# hData Network Transport Information Assurance and Security Requirements v0.3

*PUBLIC DRAFT – FOR COMMUNITY REVIEW*

*Gerald Beuchelt*
*The MITRE Corporation*
*202 Burlington Rd.*
*Bedford, MA 01730*
*U.S.A.*

## 1 Introduction

### 1.1 hData RESTful Network Transport

hData allows a 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 document 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.

### 1.2 Design Principles for hData Information Assurance

For the purposes of this paper, the following principles have been provided:

#### 1.2.1 Simple Access

Access to resources should be as simple as possible

#### 1.2.2 Privacy

All interaction patterns must support the requirements of the 1974 Privacy Act and HIPAA, and be flexible enough to support evolving requirements. In addition all transactions must be configurable at least to be pseudonymous. Only explicit patient permission or legal overrides should allow the resolution of pseudonymized interactions.

### 1.2.3 Patient Empowerment

Patients must have the greatest feasible control over how their medical data is used and with whom it is shared. When access is granted without explicit patient permission (e.g. in emergency situations), patients must notified as soon as possible unless restricted by law. Patients must also be notified in advance of situations where access will be permitted by default, and informed whether they have the right to override the default. For example, patients cannot override certain public health reporting, but can Opt-Out of certain sharing with other medical providers. (Some states – Indiana – require Opt-Out on certain fields).

### 1.2.4 Scalability

Any information assurance system for nationwide hData must scale to very large numbers of patients (350M+), providers (1M+), and other actors (1M+).

## 1.3 Scope of this Document

This document does not define a concrete architecture for securing hData, but defines the information assurance and security requirements for the hData Networking Transport. It introduces high-level concepts and a draft architecture. While it discusses components of the overall hData architecture, it is not intended to provide a comprehensive architecture description.

# 2 Conceptual Architecture

The overall architecture and its interaction with a new hData consumer is displayed below. Note that this includes the NHIN which is not yet realized.

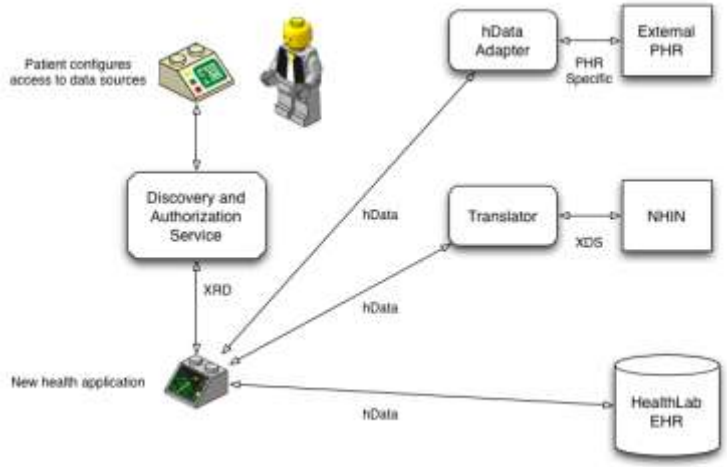


Figure 1

The following sections illustrate each of the different components.

## 2.1 hData Discovery and Authorization Service

The hData Discovery and Authorization Service (DAS) implements the service-side of the functionality described in detail in section 3, namely:

- Discovery of EHR systems
- Federation of EHR systems
- Consent and authorization

It is intended to be operable by any actor, including the patients themselves. While operation by the patient should be possible, the expectation is that most patients will use a DAS operated by an authorized 3rd party service provider such as a PHR system or their insurance company.


Figure 2

The user interacts with the DAS by establishing an account, setting his consent policies, and authorizing provider EHR systems to interact with each other, mediated by the DAS.

The DAS is described in this document from the patient's perspective: the patient sets the policy, introduces EHR systems to each other and manages consents. Obviously, this basic model would preclude any emergency override, sometime referred to as "breaking the glass". To enabled this functionality, a parallel DAS may be introduced that is not managed by the patient, but by a federal and/or state government entity:

Since the provider EHR systems are implementing the policy decision and enforcement (PDP/PEP), they can conceptually subscribe to more than one policy information point (PIP – also called policy store, PS). During normal operation, the service provider EHR will honor the patient DAS only. During declared emergencies (either geographic or medical emergencies), the service provider may honor government DAS authorized requests.

