button (ABBI) for exchanges between providers and consumers or consumer-named third parties
  - BB+ "Push" uses the Direct Protocol
  - BB+ "Pull" specifies a RESTful exchange that uses OAuth2 to authorize an application to query and pull data from an EHR, and FHIR for query and retrieval of selected EHR resources
  - BB+ "Pull" includes a Registry Service that distinguishes two categories:
    - "Trusted registration" – app is registered with the Service based on its ability to protect the OAuth2 token and the client secret returned by the data provider
    - "Open registration" – app is not registered with the Registry Service

Initiatives Reviewed (2 of 2)

- HL7 Fast Healthcare Interoperability Resources (FHIR) specification
  - Healthcare content standard used to support BB+ "Pull" query and retrieval
- RESTful Health Exchange (RHEx) Project
  - Federal Health Architecture + S&I Framework sponsored initiative developing working prototypes demonstrating the use of RESTful services to support health information exchanges
  - Uses OAuth2 for application authorization, OpenID Connect for sharing identity attributes, and hData for content (may migrate to FHIR)

Two Levels of Specifications Emerged

- Lower Level Building Blocks
  - HTTPS – secure web-based transport
  - OAuth2 – authorization of third-party applications
  - OpenID Connect – sharing of identities and attributes
  - FHIR – simplified, structured content for RESTful exchange
- Higher Level Applications
  - BB+"Pull" – consumer or authorized third-party query and retrieval of health data
  - RHEx – demonstration prototypes of RESTful health exchanges



OAuth2

- IETF Standard for remote service & third-party authorization (RFC 6749)
- Flexible framework that supports numerous options, and thus needs to be profiled for specific use cases (e.g., healthcare provider-consumer exchanges)
- Closely tied to HTTP, and thus assumes browser user-agents
- Used by both RHEx and BB+ Pull
- Status: Balloted standard widely used by major Internet companies (Google, Facebook, eBay, etc.)

