Enabling Patient-Mediated Health Data Exchange

A brief whitepaper
May 1, 2018

By:

Nancy Lush, Lush Group, Inc

Jan Oldenburg, Participatory Health Consulting

In collaboration with:

Eve Maler, ForgeRock, HEART WG co-chair

Thanks to the HEART WG in developing the HEART profile

Introduction

Over the last several months, the quest for patient mediated health data exchange solutions is accelerating. The problems are well-known. Yet many are confused about how to achieve the goal. HEART is one of the key components that will enable patient-mediated health data exchange. We realized that very few understood what HEART is and have written this short paper to explain why it is important to modern health care exchange. It is intended to provide a quick overview of HEART and it's potential.

What is HEART?

HEART (Health Relationship Trust) is a set of profiles that enables patients to control how, when, and with whom their clinical data is shared. The HEART model builds on existing state-of-the-art security and adds additional components to ensure that patient clinical data is securely exchanged. In addition to giving patients control over how their own data is shared, HEART defines the interoperable process for systems to exchange patient-authorized healthcare data consistent with open standards, specifically FHIR, OpenID Connect, OAuth and UMA (User-Managed Access).

Today, attempts to enable patients to electronically manage authorizations for sharing their data have only worked within narrow ecosystems, such as a single healthcare system. This is problematic for patients because it is difficult to share healthcare data with an external physician or with a healthcare system in a different region. It is problematic for organizations and providers because there are no processes, rules, or standards for ensuring that the clinical data being shared has been authorized by patients. This lack is likely to limit adoption and use of data-sharing APIs because it will be far more difficult to ensure that apps seeking to use APIs actually have the approval to obtain access to individual patients' data.

The goal in developing the HEART profiles was to address these issues by creating best practices that accomplish the following practical tasks:

- Enables organizations and other entities to electronically determine whether requests for data are valid (ie, have been authorized by the patient) and what data the requesting entity is authorized to obtain.
- Creates a protocol for managing both sharing of permissions and data that adheres to the highest levels of security and privacy. In the process, both patients and providers increase trust that the data is authorized and accurate.
- Supports, and integrates with, systems that allow patients to set up permissions and authorizations for sharing their clinical data to ensure that their data is only shared with individuals, institutions, and apps that they choose.

HEART provides a standard to enable patient-mediated interoperability implementation through FHIR APIs. To obtain the full benefit of open APIs, we need to enable the HEART standard and get widespread adoption.

Standards framework

HEART was developed by the HEART work group under the auspices of ONC and the OpenID Foundation, which is a non-profit international standards organization comprised of individuals and companies committed to enabling and promoting OpenID capabilities. The Foundation provides infrastructure and help in promoting and supporting adoption of OpenID. HEART is a set of profiles specifically focused on healthcare. It is developed in anticipation of the need for a set of standards to ensure that as health data is increasingly available through APIs and connected apps, consumer privacy is protected by enabling a standard way to ensure that access to a particular set of clinical data has been authorized by the consumer whose data is being accessed.

HEART has been specifically engineered to be compatible with other open standards regarding healthcare data exchange. We have highlighted below how HEART is aligned with other standards:

- HEART compliments SMART on FHIR to include OpenID Connect and User Managed Access (UMA), which both make FHIR transactions more secure. OpenID Connect also provides more authentication features and control in granularity. UMA enables user choice.
- UMA provides the underlying standard for patient-authorized data sharing by giving, "customers and employees a convenient way to determine who and what gets access to personal data, for how long, and under what circumstances." While this has always been important in healthcare, current issues with how Facebook and Google manage private data have underscored the necessity to solve this in a trusted way for healthcare. HEART can provide the transparency to the patient about who has accessed their data and how it is used.
- The SMART on FHIR standard focuses on provider interactions; HEART focuses on the patient perspective by enabling Patient Mediated Exchange.

Digging Deeper

Why is HEART good for patients and consumers?

Health data is some of the most personal and private data to consumers, second only to social security information. Consumers want to gather and control their own data and they want to be able to manage who else has access to that data. They want to be able to easily reflect changes in who has permission to access or move their data. The current environment of concern over unauthorized sharing of social media data is only heightening consumer/patient concerns about whether their health data is secure and who has access to it.

Most health data today is digital at some point in its life. It may be digital at creation, as medical devices, sensors, trackers, and apps are today, or it may be digital at some point, for instance when transcribed notes are entered into an electronic medical record (EHR) or temperature or blood pressure readings, taken manually, are entered into the electronic medical record. The wealth of health data about individuals is growing exponentially, as genomic data and health data from the Internet of Healthy Things increases the universe of what may be considered "health" information.

People with complex health conditions, or those who have moved frequently, have data in multiple systems, stretching over long periods of time that they may want to aggregate and manage access to.

Clinicians, insurers, and researchers want or need clinical data access to diagnose, plan care, and pay for care. Widespread, authorized app access to clinical data will also free developers to innovate on behalf of patients and consumers, bringing new insights informed by historical clinical data.

HIPAA was instituted to protect patients and patient data. But all too often HIPAA is an impediment to the timely flow of a patient's clinical data, which can negatively affect care and increase the cost of care. HEART provides a way for patients to exercise their right under HIPAA in a more effective way. HEART puts the individual back at the center of the health data-sharing conversation and gives each individual the power to control timely and appropriate access to his/her data.

Why is HEART good for organizations and entities?

HEART builds on existing standards already in use in the healthcare environment. When appropriate, it integrates additional consumer standards to enable the patient to control the interoperability exchange.

Because the HEART framework is built on existing standards, organizations can confidently implement HEART without fearing that their implementation will be non-standard or won't mesh well with new systems and data structures.

Widespread implementation of HEART will enable the full benefit of FHIR-APIs by bringing patient-mediated sharing to a wide ecosystem. This will enable cross-organizational sharing of data to meet the requirements of today's healthcare systems. Examples of the benefit to providers and organizations include:

- Having accurate and current medical data available to clinicians at the point of care
- Elimination or reduction of situations where long-scheduled visits to specialists are unhelpful and require a 2nd visit because adequate history is not available to the specialist at the first visit
- Simplification of access to health data by apps and systems, enabling a range of innovative ways to use medical history for the advantage of both consumers and providers

HEART makes all of this possible. By embracing HEART for the interoperability transactions that are controlled by patient consent, we simplify life for both consumers/patients and organizations.

For more information and ongoing updates see http://openid.net/wg/heart/

Recommendations:

While HEART is a cornerstone to achieving patient mediated health data exchange, there are additional components that will support this standard. Identity assurance and federated trusted IdPs need to be available and included in implementations as well as other components. The solution is a system of collaborative parts.

An Argonaut-like work group should be created to support implementations and flush out details to accelerate adoption of these technologies.

Contacts:

Nancy Lush: Nancy.Lush@lgisoftware.com
Jan Oldenburg: jan@janoldenburg.com
Eve Maler: eve.maler@forgerock.com