Health Relationship Trust (HEART) Working Group Charter (DRAFT v13)

**1) Working group name**: Health Relationship Trust (HEART) Working Group

**2) Purpose**:

The purpose of this Working Group is to harmonize and develop a set of privacy and security specifications that enable an individual to control the authorization of access to RESTful health-related data sharing APIs, and to facilitate the development of interoperable implementations of these specifications by others.

**3) Scope**:

* Develop a set of internationally applicable use cases and requirements that are specific enough to guide the specification and profiling design work, considering interrelations with risk mitigation and user experience efforts.
* Define a layered set of profiles for OAuth 2.0, OpenID Connect, and User-Managed Access (UMA), where each successively builds on and references the previous ones.
* Define additional profile specifications that define OAuth 2.0 scopes and UMA resource set types, scopes, and claims-gathering flows as required for interoperability.
* Develop and maintain liaison relationships as appropriate with external standards organizations and other bodies.
* Foster the creation of multiple interoperable reference implementations, particularly in open source.
* Promote progressive harmonization with existing specifications and protocols as appropriate.
* Develop educational materials in support of the overall Working Group effort.

The following efforts are out of scope:

* Development of a generalized resource discovery mechanism.
* Development of related trust frameworks.

All items not expressly mentioned as in scope or out of scope are to be determined by the Working Group.

**4) Proposed specifications**:

The following layered specifications will be produced, with precise specification names and boundaries subject to change:

* HEART profile for OAuth 2.0.
* HEART profile for OpenID Connect (referencing the previous specification as appropriate).
* HEART profile for Fast Healthcare Interoperability Resources (FHIR) OAuth 2.0 scopes.
* HEART profile for User-Managed Access (UMA) (referencing the previous specifications as appropriate).
* HEART profile for FHIR UMA resource set types, scopes, and claims-gathering flows (referencing the previous specifications as appropriate).

It is anticipated that the following nonnormative materials will also be produced, at a minimum:

* HEART Use Cases and Requirements
* HEART Overview
* HEART Implementation Guide

**5) Anticipated audience or users:**

The anticipated audience for the documents produced by this Working Group includes developers, deployers, and designers of online services and network devices that act on behalf of individuals in the health space. The group also anticipates gathering input from individual users of online services in order to respond to their needs and preferences.

**6) Language**:

Work will be conducted in English.

**7) Method of work:**

E-mail discussions on the working group mailing list, working group conference calls, and opportunistic face-to-face meetings.

**8) Basis for determining when the work is completed:**

The work will be considered complete once it is apparent that maximal consensus on the draft has been achieved, consistent with the purpose and scope and interoperability with at least two independently developed implementations of the specifications and profiles has been demonstrated.

Background Information

The Working Group intends to expedite the process of gathering representatives from the many different health-related technical communities worldwide (private-sector, government, and NGO) – working in areas such as patient authentication, authorization, and consent – to collaborate on normative specifications and profiles that meet their shared goals in this area.

Its impetus was an effort by the US Health IT Standards Committee (HITSC), which is charged with making [recommendations](http://www.healthit.gov/facas/health-it-standards-committee/health-it-standards-committee-recommendations-national-coordinator) to the National Coordinator for Health IT (ONC) on standards, implementation specifications, and certification criteria for the electronic exchange and use of health information. In August 2013, the HITSC Nationwide Health Information Network (NwHIN) was asked whether ONC should consider enhancing the current portfolio of transport standards to support the use of RESTful services in health information exchanges. As inputs into this task, the ONC asked its “Power Team” to review the Blue Button Plus (BB+) initiative (<http://wiki.siframework.org/BlueButton+Plus+Initiative>), the RESTful Health Exchange (RHEx) project (<http://wiki.siframework.org/RHEx>), and the Health Level Seven (HL7) work (<http://www.hl7.org/implement/standards/fhir/>) to develop a new resource-oriented, REST-friendly standard called Fast Healthcare Interoperability Resources (FHIR) to identify trends and emerging standards.

In their 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 a 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.

PoF’s primary focus is on privacy and security protocols that could demonstrate machine-executable representation of patient authorization and consent. At the center of the effort is the notion that both implicit and explicit authorizations are necessary for the exchange. The authorization could be managed through a recognized/trusted Patient Authorization Service that the patient to could use mediate the exchange of their own personal health from a number of patient portals that they may have access to.