## 2.2 Patient

The patient is a crucial element to the entire architecture. Patients have to authorize access of service consumers to any of the hData DAS functions. The patient also sets the access policies for categories of data items (such as medications) or specific data (such as any mental health-related information).

## 2.3 EHR Systems

To participate in a patient's EHR federation, a system will support:

1. Publish data about the patient as hData Records (in the hData service provider role),
2. Subscribe to other system's hData Records (in the hData service consumer role),
3. Utilize the hData DAS discovery and federation functions, and
4. Implement the access control and consent policies.

Requirements 3 and 4 are strictly required for cross-organizational hData deployments. If hData is used as an internal interface between systems within the same trust domain, these functions might not be required or replaced by deployment-specific controls.

### 2.3.1 Actor EHR Systems

The EHR systems of any of the common actors (providers, payers, HIEs) can act both as service providers and service consumers. They typically provide the patient's hData Record through the hData Network Transport.

### 2.3.2 PHR Systems

Any PHR system chosen by the patient will act very similarly to other actor's EHR systems: it provides access to the patient record, which will typically contain information entered by the patient, such as weight charts, etc.

### 2.3.3 Other Health Record Systems

In addition, other systems such as medical devices can participate in the hData record exchange as well: once they are added to the DAS as members of the medical federation of the patient, any other authorized system can subscribe to health data published from these devices.

## 2.4 Translator

hData based EHR systems must be able to connect to non-hData enabled systems. This will be achieved through an hData translator, typically to HITSP/HL7 based exchanges. Since these legacy exchange protocols lack the features and expressiveness of the hData information assurance and security components, the high fidelity of authorization and consent may not carry over into those systems. Another reason, even if all are expressive, is that the systems may simply conceptualize the world differently, and the semantics to not map to each other.

# 3 Functionality

In this section the high-level functions of the conceptual architecture are introduced. Any implementation of these functions must be consistent with the RESTful architectural of the hData Network Transport specification.

## 3.1 Discovery Service

### 3.1.1 Description

The Discovery service allows any service consumer to find hData service endpoints for a given patient.

### 3.1.2 Key Goals

The discovery service must provide the following:

1. Unique discovery service endpoint: there should be one resource per patient, identified by an URL that maps directly to the patient. The service must allow securing the endpoint for access by the patient, their medical proxy, or an authorized entity. Depending on the identity of the accessor, different discovery results will be produced.
2. Discovery document: the discovery service endpoint returns a list of hData-enabled EHR systems that the authenticated entity may know about. Note that this is independent of access authorization: a service consumer may see certain EHR systems, but may not be granted access to them.
3. Registration mechanism: a service should be able to register itself for discovery. This request must be accompanied by a patient authorization. This authorization should also include any restrictions on the discoverability of this new service, if applicable.

### 3.1.3 Mode of Operation

#### *3.1.3.1 First contact*

When a service consumer contacts the discovery service for the first time, the discovery service must require an authorization from the patient with the access request. This may be a generic authorization, or it may contain additional entitlements or restrictions, essentially determining the appropriate list of discoverable systems. Conceptually, this authorization could be a cryptographically signed authorization statement. It should include an expiration time.

During this first exchange, the discovery consumer and the service must establish a handle/pseudonym or exchange a shared secret for re-identification.

#### *3.1.3.2 Subsequent contact*

In any subsequent contact, the discovery consumer should use the handle or shared secret that was negotiated in the first contact. As long as the authorization statement is not expired or revoked, the discovery request should be answered, with any caveats from the authorization statements.

#### *3.1.3.3 Discovery Registration*

Similar to the first contact, a service that wants to make itself discoverable for other services must provide a patient-signed authorization for inclusion in the discovery results.

## 3.2 Federation

### 3.2.1 Description

The federation manages authorizations and machine readable policies.

### 3.2.2 Key Goals

The federation component must provide:

1. The authorization token service will create short-lived access tokens for a federation consumer. These access token are specific for the patient, the (pseudonymous) identity of the service consumer, and the (pseudonymous) identity of the service provider. The token must be cryptographically protected against tampering.
2. Patients must be able to manage and terminate long-lived access permission. Note that this does not necessarily require the revocation of short-lived tokens.
3. A token must be able to carry patient authorization information and limited attributes about the authenticated entity, either contained within the token or resolvable through the presentation of the token at a federation component facility.

### 3.2.3 Mode of Operation

#### *3.2.3.1 First contact*

The first token request for accessing a given service provider must be accompanied by an authorization by the patient, similar to the authorization for discovery. While not required, it is recommended to re-use the pseudonym/shared secret that might have been established between the discovery service and the discovery service consumer.

