

U.S. Health and Human Services

Office of the National Coordinator for Health IT

Data Access Framework (DAF) Document Metadata Based Access Implementation Guide

Revision History

|  |  |  |
| --- | --- | --- |
| Date | Document Version | Document Revision Description |
|  |  |  |

Copyrights

This material includes materials from Health Level 7 International (HL7), Integrating the Healthcare Enterprise (IHE), the Office of the National Coordinator for Health IT (ONC) Standards and Interoperability (S&I) Framework Data Segmentation Use Case, and other Data Access Framework Initiative documents. **All materials used in this document are for prototype and development purposes ONLY, with permission from the underlying organizations.**

Table of Contents

[1. Introduction 6](#_Toc416513999)

[1.1. Definition of Terms 6](#_Toc416514000)

[1.2. Purpose of this Implementation Guide 8](#_Toc416514001)

[1.3. Intended Audience and Goals 8](#_Toc416514002)

[1.3.1. Pre-Requisite Knowledge 8](#_Toc416514003)

[1.3.2. Reader Guidance 9](#_Toc416514004)

[1.4. Assumptions and Pre-Conditions 10](#_Toc416514005)

[1.4.1. Assumptions for Data Access Framework 10](#_Toc416514006)

[1.4.2. Pre-Conditions for Data Access Framework 10](#_Toc416514007)

[1.5. Structure of Implementation Guidance 11](#_Toc416514008)

[1.5.1. Definition of Actors 12](#_Toc416514009)

[1.5.2. Specification References 12](#_Toc416514010)

[1.5.3. Use of Conformance Language 13](#_Toc416514011)

[1.6. Data Access Framework Enhancements to Standards and Profiles 15](#_Toc416514012)

[1.7. Scope of DAF Technical Approach 15](#_Toc416514013)

[2. DAF Technical Approach – Query Stacks and Building Blocks 17](#_Toc416514014)

[2.1. Query Stack 18](#_Toc416514015)

[2.2. DAF Query Execution Context (Governance) 18](#_Toc416514016)

[2.2.1. Local or Intra-Enterprise 18](#_Toc416514017)

[2.2.2. Targeted or Inter-Enterprise 19](#_Toc416514018)

[2.3. Query Stacks and Modularity 19](#_Toc416514019)

[2.4. Query Stacks and Substitutability 19](#_Toc416514020)

[2.5. DAF Behavior Models Supported 19](#_Toc416514021)

[2.5.1. Synchronous Request/Response model 19](#_Toc416514022)

[2.5.2. Asynchronous Request/Response model 20](#_Toc416514023)

[2.6. DAF Query Stacks and Standards 21](#_Toc416514024)

[2.6.1. SOAP Query Stack 22](#_Toc416514025)

[2.6.2. RESTful Query Stack 23](#_Toc416514026)

[3. DAF Implementation Guidance – SOAP Query Stack 23](#_Toc416514027)

[3.1. SOAP Query Stack Standards Summary 23](#_Toc416514028)

[3.2. Transport and Application Protocol Implementation 23](#_Toc416514029)

[3.2.1. Authentication, Message Integrity and Message Confidentiality 23](#_Toc416514030)

[3.2.2. SOAP 1.2 Implementation Guidance 23](#_Toc416514031)

[3.3. Query Implementation 23](#_Toc416514032)

[3.3.1. DAF Queries and XDS Metadata 24](#_Toc416514033)

[3.3.2 Using XCA for DAF 24](#_Toc416514034)

[3.3.3 Using MPQ for DAF 25](#_Toc416514035)

[3.3.4 Anatomy of a DAF Sample Query 26](#_Toc416514036)

[3.4. Query Results Implementation 26](#_Toc416514037)

[3.4.1. Query Results 27](#_Toc416514038)

[3.5. Security Implementation 27](#_Toc416514039)

[3.5.1. Local DAF Security Requirements 27](#_Toc416514040)

[3.5.2. Targeted DAF Security Requirements 29](#_Toc416514041)

[3.6. SOAP Query Examples 32](#_Toc416514042)

[4. DAF Implementation Guidance – RESTful Query Stack 32](#_Toc416514043)

[4.1. RESTful Query Stack Standards Summary 32](#_Toc416514044)

[4.2. Transport and Application Protocol Implementation 33](#_Toc416514045)

[4.2.1. Authentication, Message Integrity and Message Confidentiality 33](#_Toc416514046)

[4.2.2. Implementation Guidance for RESTful Resources for Document Access 33](#_Toc416514047)

[4.3. Query Implementation 34](#_Toc416514048)

[4.3.1. DAF Queries and XDS Metadata 34](#_Toc416514049)

[4.3.2 Using MHD for DAF 34](#_Toc416514050)

[4.3.3 Querying for Documents related to Multiple Patients 35](#_Toc416514051)

[4.4. Query Results Implementation 35](#_Toc416514052)

[4.4.1. Query Results 35](#_Toc416514053)

[4.5. Security Implementation 35](#_Toc416514054)

[4.5.1. Local DAF Security Requirements 36](#_Toc416514055)

[4.5.2. Targeted DAF Security Requirements 38](#_Toc416514056)

[4.6. RESTful Query Examples 40](#_Toc416514057)

[5. Appendix A - Acronyms and Definitions 41](#_Toc416514058)

Table of Figures

[Figure 1 –Building Blocks – Data Access Framework Technical Approach 17](#_Toc416514066)

Table of Tables

Table 1 – Pre-Requisite Knowledge 9

Table 2 – Reader Guidance 10

Table 3 – Definition of Actors 12

Table 4 – Namespace Prefixes 12

Table 5 – Consolidated Conformance Verb Matrix DAF IG 14

Table 6 – Optionality Definition 15

Table 7 – Key Acronyms and Definitions 43

# Introduction

Many countries are reaching a critical mass of Health IT systems (EHR Systems, EMRs, hospital information systems, medical record systems, data warehouses, etc.) that comply with data and vocabulary standards. The wide deployment of Health IT systems has created unique opportunities for providers, provider support teams, patients, public health agencies, healthcare professionals and organizations and others to access and use the patient data that is already collected during clinical workflows. This information may not be readily accessible through the applications to which the relevant party has access. Allowing access to this data can enable a provider to further analyze the collected data to understand a patient’s overall health, the health of a provider’s collective patient population, and use the data to power analytics applications and tools to take better care of patients and populations.

The Standards and Interoperability (S&I) Data Access Framework (DAF) Initiative outlines the standards and profiles that can be used to enable data access within an organization and across organizations. These standards and their associated implementation guidance are outlined in this document.

## Definition of Terms

The section defines some of the terminology used through the rest of the document.

**Data Access Mechanisms:**  
Data Access mechanism refers to how the data is accessed. This is commonly done via queries. These queries fall into different categories based on the type of information used to create the queries. Examples of Data Access mechanisms include Document Metadata based access and Data Element based access which is defined below.  
  
**Document Metadata based access:**  
Document Metadata based DAF Queries are created using the metadata associated with clinical documents. The metadata associated with clinical documents is typically captured as part of clinical workflows. Examples of metadata include

* Type of the clinical documents (for e.g. Office Visit Summaries, Discharge Summaries, Operative Notes, History and Physical notes) used to record various clinical encounters.
* Patient identifier information such as patient id or medical record number.
* Metadata such as time of creation, modification time, Practice Type, and other ebRS/ebRIM based metadata as documented in IHE ITI TF: 2a : 3.18.4.1.2.3.7
* There are no limitations on the types of the documents that can be accessed using Document Metadata. Some example document types include Consolidated Clinical Document Architecture (C-CDA), Referral Notes, Lab Reports among others.

**Data Element based access:**  
Data Element based DAF Queries are created using information that is part of the patient's clinical record. Information that is typically present within a patient's record include

* Patient Demographics information such as race, ethnicity, gender, age.
* Lab Results information
* Medications, Immunizations, Problems etc.
* **Granularity of Data being returned or accessed:**  
  Granularity of Data being returned refers to the information that is returned due to the execution of a DAF query. This is commonly known as Query Results. Query Results can contain individual Patient Level Data or aggregate Population Level data which are defined below.  
    
  **Patient Level Data:**  
  When the granularity of data access is “Patient Level Data”, the Health IT systems responding to the queries are expected to return information for each patient(s) that meets the query criteria. The returned information can be complete clinical documents such as C-CDA or it could be in the form of HL7 FHIR resources such as Problems, Medications. Standards such as C-CDA, HL7 FHIR resources, QRDA Category I and HL7 v2.5.1 message formats are used to encode individual patient level data.

**Population Level Data:**  
When the granularity of data access is “Population Level Data”, the Health IT systems responding to the queries are expected to return summary information about the population that meets the criteria. Population information could be

* Number of patients that meet a criterion.
* Percentage of Patients that meet criteria.
* De-identified Patient List Report (Patient List Report is essentially a list of patients)
* Standards such as QRDA Category III Report, conceptual QRDA Category II Report and HL7 FHIR resources are used to encode population level data.

**Trusted Healthcare Organization:**   
In the context of Data Access Framework, a trusted external healthcare organization can be either a Covered Entity or a Business Associate as defined by HIPAA rule. A trusted healthcare organization is defined as an independent legal entity, with which a pre-established agreement and/or relationship is in place with the requesting organization to share patient information.

**Local Data Access Framework (LDAF):**   
Local Data Access Framework (LDAF) which is a part of overall Data Access Framework specifically outlines the standards and profiles used to access data within an organization.

**Targeted Data Access Framework (TDAF):**   
Targeted Data Access Framework (TDAF) which is a part of overall Data Access Framework specifically outlines the standards and profiles used to access data from a single known external organization.

