hdata_scenario

Scenario: Controlling Access to Health Data (Pending)

Submitted by: Gerald Beuchelt

Project hData defines the Representational State Transfer (RESTful) exchange of health-related hData Records and Section Documents. While systems with a single health organization may exchange health data without strong security controls in some cases, any exchange of health data across public data networks or between different actors will require strong information assurance. This scenario outlines the basic requirements and a high-level conceptual architecture for patient access-controlled hData network exchanges with a specific focus on cross-organizational interactions.

For other deployments of hData, a different set of information assurance and security requirements might apply: for example, if two separate hData enabled record systems are used within an organization – one as the authoritative medical record store for patient data, and another as the financial accounting system – there will be fewer requirements on security constraints, since the two systems are likely within the same trust domain.

Additional details about Project hData are available in its document repository.

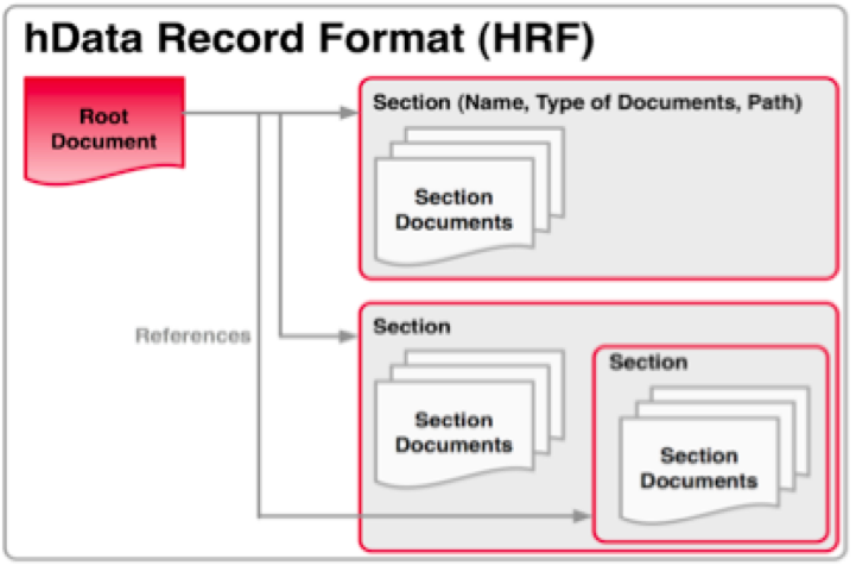
Distinctive aspects:

- High-value, personal, sensitive data that requires appropriate security, access controls, and privacy controls
- A Discovery and Authorization Service component dictated by the hData architecture that requires its own access-control protection ("trusted discovery"), in addition to providing protection for actual health data
- Services that are frequently in the position of being both hosts and requesters

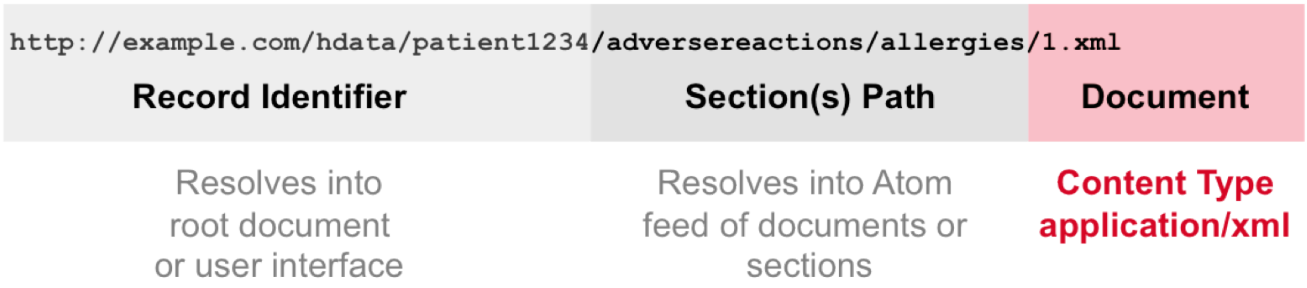
hData Format and Data Exchange

The hData format consists of a collection of individual documents (Section Documents), organized in Sections. Sections may contain Section Documents (i. e. individual data points) or other sections.

