Integrating the Healthcare Enterprise

IHE IT Infrastructure Technical Framework Supplement

Mobile Health Document Sharing (MHDS)

HL7® FHIR®

Revision 2.1 – Trial Implementation

Date: May 29, 2020
Author: ITI Technical Committee
Email: iti@ihe.net

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.

Copyright © 2020: IHE International, Inc.

Foreword

This is a supplement to the IHE IT Infrastructure Technical Framework V16.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on May 29, 2020 for trial implementation and may be available for testing at subsequent IHE Connectathons. The supplement may be amended based on the results of testing. Following successful testing it will be incorporated into the IT Infrastructure Technical Framework. Comments are invited and may be submitted at http://www.ihe.net/ITI_Public_Comments.

This supplement describes 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.

Amend Section 50.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 IT Infrastructure 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.

 Copyright © 2020: IHE International, Inc.

CONTENTS

 Copyright © 2020: IHE International, Inc.

 Copyright © 2020: IHE International, Inc.

This profile does not specify any FHIR encoding as it leverages the grouped profiles. Thus this profile is not FHIR version specific.

Introduction to this Supplement

This profile will show how to build a Document Sharing Exchange using IHE-profiled FHIR® standard, rather than the legacy IHE profiles that are dominated by XDS and HL7® v2. This profile will assemble profiles and define a Document Registry.

The central HIE infrastructure defined in this Profile might be a single FHIR Server implementing all the defined central service actors or may be virtual cloud of the systems implementing the defined profile actors. These deployment models allow for modularity where each service function could be provided by different vendors, leveraging as much as possible from a reference implementation of a FHIR Server, and also leverage as much as possible of modularity enabled by defined Profiles.

Core business functions provided by MHDS Profile:

- Publication of Document based information
  - Content agnostic but CDA® and FHIR preferred
- Persistence and lifecycle management of Documents, DocumentManifest, DocumentReference, and List resources
  - Enabling centralized document storage, or distributed document storage at a service identified at the source
- Patient Identity Management –
  - specifically, a golden patient identity for use within the domain, cross-reference to other identities, and lifecycle of updates
  - Appropriate comprehensive handling of patient identity updates including merge
- Participant Organizations management
  - Enabling use of mCSD directory for author identity management
- Authorization management
  - Consent

 Copyright © 2020: IHE International, Inc.

  - User Role-Based-Access-Control (RBAC) or Attribute-Based-Access-Control (ABAC)
  - Application
  - PurposeOfUse
- Encryption and Integrity requirements
- Audit Log Management
- Consumption side can be further refined using mXDE and QEDm

Open Issues and Questions

1. Given that this profile audience is likely to include those new to IHE Document Sharing exchange, there is more detail included in this supplement in order to be more self-contained and not rely on the reader referencing other whitepapers and handbooks. Section 50.7 could be considered to be removed if and when the ITI whitepaper on using IHE Profiles for and HIE is updated to include MHD and MHDS.

Closed Issues

1. This profile was renamed from MHD-HIE to Mobile Health Document Sharing (MHDS). This name leverages the concept of "Document Sharing" as defined in the HIE whitepaper and includes the original MHD acronym while removing the word "access" which is important in MHD to define it as an API and inserting the word "Sharing" which indicates persistence.
2. There is no action defined for the Document Registry when the PMIR feed transaction indicated a Delete action on a Patient that the Document Registry has records for. The concern is that this action is not clear outside of a policy. It is reasonable that policy may choose to ignore Delete, may choose to mark the affected Resources inactive, or may choose to delete the affected Resources. Thus, we have left this action undefined. It is expected that a Delete action is unusual, and that administrative user interface may be the better solution.
3. Where XDS/XCA is used the MHDS Profile does not apply, as the MHD Profile provides the API functionality to XDS/XCA
4. MHDS defines an OAuth scope for use with MHDS and IUA to support Patient Privacy Disclosure Consent functionality. This scope is crafted to be minimally impacting on uses of IUA and SMART-on-FHIR. See the "Consent Management Option" for details.
5. In this profile, there is no formal Document Repository, although the functionality is provided virtually when a Document Source chooses to not include the document as a Binary resource, but rather include a URL to a repository that is recognized as part of the trust domain. This distinction is available in MHD today, although it is not pointed out as

 Copyright © 2020: IHE International, Inc.

such and thus not well known. There is description of this virtual Document Repository functionality.

6. The MHDS environment allows for some normally contained Resources be recorded as a link to data in the mCSD managed Directory or PMIR Patient Identity Manager. This is defined in the "UnContained Reference Option". The necessary change to MHD has not been done yet in order to get feedback from Public Comment. CP-ITI-1200 has updated MHD to add an UnContained Reference Option for this support

 Copyright © 2020: IHE International, Inc.

IHE Technical Frameworks General Introduction

The IHE Technical Framework General Introduction is shared by all of the IHE domain technical frameworks. Each technical framework volume contains links to this document where appropriate.

9 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.

9.1 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. Copyright license information for frequently referenced base standards is provided below.

9.1.1 DICOM (Digital Imaging and Communications in Medicine)

DICOM® is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.

9.1.2 HL7 (Health Level Seven)

HL7®, Health Level Seven®, CCD®, CDA®, FHIR®, and the FHIR [FLAME DESIGN] ® are registered trademarks of Health Level. Seven International and the use does not constitute endorsement by HL7.

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.

9.1.3 LOINC (Logical Observation Identifiers Names and Codes)

LOINC® is registered United States trademarks of Regenstrief Institute, Inc.

9.1.4 SNOMED CT (Systematized Nomenclature of Medicine -- Clinical Terms)

Some IHE Profiles incorporate SNOMED® CT, which is used by permission of the International Health Terminology Standards Development Organisation. SNOMED CT© was originally created by the College of American Pathologists. SNOMED CT is a registered trademark of the International Health Terminology Standards Development Organisation, all rights reserved.

10 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.

 Copyright © 2020: IHE International, Inc.

IHE Technical Frameworks General Introduction Appendices

The IHE Technical Framework General Introduction Appendices are components shared by all of the IHE domain technical frameworks. Each technical framework volume contains links to these documents where appropriate.

*Update the following appendices to the General Introduction as indicated below. Note that these are **not** appendices to this domain's Technical Framework (TF-1, TF-2, TF-3 or TF-4) but rather, they are appendices to the IHE Technical Frameworks General Introduction located here.*

Appendix A – Actor Summary Definitions

*Add the following **new or modified** actors to the IHE Technical Frameworks General Introduction Appendix A:*

No *new* actors.

The table below lists *existing* actors that are utilized in this profile.

List of Existing Actors Utilized in this Profile

Existing Actor Name	Definition
Document Registry	The Document Registry maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer Actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration.

Appendix B – Transaction Summary Definitions

*Add the following **new or modified** transactions to the IHE Technical Frameworks General Introduction Appendix B:*

No new transactions

Appendix D – Glossary

*Add the following **new or updated glossary** terms to the IHE Technical Frameworks General Introduction Appendix D.*

No new terms.

 Copyright © 2020: IHE International, Inc.

Volume 1 – Profiles

Add new Section 50

50 Mobile Health Document Sharing (MHDS) Profile

The MHDS Profile specifies how a collection of IHE profiles can be used by communities for exchanging health information. These IHE profiles include support for patient identification, health document location and retrieval, provider directories, and the protection of privacy and security. MHDS shows how several IHE profiles work together to provide a standards-based, interoperable approach to community health information sharing.

The IHE IT Infrastructure Domain has published several resources to support document sharing:

- ITI Technical Framework: Vol. 3 - Section 4.0 Metadata used in Document Sharing
- Health Information Exchange: Enabling Document Sharing Using IHE Profiles
- Document Sharing Metadata Handbook
- Template for XDS Affinity Domain Deployment Planning

This MHDS Profile defines a Document Sharing Exchange that is based around the HL7 FHIR standard, following the principles described in the Health Information Exchange: Enabling Document Sharing Using IHE Profiles whitepaper. This Document Sharing exchange requires the same management of metadata as described in the Document Sharing Metadata Handbook.

 Copyright © 2020: IHE International, Inc.

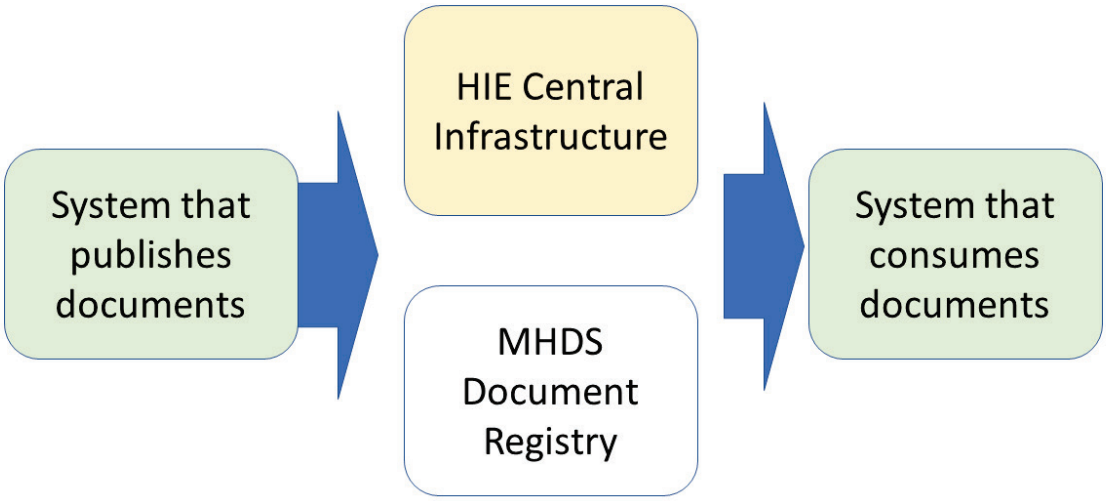

Figure 50-1: MHDS High Level View Diagram

Readers that need background on high level concepts of Document Sharing should first review Section 50.7 "MHD Background". The MHDS Profile is described in the following sections:

- 50.1 – MHDS Actors, Transactions, and Content Modules
- 50.2 – MHDS Actor Options
- 50.3 – MHDS Required Actor Groupings
- 50.4 – MHDS Overview and Use-cases
- 50.5 – MHDS Security Considerations
- 50.6 – MHDS Cross Profile Considerations
- 50.7 – MHDS Background

50.1 MHDS Actors, Transactions, and Content Modules

This profile orchestrates actors in many existing IHE profiles and creates one new actor. The actor that is specific to this profile is a Document Registry. Figure 50.1-1 shows a detailed actor diagram for the MHDS Document Registry.

 Copyright © 2020: IHE International, Inc.

