Integrating the Healthcare Enterprise

IHE Patient Care Coordination (PCC)

US National Extension Implementation Guide

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

Draft for Public Comment

June 1, 2015

Please verify you have the most recent version of this document. See here for Trial Implementation and Final Text versions and here for Public Comment versions.

Foreword

This is an IHE PCC Implementation Guide.

This Implementation Guide is published on June 1, 2015 for public comment. Comments are invited and may be submitted at http://www.ihe.net/PCC_Public_Comments. In order to be considered by the IHE PCC Technical Committee, comments must be received by July 1, 2015.

This supplement may describe changes to the existing technical framework documents.

"Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume, if applicable.

Amend Section X.X by the following:

Where the amendment adds text, make the added text **bold underline**. Where the amendment removes text, make the removed text **~~bold strikethrough~~**. When entire new sections are added, introduce with editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.

General information about IHE can be found at: http://ihe.net.

Information about the IHE Patient Care Coordination domain can be found at: http://ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at: http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE IT Infrastructure Technical Framework can be found at: http://ihe.net/Technical_Frameworks.

CONTENTS

1 Introduction 5
1.1 Introduction to IHE 5
1.2 Overview of this Implementation Guide USA Extension 5
1.3 Comment Process 5
1.4 Copyright Licenses 6
1.4.1 Copyright of Base Standards 6
1.5 Trademark 6
1.6 Disclaimer Regarding Patent Rights 6
1.7 History of Document Changes 7
2 Overview of National Extensions 8
2.1 Scope of National Extensions 8
2.2 Process for Developing National Extensions 8
2.3 Process for Proposing Revisions to the Technical Framework 9
3 National Extensions for IHE USA 10
3.1 IHE USA Scope of Changes 10
Appendices 12
Appendix A – Data Access Framework (DAF) Document Metadata Based Access Implementation Guide 12
Copyrights 13
1 Open Issues 14
2 Introduction 15
2.1 Definition of Terms 15
2.2 Purpose of this Implementation Guide 17
2.3 Intended Audience and Goals 17
2.3.1 Pre-Requisite Knowledge 17
2.3.2 Reader Guidance 18
2.4 Assumptions and Pre-Conditions 19
2.4.1 Assumptions for Data Access Framework 19
2.4.2 Pre-Conditions for Data Access Framework 19
2.5 Structure of Implementation Guidance 20
2.5.1 Definition of Actors 21
2.5.2 Specification References 22
2.5.3 Use of Conformance Language 22
2.6 Scope of DAF Technical Approach 24
3 DAF Technical Approach – Query Stacks and Building Blocks 26
3.1 Query Stack 27
3.2 DAF Query Execution Context (Governance) 27
3.2.1 Local or Intra-Enterprise 27
3.2.2 Targeted or Inter-Enterprise 28
3.3 Query Stacks and Modularity 28
3.4 Query Stacks and Substitutability 28
3.5 DAF Behavior Models Supported 28

3.5.1 Synchronous Request/Response model 28
3.5.2 Asynchronous Request/Response model 29
3.6 DAF Query Stacks and Standards 30
3.6.1 SOAP Query Stack 31
3.6.2 RESTful Query Stack 32
4 DAF Implementation Guidance – SOAP Query Stack 34
4.1 Transport and Application Protocol Implementation 34
4.1.1 Authentication, Message Integrity and Message Confidentiality 34
4.1.2 SOAP 1.2 Implementation Guidance 34
4.2 Query Implementation 34
4.2.1 DAF Queries and XDS Metadata 34
4.2.2 Using XCA for DAF 35
4.2.3 Using MPQ for DAF 36
4.3 Query Results Implementation 37
4.3.1 Query Results 37
4.4 Security Implementation 37
4.4.1 Local DAF Security Requirements 37
4.4.2 Targeted DAF Security Requirements 40
4.5 SOAP Query Examples 43
4.5.1 Synchronous XCA Sample Query: 43
4.5.2 Synchronous XCA Sample Response 44
4.5.3 Asynchronous XCA Sample Query 45
4.5.4 Asynchronous XCA Sample Response 46
4.5.5 Synchronous Multipatient Query Example 48
4.5.6 Synchronous Multipatient Query Response Example 48
5 DAF Implementation Guidance – RESTful Query Stack 49
5.1 RESTful Query Stack Standards Summary 49
5.2 Transport and Application Protocol Implementation 50
5.2.1 Authentication, Message Integrity and Message Confidentiality 50
5.2.2 Implementation Guidance for RESTful Resources for Document Access 50
5.3 Query Implementation 50
5.3.1 DAF Queries and XDS Metadata 50
5.3.2 Using MHD for DAF 51
5.3.3 Querying for Documents related to Multiple Patients 52
5.4 Query Results Implementation 52
5.4.1 Query Results 52
5.5 Security Implementation 52
5.5.1 Local DAF Security Requirements 52
5.5.2 Targeted DAF Security Requirements 55
5.6 RESTful Query Examples 58
DAF Document Metadata Based Access Implementation Guide Appendices 59
Appendix A – Acronyms and Definitions 60
Appendix B – Document Sharing Metadata Constraints 62
B.1 Document Metadata 62

B.1.1 Class Code Value Set 63
B.1.2 Confidentiality Code Value Set 64
B.1.3 Healthcare Specialty 64
B.1.4 Format Code 65
B.1.5 Healthcare Facility Type Code 65
B.2 Submission Set Metadata 66
B.2.1 Submission Set Content Type 67
B.3 Folder Metadata 67

1 Introduction

This document, The Data Access Framework (DAF) Document Metadata Based Access Implementation Guide describes United States implementation guidelines for specific ITI transactions and content modules to meet United States ONC S&I Frameworks requirements for the Data Access Framework. This Implementation Guide was developed as a joint collaboration of ONC S&I Frameworks and IHE USA. This national extension is being submitted through PCC rather than ITI because of its focus on care coordination; this IG bundles and further constrains ITI profiles in specific document query use cases.

1.1 Introduction to IHE

Integrating the Healthcare Enterprise (IHE) is an international initiative to promote the use of standards to achieve interoperability among health information technology (HIT) systems and effective use of electronic health records (EHRs). IHE provides a forum for care providers, HIT experts and other stakeholders in several clinical and operational domains to reach consensus on standards-based solutions to critical interoperability issues.

The primary output of IHE is system implementation guides, called IHE profiles. IHE publishes each profile through a well-defined process of public review and Trial Implementation and gathers profiles that have reached Final Text status into an IHE Technical Framework, of which this volume is a part.

For more general information regarding IHE, refer to www.ihe.net. Intended Audience

The intended audience of IHE Technical Frameworks Volume 4 is:

- Those interested in integrating healthcare information systems and workflows on an international or country basis
- IT departments of healthcare institutions
- Technical staff of vendors participating in the IHE initiative
- Experts involved in standards development

1.2 Overview of this Implementation Guide USA Extension

This volume contains an Implementation Guide USA Extension. Section 2 describes the permitted scope of national extensions and the process by which national IHE initiatives can propose such extensions for approval by the IHE Technical Committee.

