Emerging Standards in Healthcare

Eve Maler and Debbie Bucci, HEART WG co-chairs

eve.maler@forgerock.com| @xmlgrrl

debbucci@gmail.com

27 June 2018

http://openid.net/wg/heart/

It’s an exciting but challenging time for healthcare intersecting with digital information

- Health data is some of the most personal and private consumer data
- It is increasingly digital, either at the source or when transcribed
- The Internet of medical/healthy things and genomic data are having an impact
- See recent moves by Apple, bodies such as Health Level Seven and the CARIN Alliance, and government efforts such as MyHealthEData/Promoting Interoperability

carin
Creating Access to Real-time Information Now through Consumer-Directed Exchange

HL7 INTERNATIONAL

What is HEART (Health Relationship Trust)?

- Individuals want to be in control of gathering and sharing health data
  - Including giving permission for access – and revoking permission
  - Especially if they have complex conditions or have moved frequently
- Clinicians, insurers, and researchers seek data access to diagnose, plan care, and pay for care, and need to know it's authorized for use
- The work of the HEART Work Group puts the individual back at the center of the health data-sharing conversation

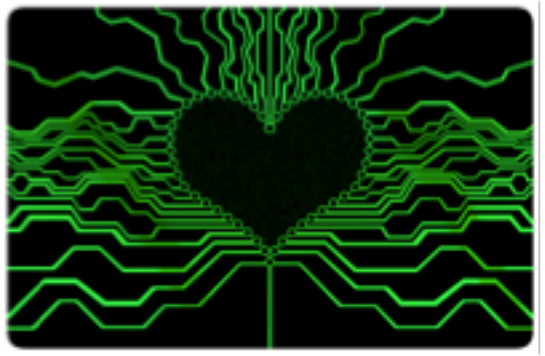
What does HEART do?

To achieve RESTful, patient-centric, privacy-sensitive health data sharing…

- It profiles OAuth, OpenID Connect, UMA, and the HL7 FHIR (Fast Healthcare Interoperability Resources) API
- It has aligned with the SMART on FHIR OAuth standard developed for use with EHR systems, health portals, and Health Information Exchanges

Who is involved?

- Health/health IT subject matter experts
  - Doctors, government health agency reps…
- Technology experts
  - Implementers, health startups, spec authors…
- Leadership team:
  - Co-chair Debbie Bucci (US Health and Human Services Office of the National Coordinator)
  - Co-chair Eve Maler (ForgeRock)
  - Spec editor Justin Richer (Bespoke Engineering)



Current state of the deliverables

(see https://openid.bitbucket.io/HEART/)

- Mechanical = security profile
- Semantic = API-specific profile
- Considering whether to deprecate the UMA1 profiles

Profile	Implementer's Draft	Working Group Drafts	Spec Type
Profile of **OAuth 2.0**	OIDF-approved Implementer's Draft 2 *(approved May 31 2017)*	Most Recent Working Group Draft *(updated Mon Feb 19 2018)*	Mechanical
Profile of **OpenID Connect 1.0**	OIDF-approved Implementer's Draft 2 *(approved May 31 2017)*	Most Recent Working Group Draft *(updated Mon Apr 10 2017)*	Mechanical
Profile of **UMA 1.0**	OIDF-approved Implementer's Draft 2 *(approved May 31 2017)*	Most Recent Working Group Draft *(updated Mon Apr 10 2017)*	Mechanical
Profile of **FHIR resources on OAuth 2.0**	OIDF-approved Implementer's Draft 1 *(approved May 31 2017)*	Most Recent Working Group Draft *(updated Thu Mar 01 2018)*	Semantic
Profile of **FHIR resources on UMA 1.0**	OIDF-approved Implementer's Draft 1 *(approved May 31 2017)*	Most Recent Working Group Draft *(updated Thu May 25 2017)*	Semantic
Profile of **UMA 2.0**	N/A	Most Recent Working Group Draft *(updated Thu Mar 01 2018)*	Mechanical
Profile of **FHIR resources on UMA 2.0**	N/A	Most Recent Working Group Draft *(updated Mon Feb 26 2018)*	Semantic

New white paper and use case work
(unpublished as yet)

- Focused on new urgency in the quest for patient-mediated health data exchange solutions, e.g., in the US:
  - MyHealthEData
  - Promoting Interoperability (was “Meaningful Use”)
- Enabling Patient-Mediated Health Data Exchange
  - With assistance from Jan Oldenburg of Participatory Healthcare
- Use cases:
  - Alice shares clinical records with her spouse
  - Alice electronically shares data from her PHR (personal health record)
  - Sharing smart pulse oximeter data in a consented way with third parties