## Purpose of this Implementation Guide

The purpose and value of this document is to provide specific implementation guidance around the usage of standards and profiles for Data Access Framework Document Metadata based Access capability. Specifically:

* Identify standards and profiles that will be used to support LDAF and TDAF using document metadata.
* Show how standards can be modularized leading to substitutability.
* Identify additional constraints on the base standards and profiles that may be applicable in the context of DAF.
* Identify APIs for the usage of standards that can be leveraged in both LDAF and TDAF.
* Define examples of queries for both LDAF and TDAF.

This document complements the [DAF Data Element based access Implementation Guide](http://hl7.org/implement/standards/FHIR-Develop/daf.html) which is currently being developed by the ONC S&I Framework working with HL7.

## Intended Audience and Goals

This implementation guidance is designed to support developers and implementers who will be implementing standards and technologies to enable data access within their organization and across organizations.

Within this implementation guidance, the focus is on the following key goals:

* Provide a robust set of standards and profiles that will enable Document Metadata based Access in a modular fashion. This will allow for incorporation of new standards and profiles as they mature into the framework.
* Support the HITSC recommendations to incorporate both existing standards and emerging standards that will enable data access via queries.

### Pre-Requisite Knowledge

The implementer must be familiar with the following information prior to reading this guidance. It is absolutely essential for implementers to familiarize themselves with these standards and profiles in order to be prepared for full implementation of this guidance. These specific guides and standards are referenced in Appendix G with links to their locations and we **HIGHLY RECOMMEND** referring to them prior to building implementations using this guide.

|  |  |
| --- | --- |
| DAF Project Charter | http://wiki.siframework.org/Data+Access+Framework+Charter+and+Members |
| DAF Use Cases | http://wiki.siframework.org/DAF+Use+Cases |
| DAF IHE PCC White Paper | <http://ihe.net/uploadedFiles/Documents/PCC/IHE_PCC_White_Paper_DAF_Rev1.1_2014-10-24.pdf> |
| IHE ITI Technical Framework Vol 3 | <http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf> |
| IHE XDS Profile | http://wiki.ihe.net/index.php?title=Cross\_Enterprise\_Document\_Sharing |
| IHE XCA Profile | http://wiki.ihe.net/index.php?title=Cross-Community\_Access |
| IHE XUA Profile | http://wiki.ihe.net/index.php?title=Cross-Enterprise\_User\_Assertion |
| IHE XCPD Profile | http://wiki.ihe.net/index.php?title=Cross-Community\_Patient\_Discovery |
| IHE ATNA Profile | http://www.ihe.net/Technical\_Framework/upload/IHE\_ITI\_Node\_Authentication\_Security\_2004\_08-15.pdf |
| IHE Technical Framework Appendix V | http://www.ihe.net/uploadedFiles/Documents/ITI/IHE\_ITI\_TF\_Vol2x.pdf |
| IHE IUA Profile | <http://wiki.ihe.net/index.php?title=Internet_User_Authorization> |
| IHE MHD v2 Profile | <http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_MHD.pdf>  <http://wiki.ihe.net/index.php?title=MHD-rev2-vol-3>  http://wiki.ihe.net/index.php?title=Mobile\_access\_to\_Health\_Documents\_-\_Supplement\_revision\_2 |

Table – Pre-Requisite Knowledge

### Reader Guidance

This convenient table provides direct access to sections of the implementation guidance of most relevance to the reader:

|  |  |
| --- | --- |
| What are the different Query Stacks proposed in this implementation guidance to implement DAF | [DAF Technical Approach – Query Stacks and Building Blocks](#_DAF_Technical_Approach) |
| What are the behavior models supported by DAF | [DAF Behavior Models Supported](#_DAF_Behavior_Models) |
| What are the standards used for DAF | [DAF Query Stacks and Standards](#_DAF_Query_Stacks) |
| Where can I learn about the SOAP query stack | [SOAP Query Stack](#_SOAP_Query_Stack) |
| Where can I learn about the RESTful query stack | [RESTful Query Stack](#_RESTful_Query_Stack) |
| How do I implement the SOAP query stack | [DAF Implementation Guidance – SOAP Query Stack](#_DAF_Implementation_Guidance) |
| How do I implement the RESTful query stack | [DAF Implementation Guidance – RESTful Query Stack](#_DAF_Implementation_Guidance_1) |
| Where can I find examples for SOAP query stack | [SOAP Query Examples](#_SOAP_Query_Examples) |
| Where can I find examples for RESTful query stack | [DAF Implementation Guidance – RESTful Query Stack](#_DAF_Implementation_Guidance_1) |
| Where can I find working example code to use in my implementation? | TBD |
| Where is a summary of conformance statements that my implementation needs to follow? | TBD |

Table – Reader Guidance

## Assumptions and Pre-Conditions

It is important for the reader to understand the following assumptions and pre-conditions as defined in the S&I Framework Data Access Framework Project Charter and Use Cases:

### Assumptions for Data Access Framework

The main assumptions that are derived from the S&I Framework DAF Project Charter and Use Case are listed below:

* An organization refers to a legal entity which can have any number of sub-entities within the organization.
* An organization’s local Health IT system is comprised of any and all IT systems (i.e. varying EHR systems or other Health IT systems such as Pharmacy and Lab).
* Federated query within a local Health IT system will be handled by the organization as required.
* Information requestor (business user) knows how to query the local Health IT System.
* Actors and systems shall execute queries and return query results based on their own internal service level agreements (SLAs).
* Patient data can be queried as long as it has been documented and the organization's Local Health IT system makes it available to be queried against.

Additional assumptions for this implementation guide include:

* This implementation guide is built on existing IHE profiles for Document Metadata based access and does not create any new profiles or fill any gaps identified by the DAF IHE White paper.

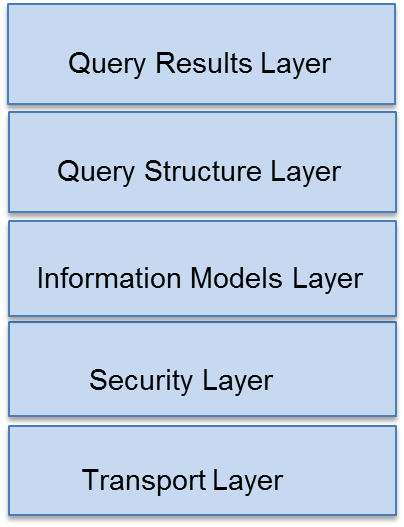
### Pre-Conditions for Data Access Framework

The main pre-conditions that are derived from the S&I Framework DAF Use Case are listed below:

* Query parameters required to create the query in a standardized format are known to the Query Requesting Application (for e.g. patient id)
* Query Requesting Application has knowledge about the Query Responding Application end point to send a query.
* Query Requesting and Query Responding Applications have a common understanding of the shared vocabulary that is used to create the queries and provide the query results.
* Query Requesting Application is able to determine the Query Responding Application that may have the data being requested.
* Query Responding Application can provide a query response in the standardized format.

## Structure of Implementation Guidance

The following figure summarizes the DAF building blocks used to meet the requirements of the S&I Framework DAF Use Case.



DAF Building Blocks

The standards and implementation guidance will be provided for each of the following areas

* Transport and Application Protocols
* Query Structure, Vocabularies and Value Sets
* Query Results, Vocabularies and Value Sets
* Security Layer
* DAF will reuse existing data models and not develop or create any new data models.

The advantages of this approach are as follows:

* Allows for vendor and implementer flexibility to implement the building blocks specific to their environment
* Allows for the separation of between the various layers of standards required for queries namely Transport and Application Protocols, Query Structure, Query Results and Security Layers.
* Allows re-use of off-the-shelf security and transport components developed in general IT - lowering the cost to implement in healthcare
* Allows for scalability of the solution

### Definition of Actors

Several actors are defined within this implementation guidance document based on the S&I Framework DAF Use Case.

|  |  |  |
| --- | --- | --- |
| **Actor within Implementation Guidance** | **Role of Actor within Implementation Guidance** | **Other Possible Names/Roles** |
| Query Requesting Application | The Query Requesting Application will is responsible for Sending the query and receiving the response from the Responding application. | Query Requestor  Query Sender  Requestor |
| Query Responding Application | The Query Responding Application will be responsible for Receiving the query request, processing the query request, creating the query response and sending the query response. | Query Responder  Query Receiver  Responder |

Table – Definition of Actors

#### Conventions Used

XML examples that have been developed as part of this implementation guidance will use the following namespace prefixes. When no namespace prefix is present, the namespace is assumed to be:

|  |  |  |
| --- | --- | --- |
| **Prefix** | **Namespace** | **Description** |
| SOAP: |  | SOAP |
| SAML: |  | SAML Assertion |
| xi: |  | Xinclude |
| xs: |  | XML Schema |
| xsl: |  | XSLT |

Table – Namespace Prefixes

### Specification References

Specifications are referenced throughout this document by the use of bold/italic text to indicate a specific specification being referenced. Specifications are referenced to indicate that implementers should refer to that documentation for final conformance language and guidance. An example is shown below:

For conformance language, please refer to the IHE XCA profilefor further details

Working code examples are also provided in this implementation guide. Because the examples are non-normative, examples may not be complete or fully accurate. The formal specification referred to by the example will take precedence.

### Use of Conformance Language

Conformance language is defined within this guidance to be closely aligned to the standard/profile it is drawn from. The use of conformance language within this document is limited to further constraints or relaxation of constraint on existing standards. New conformance language that specifically deviates from the underlying standard/profile is avoided wherever possible. Also, in those instances where new metadata is being specified, specific constraints are offered.

Conformance language is defined throughout this implementation guide using **BOLD** and CAPS to denote the conformance criteria to be applied. The conformance language that is used in this implementation guide is drawn from RFC 2219.