1.3 Comment Process

IHE International welcomes comments on this document and the IHE initiative. They can be submitted by sending an email to the co-chairs and secretary of the Patient Care Coordination Committee domain committees at PCC@ihe.net and the IHE USA Secretary at secretary@iheusa.net.

1.4 Copyright Licenses

IHE International hereby grants to each Member Organization, and to any other user of these documents, an irrevocable, worldwide, perpetual, royalty-free, nontransferable, nonexclusive, non-sublicensable license under its copyrights in any IHE profiles and Technical Framework documents, as well as any additional copyrighted materials that will be owned by IHE International and will be made available for use by Member Organizations, to reproduce and distribute (in any and all print, electronic or other means of reproduction, storage or transmission) such IHE Technical Documents.

The licenses covered by this Copyright License are only to those copyrights owned or controlled by IHE International itself. If parts of the Technical Framework are included in products that also include materials owned or controlled by other parties, licenses to use those products are beyond the scope of this IHE document and would have to be obtained from that other party.

1.4.1 Copyright of Base Standards

IHE technical documents refer to and make use of a number of standards developed and published by several standards development organizations. All rights for their respective base standards are reserved by these organizations. This agreement does not supersede any copyright provisions applicable to such base standards.

Health Level Seven, Inc. has granted permission to IHE to reproduce tables from the HL7® standard. The HL7® tables in this document are copyrighted by Health Level Seven, Inc. All rights reserved. Material drawn from these documents is credited where used.

1.5 Trademark

IHE® and the IHE logo are trademarks of the Healthcare Information Management Systems Society in the United States and trademarks of IHE Europe in the European Community. They may only be used with the written consent of the IHE International Board Operations Committee, which may be given to a Member Organization in broad terms for any use that is consistent with the IHE mission and operating principles.

1.6 Disclaimer Regarding Patent Rights

Attention is called to the possibility that implementation of the specifications in this document may require use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. IHE International is not responsible for identifying Necessary Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of the specifications in this document are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information about the IHE International patent disclosure process including links to forms for making disclosures is available at

http://www.ihe.net/Patent_Disclosure_Process. Please address questions about the patent disclosure process to the secretary of the IHE International Board: secretary@ihe.net.

1.7 History of Document Changes

This section provides a brief summary of changes and additions to this document.

Date	Document Revision	Change Summary
2015-06-01	1.0	Initial Public Comment release

2 Overview of National Extensions

The goal of IHE is to promote implementation of standards-based solutions to improve workflow and access to information in support of optimal patient care. To that end, IHE encourages the development of IHE National Deployment Committees to address issues specific to local health systems, policies and traditions of care. The role of these organizations and information about how they are formed is available at http://ihe.net/Governance/#National_Deployment.

2.1 Scope of National Extensions

National extensions are allowed in order to address specific local healthcare needs and promote the implementation of the IHE Technical Frameworks. They may add (though not relax) requirements that apply to the Technical Framework generally or to specific transactions, actors and integration profiles. Some examples of appropriate national extensions are:

- Require support of character sets and national languages
- Provide translation of IHE concepts or data fields from English into other national languages
- Extensions of patient or provider information to reflect policies regarding privacy and confidentiality
- Changes to institutional information and financial transactions to conform to national health system payment structures and support specific local care practices

All national extensions shall include concise descriptions of the local need they are intended to address. They shall identify the precise transactions, actors, integration profiles and sections of the Technical Framework to which they apply. And they must provide technical detail equivalent to that contained in the Technical Framework in describing the nature of the extension.

2.2 Process for Developing National Extensions

National extension documents are to be developed and approved in coordination with the IHE Technical Committee and its annual cycle of activities in publishing and maintaining the Technical Framework. The first prerequisite for developing a national extension document is to establish a national IHE initiative and make information regarding its composition and activities available to other IHE initiatives.

Established IHE national initiatives may draft a document describing potential national extensions containing the general information outlined above. This draft document is submitted to the IHE Technical Committee for review and comment. Based on discussion with the Technical Committee, they prepare and submit finalized version of the document in appropriate format. The publication of National Extensions is to be coordinated with the annual publication cycle of other Technical Framework documents in the relevant domain.

2.3 Process for Proposing Revisions to the Technical Framework

In addition to developing national extension documents to be incorporated in the Technical Framework, national IHE initiatives may also propose revisions to the global Technical Framework. These may take the form of changes to existing transactions, actors or integration profiles or the addition of new ones. Such general changes would be subject to approval by the IHE Technical and Planning Committees.

National extensions that are minor in scope, such as suggestions for clarifications or corrections to documentation, may be submitted throughout the year via the ongoing errata tracking process, called the Change Proposal Process.

More substantial revision proposals, such as proposals to add new integration profiles or major country-based extensions, should be submitted directly to the IHE Technical and Planning Committees via the process for submitting new proposals called the Profile Proposal Process.

3 National Extensions for IHE USA

The national extensions documented in this section shall be used in conjunction with the definitions of integration profiles, actors and transactions provided in Volumes 1 through 3 of the IHE ITI Technical Framework. This section includes extensions and restrictions to effectively support the regional practice of healthcare in the United States. It also translates a number of English terms to ensure correct interpretation of requirements of the ITI Technical Framework.

This national extension document was authored under the sponsorship and supervision of IHE USA and the IHE United States initiative.

Alexander Lippitt
IHE USA Liaison
Senior Director, Interoperability and Standards
HIMSS
alippitt@himss.org

3.1 IHE USA Scope of Changes

This national extension implementation guide is based on the IHE Patient Care Coordination (PCC) White Paper, A Data Access Framework using IHE Profiles. It provides guidance for the following use cases:

- 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.

The extensions, restrictions and translations specified apply to the following IHE ITI Integration profiles:

- ITI: EUA
- ITI: IUA
- ITI: XUA
- ITI: MHD v2
- ITI: PDQm
- ITI: PIX/PDQ V3
- ITI: MPQ

- ITI: XDS
- ITI: XCA
- ITI: XCPD
- ITI: ATNA
- ITI: CT

The implementation guide can be found in Appendix A.

Appendices

Appendix A – Data Access Framework (DAF) Document Metadata Based Access Implementation Guide

U.S. Health and Human Services
Office of the National Coordinator for Health IT

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.**

1 Open Issues

- Is PDQm mature for inclusion in the DAF IG
- For NIST documents, what is the best way to link to the documents?
  - Where a URL is given, should it instead be a hyperlink on the document title, or remain a hyper-linked URL? This at least needs to be consistent.
  - Where a document reference is provided, should it consistently have a hyperlink? Example: security sections' reference to NIST 800 series documents.
- Should it include MUST as an equivalent to SHALL, or should all MUSTs in the document be changed to SHALLs?
- Section 3.5.2.6, 4.5.2.6, and elsewhere: Do we need to do additional analysis here to outline the metadata elements that should be always supported?
- Section 4.5.1.4: Should the statement "User authentication MAY be implemented per the IHE EUA Profile." be further qualified to leave room for ongoing but incomplete alternative efforts including HEART, Smart on FHIR® etc.
- What security metadata should DAF support for RESTful queries (i.e., MHD profiles), should it reuse the XDS Security metadata?