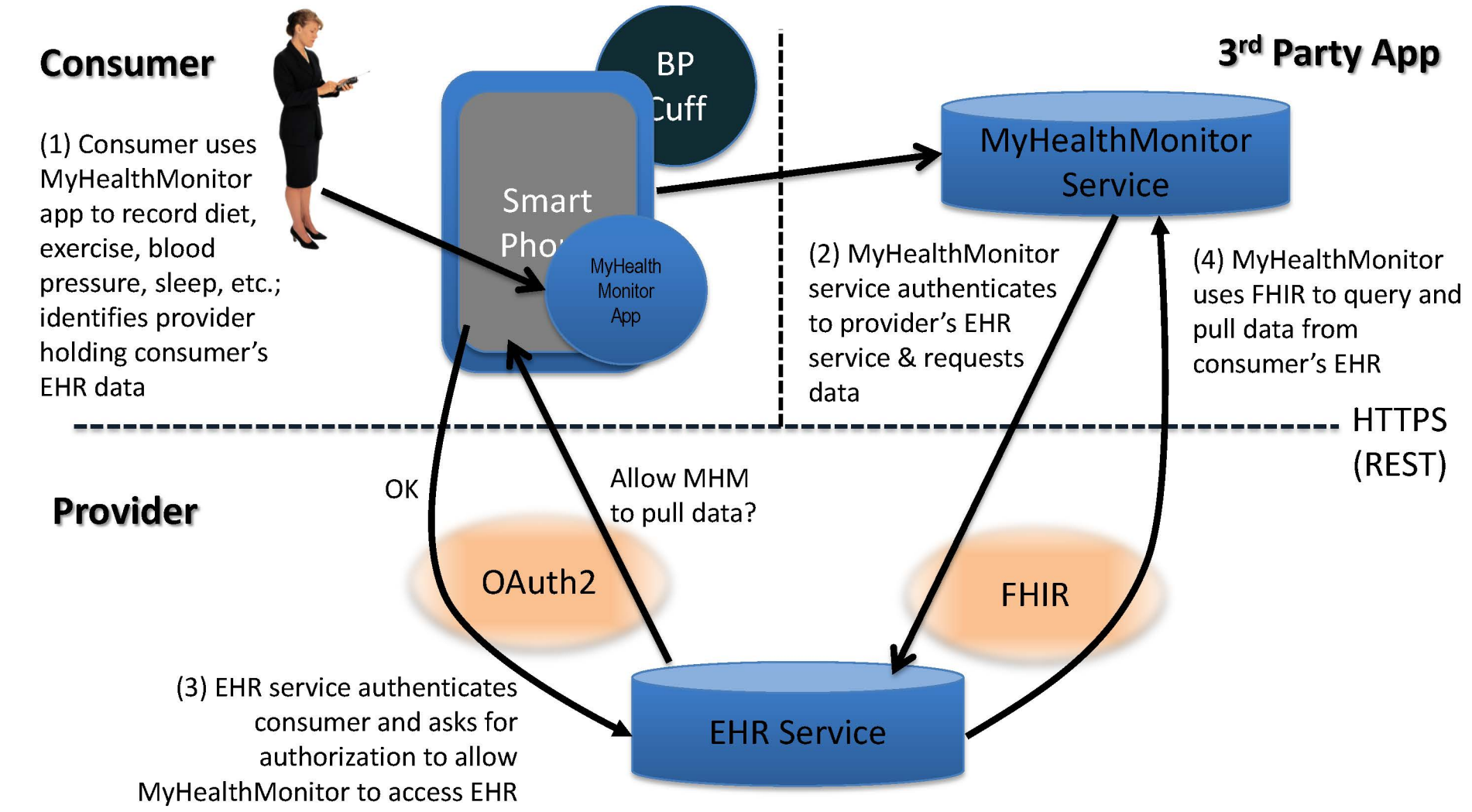
OpenID Connect

- OpenID Foundation (OIDF) Pre-standard for remote authentication
- Communicates authenticated user information from one service to another, such as for single sign-on
- Similar to how traditional SOAP web services pass security assertions using SAML
- Designed to replace “OpenID 2.0”, 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 by RHEx Project