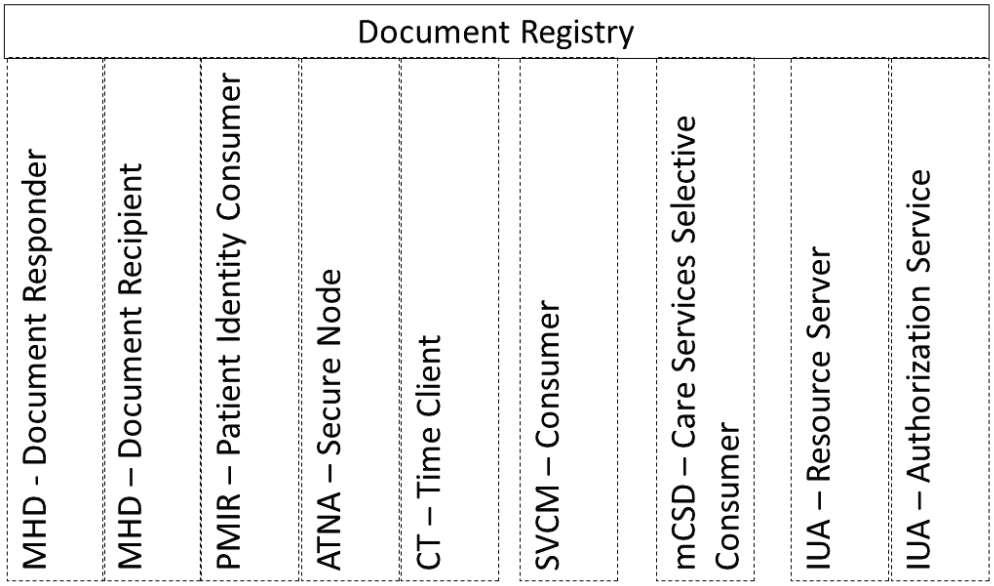

Figure 50.1-1: MHDS Registry Actor Diagram

Table 50.1-1 lists the transactions for each actor directly involved in the MHDS Profile. To claim compliance with this profile, an actor shall support all required transactions (labeled "R") and may support the optional transactions (labeled "O").

Table 50.1-1: MHDS Profile - Actors and Transactions

Actors	Transactions	Initiator or Responder	Optionality	Reference
Document Registry	(none) – transactions supported come from the grouped actors listed below	--	--	--

The Document Registry is grouped with a set of actors from other profiles:

- **MHD - Document Recipient** supports publication requests by the MHD Document Source. The Comprehensive Metadata Option is required.
- **MHD - Document Responder** supports the discovery and retrieval of documents by MHD Document Consumer.
- **PMIR - Patient Identity Consumer** provides patient identity synchronization and specifically the merge function to be applied to any data managed in the Document Registry.

 Copyright © 2020: IHE International, Inc.

- **SVCM – Terminology Consumer** enables the Document Registry to gain access to ValueSets that the Registry is enforcing Metadata consistency.
- **mCSD – Care Services Selective Consumer** enables the Registry to have access to Organization and Practitioner resources.
- **IUA – Authorization Server and Resource Server** enforces access control decisions.
- **ATNA - Secure Node** enable the Document Registry to be secure, record audit records, and support secure transactions.
- **CT - Time Client** assures that all records of time done by the Document Registry are aligned with the Time Source.

HIE Central Infrastructure Requirements

In MHDS, the Document Registry is part of a Document Sharing Health Information Exchange (HIE). See Figure 50.1-2. The Document Registry relies upon services that would be hosted within the HIE Central Infrastructure with a set of Service endpoints as illustrated in the yellow "HIE Central Infrastructure". The HIE also contains systems, illustrated in green, that submit and consume documents. The combination of MHDS Document Registry (white), HIE Central Infrastructure (yellow), and Systems that publish or consume documents (green) make up the Document Sharing Community (aka Community).

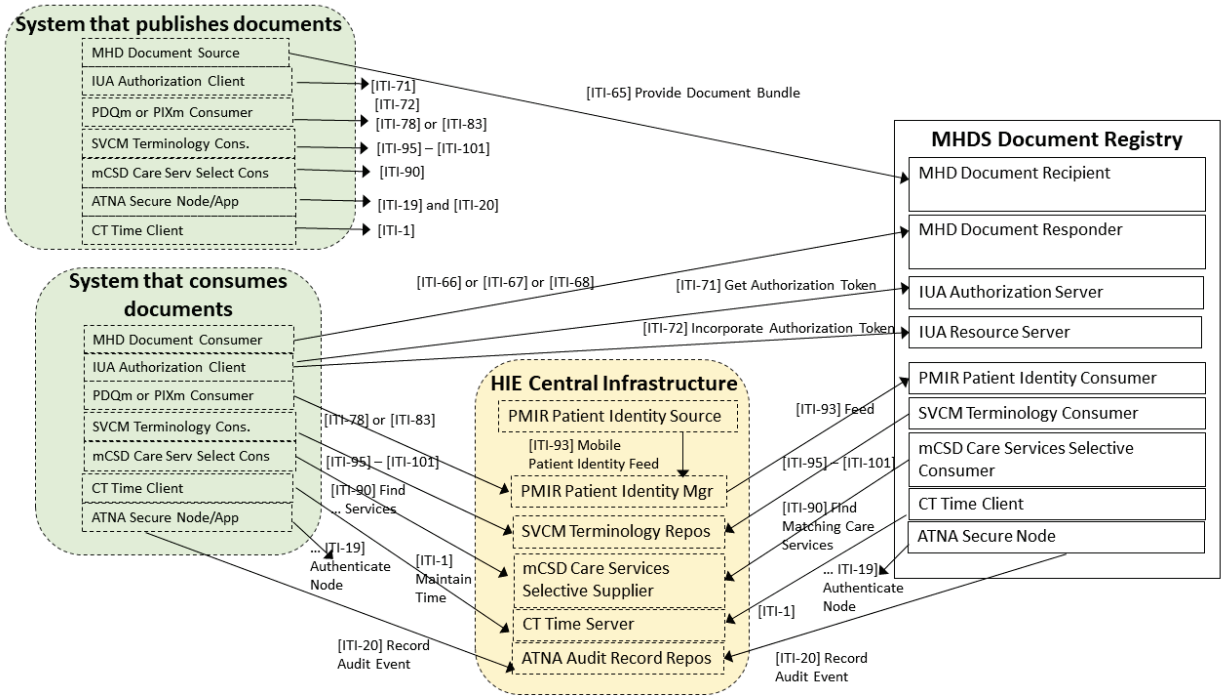

Figure 50.1-2: MHDS Document Sharing Health Information Exchange

 Copyright © 2020: IHE International, Inc.

The HIE Central Infrastructure is a set of Services based on IHE Profiles as shown in Figure 50.1-2:

- **CT - Time Server** – to provide consistent time to all participant systems
- **ATNA – Audit Record Repository** with support for the ATX: FHIR Feed Option – to capture audit events and provide appropriate audit log access for security and privacy use-cases
- **PMIR – Patient Identity Source and Patient Identity Manager** – to provide patient identity lookup by demographics or identity, and to receive create and update of patient identity from participants
- **SVCM – Terminology Repository** – Provide vocabulary and value set management within the Community
- **mCSD – Care Services Selective Supplier** – a Provider Directory to enable endpoint lookup and optionally provider identity management

There are other useful actors that are compatible with MHDS, but are not required by the MHDS Profile:

- **NPFS – File Manager** – Provide files that are needed in the community but are not patient specific such as policy documents
- **mXDE – Data Element Extractor** – to enable QEDm access to data elements derived from published documents
- **QEDm – Clinical Data Source –** to enable access to data elements (aka FHIR clinical Resources)
- **mACM – Alert Communication Manager** – to enable community supported alert communications

In addition to these IHE-defined actors, the Community will also select how they will manage Digital Certificates through a Certificate Authority, and other functionalities and non-functional requirements such as response-time, service-level-agreements, remediation-planning, remediation-access, etc.

The Document Registry and the supporting services listed above provide a set of services that make up a Document Sharing Infrastructure that is based on FHIR. This set of services enable systems that publish documents and systems that consume documents. Additionally, the mXDE Profile may be used to make the information in shared documents more consumable as FHIR Resources using QEDm Profile. See Section 50.6 Cross Profile Considerations for more details.

50.1.1 Actor Descriptions and Actor Profile Requirements

This profile assumes that some Health Information Exchange (HIE) authority manages the configuration of the Community. This includes specification of an appropriate Certificate

 Copyright © 2020: IHE International, Inc.

Authority, Time Source, Domain Name Service, Valueset Management, Provider Directory, Audit Record Repository, Patient Identity Manager, and Authorization Service.

The HIE authority is responsible for setting Patient Identity quality criteria including the minimally acceptable Patient identity constraints. This would set the data elements that describe the Patient within the Community and the quality of the identity proofing and identity confirmation necessary by all participants in the Community.

The HIE authority is responsible for setting Document Sharing Metadata rules, following the metadata rules and using the Metadata Handbook to set specific metadata element requirements including the specification of mandatory ValueSets. See the Document Sharing Metadata Handbook.

50.1.1.1 Document Registry

The functions of the MHDS Document Registry rely on grouped actors from the other IHE Profiles; see Section 50.3.

The Document Registry SHALL include a configuration management function to enable configuration of the grouped actors, including Metadata rules, policy, and security.

The Document Registry SHALL be grouped with CT – Time Client to keep internal clocks synchronized to the identified Time Source so that records of time are correlated.

The Document Registry SHALL be grouped with an ATNA Secure Node or Secure Application:

- The Document Registry SHALL obtain a Digital Certificate from the HIE-defined Certificate Authority.
- The Document Registry SHALL support at least the ATNA "STX: TLS 1.2 Floor using BCP195" Option.
- The Document Registry SHALL allow only authorized access to the protected resources managed by the Document Registry.
- The Document Registry SHALL record all security relevant events to ATNA Audit Record Repository with the "ATX: FHIR Feed" Option. This SHALL include all IHE-defined audit events that are in the control of the Document Registry, including its grouped actors.

50.1.1.1.1 When the grouped MHD Document Recipient – is triggered

Triggered by: a Provide Document Bundle [ITI-65] transaction.

 Copyright © 2020: IHE International, Inc.