2 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.

2.1 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 includes:

- 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.

2.2 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 which is currently being developed by the ONC S&I Framework working with HL7®.

2.3 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.

2.3.1 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.

Table 2.3.1-1: Pre-Requisite Knowledge

Reference Material	Location
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

2.3.2 Reader Guidance

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

Table 2.3.2-1: Reader Guidance

Section	Location
What are the different Query Stacks proposed in this implementation guidance to implement DAF	DAF Technical Approach – Query Stacks and Building Blocks
What are the behavior models supported by DAF	DAF Behavior Models Supported
What are the standards used for DAF	DAF Query Stacks and Standards
Where can I learn about the SOAP query stack	SOAP Query Stack
Where can I learn about the RESTful query stack	RESTful Query Stack
How do I implement the SOAP query stack	DAF Implementation Guidance – SOAP Query Stack
How do I implement the RESTful query stack	DAF Implementation Guidance – RESTful Query Stack
Where can I find examples for SOAP query stack	SOAP Query Examples
Where can I find examples for RESTful query stack	DAF Implementation Guidance – RESTful Query Stack

2.4 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:

2.4.1 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.

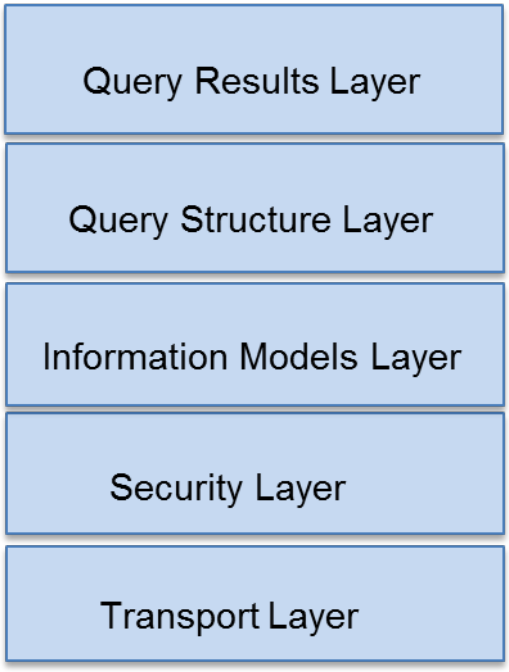
2.4.2 Pre-Conditions for Data Access Framework

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.

2.5 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

2.5.1 Definition of Actors

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

Table 2.5.1-1: Definition of Actors

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

2.5.1.1 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:

Table 2.5.1.1-1: Namespace Prefixes

Prefix	Description
SOAP:	SOAP
SAML:	SAML Assertion
xi:	Xinclude
xs:	XML Schema
xsl:	XSLT

2.5.2 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.

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.

2.5.3 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:

Table 2.5.3-1: Consolidated Conformance Verb Matrix DAF IG

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	-

RFC 2119	HL7	IHE
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.

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:

Table 2.5.3-2: Optionality Definition

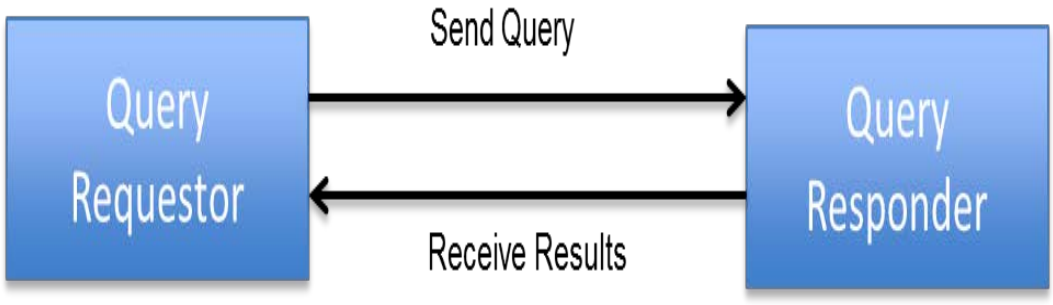
Optionality	Definition
Required	Element must be present and CANNOT BE NULL (no NULL flavors allowed).
Required if Known	The sending system must be able to demonstrate that it can send all required elements, unless it does not gather that data. If the information cannot be transmitted, the data element contains a value indicating the reason for omission of the data.
Optional	No need to include unless the implementer so desires.

Optionality	Definition
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.

Finally all examples are non-normative and are only provided for informational purposes.

2.6 Scope of DAF Technical Approach

DAF Use Cases and User Stories 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.

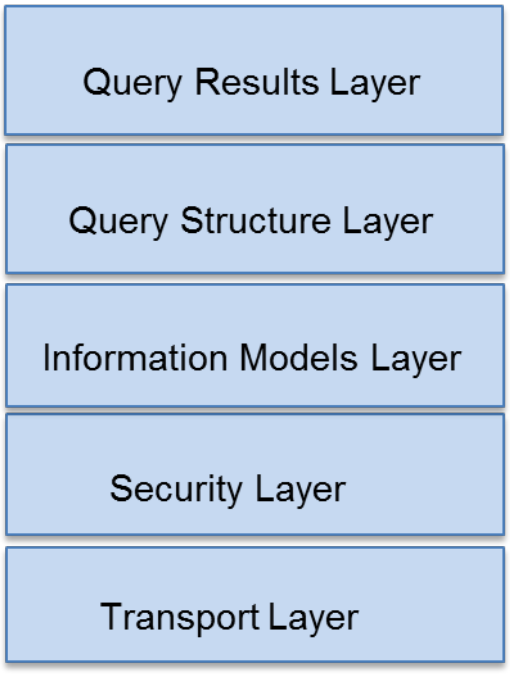
595

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.

3 DAF Technical Approach – Query Stacks and Building Blocks

600 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.



605 **Figure 3-1: 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.

Building Block	Purpose
Security Layer	• The layer is used to specify standards for various security aspects which include the following o Authentication o Access Control and Authorization o Message Integrity o Confidentiality o Auditing o Disclosure requirements o Consent o 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.

3.1 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.

3.2 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.

3.2.1 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.

3.2.2 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.

3.3 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.