All Sections are referenced in a manifest called the Root Document. By default, Sections contain Section Documents of a specific type (e.g. medications, x-ray images, etc), but when explicitly tagged in the meta-data portion of the specific Section Document, Sections may contain Section Documents that are different from the default Section type.



hData records may be accessed through a RESTful Application Programming Interface (API), with the abstract Section structure providing a canonical mapping to a Uniform Resource Locator (URL) pattern.



Use Case: Protecting Health Data and Metadata (Pending)

Actors:

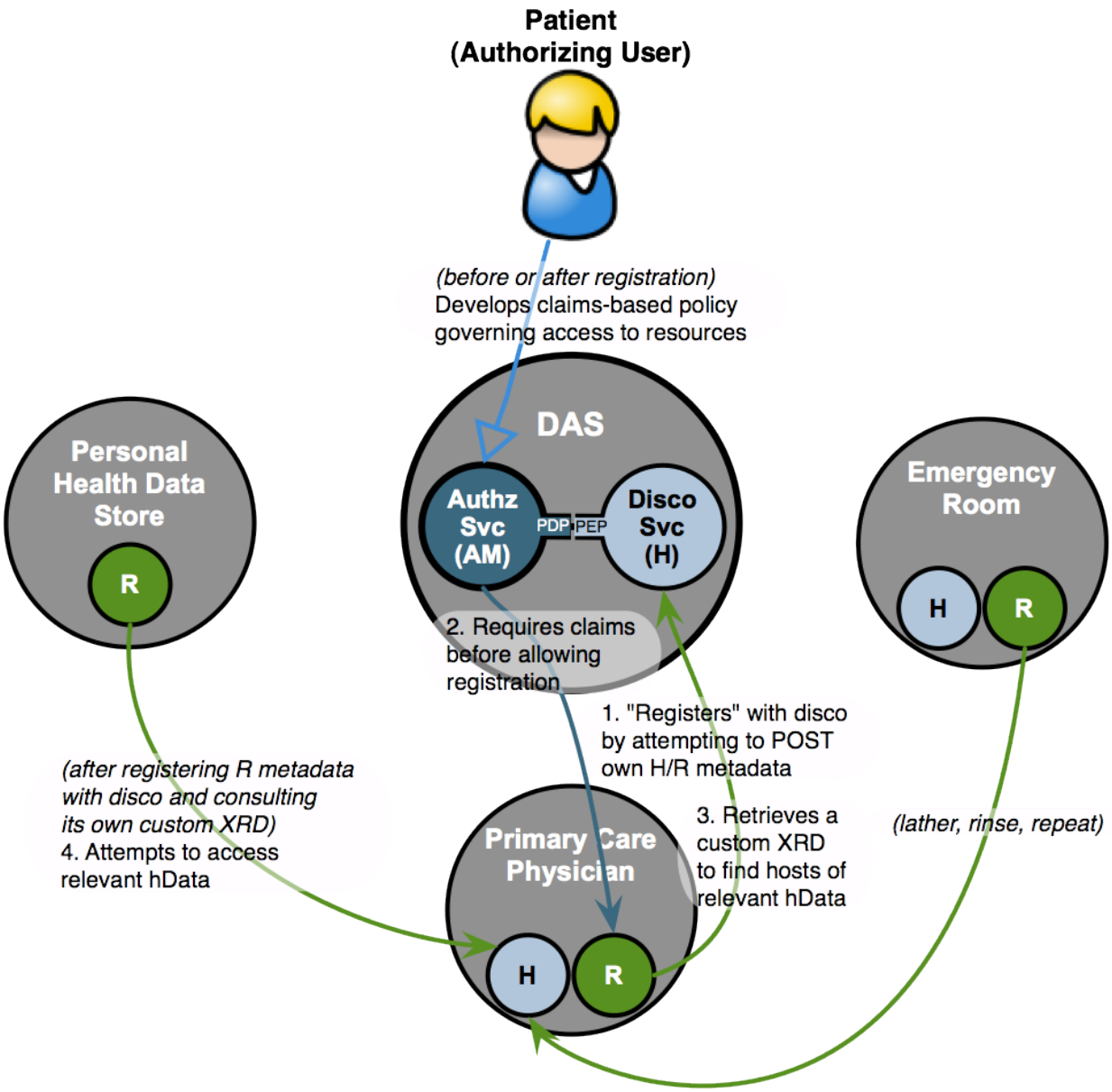
- Patient as Authorizing User
- hData DAS component in dual roles as an Authorization Manager and as a Host of health resource metadata
- Various parties such as primary care physicians, emergency rooms, testing laboratories, and personal health datastores in potentially dual roles as hosts of health data, requesters of health data from other hosts, and requesters of metadata services from the metadata Host