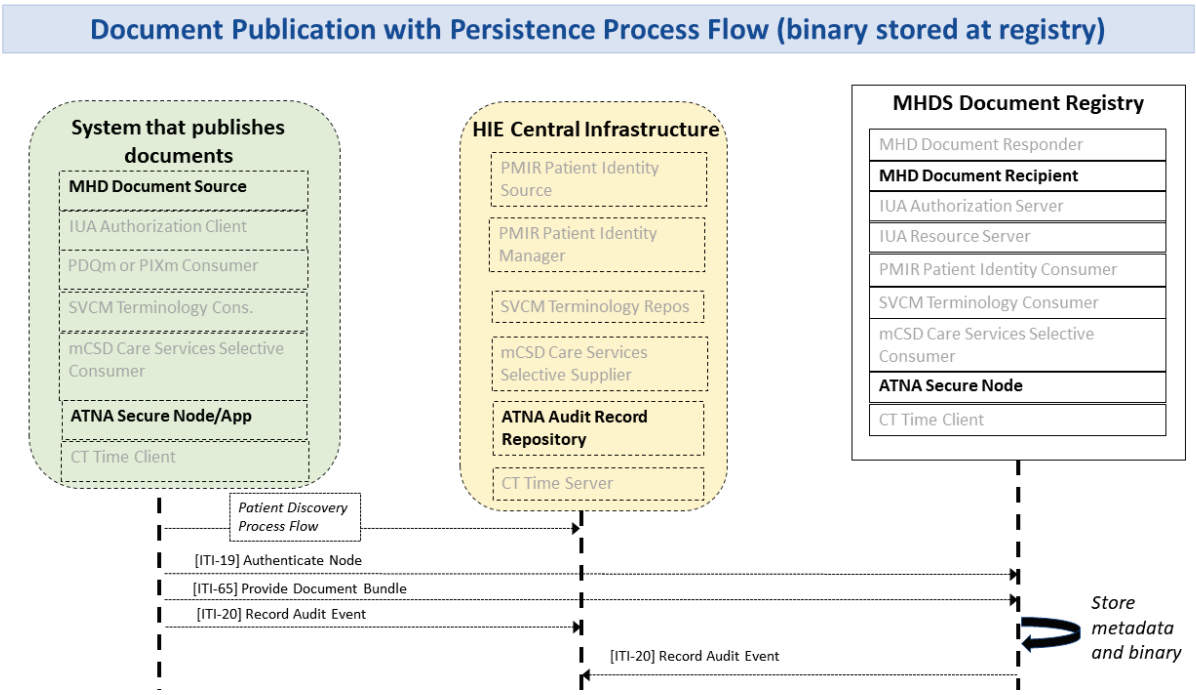

Figure 50.1.1.1.1-1: Document Publication Process Flow

1. The Document Registry SHALL confirm its identity to the requesting system by use of the ATNA Secure Node or Secure Application TLS protocol using a Certificate assigned to the Document Registry.
2. When the Authorization Option (Section 50.2.1) is implemented and enabled, the Document Registry SHALL confirm the client identity using the IUA Profile.
3. The Document Registry SHALL validate to the requirements of MHD Document Recipient using the MHD Comprehensive Metadata Option. Additional policy driven requirements, not specified here, may also apply.
4. When the UnContained Reference Option is used in the grouped MHD Document Recipient, the Document Registry SHALL not require that the references are contained, but SHALL validate that the reference is found in the central registries. (See Section 50.2.4 UnContained Reference Option.)
5. The Document Registry SHALL validate that the subject of the DocumentReference, DocumentManifest, and List Resources is the same Patient, and that Patient is a recognized and active Patient within the Community. The Patient identity must be recognized and active by the PMIR Patient Identity Manager in the document sharing community. This may be accomplished by a query of the PMIR Patient Identity Manager, by way of a cached internal patient database, or other means.

 Copyright © 2020: IHE International, Inc.

6. The Document Registry SHALL validate the metadata conformance received according to the appropriate validation rules, and configured ValueSets to assure that the document submission request is valid. If any of the metadata are found to be not valid then the transaction shall be rejected.
7. When the SVCM Validation Option (Section 50.2.3) is implemented and enabled, the Document Registry SHALL use the grouped SVCM Terminology Consumer to validate metadata elements as appropriate to configured policy. For example, the DocumentReference.type often must be a value within a ValueSet agreed to by the Community.
8. Provided the request is valid, the Document Registry SHALL persist all DocumentManifest, DocumentReference, List, and Binary that are received by way of the grouped MHD - Document Recipient – Provide Document Bundle [ITI-65] Transaction.
9. When the request includes a DocumentReference intended to replace an existing DocumentReference, the Document Registry SHALL mark the replaced DocumentReference as deprecated. The Replace action in the request is indicated when the Bundle contains a new DocumentReference with `DocumentReference.relatesTo.code` of `replaces` and `DocumentReference.relatesTo.target` pointing at the existing DocumentReference to be deprecated. The Document Registry sets the existing `DocumentReference.status` element to `inactive`.
10. Any of the above checks that fail will result in the whole Provide Document Bundle [ITI-65] failing and returning errors as defined in [ITI-65].
11. The Document Registry SHALL record success and failure events into the ATNA Audit Record Repository.

50.1.1.1.2 When the grouped MHD Document Responder – is triggered

Triggered by: any Find Document Manifests [ITI-66], Find Document References [ITI-67], and Retrieve Document [ITI-68] Transactions.

 Copyright © 2020: IHE International, Inc.

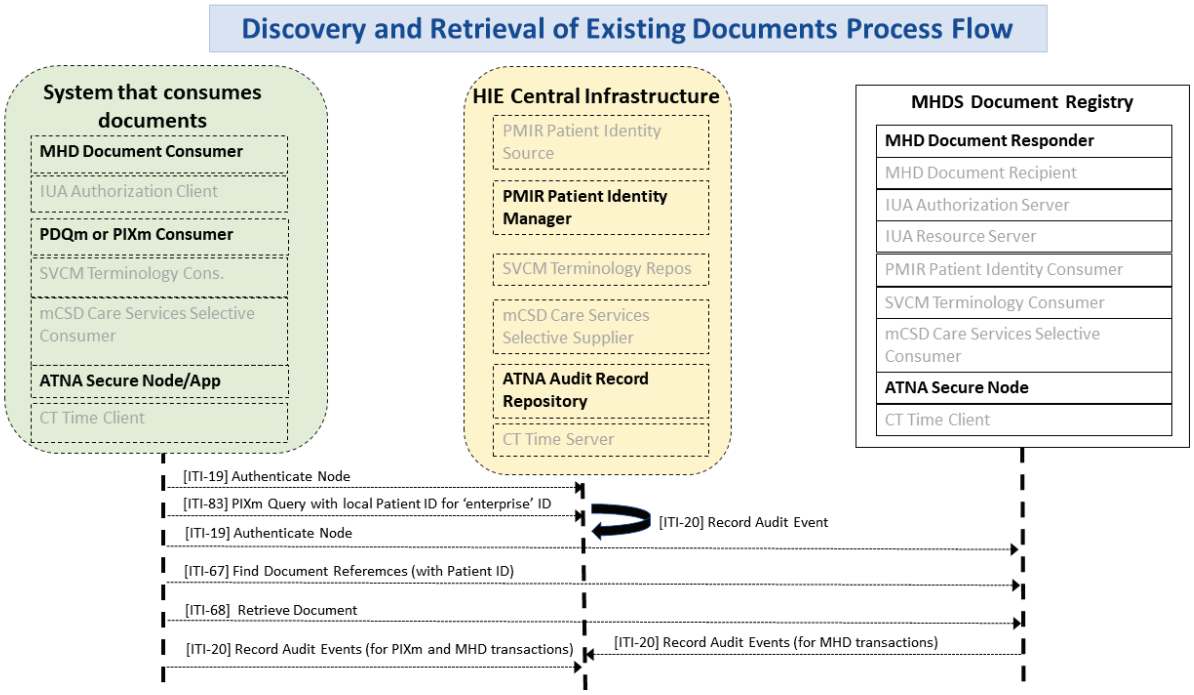

Figure 50.1.1.1.2-1: Discovery and Retrieval of Existing Document Process Flow

1. The Document Registry SHALL confirm its identity to the requesting system by use of the ATNA Secure Node or Secure Application TLS protocol using a Certificate assigned to the Document Registry.
2. When the Authorization Option is implemented and enabled, the Document Registry SHALL confirm the client identity using the IUA Profile.
3. Additional policy driven requirements, not specified here, may also apply. Such as enforcement at the Document Registry of Patient-specific Consent Directives.
4. The Document Registry SHALL validate that the subject of the find or retrieve request is a Patient that is a recognized Patient within the Community. The Patient identity must be recognized by the approved PMIR Patient Identity Manager system. This may be accomplished by a query of the PMIR manager, by way of a cached internal patient database, or other means.
5. The Document Registry SHALL provide the persisted resources to the grouped MHD Document Responder in support of the Document Responder duties to return results.
6. The Document Registry, if the Authorization Option is used, SHALL confirm that only authorized results are returned.
7. The Document Registry SHALL record a success or failure event into the ATNA Audit Record Repository.

 Copyright © 2020: IHE International, Inc.

50.1.1.1.3 When the grouped PMIR Patient Identity Consumer – is triggered

Triggered by: a Mobile Patient Identity Feed [ITI-93] transaction with a Merge:

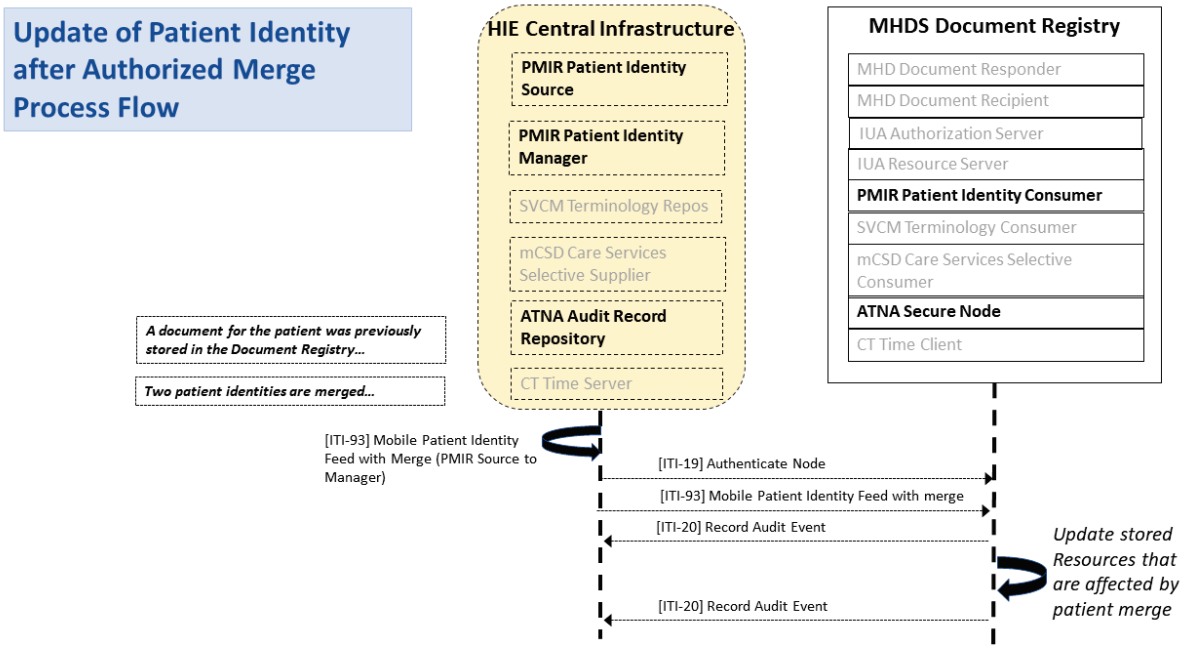

Figure 50.1.1.1.3-1: Patient Merge Process Flow

The Document Registry SHALL search for any resources with the deprecated `_id` value in the `DocumentManifest.subject`, `DocumentReference.subject`, and `List.subject`; and replace subject value of with the surviving `id`. The Document Registry SHALL record a single audit event indicating the Merge action, with an `.entity` element for each of the updated Document Registry Resources updated. The Document Registry SHOULD create within the Document Registry a single Provenance Resource indicating the Merge action, with the `.target` element pointing at all of the resources updated by the Document Registry.