3.4 Query Stacks and Substitutability

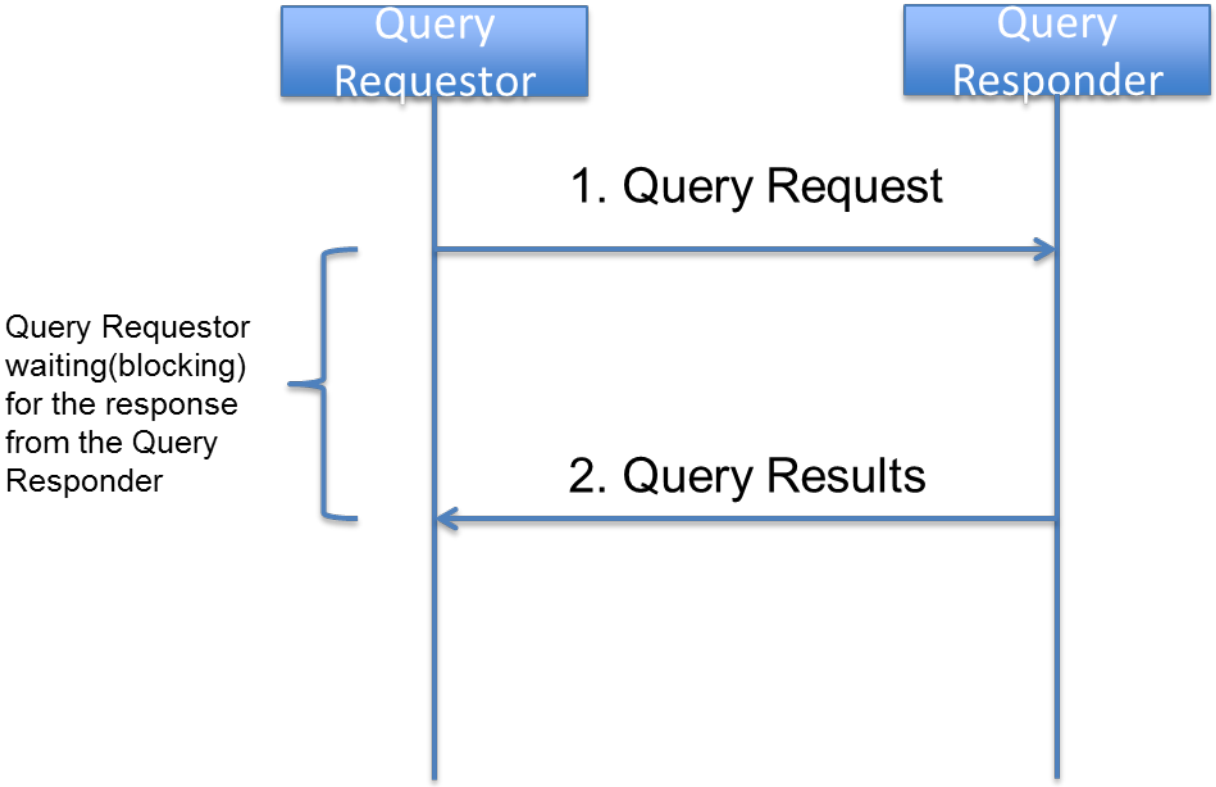
A modular Query Stack lends itself to substitutability of standards as use cases and requirements change. The ability to introduce or vary the standards within a layer of the query stack is called substitutability. For example, systems currently may use HTTP based SOAP transport as the mechanism to transport 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.

3.5 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.

3.5.1 Synchronous Request/Response model

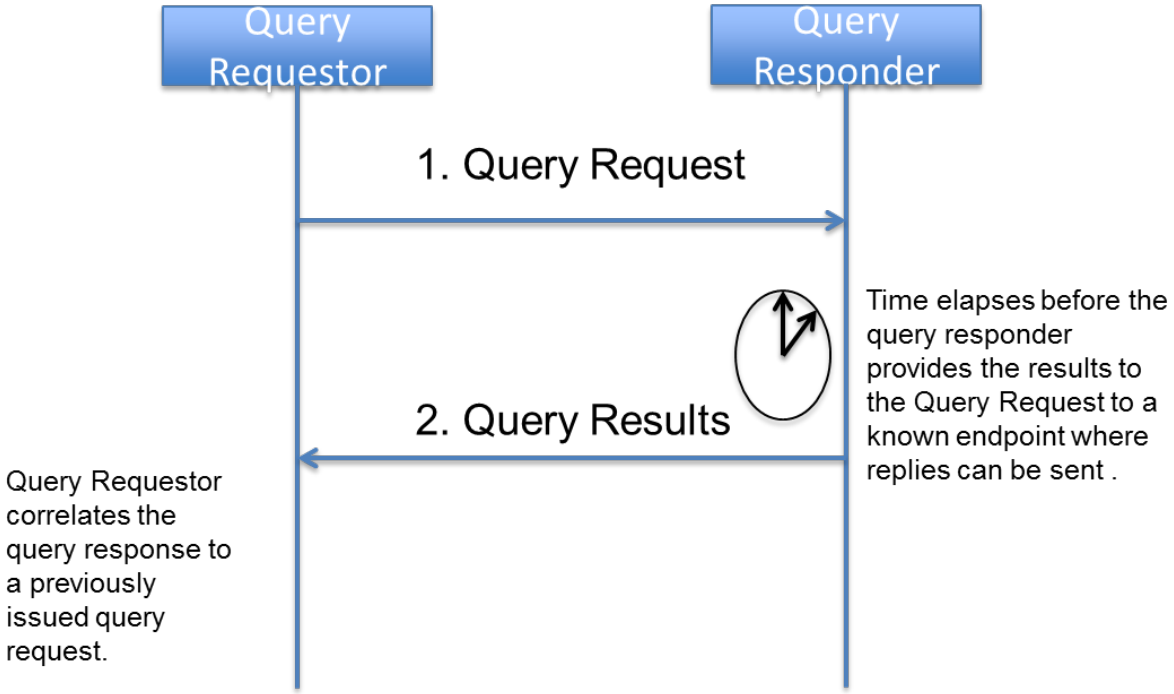
The Synchronous Request/Response model is one in which, a Query Requestor makes a request (1), and a Query Responder (2) replies to the request, providing the results in a single interaction. In a Synchronous Request/Response model the Query Requestor is waiting (blocking) for the Query Responder to 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.

3.5.2 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.

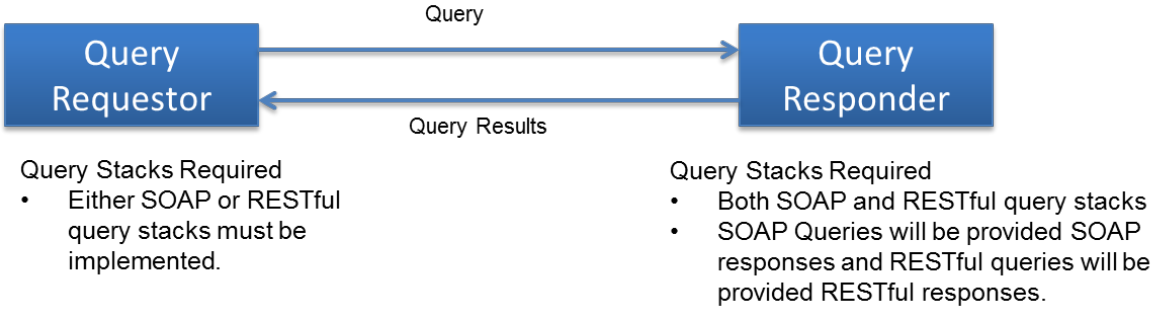


An organization implementing DAF queries using Asynchronous Request/Response models needs to consider SLA's for the systems involved to ensure robustness in query/response behavior because a Query Requestor cannot wait infinitely for a Query Response and there has to be a timeout setup after which the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

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

3.6 DAF Query Stacks and Standards

The DAF Candidate Standards and the corresponding analysis are documented in the DAF IHE white paper. 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)

3.6.1 SOAP Query Stack

The following is a detailed description of the SOAP Query Stack and its components for the various DAF Queries. All the DAF queries use the following as common specifications/profiles for SOAP Query Stack:

- HTTP as the transport protocol
- SOAP 1.2 as the packaging/envelope specification
- TLS for Message Integrity and Confidentiality.