* **SHALL/MUST**: an absolute requirement for all implementations
* **SHALL NOT**: an absolute prohibition against inclusion for all implementations
* **SHOULD/SHOULD NOT**: A best practice or recommendation to be considered by implementers within the context of their requirements; there may be valid reasons to ignore an item, but the full implications must be understood and carefully weighed before choosing a different course
* **MAY**: This is truly optional language for an implementation; can be included or omitted as the implementer decides with no implications

The Consolidated Conformance Verb Matrix included as part of the HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, Release 1 (shown below) summarizes how the different standards/profiles are used within the implementation guide:

| **RFC 2119** | **HL7** | **IHE** |
| --- | --- | --- |
| SHALL  Absolute requirement of the specification | SHALL  Required/Mandatory | R (Required)  Element must be present but can be NULL. |
| SHALL NOT  Absolute prohibition of the specification | SHALL NOT  Not Required/Mandatory | - |
| SHOULD  Recommended  There may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. | SHOULD  Best Practice or Recommendation | R2 (Required if known)  The sending application must be able to demonstrate that it can send all required if known elements, unless it does not in fact gather that data. If the information cannot be transmitted, the data element contains a value indicating the reason for omission of the data. |
| SHOULD NOT  Not Recommended | SHOULD NOT  Not Recommended | - |
| MAY  Optional | MAY  Accepted/Permitted | O (Optional) |
| - | - | C (Conditional)  A conditional data element is one that is required, required if known or optional depending upon other conditions. |

Table 5 – Consolidated Conformance Verb Matrix DAF IG

The use of the word “recommendation” is also used in this documentation. Recommendation is used to offer implementers flexibility in their environments, by recommending an approach to be followed while not constraining in any way the use of alternative options. Recommendations are primarily used in those areas where the S&I Framework requests further implementation feedback from implementers and pilot sites prior to defining conforming criteria.

Optionality is defined for implementers for each of the metadata elements that were outlined within this implementation guide, using IHE guidelines:

|  |  |
| --- | --- |
| Required | Element must be present and CANNOT BE NULL (no NULL flavors allowed). |
| Required if Known | The sending system must be able to demonstrate that it can send all required elements, unless it does not gather that data. If the information cannot be transmitted, the data element contains a value indicating the reason for omission of the data. |
| Optional | No need to include unless the implementer so desires. |
| Conditional | A conditional data element is one that is required, required if known or optional depending upon other conditions.  Implementers have some latitude to apply conditions to specific metadata or other data elements that do not apply to their environment. |

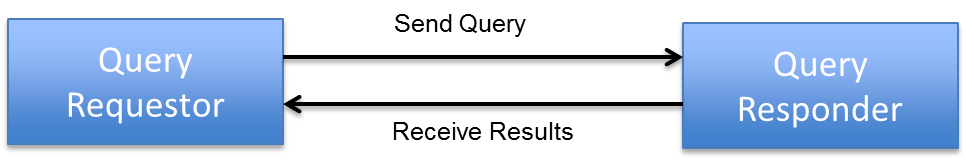
Table – Optionality Definition

## Data Access Framework Enhancements to Standards and Profiles

The following are a summary of additional changes to the standards and profiles used for DAF

## Scope of DAF Technical Approach

[DAF Use Cases and User Stories](http://wiki.siframework.org/DAF+Use+Cases) were used to derive the technical approach discussed below. The DAF Technical Approach scope can be described using the following diagram where a Query Requestor actor sends a query to a Query Responder actor who processes the query and responds to the Query Requestor with the results of the query.



The following table outlines the requirements that are in-scope for the DAF Technical Approach for each actor.

| **Actor** | **DAF Requirements** |
| --- | --- |
| Query Requesting Application | 1. Generate a query for patient data or documents 2. Assemble authentication, authorization and consent information 3. Package the request in a specified standardized format |
| Query Responding Application | 1. Authenticate requesting application credentials and validate authorization for data access 2. Identify patient data that matches the query 3. Make determination to release patient data 4. Transform queried patient data in a specified standardized format 5. Package the response in a specified standardized format |

The following table outlines specific queries that are in-scope for the DAF Technical Approach based on the DAF Use Cases and user stories.

| **DAF Queries** |
| --- |
| Find Document(s) based on Patient Identifiers |
| Find Document(s) based on Patient Demographics |
| Get Document(s) based on Patient Identifiers |
| Get Document(s) based on Patient Demographics |
| Get Document(s) based on Document Identifiers |
| Get Document(s) for multiple patients based on patient identifiers |
| Find Patient Identifiers based on Patient Demographics |
| Find Patient Demographics based on Patient Identifiers |

In addition to the above requirements and queries the following supporting capabilities are in-scope for the DAF Technical Approach.

| **DAF Supporting Capabilities** |
| --- |
| Provide message integrity and confidentiality of queries and results exchanged between the Query Requestor and the Query Responder |
| Ability to provide user and system identities as necessary for authentication and authorization |
| Ability to tag the queries and the query results with security metadata that will enable policy enforcement for query execution and data disclosure |

The next section defines the DAF Technical Approach and identifies the standards that have been selected to support the necessary requirements outlined in this section.

# DAF Technical Approach – Query Stacks and Building Blocks

The DAF Technical Approach outlines the various building blocks that will be used to implement the DAF Use Cases. The building blocks used by the DAF Technical Approach are shown in the Figure below.

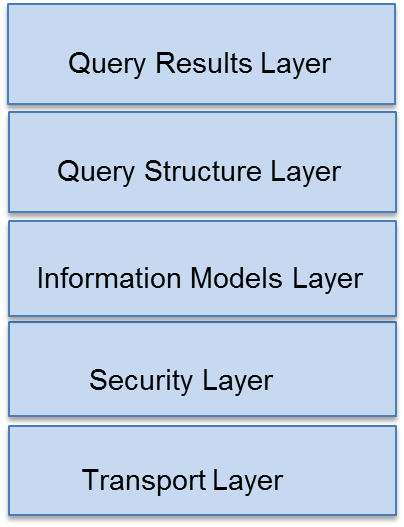


Figure –Building Blocks – Data Access Framework Technical Approach

The DAF Technical Approach building blocks are defined in the table below.

| **Building Block** | **Purpose** |
| --- | --- |
| Transport Layer | * Transport Layer defines the standards and specifications used to transport queries and query results between the Query Requestor and the Query Responder. An example standard would be HTTP. * Transport Layer also identifies the standards used to package the queries and query results along with the necessary metadata. These standards typically bridge the generic transport standards like HTTP to specific domains like healthcare. An example standard would be SOAP 1.2 which is used to bridge HTTP and the healthcare specific queries. |
| Security Layer | * The layer is used to specify standards for various security aspects which include the following   + Authentication   + Access Control and Authorization   + Message Integrity   + Confidentiality   + Auditing   + Disclosure requirements   + Consent   + Security Metadata for Query and Query Results to enable any of the above security functions |
| Information Models Layer | * The layer is used to specify the information models and the corresponding data definitions that are used to define the queries and the query results. |
| Query Structure Layer | * Query Structure Layer is used to specify the standards, vocabularies and value sets that will be used to construct queries. |
| Query Results Layer | * Query Results Layer is used to specify the standards, vocabularies and value sets that will be used to construct query results. |

The DAF building blocks defined above are chosen to minimize the impact of changes in a particular layer propagating to the other layers. For example, changing the standards used for security functions should have minimal effect on query structure and query results. Similarly changes to query structure or query results should also have minimal impact on the standards used to transport queries.

## Query Stack

The DAF Technical Approach building blocks defined above is called a Query Stack for the purposes of DAF and will be referenced throughout the document going forward.

## DAF Query Execution Context (Governance)

The context in which a DAF query is executed has a larger impact on the standards specified in the Security Layer. In order to define these standards it is important to define the various contexts in which a DAF query is executed. The DAF query execution context is sometimes also referred to as the governance model under which the query is executed. The next few paragraphs define the various contexts in which a DAF query can be executed.

### Local or Intra-Enterprise

In the context of a Local or Intra-Enterprise query, a single enterprise controls both the Query Requesting Application and the Query Responding Application and hence will prescribe the necessary and appropriate security controls for this to occur. The controls will be based on additional security controls that are already in place within the enterprise.

### Targeted or Inter-Enterprise

In the context of a Targeted or Inter-Enterprise query, Query Requesting Application and Query Responding Application belong to two different organizations which have two distinct security domains. In order to execute a query across security domains, each query request and the corresponding query results will require the appropriate security information such as authentication information, authorization information etc.

## Query Stacks and Modularity

A modular approach is used to define the DAF Query Stack. The standards defined by each layer of the Query Stack need to be independent of the other layers. For example if the query structure uses ebRIM/ebXML based standards and query results uses C-CDA document standards, changes to standards in either layer should have minimal to no-effect on each other and similarly should have minimal effect on the transport and security standards selected.

This modular capability of the Query Stack will allow for evolution of DAF use cases in a flexible manner, whereby a new DAF use case can prescribe new standards for query structures while reusing the standards for security, transport and query results.