No behavior is expected of the Document Registry on receipt of a feed containing create, delete, or update, although the Document Registry may consume and persist these to support the Document Registry requirements to validate Patient references as a recognized Patient within the Community.

50.1.1.2 Storage of Binary

There are two alternatives for storing the Binary Resource for documents stored in the community: (1) The Document Source includes the Binary Resource in the [ITI-65] transaction, and the Document Registry is required to store it. (2) The Community allows the Binary to be stored elsewhere in the Community.

 Copyright © 2020: IHE International, Inc.

The second alternative requires that the Community has the alternative to store the Binary in a system in the Community other than the Document Registry. This might be other centralized infrastructure, distributed infrastructure, or within the system implementing the Document Source. The [ITI-65] transaction does not include the Binary, and the `DocumentReference.content.attachment.url`. value is a persistent URL to the Binary content. When this is used by the Community, the service hosting the Binary shall:

- persist the Binary for the lifecycle expected of the Community,
- provide access to the community members,
- use the security model agreed to by the community members

50.2 MHDS Actor Options

Options that may be selected for each actor in this profile, if any, are listed in the Table 50.2-1. Dependencies between options, when applicable, are specified in notes.

Table 50.2-1: MHDS – Actors and Options

Actor	Option Name	Reference
Document Registry	Authorization Option	Section 50.2.1
	Consent Manager Option (Note 1)	Section 50.2.2
	SVCM Validation Option	Section 50.2.3
	Uncontained Reference Option	Section 50.2.4

Note 1: The Consent Manager Option requires the Authorization Option

50.2.1 Authorization Option

The Document Registry SHALL be grouped with an IUA Resource Server and IUA Authorization Server Actors. The IUA Resource Server enforces OAuth Authorization decisions made by the grouped IUA Authorization Server. Thus, all accesses to the Document Registry must have a token issued by the IUA Authorization Server. These IUA Authorization Server decisions protect both requests from MHD Document Source Actors for publication, and from MHD Document Consumer actors for access and disclosure. The rules used for this authorization decision are not defined in the MHDS Profile. See the Consent Manager Option for specific access control rules associated with that option.

 Copyright © 2020: IHE International, Inc.

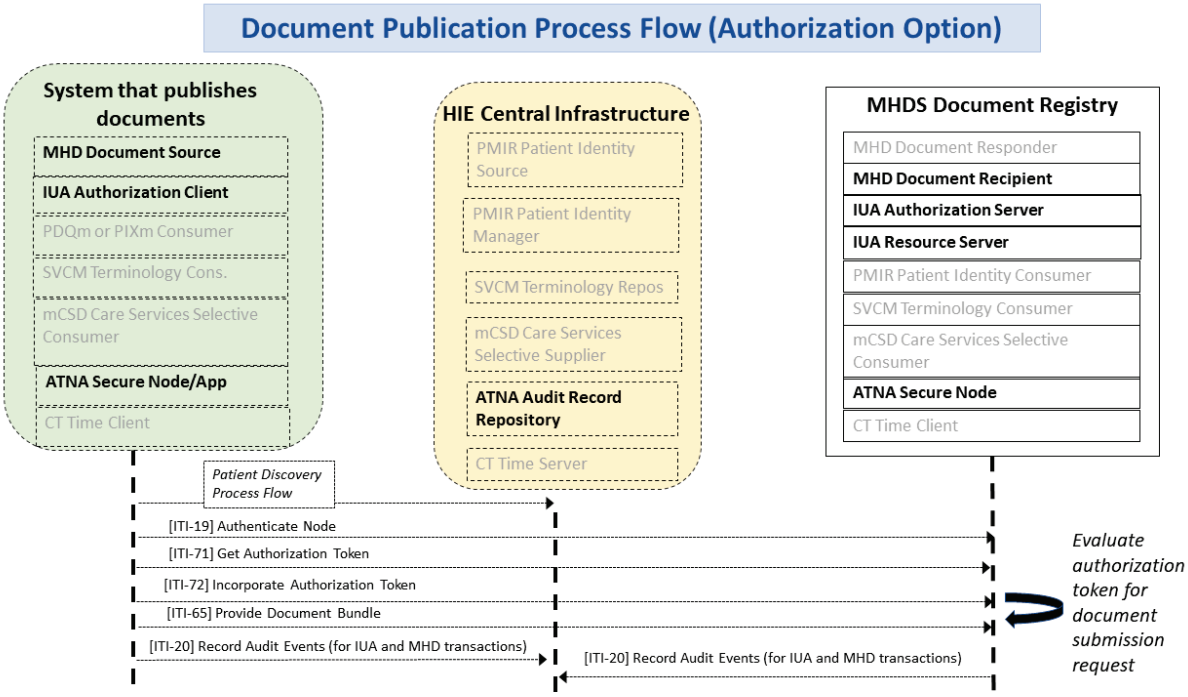

Figure 50.2.1-1: Document Publication Process Flow with Authorization Option

50.2.2 Consent Manager Option

The Document Registry SHALL be grouped with an IUA Resource Server and the IUA Authorization Server in order to enforce simple Permit and Deny access patient specific privacy disclosure consents for Treatment purpose. The Consent Manager Option does not affect publication by Document Source to the Document Registry, but rather only affects disclosure activities between a Document Consumer and the Document Registry.

The grouped IUA Authorization Server would be used to manage the consent status and make authorization decisions based on the consent status. The changing of the status is a functional requirement that is not defined by IHE. The IUA Resource Server that is grouped with the MHDS Document Registry would enforce these decisions.

 Copyright © 2020: IHE International, Inc.

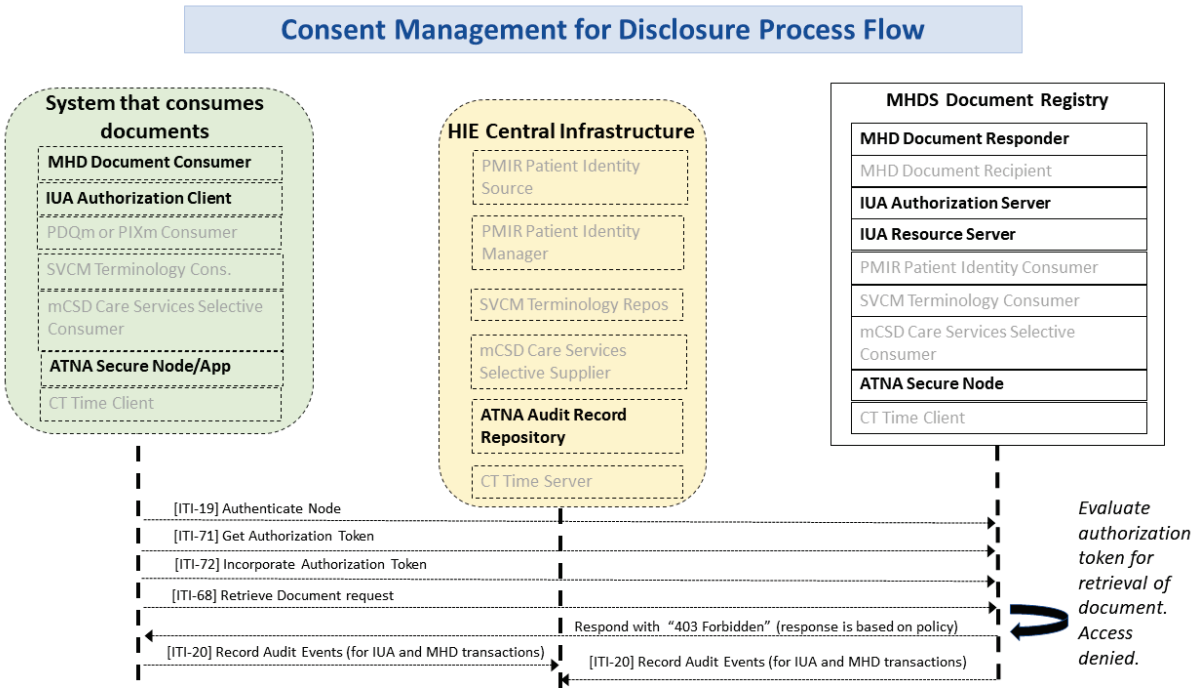

Figure 50.2.2-1: Consent Management for Disclosure Process Flow

The grouped IUA Authorization Server SHALL support consent configuration to enable Implied Consent and Explicit Consent environments. Implied Consent environments allow disclosure when no Consent has been recorded for that patient, Explicit Consent environments Deny disclosure when no Consent has been recorded for that patient.

The Permit policy is specific to requests from an authorized Document Consumer from authorized identities (applications and/or users) with appropriate roles, and authorized Treatment PurposeOfUse.

Figure 50.2.2-2: Simple Consent state diagram

 Copyright © 2020: IHE International, Inc.

The IUA Authorization Server SHALL

- support Permit and Deny policies and may support other policies.
- support through some functionality the patient consent state to be changed: Authorize action to move from Deny to Permit state, and Revoke action to move from Permit to Deny state.
- support consent state for PurposeOfUse of Treatment (HL7 PurposeOfUse code of "TREAT") and may support consent states for other PurposeOfUse values within the scope of the MHDS community.
- Deny access to any PurposeOfUse not authorized.
- support expiring a consent that results in a Permit state automatically transitioning to Deny at expiration.

The IUA Resource Server enforcement point grouped with the MHDS Document Registry SHALL enforce the security authorization decision. This includes confirming all data requested are for the specific patient. This prevents a Document Consumer from requesting access to resources outside the scope of the security token given it by the IUA Authorization Server.

Note that this option does not protect Binary content stored outside of the Document Registry; see Section 50.1.1.2. When documents are stored outside of the Document Registry, the Document Source system takes on the burden of protecting the document.