The table below shows the specifications/profiles that vary for each of the DAF queries.

		Governance	Security				Query Structure		Query Results		API
DAF Query Requirement	Behavior Model	Local/Targeted/Federated	Authentication	Access Control	Audit	Consent	Patient	Population	Patient	Population	Interface Specification
Find Document(s) based on Patient Identifiers Get Document(s) based on Document Identifiers Get Document(s) based on Patient Identifiers Get Document(s) for Multiple Patients based on Patient Ids Supply and Consume User Assertions (Access Control) Capture Patient Consent (Consent)	Request / Response	Local	Mutual TLS	N/A	ATNA Logging	N/A	XCA	MPQ	Collection of CCDA Document Entries/CCDA Documents	Collection of CCDA Document Entries/CCDA Documents	XCA/MPQ WSDL
		Targeted	Mutual TLS	XUA (SAML)	ATNA Logging	BPPC/DS4P	XCA	N/A	Collection of CCDA Document Entries/CCDA Documents	N/A	XCA WSDL
	Asynchronous Request / Response	Local	Mutual TLS	N/A	ATNA Logging	N/A	XCA	MPQ	Collection of CCDA Document Entries/CCDA Documents	Collection of CCDA Document Entries/CCDA Documents	XCA/MPQ WSDL
		Targeted	Mutual TLS	XUA (SAML)	ATNA Logging	BPPC/DS4P	XCA	N/A	Collection of CCDA Document Entries/CCDA Documents	N/A	XCA WSDL
Find Patient Identifiers based on Patient Demographics Find Patient Demographics based on Patient Id	Request / Response	Local	Mutual TLS	N/A	ATNA Logging	N/A	XCPD	N/A	Patient Information based on PIX/PDQ V3 model.	N/A	XCPD WSDL
		Targeted	Mutual TLS	XUA (SAML)	ATNA Logging	BPPC/DS4P	XCPD	N/A	Patient Information based on PIX/PDQ V3 model.	N/A	XCPD WSDL

3.6.2 RESTful Query Stack

The following is a detailed description of the RESTful Query Stack and its components for the various DAF Queries. . All the DAF queries use the following as common specifications/profiles for RESTful Query Stack:

- HTTP as the transport protocol
- HTTP Message Structure as the packaging/envelope specification
- TLS for Message Integrity and Confidentiality.

The table below shows the specifications/profiles that vary for each of the DAF queries.

		Governance	Security			Query Structure		Result Structure		API
DAF Query Requirement	Behavior Model	Local/Targeted	Authorization/Access Control	Audit	Consent	Patient	Population	Patient	Population	Interface Specification
Find Document(s) based on Patient Identifiers Get Document(s) based on Document Identifiers Get Document(s) based on Patient Identifiers Get Document(s) for Multiple Patients based on Patient Ids Supply and Consume User Assertions (Access Control) Capture Patient Consent (Consent)	Request / Response	Local /Targeted	IUA + FHIR Tags	ATNA Logging + FHIR Security Event Resource	FHIR Consent Resource /DS4P	MHD_v2	TBD	Document Entry with CCDA Documents.	TBD	MHD_v2 API
Find Patient Identifiers based on Patient Demographics * Find Patient Demographics based on Patient Id *	Request / Response	Local /Targeted	IUA + FHIR Tags	ATNA Logging + FHIR Security Event	FHIR Consent Resource /DS4P	PDQm	N/A	Patient Information based on PIX/PDQ V3 model.	N/A	PDQm API *

730 * PDQm will be adopted as it gets published and matures. This is mostly included here for completeness and there are no specific PDQm transactions required to be implemented by DAF actors.

4 DAF Implementation Guidance – SOAP Query Stack

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

4.1 Transport and Application Protocol Implementation

The SOAP Query Stack uses Transport Layer Security protocol along with Hyper Text Transfer Protocol and Simple Object Access Protocol to send queries and receive responses. The specific implementation guidance to implement these protocols for DAF Document based access is outlined in this section.

4.1.1 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 Authenticate Node Transaction (ITI-19) in section IHE ITI-2a: 3.19 Rev 10.0 to secure the communication channel between each other. (CONF: 100)

4.1.2 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 in IHE ITI Volume 2 Appendices Rev 10.0. (CONF: 110)

4.2 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.

4.2.1 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 along with the constraints specified in Appendix B of this IG 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 to construct the following DAF Patient Demographics related queries. (CONF: 175)
  - Find Patient Id based on Patient Demographics

4.2.2 Using XCA for DAF

In the context of DAF IHE XCA 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

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 are outlined below.

- For DAF Query Requestor MUST implement the following XCA transactions. (CONF: 200)
  - Cross Gateway Query (ITI -38)
  - Cross Gateway Retrieve (ITI -39)

- Registry Stored Query (ITI-18)
- Retrieve Document Set(ITI-43)

- For DAF Query Requestor MUST implement the following XCA options. (CONF: 210)
  - XDS Affinity Domain Option
  - Asynchronous Web Services Exchange
- For DAF, Query Responders MUST implement the following XCA transactions. (CONF: 220)
  - Cross Gateway Query (ITI -38)
  - Cross Gateway Retrieve (ITI -39)
- For DAF, Query Responders MUST support the following behavior model. (CONF: 280)
  - Asynchronous Web Services following Appendix V: Web Services for IHE Transactions in IHE ITI Volume 2 Appendices Rev 10.0.

4.2.3 Using MPQ for DAF

In the context of DAF IHE MPQ 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.

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 are outlined below.

- For DAF, Query Requestor MUST implement the following MPQ transactions. (CONF: 250)
- Multi-patient Stored Query (ITI-51)
- For DAF, Query Requestor MUST support the following behavior model. (CONF: 260)
- Asynchronous Web Services following Appendix V: Web Services for IHE Transactions in IHE ITI Volume 2 Appendices Rev 10.0.

- For DAF, Query Responders MUST implement the following MPQ transactions. (CONF: 270)
- Multi-patient Stored Query (ITI-51)
- For DAF, Query Responders MUST support the following behavior model. (CONF: 280)
- Asynchronous Web Services following Appendix V: Web Services for IHE Transactions in IHE ITI Volume 2 Appendices Rev 10.0.

4.3 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.

4.3.1 Query Results

The advancement of Meaningful Use regulation and certification of EHR technology allows for using the certified technology to support DAF Query Results.