In addition to profiling OAuth and OpenID Connect to manage consented sharing between two applications that the resource owner uses, PoF will utilize the UMA authorization model to enable person-to-person data sharing and other authorized data sharing relationships between resource owners and autonomous requesting parties with whom the individual does not share credentials, as well as centralized authorization management for resources residing in many resource servers.

**1) Related work and liaison relationships:**

This Working Group has a number of dependencies on, and shared goals with, the output of other efforts. The OIDF groups and external efforts with which this Working Group intends to liaise informally include (but are not limited to):

* IETF OAuth Working Group
* OpenID Connect Work Group
* Kantara UMA Work Group
* Kantara Consent and Information Sharing (CIS) Work Group
* Kantara Identity Relationship Management (IRM) Work Group
* ISO/IEC SC 27/WG 5
* NSTIC IDESG Healthcare Working Group

**2) Proposers**:

* Justin Anderson (MIT)
* Nagesh “Dragon” Bashyam (HHS ONC) – proposed editor
* John Bradley (Ping Identity)
* Debbie Bucci (HHS ONC) – proposed co-chair
* Adrian Gropper (HealthURL)
* Thomas Hardjono (MIT)
* Robert Horn (AGFA)
* Satoru Kanno (NTTS)
* Kohei Kasamatsu (NTTS)
* William Kim (The Mitre Corporation)
* Eve Maler (ForgeRock) – proposed co-chair
* Josh Mandel (Boston Children’s Medical - Harvard)
* Randy Miskanic (US Postal Inspection Service)
* Puneet Nagpal (WebMD)
* Justin Richer (The Mitre Corporation)
* Nat Sakimura (NRI)
* Haruo Takasaki (KDDI)
* Lucy Thomson
* Zhanna Tsitkov (MIT)
* John Zic (CSIRO)

**3) Anticipated contributions**:

* Draft profiles developed by The Mitre Corporation for securing RESTful services that support patient/consumer health exchanges

**4) Proposed timeline:**

This Working Group will target producing use cases and requirements within 6 months of inception in order to guide its design effort, and will target 18-24 months overall to develop a V1.0 set of technical specifications and profiles and other auxiliary materials, facilitating the development of multiple independent draft implementations as appropriate during this time. The following are suggested initial milestones for consideration by the Working Group:

* IIW Oct 2014: Approval of WG creation
* HIMSS conference Apr 2015: First F2F meeting and review of initial draft of use cases

**5) Input requirements and design principles:**

The specifications must meet the following basic requirements, in addition to specific use cases and requirements later identified by this Working Group:

* Support the exchange of health-related data across security domains.
* Support independent authorization services and identity providers, to be chosen by people who may build, run, or outsource these services.
* Recognize that health data is high-value, personal, sensitive data that requires appropriate security, access controls, privacy protections, and consent obligations.
* Recognize that health-related systems are often both requesters and providers of data.
* Allow an individual to manage data sharing relationships, including modifying the conditions of access or terminating the relationship entirely.
* Allow an individual to audit and monitor various aspects of data-sharing relationships, notably access and usage.

The specifications and profiles must meet the following basic design principles, in addition to any emergent design principles later identified by this Working Group:

* Simple to understand, to implement in an interoperable fashion, and to deploy on an Internet-wide scale.
* Based on the OAuth 2.0 IETF RFCs, the OpenID Connect specifications published by the OpenID Foundation, and the User-Managed Access (UMA) specifications developed at the Kantara Initiative and submitted to the IETF to the extent possible, while contributing bug reports and RFEs around extensibility, security, and privacy to the relevant working groups.
* Leverage lessons learned from the Blue Button+, RHEx and other initiatives and their profiles to the extent possible, and leverage FHIR as a key exemplar of a health data API, recognizing that additional features may be required.
* Resource-oriented (for example, as suggested by the REST architectural style) and operating natively on the Web to the extent possible.
* Layered and loosely coupled.
* Generative (able to be combined and extended to support a variety of use cases in other application domains and emerging application functionality).
* Developed rapidly, in an "agile specification" process that can refactor for emerging needs.

**6) Glossary:**

* This charter uses the word “individual” in the ordinary English sense vs. in the sector-specific sense defined by HIPAA.
* This charter uses the phrase “layered specification” to distinguish the generic notion of a modular technical specification (broken into reusable pieces to enable a “call tree” of references from multiple higher-level specifications) vs. the sector-specific sense of a “mod spec”.