## Query Stacks and Substitutability

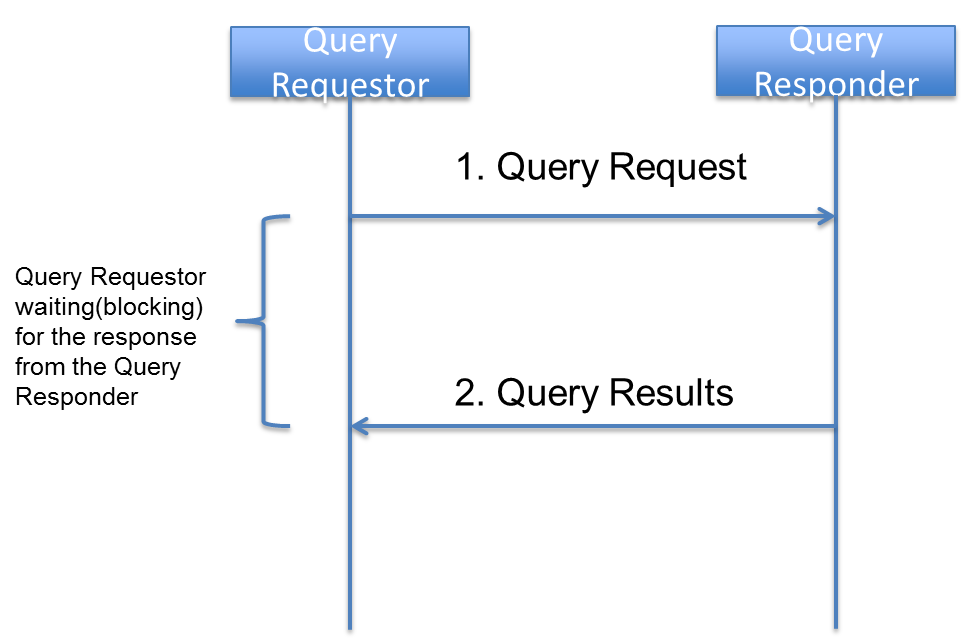
A modular Query Stack lends itself to substitutability of standards as use cases and requirements change. The ability to introduce or vary the standards within a layer of the query stack is called substitutability. For example, systems currently may use HTTP based SOAP transport as the mechanism to transport queries and query results. However as standards evolve there may be a need to incorporate SMTP based standards to transport queries and query results. This is feasible in a modular query stack where the structures defined by the other layers can be reused with the appropriate bindings (message structures) for the transport mechanism chosen. For example instead of using SOAP bindings for HTTP stack, a new standard might use a MIME binding along with SMTP stack to carry the payload which contains security, query and query results information.

## DAF Behavior Models Supported

The DAF Behavior Models define the flow of activities between actors and systems and the corresponding requirements which need to be supported by the standards selected for the transport layer. The following behavior models need to be supported by DAF.

### Synchronous Request/Response model

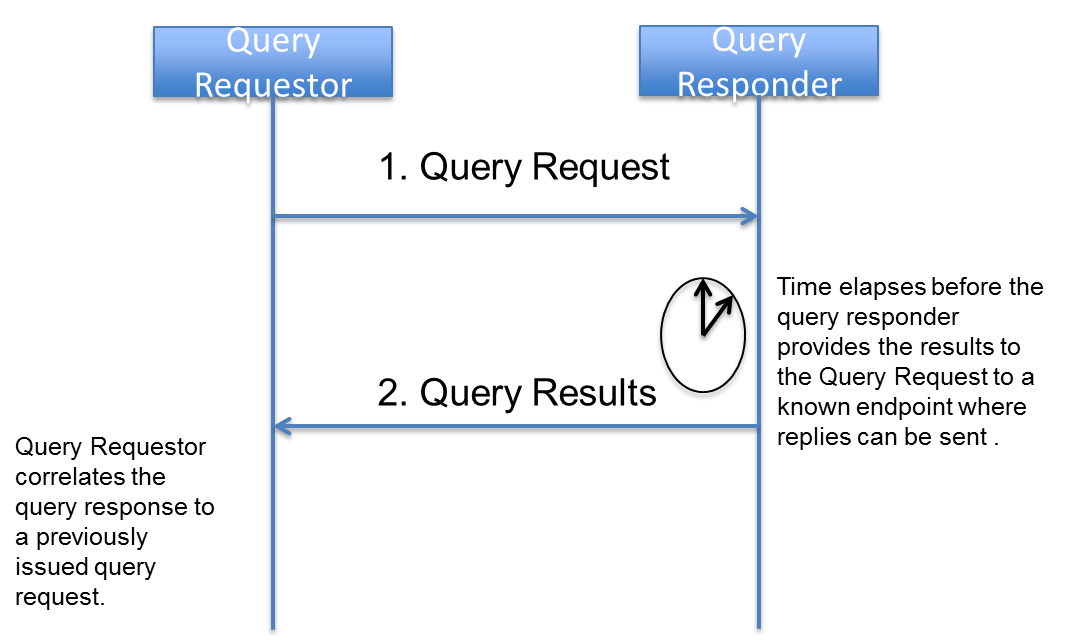
The Synchronous Request/Response model is one in which, a Query Requestor makes a request (1), and a Query Responder (2) replies to the request, providing the results in a single interaction. In a Synchronous Request/Response model the Query Requestor is waiting (blocking) for the Query Responder to send the results back. This model is appropriate for queries which are not time intensive and can return the results within 30 seconds to 60 seconds. The 30 seconds to 60 seconds is configured by enterprises based on their security policies. However web transactions typically timeout after 30 seconds.



An organization implementing DAF queries using Synchronous Request/Response models needs to consider SLA’s for the systems involved to ensure robustness in query/response behavior.

### Asynchronous Request/Response model

The Asynchronous Request/Response model is one in which, a Query Requestor makes a request (1), and a Query Responder (2) replies to the request with the results typically after a time lag. It is important to understand that the “asynchronous” nature of the response here refers to the application results being delivered and not to responses and acknowledgements that happen as part of transport protocols such as HTTP and SMTP. In this model, there is an inherent need to correlate the query request to the query response. In an asynchronous model, the Query Requestor submits a query and does not wait for a response from the Query Responder; hence the Query Responder needs to know the end point to return the response when the response is ready. This information is provided as part of the Query Request which is reused by the Query Responder when the response is ready.

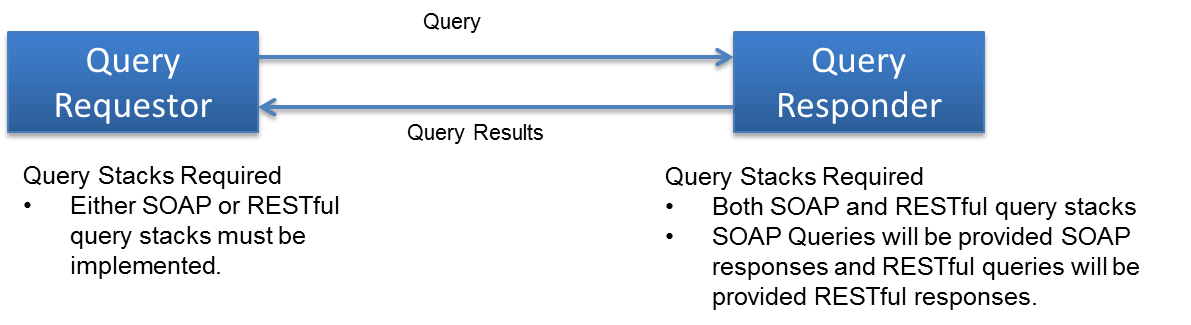


An organization implementing DAF queries using Asynchronous Request/Response models needs to consider SLA’s for the systems involved to ensure robustness in query/response behavior because a Query Requestor cannot wait infinitely for a Query Response and there has to be a timeout setup after which the response is not valuable or not desired.

As DAF use cases and requirements evolve the behavior models could be expanded as necessary.

## DAF Query Stacks and Standards

The DAF Candidate Standards and the corresponding analysis [are documented in the DAF IHE white paper](http://ihe.net/uploadedFiles/Documents/PCC/IHE_PCC_White_Paper_DAF_Rev1.1_2014-10-24.pdf). After performing the necessary environment scans, obtaining industry feedback, and HITSC feedback. DAF will be specifying two different Query Stacks for Document Metadata based access to data. The first one is called is the SOAP Query Stack and the second one is called the RESTful Query Stack. The names SOAP and RESTful were chosen based on the bindings and packaging that is used to transport security information, query structures and query results. The diagram below shows the abstract model and the query stacks to be used.



While there are many vendor systems who have implemented the SOAP Query Stack, many of the newer platforms and systems are using RESTful Query Stacks. In order to enable these systems to interoperate and provide an eco-system where queries can thrive, DAF will be specifying the following

* A Query Requestor MAY choose either the SOAP Query Stack or the RESTful Query Stack to implement DAF queries. (CONF: 1)
* A Query Responder MUST implement both the SOAP Query Stack and the RESTful Query Stack to support interoperability. (CONF: 2)

### SOAP Query Stack

The following is a detailed description of the SOAP Query Stack and its components for the various DAF Queries.



### RESTful Query Stack

The following is a detailed description of the RESTful Query Stack and its components for the various DAF Queries.

# DAF Implementation Guidance – SOAP Query Stack

This section explains the SOAP Query Stack in detail and provides necessary implementation guidance for implementers.

## SOAP Query Stack Standards Summary

Describe the SOAP Query Stack and the various components in detail.

## Transport and Application Protocol Implementation

The SOAP Query Stack uses [Transport Layer Security](http://www.ietf.org/rfc/rfc2246.txt) protocol along with [Hyper Text Transfer Protocol](https://www.ietf.org/rfc/rfc2616.txt) and [Simple Object Access Protocol](http://www.w3.org/TR/2007/REC-soap12-part1-20070427/) to send queries and receive responses. The specific implementation guidance to implement these protocols for DAF Document based access is outlined in this section.

### Authentication, Message Integrity and Message Confidentiality

In the context of DAF, it is important to authenticate the Query Requestor and the Query Responders to ensure that communication is happening between trusted systems. This is achieved via TLS where both clients and servers are authenticated with each other. The TLS protocol also provides message integrity and confidentiality. For interoperability the following requirements are outlined for DAF actors.