- For DAF queries related to CDA® documents, Query Responders MUST create a C-CDA® document following the ONC 2014 CEHRT requirements or future editions of ONC CEHRT requirements. (CONF: 300)
  - NOTE: The S&I Framework Companion Guide provides implementers guidance on how to comply with the ONC 2014 CEHRT requirements.
  - 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 XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications along with the constraints specified in Appendix B of this IG as part of the query results to facilitate processing by Query Requestors.

4.4 Security Implementation

The section provides security requirements for LDAF and TDAF.

4.4.1 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.

4.4.1.1 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.

4.4.1.2 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.

4.4.1.3 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.

4.4.1.4 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.
        - 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.

4.4.1.5 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.

4.4.1.6 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 XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications along with the constraints specified in Appendix B of this IG 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 XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction

specifications along with the constraints specified in Appendix B of this IG 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.

4.4.1.7 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.

4.4.2 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.

4.4.2.1 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.

4.4.2.2 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.

4.4.2.3 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.

4.4.2.4 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
  - Query Requestors and Query Responders SHALL support all the IHE XUA++ 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.
  - 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.

4.4.2.5 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.

4.4.2.6 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 XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications along with the constraints specified in Appendix B of this IG 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 XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications along with the constraints specified in Appendix B of this IG 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.

4.4.2.7 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.

4.5 SOAP Query Examples

The following are examples of XCA queries and responses taken from IHE implementation material which can be found at ftp://ftp.ihe.net/TF_Implementation_Material/ITI/ .

4.5.1 Synchronous XCA Sample Query:

```
<s:Envelope
                xmlns:s="http://www.w3.org/2003/05/soap-envelope"
                xmlns:a="http://www.w3.org/2005/08/addressing">
        <s:Header>
                <a:Action
s:mustUnderstand="1">urn:ihe:iti:2007:CrossGatewayRetrieve</a:Action>
                <a:MessageID>urn:uuid:0fbfdced-6c01-4d09-a110-
2201afedaa02</a:MessageID>
                <a:ReplyTo>

        <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
                </a:ReplyTo>
                <a:To
s:mustUnderstand="1">http://localhost:2647/XcaService/IHEXCAGateway.svc</a:To
>
        </s:Header>
        <s:Body>
                <RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007">
                        <DocumentRequest>

        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>

        <RepositoryUniqueId>1.3.6.1.4...1000</RepositoryUniqueId>
```



```
        <DocumentUniqueId>1.3.6.1.4...2300</DocumentUniqueId>
                        </DocumentRequest>
                        <DocumentRequest>

        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>

        <RepositoryUniqueId>1.3.6.1.4...2000</RepositoryUniqueId>

        <DocumentUniqueId>1.3.6.1.4...2301</DocumentUniqueId>
                        </DocumentRequest>
                </RetrieveDocumentSetRequest>
        </s:Body>
</s:Envelope>
```

4.5.2 Synchronous XCA Sample Response

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
        <s:Header>
                <a:Action
s:mustUnderstand="1">urn:ihe:iti:2007:CrossGatewayRetrieveResponse</a:Action>
                <a:RelatesTo>urn:uuid:0fbfdced-6c01-4d09-a110-
2201afedaa02</a:RelatesTo>
        </s:Header>
        <s:Body>
                <RetrieveDocumentSetResponse
                                xmlns="urn:ihe:iti:xds-b:2007"
                                xmlns:lcm="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0"
                                xmlns:query="urn:oasis:names:tc:ebxml-
regrep:xsd:query:3.0"
                                xmlns:rim="urn:oasis:names:tc:ebxml-
regrep:xsd:rim:3.0"
                                xmlns:rs="urn:oasis:names:tc:ebxml-
regrep:xsd:rs:3.0">
                        <rs:RegistryResponse status="urn:oasis:names:tc:ebxml-
regrep:ResponseStatusType:Success"/>
```



```
                        <DocumentResponse>
        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>
        <RepositoryUniqueId>1.3.6.1.4...1000</RepositoryUniqueId>
        <DocumentUniqueId>1.3.6.1.4...2300</DocumentUniqueId>
                            <mimeType>text/xml</mimeType>
        <Document>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</Document>
                        </DocumentResponse>
                        <DocumentResponse>
        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>
        <RepositoryUniqueId>1.3.6.1.4...2000</RepositoryUniqueId>
        <DocumentUniqueId>1.3.6.1.4...2301</DocumentUniqueId>
                            <mimeType>text/xml</mimeType>
        <Document>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</Document>
                        </DocumentResponse>
                </RetrieveDocumentSetResponse>
        </s:Body>
</s:Envelope>
```

4.5.3 Asynchronous XCA Sample Query

In an asynchronous query, the responses are delayed to allow for the DAF Responder to process the query and provide the responses at a later time. So the “Reply To” header within the SOAP header is populated with an end point which can receive this message at a later time.

```
<s:Envelope
                xmlns:s="http://www.w3.org/2003/05/soap-envelope"
                xmlns:a="http://www.w3.org/2005/08/addressing">
        <s:Header>
                <a:Action
s:mustUnderstand="1">urn:ihe:iti:2007:CrossGatewayRetrieve</a:Action>
```



```
                <a:MessageID>urn:uuid:0fbfdced-6c01-4d09-a110-
2201afedaa02</a:MessageID>
                <a:ReplyTo>

        <a:Address>http://192.168.2.4:9080/XcaService/InititatingGatewayReceiv
er.svc</a:Address>
                </a:ReplyTo>
                <a:To
s:mustUnderstand="1">http://localhost:2647/XcaService/IHEXCAGateway.svc</a:To
>
        </s:Header>
        <s:Body>
                <RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007">
                        <DocumentRequest>

        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>

        <RepositoryUniqueId>1.3.6.1.4...1000</RepositoryUniqueId>

        <DocumentUniqueId>1.3.6.1.4...2300</DocumentUniqueId>
                        </DocumentRequest>
                        <DocumentRequest>