In order to support this Consent Manager Option, the following IUA constraint is defined. This constraint impacts the Document Consumer grouped IUA Authorization Client, and the IUA actors within the Document Registry. The important elements for the Document Consumer to convey are the scope values for PurposeOfUse and the identity of the Patient. This OAuth Scope specification does not require the use of SMART-on-FHIR but is compatible with it. There are two defined scope values that are included in the scope separated by a space and repeated as necessary:

```
"PurposeOfUse" '.' PurposeOfUse
queryParam (e.g. "patient" '=' Patient)
```

e.g., a simple request for Treatment access to patient f5c7395

```
PurposeOfUse.TREAT patient="http://myserver.example/fhir/Patient/f5c7395"
```

e.g., a request for Treatment, Payment, and Operations access to patient f5c7395 in addition to SMART-on-FHIR scopes for read access to DocumentReference, DocumentManifest, List, and Binary

```
user/DocumentReference.read user/DocumentManifest.read user/List.read user/Binary.read
PurposeOfUse.TREAT PurposeOfUse.HPAYMT PurposeOfUse.OPERAT
patient="http://myserver.example/fhir/Patient/f5c7395"
```

 Copyright © 2020: IHE International, Inc.

50.2.3 SVCM Validation Option

The Document Registry that supports the SVCM Option SHALL be grouped with a SVCM Terminology Consumer and uses this interface to do validation of submitted metadata codes in the [ITI-65] submission as being within in the community assigned valueSet. If any of the codes are found to be not valid then Document Registry SHALL reject the [ITI-65] transaction.

50.2.4 UnContained Reference Option

By default in [ITI-65], an MHD Document Source is required to include by containment the information in the `DocumentReference.author`, the `DocumentReference.authenticator`, the `DocumentReference.context.sourcePatientInfo`, and the `DocumentManifest.author`. This requirement encourages the persisting of the information at the time the document is published. This supports lifecycle management that recognizes that these identities change over time, and often become invalid due to individual retirement or other reasons to no-longer be active (e.g., the document is utilized 20 years after it was first published, and thus the original author has long since retired and would therefore not be in an active provider directory.)

The UnContained Reference Option recognizes that a Community may choose to longitudinally maintain their mCSD provider directory and PMIR patient directory. When this longitudinal consistency is managed, then the entries in the MHDS Document Registry do not need to make a copy of the information known at the time of publication since a Reference to the information in these directories will be valid over the full lifecycle of the Document Registry entries.

The UnContained Reference Option requires the grouped MHD Document Recipient to support the MHD UnContained Option. An MHD Document Source may implement the MHD UnContained Option so as to be able to send UnContained References. The MHD and MHDS UnContained Option allows `DocumentReference.author`, `DocumentReference.authenticator`, `DocumentReference.context.sourcePatientInfo`, and `DocumentManifest.author` to be a Reference to a (Practitioner|PractitionerRole|Organization|Patient) Resource, where the referenced resource is published in the associated centrally managed mCSD Care Services Selective Supplier, or PMIR Patient Identity Manager.

 Copyright © 2020: IHE International, Inc.

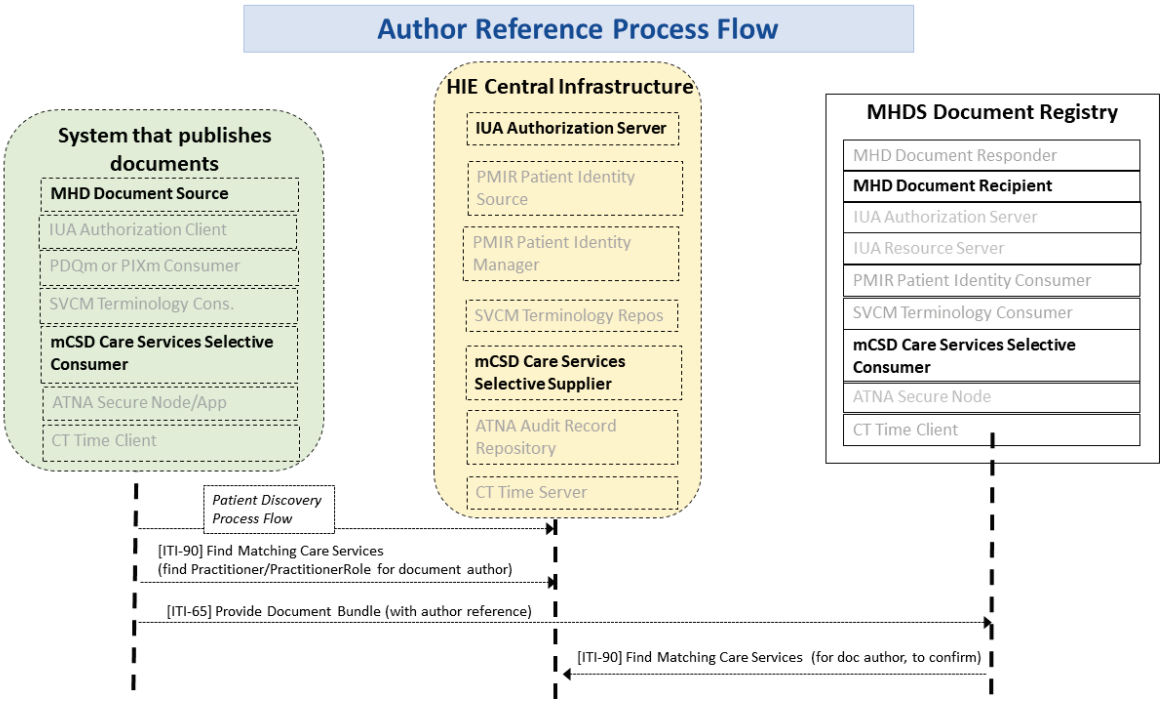

Figure 50.2.4-1: Author Reference Process Flow

The mCSD Care Services Selective Supplier and the PMIR Patient Identity Manager are persisting long term the data so that the Resources within the Document Registry are available for the life of the Document Registry entry.

The Document Registry shall validate publication requests to ensure that all `DocumentReference.author`, `DocumentReference.authenticator`, `DocumentReference.context.sourcePatientInfo`, and `DocumentManifest.author`; elements are either contained or are references to valid and active entry in the mCSD Care Services Selective Supplier or PMIR Patient Identity Manager. The Document Registry shall validate this by use of mCSD Care Services Selective Consumer using the Find Matching Care Services [ITI-90] transaction, and Patient identity either internal Patient identity cache or possibly by PMIR Patient Identity Manager using the PDQm Query [ITI-78].

50.3 MHDS Required Actor Groupings

An actor from this profile (Column 1) shall implement all of the required transactions in this profile ***in addition to all*** of the requirements for the grouped actor (Column 3).

Section 50.5 describes some optional groupings that may be of interest for security considerations and Section 50.6 describes some optional groupings in other related profiles.

 Copyright © 2020: IHE International, Inc.

Table 50.3-1: Required Actor Groupings

MHDS Actor	Grouping Condition	Actor(s) to be grouped with	Reference
Document Registry	Required	CT / Time Client	ITI TF-1:7
	Required	ATNA / Secure Node or Secure Application with the STX: TLS 1.2 with the BCP195 Option and the ATX: FHIR Feed Option	ITI TF-1:9
	Required	MHD / Document Responder	ITI TF-1:33
	Required	MHD / Document Recipient with the Comprehensive Metadata Option	ITI TF-1:33
	Required	PMIR / Patient Identity Consumer	ITI TF-1:49
	if the Authorization Option	IUA / Resource Server	ITI TF-1:34
	if the Authorization Option	IUA / Authorization Server	ITI TF-1:34
	if the UnContained References Option	mCSD / Care Services Selective Consumer	ITI TF-1:46
	if the SVCM Validation Option	SVCM / Terminology Consumer	ITI TF-1:51

50.4 MHDS Overview

The MHDS Profile provides a Document Registry that persists, manages, and provides access using the MHD access methods. This is in support of IHE Document Sharing as described in Section 50.7.

50.4.1 Concepts

The MHDS Profile supports Document Sharing utilizing only FHIR infrastructures. This is similar functionality to XDS but using the FHIR standard and not SOAP. The advantage of the FHIR infrastructure is that it is based on more accessible technology, especially for mobile devices; but the solution is not limited to mobile devices.

50.4.2 Use Cases

50.4.2.1 Use Case #1: Publication of a new document with persistence

This use case utilizes MHD Document Source using the Provide Document Bundle [ITI-65] transaction to the Document Recipient that is grouped with the MHDS Document Registry. The Document Registry validates the publication request and persists the information if approved. The MHD Comprehensive Metadata Option is required of the MHD Document Source as the MHD Document Recipient within the MHDS Document Registry will implement the Comprehensive Metadata Option. See Section 50.1.1.1.1.

 Copyright © 2020: IHE International, Inc.

50.4.2.2 Use Case #2: Update of patient identity after an authorized Merge

This use case utilizes the grouped PMIR Patient Identity Consumer to enable the Document Registry to receive updates of Patient Identity, so that when a Merge is authorized, the Document Registry will update any of the references to the former Patient Identity with the Patient Identity that survives. See Section 50.1.1.1.3.

50.4.2.3 Use Case #3: Discovery and Retrieval of existing documents

The MHD Document Consumer is supported by the Document Registry grouped with the MHD Document Responder to allow for the Document Consumer to discover and retrieve document metadata and content. See Section 50.1.1.1.2.

50.4.2.4 Use Case #4: Consent Management for disclosure under Use Case #3

With the use of the Consent Management Option the Document Registry supports simple Allow and Deny patient privacy consents for disclosure. These controls are available to prevent unauthorized disclosure. These Consent Management function does not prevent publication from Use Case #1 to enable documentation longitudinal consistency and for accesses not mediated by Patient Privacy Consent. See Section 50.2.2.

50.5 MHDS Security Considerations

The security considerations for a content module are dependent upon the security provisions defined by the grouped actor(s).

This section will discuss how a community that leverages the MHDS Profiles for document sharing can protect patient privacy and information security.

An especially important aspect that is beyond the scope of IHE is the definition of the overall Policies of the community. There are whitepapers and handbooks from IHE (see Section 50.1), but there is no single policy that must be put in place by an IHE based community to ensure privacy and security. In this section, we will discuss potential policy decisions and positions with regard to the profiles. It is especially important for the reader to understand that the scope of an IHE profile is only the technical details necessary to ensure interoperability. It is up to any organization building a community to understand and carefully implement the policies of that community and to perform the appropriate risk analysis. Although this section is not going to define the policies that a community should have, it will explore some of the policy building activities to demonstrate how such policies can be supported.

The Policy Environment is made up of many layers of policies. These policies work together in an interlocking hierarchy. We will introduce some of these layers in this section and show how they influence the technology. At the highest layer are international policies, like the International Data Protection Principles. Countries or regions will have specific policies. Some examples are USA HIPAA Security and Privacy Rules, with further refinement by the states. There are horizontal policies that are common among a specific industry, such as those from medical professional societies. Then within the enterprise will be specific information

 Copyright © 2020: IHE International, Inc.

technology policies. As shown in this section, the IHE Profiles offer not only the means to exchange information, but to do so in a way that is supportive of many of the policies mentioned.

The policy landscape that the community is built on needs to be defined well before the community is built.