#### *3.2.3.2 Subsequent contact*

Similar to the subsequent discovery request, subsequent requests for authorization tokens do not need a patient authorization, as long as the first authorization is still valid.

#### *3.2.3.3 Access Termination*

At the patient's request, the federation service must stop issuing access tokens to service consumers. Existing short-lived tokens are not required to be revoked, as long as the token lifetime does not extend beyond e.g. 24 hours. The patient or regulations determine what constitutes "short lived".

## 3.3 Access Control and Consent

### 3.3.1 Description

Access control and consent to share specific data items in a patient's EHR should be configurable for the patient. This subsystem contains mechanisms to communicate patient information sharing requirements, i.e. the patient policies.

The access control policies are only available to systems participating in the federation.

### 3.3.2 Key Goals

This functionality must satisfy these goals:

1. Patients must be able to configure a set of access control policies for their EHR. This must include the possibility to restrict access to categories of medical data (such as allergies, medications, etc.) or specific medical data (such as e.g. all psycho pharmaceuticals, cancer diagnosis, etc.). Access control policies must be configurable through a simple user interface.
2. Systems providing hData Records to members of the federation must ensure that they use reasonably current information about the patient's access control and consent policies. If a change occurs, the hData service provider must update all own section document meta-data entries, specifically the sections that represent the policy set by the patient.

### 3.3.3 Mode of Operation

#### *3.3.3.1 Federation Join*

Any new EHR system joining the patient's hData Federation (i.e. creating a record about the patient that becomes discoverable by other federation members, and getting the ability to discover and access other hData EHR systems in the federation) requires the patient's authorization to access other EHR systems. Since this authorization may come with restrictions (e.g. a optometrist's EHR system may not be permitted to access the patient's mental health data), this authorization must be provided to all hData service providers by the hData DAS upon access request. Ideally, the identity of the consumer should not be revealed, unless explicitly required by the patient or the law.

In addition, the newly joining EHR system must download the patient's consent polices and preference, and apply these to all local hData section document meta-data. It is the responsibility of the providing EHR system to frequently connect to the hData DAS and obtain any changes in these access policies.

#### *3.3.3.2 Resource Request*

When a request for an hData resource is received, the hData service provider must perform the following conceptual steps:

1. Verify the authority of the service consumer at the EHR system level. This may be done through verifying the pseudonymous identity of the service consumer EHR system through the hData DAS, e.g. in the form of an access token. It will be the responsibility of the consuming EHR system to guarantee that only authorized end-user get access to a given patient's data.
2. Once the token is confirmed to be valid, the patient's federation join authorization for the requesting service consumer must be obtained or verified. Any restriction for this authorization must be obtained by the service provider.
3. The authorization of the patient and any included restrictions must very evaluated against the access policies obtained from the hData DAS. This amounts to a policy decision. Note that this PDP functionality could be delegated to an external PDP in a future version of these requirements.

4. Based on the result of the access decision in the above step, the access request is allowed or denied by the service provider, enforcing the policy.

# 4 hData Constructs

The hData Record Format specification provides a number of constructs that are intended to be used in the context of the information assurance and security architecture.

## 4.1 hData Record Sections

The hData Record Format specification stipulates the division of a patient's EHR record into "Sections". These sections are intended to provide information about a specific type of health data, e.g. allergies, medications, or results. At the same time, the data may also be grouped in other ways, such as ordered by visits or pretty much any other criteria. While this is a relatively coarse system, it allows simple access control based on the section path (represented in the RESTful API as resource path) to sections.

## 4.2 Section Document Meta Data

In addition hData provides a meta-data structure with every Section Document. It contains clerical information such as creation and modification dates, document name, media and hData content types, linked section documents, and pedigree information. In addition, there are fields reserved for access control and consent management.

These latter fields may be used for creating an access control and consent mechanism, as required in the above section.

# 5 Benefits and Supported Use Cases

*Note: the use cases will need to be mapped to ARRA requirements/AHIC use cases*

## 5.1 Use Case: Specialist Visit

## 5.2 Use Case: Emergency Access

## 5.3 Use Case: Access to Sensitive Data

## 5.4 Use Case: Patient/Actor Notification

## 5.5 Benefit: Medical Identity Theft

## 5.6 Benefit: Health Monitoring

## 5.7 Benefit: Sensor Integration