        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>

        <RepositoryUniqueId>1.3.6.1.4...2000</RepositoryUniqueId>

        <DocumentUniqueId>1.3.6.1.4...2301</DocumentUniqueId>
                        </DocumentRequest>
                </RetrieveDocumentSetRequest>
        </s:Body>
</s:Envelope>
```

4.5.4 Asynchronous XCA Sample Response

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
        <s:Header>
                <a:Action
s:mustUnderstand="1">urn:ihe:iti:2007:CrossGatewayRetrieveResponse</a:Action>
```



```
                <a:MessageID>urn:uuid:D6C21225-8E7B-454E-9750-
821622C099DB</a:MessageID>
                <a:RelatesTo>urn:uuid:0fbfdced-6c01-4d09-a110-
2201afedaa02</a:RelatesTo>
        </s:Header>
        <s:Body>
                <RetrieveDocumentSetResponse
                                xmlns="urn:ihe:iti:xds-b:2007"
                                xmlns:lcm="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0"
                                xmlns:query="urn:oasis:names:tc:ebxml-
regrep:xsd:query:3.0"
                                xmlns:rim="urn:oasis:names:tc:ebxml-
regrep:xsd:rim:3.0"
                                xmlns:rs="urn:oasis:names:tc:ebxml-
regrep:xsd:rs:3.0">
                        <rs:RegistryResponse status="urn:oasis:names:tc:ebxml-
regrep:ResponseStatusType:Success"/>
                        <DocumentResponse>

        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>

        <RepositoryUniqueId>1.3.6.1.4...1000</RepositoryUniqueId>

        <DocumentUniqueId>1.3.6.1.4...2300</DocumentUniqueId>
                                <mimeType>text/xml</mimeType>

        <Document>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</Document>
                        </DocumentResponse>
                        <DocumentResponse>

        <HomeCommunityId>urn:oid:1.2.3.4</HomeCommunityId>

        <RepositoryUniqueId>1.3.6.1.4...2000</RepositoryUniqueId>

        <DocumentUniqueId>1.3.6.1.4...2301</DocumentUniqueId>
                                <mimeType>text/xml</mimeType>

        <Document>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</Document>
                        </DocumentResponse>
```



```
                </RetrieveDocumentSetResponse>
        </s:Body>
</s:Envelope>
```

4.5.5 Synchronous Multipatient Query Example

The examples can be found in the IHE MPQ supplement in section 3.51.4.1.2.4 at http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_MPQ_Rev2-1_TI_2010-08-10.pdf .

4.5.6 Synchronous Multipatient Query Response Example

The examples can be found in the IHE MPQ supplement in section 3.51.4.1.2.4 at http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_MPQ_Rev2-1_TI_2010-08-10.pdf

5 DAF Implementation Guidance – RESTful Query Stack

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

5.1 RESTful Query Stack Standards Summary

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

Query Stack Protocol	
Transport Protocols	HTTP
Message Packaging Envelope	HTTP Message Structure
Message Integrity	TLS
Confidentiality	TLS
System Authentication	TLS (Server side only)
Access Controls/Authorization*	IHE IUA (Based on OAuth2) + FHIR Tags
Consent and Security Metadata*	DS4P + FHIR Tags
Auditing	ATNA + FHIR Security Event
Query Structure	IHE MHD v2** + FHIR Queries based on RESTful resources (FHIR Query Resource may be used along with resources)
Result Structure	FHIR Resources + C-CDA and other documents as applicable
API's	FHIR API's + IHE MHD v2**

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

** IHE MHD v2.x aligns with FHIR® DSTU 1 and has been tested at the IHE NA 2014 New Directions Connectathon. NOTE: FHIR® DSTU 2 is under ballot currently and eventually IHE MHD v2.x has to be updated to reflect the FHIR® DSTU 2 formats and requirements.

5.2 Transport and Application Protocol Implementation

The RESTful Query Stack uses Transport Layer Security (TLS 1.0) protocol along with Hyper Text Transfer Protocol and RESTful 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.

5.2.1 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 Authenticate Node Transaction (ITI-19) in section IHE ITI-2a: 3.19 Rev 10.0 to secure the communication channel between each other. (CONF: 500)
- DAF actors SHALL implement one-way TLS which provides server authenticity. DAF actors MAY implement Mutual TLS in their local

5.2.2 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

5.3 Query Implementation

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

5.3.1 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 XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications along with the constraints specified in Appendix B of this IG 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
- PDQm: For finding patient identifiers which are required for other MHD transactions, DAF project is evaluating the use of PDQm as an option.

5.3.2 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

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 are outlined below.

- For DAF, Query Requestor MUST implement the following MHD transactions. (CONF: 600)
  - Find Document References (ITI -67)
  - Retrieve Document (ITI-68)
- For DAF, Query Responders MUST implement the following MHD transactions. (CONF: 620)
  - Find Document References (ITI -67)
  - Retrieve Document (ITI-68)
- Currently only synchronous queries (Request/Response Behavior Model)

5.3.3 Querying for Documents related to Multiple Patients

In the context of DAF MHD v2 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.

5.4 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.

5.4.1 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 ONC 2014 CEHRT requirements or future editions of ONC CEHRT requirements. (CONF: 700)
  - NOTE: The S&I Framework Companion Guide provides implementers guidance on how to comply with the ONC 2014 CEHRT requirements.
  - 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 XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications along with the constraints specified in Appendix B of this IG as part of the query results to facilitate processing by Query Requestors.

5.5 Security Implementation

5.5.1 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.

5.5.1.1 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.

5.5.1.2 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.

5.5.1.3 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.

5.5.1.4 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 authentication of the systems per the Authenticate Node transaction for HTTP connections per IHE ATNA Profile to authenticate the DAF Responder.
        - 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.

5.5.1.5 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.

5.5.1.6 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 however the equivalent metadata for RESTful queries has not been complexly approved and hence this will be evolving over time.

5.5.1.7 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.

5.5.2 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.

5.5.2.1 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.

5.5.2.2 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.

5.5.2.3 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.

5.5.2.4 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
- Query Responders SHALL support all the IHE 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.
- 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.

5.5.2.5 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.

5.5.2.6 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 however the equivalent metadata for RESTful queries has not been complexly approved and hence this will be evolving over time.

5.5.2.7 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.

5.6 RESTful Query Examples

The IHE MHD v2 examples tested at the IHE NA Connectathon 2014 can be found here. ftp://ftp.ihe.net/IT_Infrastructure/iheitiyr13-2015-2016/Technical_Cmte/Workitems/MHD2/Testing/

NOTE: These examples are based on FHIR® DSTU 1 since IHE MHD v2 is based on FHIR® DSTU 1 and will be updated to use FHIR® DSTU 2 formats when IHE MHD v2 gets updated.

DAF Document Metadata Based Access Implementation Guide Appendices

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.

Table A-1: Key Acronyms and Definitions

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

Acronym	Definition
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

1525

Appendix B – Document Sharing Metadata Constraints

This appendix builds upon the XDS Metadata in Section 4 from IHE ITI Volume 3 Cross Transaction specifications. It further constraints these profile specifications for specific Metadata elements by:

- providing a more precise semantic description to foster consistent use
- specifying terminology value sets where applicable

Some metadata elements do not need to be further constrained beyond the XDS Metadata in Section 4 from IHE ITI Volume 3 and are not addressed by this Appendix such as:

- related to the configuration performed by deployment projects (e.g., repositoryUniqueID)
- related to the design of specific query requester (e.g., uniqueID of the document)
- fully specified by Section 4 of IHE ITI Volume 3 (e.g., entryUUID, service start time, hash)
- left to a specific deployment projects given the document content shared (e.g., patient Id, language, eventCodeList, type of document)

B.1 Document Metadata

Table B.1-1 below lists the metadata elements that are required to be supported in the context of this implementation specification.

