hData Use Cases

Introduction

hData allows a Representational State Transfer (RESTful) exchange of 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 use case outlines the basic requirements and a high-level conceptual architecture for hData network exchanges with a specific focus on cross-organizational interactions.

For other deployment 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 less requirements on security constraints, since the two systems are likely within the same trust domain.

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 metadata 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.

<table>
<thead>
<tr>
<th>Record Identifier</th>
<th>Section(s) Path</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://example.com/hdata/patient1234/adversereactions/allergies/1.xml">http://example.com/hdata/patient1234/adversereactions/allergies/1.xml</a></td>
<td>Resolves into Atom feed of documents or sections</td>
<td>Content Type: application/xml</td>
</tr>
</tbody>
</table>
hData Security Requirements

The hData project (http://projecthdata.org) has published a document and slide deck describing the high-level requirements for hData RESTful exchanges. The overall architecture consists of hData hosts (H), requestors (R), the Discovery and Authorization Service (DAS) including the Authorization Manager (AM), and the patient interacting with these components.

There are a few simple workflows that must be implemented:

0. The patient establishes an account at the DAS and set the default policies.

1. When visiting a provider such as the Primary Care Physician (PCP), the patient directs the PCP’s Electronic Health Record (EHR) system to the DAS.
2. The request includes an authorization statement describing the roles of the PCP. The PCP’s EHR systems – pending patient controlled policies – now becomes discoverable for requestors.

3. The Discovery Service can now provide to the new EHR system a list of accessible EHR systems, which must be created specifically for the discovery consumer. This is to make sure that a discovery consumer only gets to see those EHR systems that the patient permitted them to see.

4. In subsequent transactions, the system may act as requestor or host, using the DAS to discover new systems and obtain coarse-grained authorization tokens.