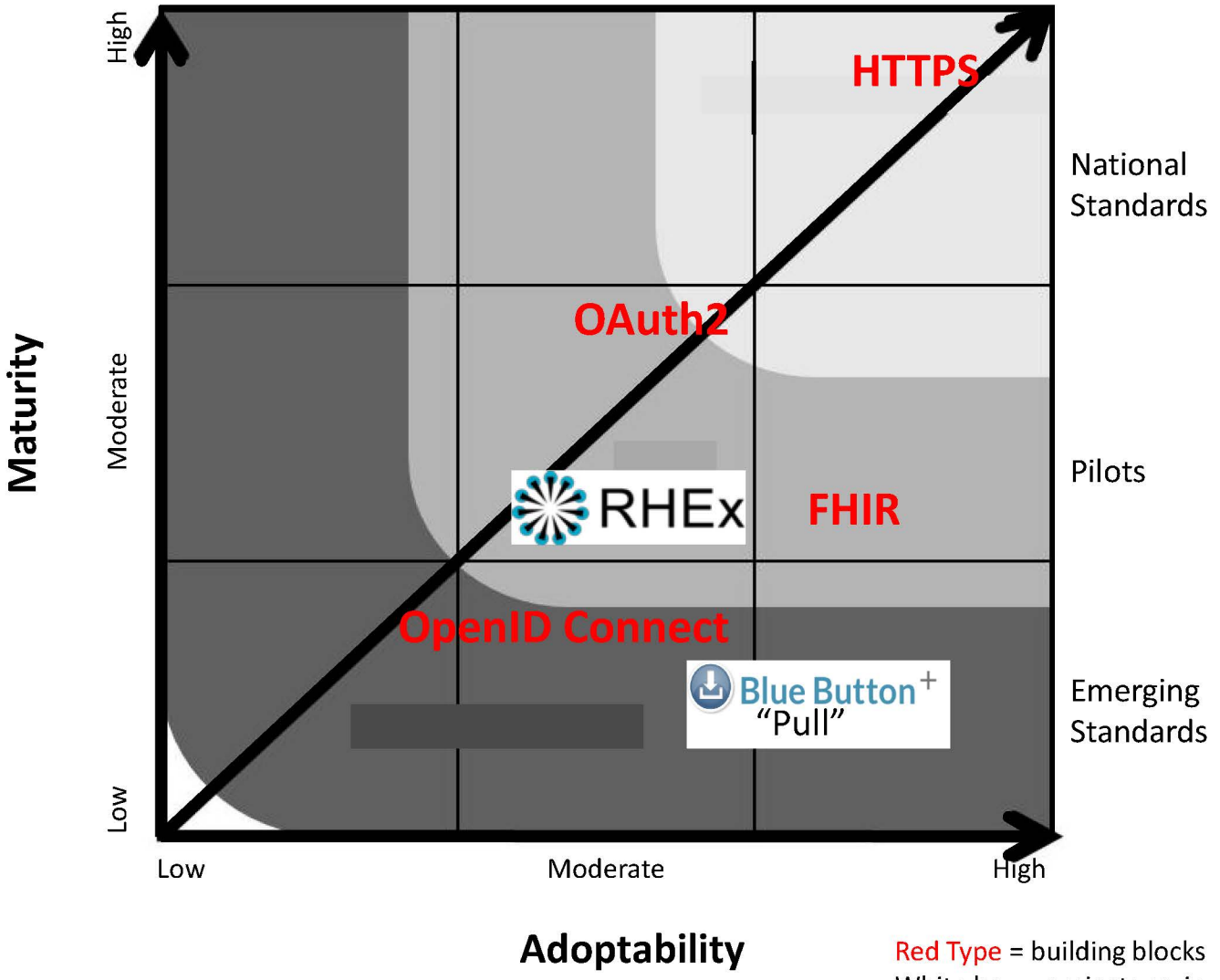
FHIR

- 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 (may be 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
- Licensed free of charge
- Status: Base specification published as DSTU on August 13, 2013, now defining resources; used by BB+ for query and retrieval

BB+ "Pull" Example



Initial Readiness Assessment



Red Type = building blocks
White box = projects reviewed

Initial 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

Since we last talked about this subject…

- NwHIN Power Team has presented these concepts, and its conclusions and recommendations to the Privacy and Security Workgroup and the Consumer Technology Workgroup

Privacy and Security Workgroup Recommendation: IHE Internet User Authorization (IUA) Profile

- Leverages NwHIN-recommended standards to address use cases in which a resource service needs to make additional access-control decisions beyond those made by the OAuth2 system
  - e.g., data segmentation for privacy, emergency break-the-glass override, role-based enforcement, purpose-of-use decisions
  - Uses JSON Web Tokens (JWT) and optionally SAML tokens, with well-defined user-context attributes
- Status: Draft for Public Comment published in June 2013

Consumer Technology Workgroup Observation: OAuth2 Dependency on Portal Identity Management

- BB+ "Pull" redirects patient authentication to provider's portal authentication service – so OAuth2 authorization of a requesting app depends upon the strength of the portal's identity management policies and technology
  - Providers need to make sure that the level of assurance provided by their portal identity management approach is sufficiently robust