From a single patient's perspective, an hData deployment that crosses trust domains acts like a "circle of access" for the online services that handle the patient's health data in any fashion. (See this hData presentation for a step-by-step accounting of how a patient's visits to a primary care physician, and subsequently an emergency room doctor, would occasion a need for data-sharing by those two parties on the patient's behalf, and therefore a need for them to obtain authorization for the sharing and discovery of the resources in question.)

In the following diagram, the following services handle the patient's health data:

- The primary care physician, as both a Host of data generated from patient visits and tests performed in the PCP's office, and a Requester of data from emergency room visits
- The emergency room, as both a Host of data generated from patient visits and tests performed at the ER, and a Requester of data from the PCP
- A personal health datastore service chosen by the patient, as a Requester of data from the patient's medical visits (it could as easily have been a Host itself, if, say, the person chose to store the ongoing results of self-administered weight or blood pressure tests there and wanted to make that data available to a third-party health assessment website)

The "DAS" in the center is the Discovery and Authorization Service, an hData conceptual function. The XRD standard has been discussed as the likely metadata format to be used in the discovery component of the DAS.



This diagram describes how hData can use UMA to give the patient control over both health data and the mechanisms of introducing a new provider or other health data source/destination into the picture.

Assumptions:

- Health care provider systems are able to produce signed attestations of their identity and/or medical credentials when asked by the DAS to do so.
- The patient is able to craft authorization policies that constrain access according to identity and medical credentials.
- The discovery service component of the DAS is able to deliver up custom metadata (or equivalent resource lookup services) to each seeker of health data, based on the patient's policies.

Preconditions:

- The patient establishes an account at the DAS.
- The patient, when visiting a health care provider such as the PCP, direct's the PCP's electronic health record (EHR) system to the patient's DAS in some fashion.

Steps as shown in the diagram:

1. The PCP's EHR system registers with the DAS discovery service's Host component by interacting with it as a Requester, attempting to add the PCP's own metadata to it to join the patient's circle of access.
2. The DAS authorization service's AM component imposes user-managed policy over the adding of PCP metadata, based on the PCP's credentials, ultimately allowing the PCP to add its metadata to the DAS. (In future, the PCP can update its metadata in the same fashion as necessary.)
3. The PCP then interacts with the DAS again, this time as a Requester retrieving the metadata resources that will help it discover where relevant health data is hosted for this patient. It can then approach the appropriate Hosts of patient health data in the usual UMA-protected fashion.
4. ... At some later time, the personal health datastore, having already performed its equivalent of steps 1 through 3, approaches the PCP system to read the latest versions of the patient's health data stored there. Once the personal health datastore successfully retrieves health data from all the systems it is authorized to access, the patient can get an aggregated view of this data in one place.