* DAF Query Requestors and Query Responders MUST implement requirements from the [IHE ATNA profile](http://wiki.ihe.net/index.php?title=Audit_Trail_and_Node_Authentication) Authenticate Node Transaction (ITI-19) in section [IHE ITI-2a: 3.19 Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf) to secure the communication channel between each other. (CONF: 100)

### SOAP 1.2 Implementation Guidance

The IHE profiles selected for the SOAP Query Stack use SOAP web services as the application protocols based on HTTP and provides the necessary packaging mechanism for various payloads. In order to enable interoperability at the application protocol layer the following requirements are outlined for DAF actors.

* DAF Query Requestor and Query Responder MUST implement requirements from [Appendix V: Web Services for IHE Transactions](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf) in [IHE ITI Volume 2 Appendices Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf). (CONF: 110)

## Query Implementation

DAF Document based queries will be created using the XDS Metadata along with XCA for single patient queries and using MPQ for multi-patient queries.

### DAF Queries and XDS Metadata

The query parameters for DAF Queries are constructed using XDS metadata. The metadata is common to multiple IHE profiles and is encoded using ebRIM/ebRS specifications for XCA, XDS and XDR profiles. Shared vocabulary and value sets are necessary for interoperability between Query Requestors and Query Responders. This shared vocabulary and value sets are represented in the XDS metadata.

* DAF Query Requestor and Query Responder MUST use the [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) to construct the following DAF Document Metadata based queries. (CONF: 150)
  + Find Documents for a single patient based on Patient Identifiers
  + Get Documents for a single patient based on Patient Identifiers
  + Get Documents based on Document Identifiers
  + Find Documents for multiple patients based on Patient Identifiers
* DAF Query Requestor and Query Responder MUST use the [Message Information Model of the Patient Registry Query By Patient Demographics in section 3.55.4.1.2.2 of IHE XCPD Rev2.4 profile](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCPD.pdf) to construct the following DAF Patient Demographics related queries. (CONF: 175)
  + Find Patient Id based on Patient Demographics

### 3.3.2 Using XCA for DAF

In the context of DAF [IHE XCA](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf) profile is used to perform discovery of documents and retrieval of documents for a single patient both within the context of LDAF (Intra-Enterprise) and TDAF (Inter-Enterprise).

The following is a mapping of DAF Actors/transactions to XCA Actors/transactions based on [IHE XCA profile Rev 2.1](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)

|  |  |
| --- | --- |
| DAF Actor or Transaction | XCA Actor or Transaction |
| Query Requestor | Initiating Gateway |
| Query Responder | Responding Gateway |
| Find Documents for single patient based on patient identifiers. | Registry Stored Query (Local context)  Cross Gateway Query (Targeted context) |
| Get Documents for a single patient based on patient identifiers  Get Documents based on Document Identifiers | Retrieve Document Set (Local context)  Cross Gateway Retrieve (Targeted context) |

The specific transactions and options that must be supported for DAF based on [IHE XCA profile Rev 2.1](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf) are outlined below.

* For DAF Query Requestor MUST implement the following XCA transactions. (CONF: 200)
  + [Cross Gateway Query (ITI -38)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
  + [Cross Gateway Retrieve (ITI -39)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
  + [Registry Stored Query (ITI-18)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
  + [Retrieve Document Set(ITI-43)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
* For DAF Query Requestor MUST implement the following XCA options. (CONF: 210)
  + [XDS Affinity Domain Option](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
  + [Asynchronous Web Services Exchange](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
* For DAF, Query Responders MUST implement the following XCA transactions. (CONF: 220)
  + [Cross Gateway Query (ITI -38)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
  + [Cross Gateway Retrieve (ITI -39)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
* For DAF, Query Responders MUST support the following behavior model. (CONF: 280)
  + Asynchronous Web Services following [Appendix V: Web Services for IHE Transactions](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf) in [IHE ITI Volume 2 Appendices Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf).

### 3.3.3 Using MPQ for DAF

In the context of DAF [IHE MPQ](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf) profile is used to find documents for multiple patients. This is only applicable within the context of LDAF (Intra-Enterprise). While MPQ profile could be used across enterprises with the right security controls, the policies required to enable these multi-patient queries across are still evolving and as a result in DAF, MPQ is only used for LDAF.

The following is a mapping of DAF Actors/transactions to MPQ Actors/transactions based on IHE MPQ profile documented in [IHE ITI TF Volume 2b Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf).

|  |  |
| --- | --- |
| DAF Actor or Transaction | MPQ Actor or Transaction |
| Query Requestor | Document Consumer |
| Query Responder | Document Registry |
| Find Documents for multiple patients based on patient identifiers. | Multi-patient Stored Query (Local context) |

The specific transactions and options that must be supported for DAF based on IHE MPQ profile documented in [IHE ITI TF Volume 2b Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf) are outlined below.

* For DAF, Query Requestor MUST implement the following MPQ transactions. (CONF: 250)
  + [Multi-patient Stored Query (ITI-51)](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf)
* For DAF, Query Requestor MUST support the following behavior model. (CONF: 260)
  + Asynchronous Web Services following [Appendix V: Web Services for IHE Transactions](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf) in [IHE ITI Volume 2 Appendices Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf).
* For DAF, Query Responders MUST implement the following MPQ transactions. (CONF: 270)
  + [Multi-patient Stored Query (ITI-51)](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf)
* For DAF, Query Responders MUST support the following behavior model. (CONF: 280)
  + Asynchronous Web Services following [Appendix V: Web Services for IHE Transactions](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf) in [IHE ITI Volume 2 Appendices Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf).

### 3.3.4 Anatomy of a DAF Sample Query

#### Find documents for a single patient based on patient identifiers for LDAF

#### Find documents for a single patient based on patient identifiers for TDAF

#### Find documents for a single patient based on patient identifiers using Asynchronous Web Services

#### Find documents for multiple patients based on patient identifiers for LDAF

#### Find documents for multiple patients based on patient identifiers using Asynchronous Web Services

#### Retrieve documents based on document identifiers for LDAF

#### Retrieve documents based on document identifiers for TDAF

#### Retrieve documents based on document identifiers using Asynchronous Web Services

#### Find Patient Identifiers based on Patient Demographics

## Query Results Implementation

DAF Document Metadata based Access queries are expected to return clinical documents as query results. These clinical documents may conform to different formats and hence may require additional processing by Query Requestor before they can be made available to downstream systems. To facilitate interoperability between Query Requestors and Query Responders with minimum capabilities the next few sections outline specific requirements for Query Result structures.

### Query Results

The advancement of MU2 regulation and certification of EHR technology allows for using the certified technology and leveraging the MU2 objectives to support DAF Query Results.

* For DAF queries related to CDA documents, Query Responders MUST create a C-CDA document following the MU2 requirements outlined in the [MU2 Companion Guide](file:///C:/Business/Drajer/Contracts/Ai/SIT%20Platform%20TO/DAF/TechnicalWorkGroup/Document%20Based%20WG/Implementation%20Guide/•%09http:/www.hl7.org/documentcenter/public/ballots/2013SEP/downloads/CDA_SIFRAME_CCG2CCDA_R1_I1_2013SEP.zip). (CONF: 300)
  + NOTE: For DAF queries related to non-CDA documents, Query Responders may choose appropriate documents to provide the query results.
* Query Responders MUST include metadata from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) as part of the query results to facilitate processing by Query Requestors.

## Security Implementation

The section provides security requirements for LDAF and TDAF.

### Local DAF Security Requirements

In the context of LDAF, enterprises may use a variety of local security controls to implement state, local, and institutional policies.

In the absence of comparable local applications, the IHE profiles cited in previous sections SHOULD be implemented. Each IHE profile has required actor groupings for security auditing via the IHE ATNA profile.

#### Risk Management

* The LDAF SHALL establish a risk analysis and management regime that conforms to HIPAA security regulatory requirements.
  + US Federal systems SHOULD conform to the risk management and mitigation requirements defined in NIST 800 series documents. This SHOULD include security category assignment in accordance with NIST 800-60 vol. 2 Appendix D.14.

#### Consistent Time

* All computing nodes in the LDAF SHALL reference a single time source according to the IHE CT profile. This establishes a common time base for security auditing, as well as clinical data records, among computing systems.

#### Auditing

* For HIPAA compliance, the LDAF SHOULD implement security auditing for all local applications that perform functions comparable to the IHE profiles cited in previous sections, and MAY implement an IHE ATNA repository for recording audit events.
* When IHE profiles are implemented, the LDAF SHALL implement the required actor groupings for IHE ATNA auditing and SHALL implement an IHE ATNA repository for recording.
* Reviews of audit data SHOULD be performed as part of HIPAA-compliant risk management.
  + The LDAF MAY merge ATNA and non-ATNA audit repositories, collated by time-stamps, prior to performing audit reviews.

#### Authentication and Authorization

* In cases where the personal identity and authorities of a data source or consumer must be assured, the system SHALL perform user authentication and authorization.
  + Query Requestors and Query Responders SHOULD support mutual authentication of the systems per the Authenticate Node transaction for HTTP connections per [IHE ATNA profile](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Node_Authentication_Security_2004_08-15.pdf).
    - US Federal systems SHOULD conform with authentication and authorization control requirements, per risk management guidelines in NIST 800-series documents, with particular reference to security controls documented in NIST 800-53.
  + User authentication and authorization SHOULD be uniformly implemented on all end-users’ computing systems via an LDAF method.
    - User authentication MAY be implemented per the IHE EUA profile.
* In cases where the provenance, authenticity, integrity, and accountability must be established, the user’s personal identity for concurrent or later review:
  + SHOULD be recorded in a local audit log for locally-implemented applications that perform functions comparable to the IHE profiles cited in previous sections
  + SHALL be recorded in an IHE ATNA conformant audit log when IHE profiles are implemented.
  + MAY be recorded with the associated data itself, in cases where data provenance must persist.
* Authentication or authorization failures SHALL produce a negative response to the requestor and SHALL be recorded in an audit log – system or ATNA - depending on implementation-specific capabilities.
* Organizations MAY implement additional authentication and authorization policies per their state, local, and institutional requirements.