Final, Coordinated Conclusions and Recommendations

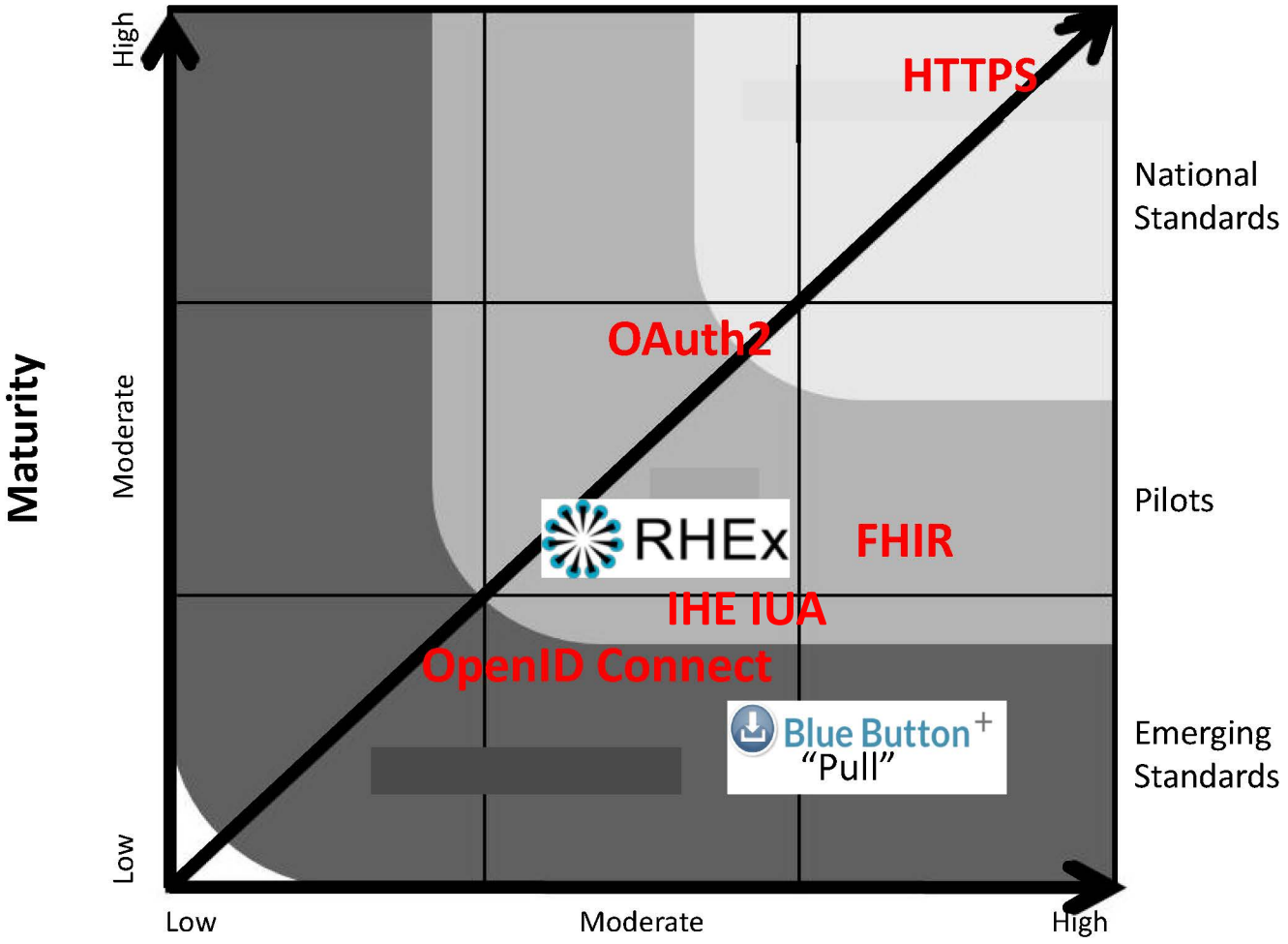
Coordinated Conclusions and Recommendations (1 of 2)

- Secured RESTful transport (HTTPS), OpenID Connect, OAuth2, and FHIR can be used together to build safe healthcare applications: **we recommend ONC support the development and piloting of these standards as candidate building blocks for healthcare applications**
  - BB+ "Pull" holds potential as a national implementation specification for future meaningful-use Editions, but further development and piloting are needed
  - RHEx Project is a useful demonstration of how these standards can be used together to support robust, but simple healthcare exchange

Coordinated Conclusions and Recommendations (2 of 2)

- **IHE IUA profile** appropriately constrains and structures OAuth2 tokens to support sharing of user-context assertions such as "purpose of use" and **is recommended for use in environments that require coexistence with existing profiles based on IHE constrained user-context assertions**
- BB+ concept of implementing a Registry Service to recognize two types of registration – "trusted" and "open" – assumes policy that has not been established and implies a level of app "trustworthiness" that may not be justified: **we recommend ONC ask the Privacy and Security Tiger Team to address the questions of whether "trusted registration" with a Registry Service should be required for BB+ "Pull" applications, and if so, what should "trusted" entail**

FINAL Readiness Assessment



Red Type = building blocks
White box = projects reviewed

FINAL Overarching Conclusion

Secured RESTful transport (***HTTPS***)

+

OpenID Connect authentication

+

OAuth2 authorization and, as applicable, the ***IHE Internet User Authorization (IUA) Profile***

+

FHIR healthcare content

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

Acronyms

Acronym	Expansion	Acronym	Expansion
ABBI	Automated Blue Button	JWT	Javascript Object Notation (JSON) Web Token
BB+	Blue Button Plus (formerly called Automated Blue Button or ABBI)	NwHIN	Nationwide Health Information Network
DSTU	Draft Standard for Trial Use	OIDF	OpenID Foundation
EHR	Electronic Health Record	REST	REpresentation State Transfer
FHIR	Fast Healthcare Interoperability Resources	RFC	Request for Comment
IHE	Integrating the Healthcare Enterprise	RHEx	RESTful Health Exchange
HL7	Health Level Seven	RIM	Reference Information Model
HTTPS	Hypertext Transfer Protocol Secure	SAML	Security Assertions Markup Language
IETF	Internet Engineering Task Force	S&I	Standards and Interoperability
IUA	Internet User Authorization	SOAP	Simple Object Access Protocol