Table B.1-1: Document Metadata Attribute Definition

Document Entry Metadata Attribute	Description	Value Set
author	Characterizes the humans and/or machines that authored the document. This attribute contains the sub-attributes: authorInstitution, authorPerson, authorRole, authorSpecialty and authorTelecommunication.	N/A
	authorRole	Coded Values from ASTM E1986
	authorSpecialty	SNOMED Clinical Specialty concept tree
classCode	A high-level classification of documents that indicates the kind of document, e.g., report, summary, note, consent.	See Section 4.1.1
confidentialityCode	The code specifying the level of confidentiality of the document.	See Section 4.1.2
formatCode	Code globally unique specifying the format of the document.	See Section 4.1.4
healthcareFacility TypeCode	This code represents the type of organizational setting of the clinical encounter during which the documented act occurred.	See section 4.1.5
languageCode	Specifies the human language of character data in the document.	ISO 639-1

Document Entry Metadata Attribute	Description	Value Set
legalAuthenticator	Characterizes a participant who has legally authenticated or attested the document within the authorInstitution.	N/A
	authorRole.	Coded Values from ASTM E1986
	authorSpecialty	SNOMED Clinical Specialty concept tree
mimeType	MIME type of the document.	Value to be selected per the content standard used for shared documents from the MIME Media Types. Code System OID: 2.16.840.1.113883.6.10
practiceSettingCode	The code specifying the clinical specialty where the act that resulted in the document was performed (e.g., Family Practice, Laboratory, Radiology).	See 4.1.3 Healthcare Specialty
typeCode	A low-level classification of documents within a classCode that describes class, event, specialty, and setting.	LOINC. Value to be selected per the document profile/implementation guide specification.

B.1.1 Class Code Value Set

The following value set is specified for the document Class Code metadata element. It is intended to be placed under management of a terminology (e.g., IHE).

Value Set Name	Class Code
Value Set Identifier	*To be assigned by IHE*
Code System Name	Class Code
Code System Identifier	*To be assigned by IHE*
Value Set Type	Static
Purpose	The code specifying the high-level use classification of the particular kind of document (e.g., Prescription, Report, Summary, Images, Treatment Plan, Patient Preferences, Workflow). It is clearly different from the document typeCode that specifies the precise type of document from the creator perspective. This code is generally used in combination with other coded metadata (e.g., clinical specialty, format, etc.)
Method	The value set has been designed to be free (“orthogonal”) from medical specialties recorded in the “Care Setting” metadata element. An identical value set has been defined by several other countries.

Code	Concept Name
REPORTS	Reports
SUMMARIES	Summaries
IMAGES	Images
PRESCRIPTIONS	Prescribed Treatments and Diagnoses
DISPENSATIONS	Dispensations
PLANS	Treatment Plan or Protocol
HEALTH	Health Certificates and Notifications
PATIENT	Patient Expression and Preferences
WORKFLOWS	Workflow Management

B.1.2 Confidentiality Code Value Set

The following value set is specified for the Document Confidentiality Code Value Set.

Code System Identifier	2.16.840.1.113883.5.25
Value Set Type	Static
Purpose	Identifies the confidentiality level assigned by the document source for a document
Method	This value set is a subset of the HL7 confidentialityCode. The HL7 coding system contains the following codes: N-Normal/R-Restricted and V-Very restricted.

Code	Concept Name
N	normal
R	restricted
V	very restricted

B.1.3 Healthcare Specialty

This is a high-level list of Specialties (without details on the subspecialties) to enable filtering in association with Class Code (e.g., report + radiology, summary + acute care), when used in the" XDS careSetting" metadata element. The list is kept at a high level (without drilling into sub-specialties), as the intended use is to perform document query at a high level and there needs to support a simple and robust process for the document source to assign values without risks of misclassification.

The Value Set is defined by combining two partial trees of SNOMED concepts in a flat value set:

- SNOMED Medical Specialties (without lower levels concepts)

- SNOMED Clinical Specialties (without lower level concepts) without:
  - Medical Specialties and sub-tree (already included in Medical Specialties)
  - Clinical Oncology concept (already included in Medical Specialties).
  - Obstetrics Oncology concept (already included in Medical Specialties).

B.1.4 Format Code

Format Code is a globally unique code specifying the format of the document. The code values are directly related to the document profile/implementation guide specification. IHE content profiles have format codes assigned to them recorded on http://wiki.ihe.net/index.php?title=IHE_Format_Codes . The HL7® C-CDA® format codes can be accessed at the following location http://wiki.hl7.org/index.php?title=CDA_Format_Codes_for_IHE_XDS .

B.1.5 Healthcare Facility Type Code

This is the code representing the type of organizational setting where the clinical encounter, service, interaction, or treatment occurred. The value set is derived from the Healthcare Facility Type defined by HITSP from HITSP C80 Table 2-147. This value set has been simplified to align the value set to healthcare facility type that is relevant to a normal patient navigating the US healthcare system.

Code	Display
82242000	Hospital-children's
225732001	Hospital-community
79993009	Hospital-government
32074000	Hospital-long term care
4322002	Hospital-military field
224687002	Hospital-prison
62480006	Hospital-psychiatric
80522000	Hospital-rehabilitation
48311003	Hospital-Veterans' Administration
284546000	Hospice facility
42665001	Nursing home
45618002	Skilled nursing facility
73770003	Emergency department--hospital
33022008	Hospital-based outpatient clinic or department--OTHER-NOT LISTED

Code	Display
39350007	Private physicians' group office
83891005	Solo practice private office
309900005	Care of the elderly day hospital
10531005	Free-standing ambulatory surgery facility
91154008	Free-standing birthing center
41844007	Free-standing geriatric health center
45899008	Free-standing laboratory facility
51563005	Free-standing mental health center
1773006	Free-standing radiology facility
39913001	Residential school infirmary
25681007	Sexually transmitted disease health center
20078004	Substance abuse treatment center
46224007	Vaccination clinic
81234003	Walk-in clinic
35971002	Ambulatory care site--OTHER--NOT LISTED
11424001	Ambulance-based care
901005	Helicopter-based care
2081004	Hospital ship
59374000	Traveler's aid clinic
413456002	Adult day care center
413817003	Child day care center
310205006	Private residential home
419955002	Residential institution
272501009	Sports facility

B.2 Submission Set Metadata

1590

Table B.2-1: SubmissionSet Metadata Attribute Definition

Submission Set Metadata Attribute	Description	Value Set
author	The humans and/or machines that created the submission set. This attribute contains the sub-attributes: authorInstitution, authorPerson, authorRole, authorSpecialty, authorTelecommunication.	See Author in the Document Metadata Table 4.1-1 for authorrole and authorspecialty metadata elements.
contentTypeCode	The code specifying the type of clinical activity that resulted in placing these documents in this SubmissionSet.	See Section 4.2.1 Healthcare Facility Type.

B.2.1 Submission Set Content Type

Content Type Code is related to the type of clinical activity that resulted in placing these documents in this SubmissionSet. One of the uses of this content type codes is to inform returned information from queries for a list of Submission Set to obtain a view of the list of encounters that resulted in shared documents.

The value set is the same as the one used for the Healthcare facility Type Code (see Section 4.1.5).

B.3 Folder Metadata

No specific constraints are defined.