#### Confidentiality

* As determined by the risk management plan, the LDAF MAY implement data encryption to:
  + Protect the confidentiality of data in transit. This MAY be encryption as specified in the IHE ATNA profile.
    - US Federal systems SHOULD conform to FIPS PUB 140-2.
  + Protect the confidentiality of data at rest. The method used is outside the score of DAF implementation guidance.

#### Security Metadata in Queries and Query Results

The XDS metadata has security related elements which are documented in Volume 3. These data elements can be used as part of the Queries and Query Results to enable various local policies.

* Query Requestors and Query Responders SHALL support processing of security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) which are present as part of queries and query results.
* Query Requestors and Query Responders SHOULD include security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) as part of queries and query results as necessary for various transactions.
* Relevant security metadata SHALL be captured in ATNA audit records, in accordance with IHE profile requirements, for queries and results.

#### Managing Consent in Queries

* Organizations SHOULD implement consent requirements per their state, local, and institutional policies. However, and there are no mandatory requirements for consent in the LDAF context.
* Privacy preferences MAY be communicated per the IHE BPPC profile and MAY be addressed via the Data Segmentation for Privacy (DS4P) USA national extension.
  + Processing of patient consents for disclosure, per the IHE BPPC profile, SHALL be recorded in the ATNA audit log.
  + Segmentation of data, per the DS4P profile extension, MAY be recorded in the ATNA audit log.

### Targeted DAF Security Requirements

In the context of TDAF, enterprises SHALL coordinate their implementations’ mutual conformance to Federal, state, local, and institutional policies within a Business Associate Agreement that conforms with HIPAA security and privacy regulatory requirements.

The IHE profiles cited in previous sections SHALL be implemented. Each IHE profile has required actor groupings for security auditing via the IHE ATNA profile.

#### Risk Management

* Each partner in the TDAF SHALL establish a risk analysis and management regime that conforms with HIPAA security regulatory requirements
  + US Federal systems SHOULD conform to the risk management and mitigation requirements defined in NIST 800 series documents. This SHOULD include security category assignment in accordance with NIST 800-60 vol. 2 Appendix D.14.
  + Coordination of risk management and the related security and privacy controls – policies, administrative practices, and technical controls – SHALL be defined in the Business Associate Agreement.

#### Consistent Time

* All computing nodes in the TDAF SHALL reference a single time source according to the IHE CT profile. This establishes a common time base for security auditing, as well as clinical data records, among computing systems.
  + The selected time service SHALL be documented in the Business Associate Agreement.

#### Auditing

* Each partner in the TDAF SHALL implement local IHE ATNA repositories for recording audit events, per the required actor IHE profile actor groupings.
* Reviews of audit data SHOULD be performed as part of HIPAA-compliant risk management.
  + Each partner MAY merge ATNA and non-ATNA audit repositories, collated by time-stamps, prior to performing audit reviews.
  + Each partner MAY perform coordinated reviews of their audit repositories, e.g., as part of assuring conformance with Business Associate Agreement provisions.

#### User Authentication and Authorization Information

In the context of TDAF, User Authentication and Authorization are critical before data is accessed. The following is a mapping of DAF actors/transactions to IHE XUA actors/transactions.

|  |  |
| --- | --- |
| DAF Actor or Transaction | XUA Actor or Transaction |
| Query Requestor | X-Service User |
| Query Responder | X-Service Provider |
| Supply and Consumer User Assertions | Provide X-User Assertion |

* User authentication and authorization SHALL be uniformly implemented on all end-users’ computing systems via the IHE XUA profile.
  + Query Requestors and Query Responders SHALL support the Provide X-User Assertion transaction conforming to the IHE XUA profile outlined in [IHE ITI TF Volume 2b Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf)
  + Query Requestors and Query Responders SHALL support all the [IHE XUA++](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XUA-_Rev1-1_TI_2010-08-10.pdf) profile options.
* Query Requestors and Query Responders SHALL support authentication of the systems per the Authenticate Node transaction for HTTP connections per [IHE ATNA profile](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Node_Authentication_Security_2004_08-15.pdf).
  + US Federal systems SHOULD conform with authentication and authorizations control requirements, per risk management guidelines in NIST 800-series documents, with particular reference to security controls documented in NIST 800-53.
  + The Business Associate Agreement SHALL name mutually-trusted certificate authorities from which digital certificates will be obtained for the purposes of IHE ATNA node authentication.
    - Digital certificate management and provisioning MAY be a mutual activity for the TDAF partners.
* In cases where the provenance, authenticity, integrity, and accountability must be established, the user’s personal identity for concurrent or later review:
  + SHALL be recorded in each partner’s IHE ATNA conformant audit log.
  + MAY be recorded with the associated data itself, in cases where data provenance must persist.
* Authentication or authorization failures SHALL produce a negative response to the requestor and SHALL be recorded in the local partner’s ATNA audit log.
* Organizations MAY implement additional authentication and authorization policies per their state, local, and institutional requirements.

#### Confidentiality

* The TDAF SHALL implement data encryption to protect the confidentiality of data in transit. This SHALL be encryption as specified in the IHE ATNA profile.
  + US Federal systems SHOULD conform to FIPS PUB 140-2.
* Each TDAF partner MAY protect the confidentiality of data at rest. The method used is outside the score of DAF implementation guidance.

#### Security Metadata in Queries and Query Results

The XDS metadata has security related elements which are documented in Volume 3. These data elements can be used as part of the Queries and Query Results to enable various organization specific policies.

* Query Requestors and Query Responders SHALLT support processing of security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) which are present as part of queries and query results.
* Query Requestors and Query Responders SHOULD include security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) as part of queries and query results as necessary for various transactions.
  + ?
* Relevant security metadata SHALL be captured in each partner’s local ATNA audit records, in accordance with IHE profile requirements, for queries and results.

#### 3.5.2.3 Managing Consent in Queries

* Each TDAF partner SHALL implement coordinated consent requirements per their state, local, and institutional policies.
  + The Business Associate Agreement SHALL document the mutual consent requirements.
* Privacy preferences SHOULD be communicated per the IHE BPPC profile and SHOULD be addressed via the Data Segmentation for Privacy (DS4P) USA national extension.
  + Processing of patient consents for disclosure, per the IHE BPPC profile, SHALL be recorded in the ATNA audit log.
  + Segmentation of data, per the DS4P profile extension, MAY be recorded in the ATNA audit log.

## SOAP Query Examples

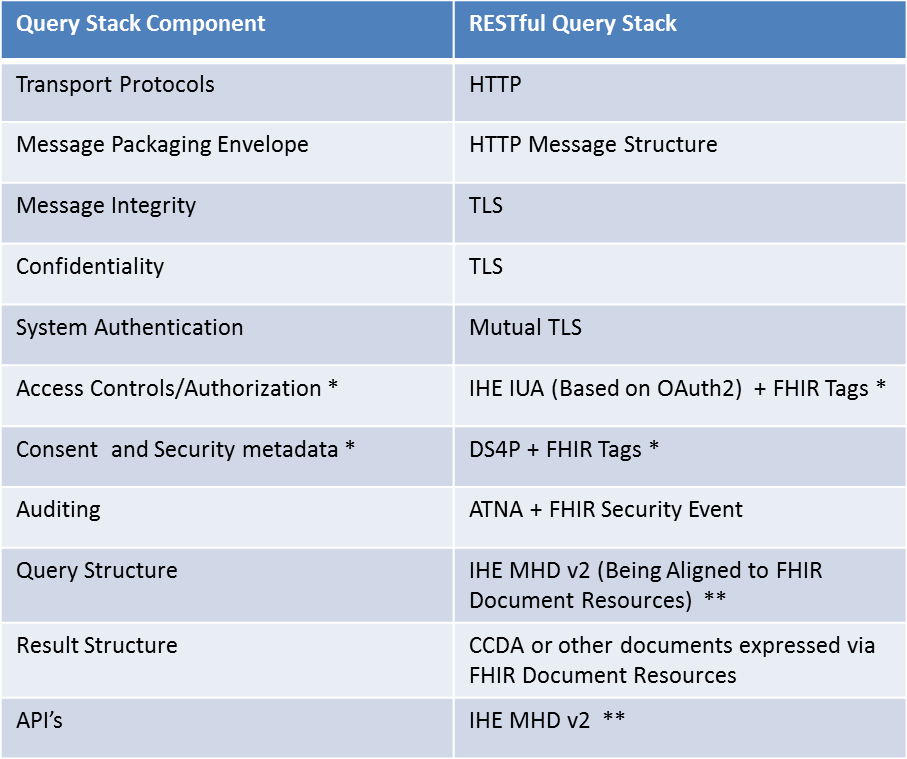
Give complete examples of how to use the various standards together in combinations to help implementers

# DAF Implementation Guidance – RESTful Query Stack

This section explains the RESTful Query Stack in detail and provides necessary implementation guidance for implementers.

## RESTful Query Stack Standards Summary

The following standards/profiles will be used for implementation of the RESTful Query Stack.



