ONC/VA Privacy on FHIR Pilot

Providing patients with Online Digital Health Services

19 Jan 2014
It was a Very Good Year...

• Jan 2014 – HL7’s 4 Security and Privacy Standards
• Today-Health Relationship Trust (HEART)
  – In their (HITSC) recommendation, they concluded that OpenID Foundation’s OpenID Connect, Internet Engineering Task Force’s OAuth 2.0, and HL7’s FHIR comprise a reasonable and appropriate set of standards to use as building blocks for more complicated healthcare applications and strongly encouraged ONC to support the development and piloting of these standards. Subsequently, it has often been noted that given the flexible optionality available in these standards, there would need to be constrained profiled for specific use cases for use within Health IT.
  – In response to the above recommendation, ONC, in collaboration with Department of Veterans Affairs (VA) and other stakeholders, has initiated the first pilot/demonstration project that uses the above-mentioned standards to support patient mediated exchange and patient consent. The effort is called Privacy on FHIR (PoF) and is the underlying effort initially driving this workgroup’s efforts.
We are on the cusp of a sea change in interoperability, population management, and clinical decision support. CCD led to CCDA which leads to FHIR for content summary exchange. The Direct protocol will evolve to a RESTful interface using OAuth/OpenID for trust fabric creation.

However, we're not going to make the move to FHIR and REST unless pilots (followed by agile development of implementation guides) are funded to enable incremental progress. FHIR is too new and REST has too many industry skeptics. The pilots will create a tipping point which mitigates risk and enables progress. Dr. John Halamka
ONC/VA Privacy on FHIR Pilot Drivers:  
*Embrace FHIR, JSON, REST and OAuth*

- Recommendations in the ONC 10 year plan “Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure” and on the MU 2017 Roadmap

- PCAST: “Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward”

- AHRQ Jason Report: “A Robust Health Data Infrastructure“
ONC/VA Privacy on FHIR Pilot: Summary of Pilot Project Plan

1. **What is it?** On-Demand bi-directional exchange of Health Information with Selected Apps...What, When and How You Want it

2. **Why do it?** Test technical feasibility of using FHIR and associated privacy and security protocols to provide Patients with meaningful access, management and use of their own information.

3. **Deliverables?**
   - Incremental pilot milestone demonstrations,
   - ONC sponsored HIMSS 2015 Interoperability Booths,
   - Open Source Reference Model for implementers,
   - RSA 2015.

1. **Who will do it?** Collaborative of Stakeholders dedicated to demonstrating the benefits of HIT cloud capabilities for consumers and providers including:

   ONC, VA, DoD, SAMHSA, Vendors, Patient Privacy Rights, HL7 Standards Development Organization, MITRE, MIT
ONC/VA Privacy on FHIR Pilot [PoF]:
What is HL7 FHIR?
Fast Healthcare Interoperability Resources

• FHIR defines a set of "Resources" that represent granular clinical concepts managed in isolation, or aggregated into complex documents.

• FHIR is designed for the web:
  — Simple XML or JSON structures,
  — http-based RESTful protocol,
  — Each resource has a predictable URL.

• FHIR Security and Privacy follows HL7 Security Labeling, Data Segmentation, and Consent Directive standards

• FHIR is under development and has not yet reached full standard status

http://www.hl7.org/implement/standards/fhir/summary.html
ONC/VA Privacy on FHIR Pilot (PoF): Applying User Managed Access (UMA)-OAuth 2.0 Profile

Patient controls Who gets What

User Managed Access (UMA)

PoF Architecture leverages cloud Privacy and Security Services that Patients use daily as Online Consumers
My Privacy on FHIR
Share Health Information Among Your Providers... Organizations, Apps, and Individuals...
My Health Information Exchange on FHIR
Share Health Information Among Your Providers... Organizations, Apps, and Individuals...

Provider  

Resource Server  
(FHIR Resources)

End-user

Provider

Resource Server  
(FHIR Resources)

Authorization Server

Policy Adjudicator

Consent Directive Management Service

ACS

1. Accept Consent Directive
2. Register Resources and Scope
3. Set Resource Authorizations
4. Request for Data
5. Redirect to Authorization Server
6. Get “Requesting Party Token (RPT)”
7. Request for Data w/RPT
8. Receive Labelled Data

ACS = Access Control Service
EHR = Electronic Health Record
HIE = Health Information Exchange
Org = Organization

IOT
UMA Protocol

• Phase 1 of the UMA core protocol involves the resource owner introducing the resource server and authorization server so they can work together.

• Phases 2 and 3 together involve the requesting party, using a client, making an access attempt, being tested for suitability by the authorization server to receive permission, and ultimately succeeding or failing in the attempt by presenting a token with permissions associated with it.
My Apps on FHIR

Share Health Information with Your Selected Apps...
What, When and How You Want it...All 24/7

Use your Information for Healthy Living, Wellness Management and Talking to Your Doctor Online

- My Personal Health Record
- My Travel App (Immunizations)
- My Diet Planner App (Diabetic)

Smart Phone ----- Tablet ----- Personal Computer
Use your Information for Healthy Living, Wellness Management and Talking to Your Doctor Online:

- **My Travel App (Immunizations)**
- **My Diet Planner App (Diabetic)**

**MY Apps on FHIR**

Share Health Information with Your Selected Apps...

*What, When and How You Want it...*

all 24/7, wherever there is Internet access.

---

**Smart Phone ----- Tablet ----- Personal Computer**

1. Create Consent Directive
2. Submit Consent Directive
3. Create Application Authorizations
4. Create/Send Authorization Token
5. Present Authorization Token
6. Enforce Consent Directive Obligations
7. Send/Receive Data
ONC/VA Privacy on FHIR Pilot (PoF): MY Apps on FHIR Enforcement

Resource Server

My “Apps on FHIR” Policy

Restrictions enforced by Resource Server Privacy Protective Service
(e.g., Redact, Mask, Anonymize, Pseudonymize)

My “Apps on FHIR” Policy

- RESTRICTED

Don’t Share

Patient creates their own personal sensitivities list (e.g., HIV, ETH, Other, …)

Privacy Protected
Clinical Resources
My Consent Directives on FHIR

Privacy...Share Only What You Want. Your Sensitive Healthcare Information Stays Secure.

**My Consent Directive Policy**

- **Treatment**
  - **Normal**
    - Non-sensitive healthcare information shared for treatment or other purposes
  - **Restricted**
    - Fine-grained restrictions on FHIR Resources
    - “Do Not Share” Organizations
    - Information restricted by clinical specialty
    - Certain named individuals

- **Share**
- **Don’t Share**

**My “Apps on FHIR” Policy**

- **Restrict**ed
  - Fine-grained restrictions on FHIR Resources

**Authorizations**

- **Normal**
  - Permissions that allow or disallow access to FHIR Resources provided by Resource Servers
- **Restricted**
  - Clearances for specified sensitive information

**Provider**

- Consent

**Patient**

- Consent
My Standards on FHIR

- HL7 Fast Healthcare Interoperability Resource (Draft)
- HL7 Patient Friendly Consent Directive (Draft)
- HL7 Healthcare Privacy and Security Classification System
- HL7 Privacy and Security Services (PASS) Security Labeling Service
- HL7 Provenance
- OpenID Foundation OpenID Connect
- IETF RFC 6749 Oauth 2
- Kantara User Managed Access (UMA)
- OASIS XACML