50.5.1 Policies and Risk Management

IHE solves interoperability problems via the implementation of technology standards. It does not ***define*** Privacy or Security Policies, Risk Management, Healthcare Application Functionality, Operating System Functionality, Physical Controls, or even general Network Controls.

While community Policies and Risk Management are outside its scope, IHE does recognize that these elements are a necessary piece of a system implementation. IHE IT Infrastructure technical white paper, "Template for XDS Affinity Domain Deployment Planning" outlines some of the issues that should be evaluated for inclusion in the local Policy creation and Risk Management decisions. It is therefore the duty of system implementers to take this guidance into account as part of their Risk Management practices.

Implementers need to be aware of different kinds of policies that need to be harmonized with those policies of the local health enterprises connected to the community. The following is a list of sample policy fragments to stimulate discussion:

- Policies for who has access to what type of documents in the community
- Policies for who is allowed to publish documents into the community
- Policies on the acceptable types of documents that can be published into the community
- Policies that indicate acceptable levels of risk within community
- Policies that indicate what sanctions will be imposed on individuals that violate the community policies
- Policies on training and awareness
- Policies on user provisioning and de-provisioning within the community and local operation
- Policies on emergency mode operations
- Policies on acceptable network use (browser, decency, external-email access, etc.)
- Policies on user authentication methods that are acceptable
- Policies on backup and recovery planning
- Policies on acceptable third-party access
- Policies on secondary use of the information in the community

 Copyright © 2020: IHE International, Inc.

- Policies on the availability of the community systems (are the community systems considered life critical, normal, or low priority)
- Policies for maintenance downtime
- Policies for length of time that information will be maintained in the community

These policies are not a flat set, but often interlock and at other times cascade. An important set of policies are those around emergency modes. There are wide definitions of cases that are referred to as emergency mode. These emergency modes need to be recognized for the risks they present. When these use cases are factored in up-front, the mitigations are reasonable.

- Natural or manmade catastrophic disaster (e.g., hurricane, earthquake) – often times additional workforce migrates into the area from other places to help out. These individuals need to quickly be screened and provisioned with appropriate access.
- Utility failure (e.g., electric failure) – this situation is common and easily handled through uninterruptible power supplies and backup generation
- IT infrastructure failure (e.g., hard drive crash) – this situation is also common and handled through common infrastructural redundancy
- Need to elevate privileges due to a patient emergency, often called break-glass (e.g., nurse needs to prescribe)
- Need to override a patient specified privacy block due to eminent danger to that patient – this override is not a breaking of the policy but would need to be an explicit condition within the policy.

Often times being in the emergency department is considered as an emergency mode, but the emergency department is really a normal mode for those scheduled to work there. When looked at as normal mode, the proper privileges and workflow flexibility can be specified.

Policy development often is frustrated by apparent conflicts in the goal or effect of multiple layers of policies. These conflicts are often only on the surface and can be addressed upfront once the details of the policy are understood. A good example of a policy conflict is in records retention requirements at the national level vs. at the Medical Records level. Medical Records regulatory retention is typically fixed at a short period after death, yet if the patient has black lung then the records must be preserved well beyond.

50.5.2 Technical Security and Privacy controls

In 1980, the Organization for Economic Cooperation and Development ("OECD") developed Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines were intended to harmonize national privacy laws, uphold human rights, and promote the free flow of information among its 30 member countries. The OECD guidelines have served as a basis for data protection laws in the United States, Europe, Canada, Japan, Australia, and elsewhere. Together, these principles and laws provide a useful framework for developing

 Copyright © 2020: IHE International, Inc.

general data protection requirements for health information systems. For more information see http://oecdprivacy.org.

Based on the experience of the IHE participants in implementing community environments there is a common set of Security and Privacy controls that have been identified. These controls are informed by a combination of the OECD data protection principles, experience with explicit policies at community implementations, and Security Risk Management.

These security and privacy controls are:

1. Audit Log Controls – The controls that can prove the system is protecting the resources in accordance to the policies. This set of controls includes security audit logging, reporting, alerting and alarming.
2. Identification and Authentication Controls – The controls that prove that a system or person is who they say that they are. For example: personal interactions, Oauth, OpenID-Connect
3. Data Access Controls – The controls that limit access by an authenticated entity to the information and functions that they are authorized to have access to. These controls are often implemented using Role Based Access Controls (RBAC), or Attribute Based Access Controls (ABAC).
4. Secrecy Controls– As sensitive information is created, stored, communicated, and modified; this control protects the information from being exposed. For example: encryption or access controls.
5. Data Integrity Controls – The controls that prove that the data has not changed in an unauthorized way. For example: digital signatures, secure hash algorithms, CRC, and checksum.
6. Non-Repudiation Controls – The controls that ensure that an entity cannot later refute that they participated in an act. For example, author of a document, order of a test, prescribe of medications.
7. Patient Privacy Controls – The controls that enforce patient specific handling instructions.
8. Availability Controls – The controls that ensure that information is available when needed. For example: backup, replication, fault tolerance, RAID, trusted recovery, uninterruptible power supplies, etc. (not an area where Interoperability applies)

50.5.3 Applying Security and Privacy to Document Sharing

IHE does not set policies but is policy sensitive. Therefore, we now discuss the policy enabling technologies but not the policies themselves.

This section shows how the existing security controls in the local health IT system are leveraged and extended when they become interconnected through document sharing.

 Copyright © 2020: IHE International, Inc.

50.5.3.1 Basic Security

IHE recognizes that in healthcare, with patient lives at stake, audit control is the primary method of accountability enforcement. The profile that provides this basic security principle is Audit Trail and Node Authentication (ATNA). This profile requires three things of each system:

1. User authentication and Access Controls are enforced accordingly,
2. Security Audit Logs are recorded, and
3. Strong network authentication and encryption for all communications of sensitive patient data

The Security Audit Logging includes a set of security relevant events that must be audited. When one of these events happens the record of the event must be described a specific way. The systems are expected to support the recording of all of the security relevant events that might happen in the system. The ATNA Profile offloads the recording, filtering, alerting, and reporting to an audit service. The more centralized this audit log analysis can be, the easier it is to prove accountability across the whole Document Sharing exchange.

Once it is known that the system will enforce Access Controls and Audit Controls then it can be connected to other systems that have also been assessed positively. In this way these systems only talk to other systems that also agree to enforce the common policies. This creates a basis for a chain of trust through accountability among all of the systems participating in the Document Sharing exchange. The communications between these trusted systems is also encrypted.

50.5.3.2 Protecting different types of documents

The IHE Document Sharing profiles, like MHDS, allow for many different types of documents to be shared. These documents are likely to have different levels of confidential information in them. For instance, one document might contain the very basic health information that the patient considers widely distributable. Another document might be made up totally of information necessary for proper billing such as insurance carrier and billing address. Yet another document might carry the results of a very private procedure that the patient wishes to be available only to direct care providers. This differentiation of the types of data can be represented using a diagram like found in Table 50.5.3.2-1: Sample Access Control Policies.

 Copyright © 2020: IHE International, Inc.

Table 50.5.3.2-1: Sample Access Control Policies

Sensitivity Functional Role	Research Information	Billing Information	Administrative Information	General Clinical Information	Sensitive Clinical Information	Mediated by Direct Care Provider
HL7 confidentialityCode (2.16.840.1.113883.5.25)	**U**	**L**	**M**	**N**	**R**	**V**
Administrative Staff		X	X			
Dietary Staff			X			
General Care Provider			X	X		
Direct Care Provider			X	X	X	X
Emergency Care Provider (e.g., EMT)				X		
Researcher	X					
Patient or Legal Representative		X	X	X	X	

Then documents can be labeled with one or more of the codes on the columns, and results in the specified Functional Roles to be given access to that type of document. In this way, the document sharing metadata informs the Role-Based Access Control (RBAC) decisions through self-describing sensitivity, known as confidentialityCode.

In the same way that the Document Sharing metadata 'doctype' defines what the document is in terms of the clinical/administrative content, the confidentialityCode defines what the document is in terms of privacy/security content, sometimes referred to as sensitivity. The confidentialityCodes should be looked at as a relatively static assessment of the document content privacy/security characteristics. Some documents are so sensitive in nature that they simply should not be shared or published.

The rows are showing a set of functional roles. These roles would be conveyed from the requesting organization through the use of the Internet User Authorization (IUA) Profile. This profile defines how a user and the security/privacy context of the request is defined. Additional information can be carried such as the PurposeOfUse, what the user intends to use the data for. Note that Privacy Policies and Access Control rules can leverage any of the user context, patient identity, or document metadata discussed above.

 Copyright © 2020: IHE International, Inc.

50.5.3.3 Patient Privacy Consent to participate in Document Sharing

The topic of Patient Privacy Consent (Authorization) to collect, use, and disclose is a complex topic. This complexity does not always need to be exposed in full detail across a Document Sharing exchange. That is, a request for information does need to consider the current status of any Patient Privacy Consent that the patient has given, but most of the time explaining the detail of this Privacy Consent to the requesting system/individual adds no value. Most often the requesting system/individual is either fully empowered to receive and use the content, or not authorized at all. In these cases, the use of user identity context, as discussed above around the IUA Profile, is sufficient to make the Access Control decision. The trust relationship of the Document Sharing exchange includes background governance on appropriate use, as discussed above around the ATNA Profile.

Privacy Consents may need to be expressed in a way that all parties in a Document Exchange can understand. IHE has published the Basic Patient Privacy Consents (BPPC) Profile that can be used to enable basic privacy consent controls, and Advanced Patient Privacy Consents (APPC) that can encode more complex rules specific to a patient consent. The encoding of Consent and advanced rules in FHIR "Consent" resource is possible but has not yet been profiled by IHE.

Some examples of the type of policy that can be necessary for Patient Privacy Consents are:

- Explicit Opt-In (patient elects to have some information shared) is required which enables document sharing
- Explicit Opt-Out (patient elects to not have information shared) stops all document sharing
- Implicit Opt-In allows for document sharing
- Explicit Opt-Out of sharing outside of use in local care events, but does allow emergency override
- Explicit Opt-Out of sharing outside of use in local care events, but without emergency override
- Explicit authorization captured that allows specific research project
- Change the consent policy (change from opt-in to opt-out)

The BPPC Profile can be used as a gate-keeper to the document sharing community. BPPC does not define the policies but does allow for a community that has defined its set of policies to capture that a patient has chosen one or more of those policies.

For example: Let's say that the above set of sample policy fragments was available to a patient sharing in a community. The patient could agree to Opt-In, and also agree to a specific research project. This set of acknowledgments would be captured as one or more BPPC documents. These documents would indicate the policy that is being acknowledged, the date it is being acknowledged, an expiration date if applicable, etc. Then the systems involved in the document

 Copyright © 2020: IHE International, Inc.

sharing can know that the patient has acknowledged these policies and thus the patient's choices can be enforced. A system that is doing research can see that this patient has acknowledged participation in the research project, while other patients have not.