\* - Specifying profiles for Targeted DAF only, Local DAF choices left to the organization

\*\* - IHE MHDv2 aligns with FHIR and has been tested at the IHE NA 2014 New Directions Connectathon

## Transport and Application Protocol Implementation

The RESTful Query Stack uses [Transport Layer Security](http://www.ietf.org/rfc/rfc2246.txt) (TLS 1.0) protocol along with [Hyper Text Transfer Protocol](https://www.ietf.org/rfc/rfc2616.txt) and [RESTful](http://www.w3.org/TR/2007/REC-soap12-part1-20070427/) resources to send queries and receive responses. The specific implementation guidance to implement these protocols for DAF Document based access is outlined in this section.

### Authentication, Message Integrity and Message Confidentiality

In the context of DAF, it is important to authenticate the Query Requestor and the Query Responders to ensure that communication is happening between trusted systems. This is achieved via TLS where both clients and servers are authenticated with each other. The TLS protocol also provides message integrity and confidentiality. For interoperability the following requirements are outlined for DAF actors.

* DAF Query Requestors and Query Responders MUST implement requirements from the [IHE ATNA profile](http://wiki.ihe.net/index.php?title=Audit_Trail_and_Node_Authentication) Authenticate Node Transaction (ITI-19) in section [IHE ITI-2a: 3.19 Rev 10.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf) to secure the communication channel between each other. (CONF: 500) ???

### Implementation Guidance for RESTful Resources for Document Access

* Discuss HL7 FHIR / MHD v2 relationship
  + HL7 FHIR Document Reference resource
  + HL7 FHIR Document Manifest resource
* RESTful Operators that need to be supported
  + GET
* Encoding Requirements
  + Minimum of JSON

## Query Implementation

DAF Document based queries will be created using the XDS Metadata expressed as query parameters using the MHD APIs.

### DAF Queries and XDS Metadata

The query parameters for DAF Queries are constructed using XDS metadata. The metadata is common to multiple IHE profiles and is encoded as query parameters using the MHD API. Shared vocabulary and value sets are necessary for interoperability between Query Requestors and Query Responders. This shared vocabulary and value sets are represented in the XDS metadata.

* DAF Query Requestor and Query Responder MUST use the [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) to construct the following DAF Document Metadata based queries. (CONF: 550)
  + Find Documents for a single patient based on Patient Identifiers
  + Get Documents based on Document Identifiers
  + Find Documents for multiple patients based on Patient Identifiers
* Maybe reference PDQm profile for RESTful queries of patient identifiers

### 4.3.2 Using MHD for DAF

In the context of DAF MHD profile is used to perform discovery of documents and retrieval of documents for a single patient both within the context of LDAF (Intra-Enterprise) and TDAF (Inter-Enterprise).

The following is a mapping of DAF Actors/transactions to MHD Actors/transactions based on [IHE MHD profile Rev 1.3](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)

|  |  |
| --- | --- |
| DAF Actor or Transaction | MHD Actor or Transaction |
| Query Requestor | Document Consumer |
| Query Responder | Document Responder |
| Find Documents for single patient based on patient identifiers. | Find Document References (ITI-67) |
| Get Documents based on Document Identifiers | Retrieve Document (ITI-68) |

The specific transactions and options that must be supported for DAF based on [IHE MHD profile Rev 1.3](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf) are outlined below.

* For DAF, Query Requestor MUST implement the following MHD transactions. (CONF: 600)
  + [Find Document References (ITI -67)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
  + Retrieve Document (ITI-68)
* For DAF, Query Responders MUST implement the following MHD transactions. (CONF: 620)
  + [Find Document References (ITI -67)](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf)
  + Retrieve Document (ITI-68)
* Currently only synchronous queries (Request/Response Behavior Model)

### 4.3.3 Querying for Documents related to Multiple Patients

In the context of DAF [MHD v2](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf) profile is used to find documents for each patient one at a time. In other words there is no current capability to find documents related to multiple patients in the existing IHE MHD transactions. So the Use Case requirement has to be accomplished by finding documents related to each patient one at a time. Queries for multiple patients are applicable only within the context of LDAF (Intra-Enterprise) because the necessary policies required to enable these multi-patient queries across enterprises are still evolving.

## Query Results Implementation

DAF Document Metadata based Access queries are expected to return clinical documents as query results. These clinical documents may conform to different formats and hence may require additional processing by Query Requestor before they can be made available to downstream systems. To facilitate interoperability between Query Requestors and Query Responders with minimum capabilities the next few sections outline specific requirements for Query Result structures.

### Query Results

The advancement of MU2 regulation and certification of EHR technology allows for using the certified technology and leveraging the MU2 objectives to support DAF Query Results.

* For DAF queries related to CDA documents, Query Responders MUST create a C-CDA document following the MU2 requirements outlined in the [MU2 Companion Guide](file:///C:\Business\Drajer\Contracts\Ai\SIT%20Platform%20TO\DAF\TechnicalWorkGroup\Document%20Based%20WG\Implementation%20Guide\•%09http:\www.hl7.org\documentcenter\public\ballots\2013SEP\downloads\CDA_SIFRAME_CCG2CCDA_R1_I1_2013SEP.zip). (CONF: 700)
  + NOTE: For DAF queries related to non-CDA documents, Query Responders may choose appropriate documents to provide the query results.
* Query Responders MUST include metadata from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) as part of the query results to facilitate processing by Query Requestors.

## Security Implementation

### Local DAF Security Requirements

In the context of LDAF, enterprises may use a variety of local security controls to implement state, local, and institutional policies.

In the absence of comparable local applications, the IHE profiles cited in previous sections SHOULD be implemented. Each IHE profile has required actor groupings for security auditing via the IHE ATNA profile.

#### Risk Management

* The LDAF SHALL establish a risk analysis and management regime that conforms to HIPAA security regulatory requirements.
  + US Federal systems SHOULD conform to the risk management and mitigation requirements defined in NIST 800 series documents. This SHOULD include security category assignment in accordance with NIST 800-60 vol. 2 Appendix D.14.

#### Consistent Time

* All computing nodes in the LDAF SHALL reference a single time source according to the IHE CT profile. This establishes a common time base for security auditing, as well as clinical data records, among computing systems.

#### Auditing

* For HIPAA compliance, the LDAF SHOULD implement security auditing for all local applications that perform functions comparable to the IHE profiles cited in previous sections, and MAY implement an IHE ATNA repository for recording audit events.
* When IHE profiles are implemented, the LDAF SHALL implement the required actor groupings for IHE ATNA auditing and SHALL implement an IHE ATNA repository for recording.
* Reviews of audit data SHOULD be performed as part of HIPAA-compliant risk management.
  + The LDAF MAY merge ATNA and non-ATNA audit repositories, collated by time-stamps, prior to performing audit reviews.

#### Authentication and Authorization

* In cases where the personal identity and authorities of a data source or consumer must be assured, the system SHALL perform user authentication and authorization.
  + Query Requestors and Query Responders SHOULD support mutual authentication of the systems per the Authenticate Node transaction for HTTP connections per [IHE ATNA profile](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Node_Authentication_Security_2004_08-15.pdf).
    - US Federal systems SHOULD conform with authentication and authorization control requirements, per risk management guidelines in NIST 800-series documents, with particular reference to security controls documented in NIST 800-53.
  + User authentication and authorization SHOULD be uniformly implemented on all end-users’ computing systems via an LDAF method.
    - User authentication MAY be implemented per the IHE EUA profile.
* In cases where the provenance, authenticity, integrity, and accountability must be established, the user’s personal identity for concurrent or later review:
  + SHOULD be recorded in a local audit log for locally-implemented applications that perform functions comparable to the IHE profiles cited in previous sections
  + SHALL be recorded in an IHE ATNA conformant audit log when IHE profiles are implemented.
  + MAY be recorded with the associated data itself, in cases where data provenance must persist.
* Authentication or authorization failures SHALL produce a negative response to the requestor and SHALL be recorded in an audit log – system or ATNA - depending on implementation-specific capabilities.
* Organizations MAY implement additional authentication and authorization policies per their state, local, and institutional requirements.

#### Confidentiality

* As determined by the risk management plan, the LDAF MAY implement data encryption to:
  + Protect the confidentiality of data in transit. This MAY be encryption as specified in the IHE ATNA profile.
    - US Federal systems SHOULD conform to FIPS PUB 140-2.
  + Protect the confidentiality of data at rest. The method used is outside the score of DAF implementation guidance.

#### Security Metadata in Queries and Query Results

The XDS metadata has security related elements which are documented in Volume 3. These data elements can be used as part of the Queries and Query Results to enable various local policies.

* Query Requestors and Query Responders SHALL support processing of security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) which are present as part of queries and query results.
* Query Requestors and Query Responders SHOULD include security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) as part of queries and query results as necessary for various transactions.
* Relevant security metadata SHALL be captured in ATNA audit records, in accordance with IHE profile requirements, for queries and results.

#### Managing Consent in Queries

* Organizations SHOULD implement consent requirements per their state, local, and institutional policies. However, and there are no mandatory requirements for consent in the LDAF context.
* Privacy preferences MAY be communicated per the IHE BPPC profile and MAY be addressed via the Data Segmentation for Privacy (DS4P) USA national extension.
  + Processing of patient consents for disclosure, per the IHE BPPC profile, SHALL be recorded in the ATNA audit log.
  + Segmentation of data, per the DS4P profile extension, MAY be recorded in the ATNA audit log.

### Targeted DAF Security Requirements

In the context of TDAF, enterprises SHALL coordinate their implementations’ mutual conformance to Federal, state, local, and institutional policies within a Business Associate Agreement that conforms with HIPAA security and privacy regulatory requirements.

* For RESTful implementations, the IHE IUA Authorization Server may be a third party system. In such cases, a distinct Business Partner Agreement SHALL be established and SHALL be coordinated among Query Requestor and Query Responder organizations.