HEART scope mechanisms

Confidentiality and sensitivity

- HL7 defines many codes for sensitive data types
  - E.g., `sens/ETH` for substance abuse
- Similarly, it defines some codes for confidentiality levels
- HEART allows a resource server to define these as scopes
- If such a scope ***is not associated*** with an access token, the resource server ***SHOULD filter out*** the relevant data before delivering it, if at all possible

Break-the-glass

- HL7 defines a code `btg` for situations where the resource owner is unavailable
- HEART allows a resource server to define this as a scope
- If such a scope ***is associated*** with an access token, the RS ***MUST log access*** made on this basis in an auditable format available to the resource owner

Note: *All policy-setting UX options are "outside the scope of scope mechanisms" (e.g., policy defaulting).*

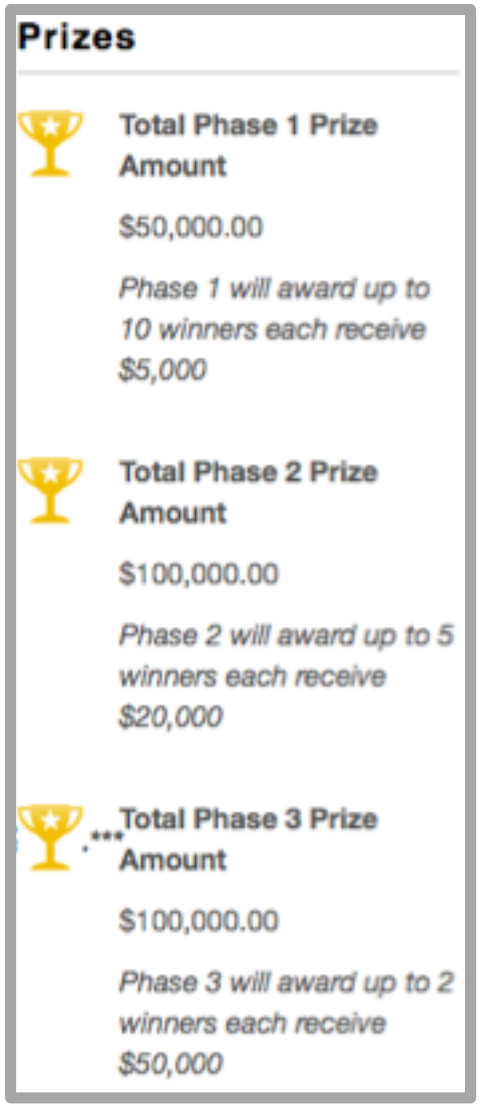
A potential third scope mechanism: de-identification

- We are currently discussing the notion of a similar scope mechanism for enabling a patient to instruct the resource server to deliver resources in **de-identified** form
- Could be used to release data for clinical research or other purposes

The Move Health Data Forward challenges

https://www.challenge.gov/challenge/move-health-data-forward-challenge/

- Starting mid-2016, HHS ONC (US Health and Human Services Office of the National Coordinator) challenged industry to create API solutions to help individuals authorize the movement of their health data
- Three phases later, several winners have won awards, including for some solutions based on the HEART profiles



OpenMedReady is a new framework making use of HEART

- Provenance
- Identity
- Consent
- Proof

1

Certified device identity

2

Strongly authenticated patient identity

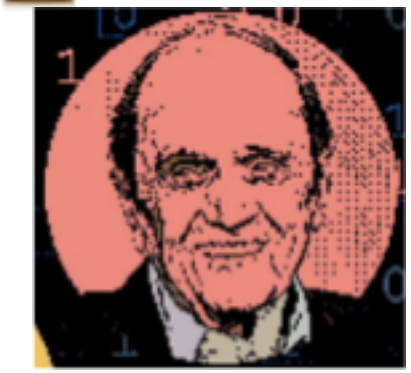
3

Patient/device association

4

Consented device data sharing with clinicians and others

5



Strongly authenticated third-party identity

Cryptographic auditability

openmedready.org

Standards

Thank you!
Questions?
Join us!

Eve Maler and Debbie Bucci, HEART WG co-chairs

eve.maler@forgerock.com| @xmlgrrl

debbucci@gmail.com

27 June 2018

http://openid.net/wg/heart/