Let's further examine what happens when the patient changes their decision. For example, the patient is moving to a totally different region that is not served by this community. The patient can acknowledge the Opt-Out policy. This policy would then be registered as a replacement for the previous Opt-In policies including the research policy. Thus, now if that research application tries to access the patient's data, it will be blocked as the patient does not have a current acknowledgement of the research policy.

50.5.3.4 Security and Privacy in a Patient Safety Environment

The IHE security and privacy model supports both centralized and distributed control. The entities that are allowed to participate in community-based document sharing need to be evaluated to assure that they have the capability to enforce the policies they are expected to enforce. This may mean that access control is enforced at the edge systems, at the center, or more likely in both places.

In healthcare, beyond the basic security principles, we must additionally be sensitive to patient care and safety. The applications closest to the patient are best informed for determining the context of the current situation. It is primarily at this level that emergency mode can be handled in a robust way (often called break-glass).

The IHE security and privacy model is very careful to include security while allowing for flexible and safe provision of healthcare by individual participants.

50.5.4 IHE Security and Privacy Controls

The following is a breakdown of the security and privacy controls and in what way the IHE profiles can help. The following table shows the set of identified Controls (identified in above) as columns and the supportive IHE Profiles as rows. In this table a '√' indicates a direct relationship. A direct relationship means that the Profile addresses the security and/or privacy principle. An '." indicates an indirect relationship, meaning that the Profile assists with the principle. Further details on the '√' direct and '.' Indirect relationships can be found in the profile text or through other webinars.

 Copyright © 2020: IHE International, Inc.

Table 50.5.4-1: Profiles relationship to Controls

Security & Privacy Controls / IHE Profile	Audit Log	Identification and Authentication	Data Access Control (Authorization)	Secrecy	Data Integrity	Non-Repudiation	Patient Privacy
Audit Trails and Node Authentication	√	√	√	√	√	√	√
Consistent Time	√	·				√	
Internet User Authorization		√	√			·	·
Cross-Enterprise User Assertion		√	·			·	·
Basic Patient Privacy Consents			·				√
Mobile Care Services Discovery		√	·			·	
Document Digital Signature		√			√	√	
Document Encryption			√	√	·		

50.6 MHDS Cross Profile Considerations

This section includes interactions between systems, with details at the actor and transaction level:

1. Overall Perspective from publication of documents to consumption of documents
2. Typical system that publishes documents
3. Typical system that consumes documents
4. Typical system that consumes data elements extracted from documents
5. Central Infrastructure supporting services

50.6.1 Interaction Diagram for the MHDS environment.

Figure 50.6.1-1 shows a simplified view, where the following simplified components are defined:

- "Publisher" – represents "System that publishes Documents"
- "Consumer" – represents "System that consumes Documents"
- "Patient" – represents actions the patient themselves might do, such as seeking care
- "PatientDir" – represents the PMIR Patient Identity Manager that is managing identity for the community
- "ConsentMgr" – represents the Consent Manager function within the Document Registry when the Consent Manager Option is used

 Copyright © 2020: IHE International, Inc.

- "Registry" – represents the MHDS Document Registry defined in this profile

The diagram has "Opt" groupings with actions of a

1) Patient Identity (PMIR feed): representing new knowledge about the Patient at the source. Deeper details on this interaction can be found in the PMIR Profile
    a. This diagram does not show the PMIR feed out to all the community participants, but this is enabled by PMIR, where all the community participants can subscribe to the PMIR manager for feed.
2) Publication of new Documents to represent a case where new data need to be published.
    a. the PDQm is used to get the golden patient identifier for use in the Document Registry.
3) the Provide transaction includes a DocumentManifest, DocumentReference, and the Binary resource containing the document. Get consent to disclose documents
    a. There is no standard protocol, this functionality would be provided by the Consent Manager. It might by a User Interface or some undefined transaction. The consent must be legally obtained according to local regulations and user experience expectations.
4) Discover Patient Master Identity and data (MHD)
    a. This portion starts with the patient visiting the Consumer. Thus there is a potential for a PMIR feed updating the PMIR manager. Not all visits will result in a feed.
    b. Given that the Consumer wants to discover documents, it will first use PDQm to get the proper identity for the community. As indicated above other methods are available other than PDQm.
    c. The Consumer must get a security token from the Consent Manager that is part of the Document Registry using the Consent Manager Option
    d. The Recipient queries the Registry to find appropriate entries, and selects the one of interest
    e. The Recipient will GET the document given the DocumentReference.content.attachment.url

 Copyright © 2020: IHE International, Inc.

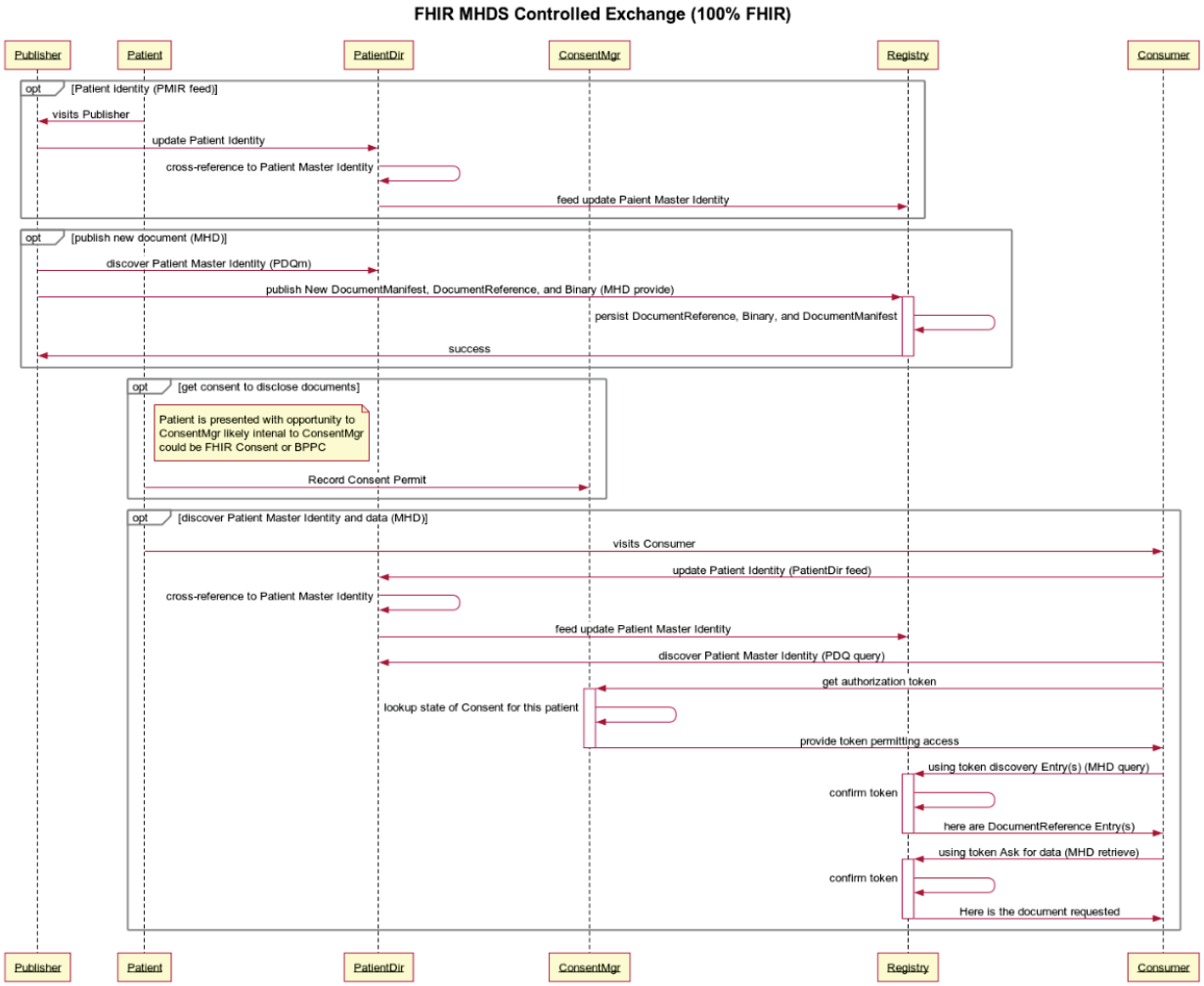

Figure 50.6.1-1: FHIR MHDS Controlled Exchange (100% FHIR)

Source for WebSequence diagram above

```
title FHIR MHDS Controlled Exchange (100% FHIR)

participant Publisher
participant Patient
participant PatientDir
participant ConsentMgr
participant Registry
participant Consumer
```

```
opt Patient identity (PMIR feed)
Patient->Publisher: visits Publisher
Publisher->PatientDir: update Patient Identity
PatientDir->PatientDir: cross-reference to Patient Master Identity
PatientDir->Registry: feed update Patient Master Identity
end

opt publish new document (MHD)
Publisher->PatientDir: discover Patient Master Identity (PDQm)
Publisher->+Registry: publish New DocumentManifest, DocumentReference, and
Binary (MHD provide)
Registry->Registry: persist DocumentReference, Binary, and DocumentManifest
Registry->-Publisher: success
end

opt get consent to disclose documents
note right of Patient
Patient is presented with opportunity to
ConsentMgr likely internal to ConsentMgr
could be FHIR Consent or BPPC
end note
Patient->ConsentMgr: Record Consent Permit
end

opt discover Patient Master Identity and data (MHD)
Patient->Consumer: visits Consumer
Consumer->PatientDir: update Patient Identity (PatientDir feed)
PatientDir->PatientDir: cross-reference to Patient Master Identity
PatientDir->Registry: feed update Patient Master Identity
Consumer->PatientDir: discover Patient Master Identity (PDQ query)
Consumer->+ConsentMgr: get authorization token
ConsentMgr->ConsentMgr: lookup state of Consent for this patient
ConsentMgr->-Consumer: provide token permitting access
```

 Copyright © 2020: IHE International, Inc.

```
Consumer->+Registry: using token discovery Entry(s) (MHD query)
Registry->Registry: confirm token
Registry->-Consumer: here are DocumentReference Entry(s)
Consumer->+Registry: using token Ask for data (MHD retrieve)
Registry->Registry: confirm token
Registry->-Consumer: Here is the document requested
end
```

50.6.2 Typical Client System Designs

This section shows a typical client system design. This is informative to help explain how these various actors interact.

The actors and transactions are not fully explained here, please see the formal profiles referenced for details on the actual actor and transaction functionality, responsibility, and interoperability.

Following the sections outline sample IHE Integration Statements for systems of various functionality. For more details on the full use and format of an IHE Integration Statement (see Appendix F).

50.6.2.1 System that publishes documents System Design

This system can publish documents using the MHD Document Source. The other actors shown are there to support this primary function.