The IHE profiles cited in previous sections SHALL be implemented. Each IHE profile has required actor groupings for security auditing via the IHE ATNA profile.

#### Risk Management

* TDAF Query Requestors, Query Responders, and Authorization Servers SHALL establish a risk analysis and management regime that conforms with HIPAA security regulatory requirements
  + US Federal systems SHOULD conform to the risk management and mitigation requirements defined in NIST 800 series documents. This SHOULD include security category assignment in accordance with NIST 800-60 vol. 2 Appendix D.14.
  + Coordination of risk management and the related security and privacy controls – policies, administrative practices, and technical controls – SHALL be defined in the Business Associate Agreements.

#### Consistent Time

* All computing nodes in the TDAF SHALL reference a single time source according to the IHE CT profile. This establishes a common time base for security auditing, as well as clinical data records, among computing systems.
  + The selected time service SHALL be documented in the Business Associate Agreements.

#### Auditing

* TDAF Query Requestors, Query Responders, and Authorization Servers SHALL implement local IHE ATNA repositories for recording audit events, per the required actor IHE profile actor groupings.
* Reviews of audit data SHOULD be performed as part of HIPAA-compliant risk management.
  + TDAF Query Requestors, Query Responders, and Authorization Servers MAY merge ATNA and non-ATNA audit repositories, collated by time-stamps, prior to performing audit reviews.
  + TDAF Query Requestors, Query Responders, and Authorization Servers MAY perform coordinated reviews of their audit repositories, e.g., as part of assuring conformance with Business Associate Agreement provisions.

#### User Authentication and Authorization Information

In the context of TDAF, User Authentication and Authorization are critical before data is accessed. The following is a mapping of DAF actors/transactions to IHE IUA actors/transactions.

|  |  |
| --- | --- |
| DAF Actor or Transaction | IUA Actor or Transaction |
| Query Requestor | Authorization Client |
| Query Responder | Resource Server |
| Supply of User Assertions | Authorization Server |

* User authentication and authorization SHALL be uniformly implemented on all end-users’ computing systems via the IHE IUA profile.
  + Query Requestors SHALL support the Get Authorization Token and Incorporate Authorization Token conforming to the IHE IUA profile outlined in [IHE ITI TF Volume 2c Rev 12.0](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf)
  + Query Responders SHALL support all the [IHE](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XUA-_Rev1-1_TI_2010-08-10.pdf) IUA profile options.
  + Identification of Authorization Servers and associated administrative requirements SHALL be documented in the Business Associate Agreement.
* Query Requestors, Query Responders, and Authorization Servers SHALL support authentication of the systems per the Authenticate Node transaction for HTTP connections per [IHE ATNA profile](http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Node_Authentication_Security_2004_08-15.pdf).
  + US Federal systems SHOULD conform with authentication and authorizations control requirements, per risk management guidelines in NIST 800-series documents, with particular reference to security controls documented in NIST 800-53.
  + The Business Associate Agreement SHALL name mutually-trusted certificate authorities from which digital certificates will be obtained for the purposes of IHE ATNA node authentication.
    - Digital certificate management and provisioning MAY be a mutual activity for the TDAF partners and the Authorization Servers.
* In cases where the provenance, authenticity, integrity, and accountability must be established, the user’s personal identity for concurrent or later review:
  + SHALL be recorded in Query Requestor’s and Query Responder’s IHE ATNA conformant audit log.
  + MAY be recorded with the associated data itself, in cases where data provenance must persist.
* Authentication or authorization failures SHALL produce a negative response to the requestor and SHALL be recorded in the local Query Requestor and Authorization Server’s ATNA audit logs.
* Organizations MAY implement additional authentication and authorization policies per their state, local, and institutional requirements.

#### Confidentiality

* The TDAF SHALL implement data encryption to protect the confidentiality of data in transit. This SHALL be encryption as specified in the IHE ATNA profile.
  + US Federal systems SHOULD conform to FIPS PUB 140-2.
* TDAF Query Requestors, Query Responders, and Authorization Servers MAY protect the confidentiality of data at rest. The method used is outside the score of DAF implementation guidance.

#### Security Metadata in Queries and Query Results

The XDS metadata has security related elements which are documented in Volume 3. These data elements can be used as part of the Queries and Query Results to enable various organization specific policies.

* Query Requestors and Query Responders SHALL support processing of security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) which are present as part of queries and query results.
* Query Requestors and Query Responders SHOULD include security metadata elements from [XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf) as part of queries and query results as necessary for various transactions.
* Relevant security metadata SHALL be captured in each partner’s local ATNA audit records, in accordance with IHE profile requirements, for queries and results.

#### Managing Consent in Queries

* Query Requestors and Query Responders SHALL implement coordinated consent requirements per their state, local, and institutional policies.
  + The Business Associate Agreement SHALL document the mutual consent requirements.
* Privacy preferences SHOULD be communicated per the IHE BPPC profile and SHOULD be addressed via the Data Segmentation for Privacy (DS4P) USA national extension.
  + Processing of patient consents for disclosure, per the IHE BPPC profile, SHALL be recorded in the ATNA audit log.
  + Segmentation of data, per the DS4P profile extension, MAY be recorded in the ATNA audit log.

## RESTful Query Examples

Give complete examples of how to use the various standards together in combinations to help implementers

# Appendix A - Acronyms and Definitions

The following table summarizes the acronyms and definitions used in this implementation guidance. Implementers should familiarize themselves with the definitions below, to ensure that examples and conformance statements, as well as the transactions and the standards/profiles used to represent them, are clearly understood.

| **Acronym** | **Definition** |
| --- | --- |
| ATNA | Audit Trail and Node Authentication |
| BPPC | Basic Patient Privacy Consent |
| C-CDA | HL7 Consolidated Clinical Document Architecture |
| CDA | HL7 Clinical Document Architecture |
| Consent Directive | Official preference by the consumer regarding the release of personal health record and personally/individually identifiable information to providers, payers, or others that may have access to patient health information |
| DAF | Data Access Framework |
| DS4P | S&I Data Segmentation for Privacy |
| DSTU | Draft Standard for Trial Use |
| ebRIM | OASIS Electronic Business Registry Information Model |
| ebRS | OASIS Electronic Business Services and Protocols |
| ebXML | OASIS Electronic Business using eXtensible Markup Language |
| EHR | Electronic Health Record |
| EMR | Electronic Medical Record |
| FIPS PUB 140-2 | The Federal Information Processing Standard (FIPS) Publication 140-2, a US government computer security standard used to accredit cryptographic modules. |
| Health IT | Healthcare Information Technology |
| HIPAA | Health Insurance Portability and Accountability: act that protects health insurance coverage for workers and their families when they change or lose their jobs |
| HITSC | Health Information Technology Standards Committee |
| HL7 | Health Level 7 International is a non-profit organization involved in development of international healthcare informatics interoperability standards |
| HL7 FHIR | HL7 Fast Healthcare Interoperability Resources, pronounced "fire" |
| HL7 v2.5.1 | HL7 healthcare messaging standard, version 2.5.1 |
| HTTP | Hypertext Transfer Protocol |
| IHE | Integrating the Healthcare Enterprise (IHE) is an initiative by healthcare professionals and industry to improve the information sharing and interoperability of healthcare systems |
| IHE ITI | IHE Information Technology Infrastructure |
| IHE PCC | IHE Patient Care Coordination |
| ITI TF | IT Infrastructure Technical Framework: a resource for users, developers and implementers of healthcare imaging and information systems |
| IUA | IHE Internet User Authentication profile |
| JSON | JavaScript Object Notation, a data interchange format |
| LDAF | Local Data Access Framework |
| MHD | IHE Mobile access to Health Documents profile |
| MPQ | IHE Multi-Patient Queries profile |
| MU2 | Meaningful Use level 2 |
| NIST 800 | National Institute of Standards and Technology SP 800 series of computer security publications |
| OASIS | A standards development organization responsible for the XML, ebXML, SAML, XSLT, and SOAP web security specifications |
| ONC | Office of the National Coordinator |
| QRDA | HL7 Quality Reporting Document Architecture |
| RESTful | Conforming to the W3C Representational State Transfer (REST) software architecture style |
| S&I | Standards and Interoperability (S&I) Framework upon which the Data Segmentation Use Case was developed |
| SAML | Security Assertion Markup Language: an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). |
| Segmentation | A security concept for differentiating between data that are to be handled differently for privacy or security reasons. |
| SLA | Service-level agreement that defines measurements for acceptable performance in an information technology system and network |
| SOAP | Simple Object Access Protocol: A protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) for its message format, and usually relies on other Application Layer protocols, most notably Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. |
| TDAF | Targeted Data Access Framework |
| TLS | Transport Layer Security: cryptographic protocols that provide communication security over the internet |
| W3C | Wide World Web Consortium, an internet standards development organization |
| XCA | Cross-Community Access |
| XCPD | IHE Cross-community Patient Discovery profile |
| XDR | An IHE-developed standard that enables a number of healthcare delivery organizations belonging to an XDS Affinity Domain (e.g. a community of care) to cooperate in the care of a 730 patient by sharing clinical records in the form of documents as they proceed with their patients’ care delivery activities. |
| XDS | A profile created to facilitate cross-enterprise document sharing between institutions |
| XML | Extensible Markup Language: a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable |
| XSLT | Extensible Stylesheet Language Transformation: a declarative, XML-based language used for the transformation of XML documents |
| XUA | Cross-Enterprise User Assertion: An IHE-developed standard that provides a means to communicate claims about the identity of an authenticated principal (user, application, system, etc.) in transactions that cross enterprise boundaries |

Table – Key Acronyms and Definitions