System that publishes documents - Integration Statement

Profiles Implemented	Actors Implemented	Options Implemented
MHD	Document Source	
CT	Time Client	
PMIR	Patient Identity Source	
PIXm	Patient Identity Consumer	
PDQm	Patient Demographics Consumer	
SVCM	Terminology Consumer	
ATNA	Secure Node	STX: TLS 1.2 Floor using BCP195 Option
		ATX: FHIR Feed Option
IUA	Authorization Client	

 Copyright © 2020: IHE International, Inc.

Profiles Implemented	Actors Implemented	Options Implemented
mCSD	Care Service Selective Consumer	
NPFS	File Consumer	

50.6.2.2 System that consumes documents System Design

This system can consume documents using the MHD Document Consumer. The other actors shown are there to support this primary function.

System that consumes documents - Integration Statement

Profiles Implemented	Actors Implemented	Options Implemented
MHD	Document Consumer	
CT	Time Client	
PMIR	Patient Identity Source	
	Patient Identity Cross-Reference Consumer	
	Patient Demographics Consumer	
SVCM	Terminology Consumer	
ATNA	Secure Node	STX: TLS 1.2 Floor using BCP195 Option
		ATX: FHIR Feed Option
IUA	Authorization Client	
mCSD	Care Service Selective Consumer	
NPFS	File Consumer	

50.6.2.3 System that consumes clinical data elements Systems Design

This system can consume data elements using the QEDm Profile that have been extracted from the documents published in the MHDS by way of the mXDE Profile. The other actors shown are there to support this primary function. Further details can be found in the referenced profiles.

 Copyright © 2020: IHE International, Inc.

System that consumes clinical data elements - Integration Statement

Profiles Implemented	Actors Implemented	Options Implemented
QEDm	Clinical Data Consumer	
MHD	Document Consumer	
CT	Time Client	
PMIR	Patient Identity Source	
	Patient Identity Cross-Reference Consumer	
	Patient Demographics Consumer	
SVCM	Consumer	
ATNA	Secure Node	STX: TLS 1.2 Floor using BCP195 Option
		ATX: FHIR Feed Option
IUA	Authorization Client	
mCSD	Care Service Selective Consumer	
NPFS	File Consumer	

50.6.2.4 Central Infrastructure as a single system

1030 This is a system that contains all of the Central Infrastructure defined in MHDS as supporting services. These actors do not need to be combined into one system. This combined system is provided for informational purposes.

Central Infrastructure Integration Statement

Profiles Implemented	Actors Implemented	Options Implemented
MHDS	Document Registry	Authorization Option
		Consent Manager Option
		UnContained Option
		SVCM Validation Option
MHD	Document Responder	
MHD	Document Recipient	

 Copyright © 2020: IHE International, Inc.

Profiles Implemented	Actors Implemented	Options Implemented
PMIR	Patient Identity Consumer	
CT	Time Client	
SVCM	Terminology Consumer	
	Terminology Repository	
IUA	Resource Server	
	Authorization Server	
ATNA	Secure Node	STX: TLS 1.0 Floor with AES Option
		STX: TLS 1.0 Floor using BCP195 Option
		STX: TLS 1.2 Floor using BCP195 Option
		ATX: FHIR Feed Option
BPPC	Content Consumer	
CT	Time Server	
PMIR	Patient Identity Manager	
ATNA	Audit Record Repository	STX: TLS 1.0 Floor with AES Option
		STX: TLS 1.0 Floor using BCP195 Option
		STX: TLS 1.2 Floor using BCP195 Option
		ATX: FHIR Feed Option
IUA	Authorization Server	
	Resource Server	
mCSD	Care Service Selective Supplier	
NPFS	File Server	
mXDE	Data Element Extractor	
QEDm	Clinical Data Source	

50.7 MHDS Background

This section is adapted from the IHE Whitepaper Health Information Exchange: Enabling Document Sharing Using IHE Profiles. The adaption is to the specifics of the MHDS Profile.

 Copyright © 2020: IHE International, Inc.

The Integrating the Healthcare Enterprise (IHE) standards profiling organization has developed a collection of profiles which can be leveraged for use by healthcare communities for the purposes of document sharing. One of the most significant applications of healthcare information technology is the exchange of health information among disparate clinical information systems and otherwise unaffiliated care providers. Across the world, various communities have developed or are developing methods for exchanging health information among healthcare providers, patients, and other authorized parties.

Effective health information exchange involves a diverse set of activities and a broad set of challenges, whether that exchange takes place among affiliated or unaffiliated care providers. The IT Infrastructure (ITI) domain of IHE has addressed many of these challenges by defining a series of integration profiles to address specific aspects of exchanging healthcare information. Each integration profiles addresses part of the broad set of challenges involved in health information exchange. The profiles, however, do not attempt to address governance and policy choices that significantly affect how the profile is adapted in any particular community. IHE cannot address all such governance and policy issues but will provide some guidance on where governance and policy issues are applicable and offer some common approaches.

It is very important to note that IHE focuses only on interoperability and does not attempt to solve every issue involved in exchanging health information. These solutions are meant to be plugged into an architecture that is designed and executed by the exchange communities themselves. Thus, while each community will generate an architecture that meets its individual needs, the use of IHE profiles will lead to the creation of standards-based communities.

The MHDS Profile focuses on explaining how IHE profiles are used to address interoperability aspects of document sharing and how they work together to solve common document sharing problems. The IHE White Paper, "Template for XDS Affinity Domain Deployment Planning", provides support for policy and deployment planning. The IHE "Document Sharing Metadata Handbook", provides guidance on developing policy and vocabulary valuesets for use within the community. For application of Document Sharing for particular clinical use cases, consider the work of the clinical IHE domains: Anatomic Pathology, Cardiology, Eye Care, Laboratory, Patient Care Coordination, Patient Care Device, Pharmacy, Quality, Research and Public Health; Radiation Oncology, and Radiology.

50.7.1 Overview

A health document sharing community (community) exists for the purpose of increasing the accessibility of patient health information across multiple organizations so that clinicians can make more informed decisions about the care that they provide. Today, there are many communities already in production and many more are being planned. The size, nature and scope of communities vary widely but can be characterized by a number of different aspects.

First, some communities are geographically focused while others are not. What often comes to mind when speaking of a community is a regional organization that facilitates information exchange across multiple organizations that are relatively close in proximity. Major metropolitan

 Copyright © 2020: IHE International, Inc.

areas tend to be the focus of these communities, but often a regional community encompasses several rural locales. On the opposite extreme of the geographic aspect of communities is the network of United States Veterans Hospitals. The VA (Veterans Administration) hospitals are spread across the entire map of the US and beyond, yet significant efforts have been spent on being able to exchange data among these geographically separated care centers.

A second characteristic by which to categorize communities is the organizational structure of the community. In some cases, the community consists of a single hospital and several out-patient clinics that have a referral relationship with the hospital. In other cases, a network of competing hospitals, laboratories and private clinics may collaborate to form a community.

A third means by which to describe communities is the scope of the content shared. Some communities have very limited exchange functionality. For instance, a community may focus entirely on electronic lab result delivery or e-prescribing. Most communities define a moderate scope to their exchange activities that might include results delivery, electronic referrals, and perhaps some sharing of encounter-based information (e.g., dictations). More advanced communities leverage their network to include even larger scopes (perhaps including the sharing of documents with the patient's Personal Health Record, exchange of clinical summaries, regional patient centric workflows, etc.). No two communities are alike in terms of the set of exchange activities that they facilitate.

Finally, a fourth aspect of a community is the size, scope and political jurisdiction(s) that regulate it. The simplest community uses only an adhoc arrangement to push documents from one organization to another. National and sub-national jurisdictions have significant effects on the organization and operations of a community.

Despite all the variance among communities, each has the same ultimate goal: to increase the authorized exchange of patient health information across organizations so that clinicians can make better decisions by being more informed about the longitudinal health history. This ultimate goal provides the reason why the community exists, it is their affinity.

Once communities are formed there is a need to exchange health documents across the communities as well as within them. IHE uses the concept of cross-community to describe a federation of communities which use mostly peer-to-peer interactions for the purposes of health document sharing. A community may be a single organization, like the USA Veterans Administration, a complex community of many organizations, or a more simple organization like a single small hospital or facility. Cross-community describes an environment where multiple communities, be they simple, small, complex or large, interact without any understanding of or access to the internal structure of any of the other participants.

The MHDS Profile designs a single community document sharing exchange.

50.7.2 Principles of IHE for Health Document Sharing

This section describes several principles which are foundational to IHE's approach to health document sharing.

 Copyright © 2020: IHE International, Inc.

50.7.2.1 General IHE principles

The following general IHE principles are applicable to the set of IHE profiles used for Document Sharing, including MHDS:

- IHE profiles describe the interactions between systems and not the implementation within systems. Interactions between systems are typically described by transactions which are technically specific and detailed enough to ensure interoperability among implementing systems. The internal implementation of the systems is not prescribed by IHE. For example, for patient demographic matching IHE specified the format of the query and response but not the algorithm or method used for the demographic matching. This allows freedom for implementations to address scalability, creative functionality, reliability, and other value-add.
- IHE profiles are designed to support a wide variety of governance and policies. Because IHE supports adoption of its profiles around the world it is rarely possible to define policies that are applicable in all countries. For this reason, IHE profiles are designed with a variety of governance and policies in mind and are therefore applicable to a wide variety of environments. IHE profiles are designed to be policy neutral and support a broad set of governance; before they can be deployed there are many governance and policy issues that the communities must agree on. Examples of governance and policy issues are things like: roles and responsibilities, privacy, signature requirements, authorization, when to publish, what to publish, administrative roles, configuration, service level agreements, clinical pathways, long-term availability, etc.
- IHE assumes there is a general understanding of widely implemented Information Technology Standards. IHE profiles typically leverage underlying technology like XML, TCP/IP, DNS, Digital Certificates (PKI), etc. without detailed explanations.

50.7.2.2 Document Sharing Governance

IHE enables interoperable sharing of documents but assumes this sharing occurs under a document sharing governance structure agreed to by all parties involved. The governance structure addresses all policy issues necessary to enable document sharing; content format and coding; and other operational characteristics. The IHE profiles are designed to be agnostic to governance and policy, while also being designed to support and enforce those governance and policy choices. The governance may apply only within a small group, such as a hospital and small physician's office, or may apply at a large level, like an entire nation. In fact, sometimes temporary or informal governance (e.g., via phone call) based on understanding of existing laws or customs is used for exchange among participants. Typically, in order to allow for effective and efficient interactions, the governance structure is formalized through some legal mechanism. Overlapping governance is common, where one set of agreements exist in the region and a different set of agreements exist across the nation, yet most organizations will eventually want to exchange documents regionally, nationally and internationally.

 Copyright © 2020: IHE International, Inc.

In addition to general governance agreements, a document sharing community should address the following issues:

- **Format of document content**: To enable interoperable transfer of documents the receiving side must understand the format and structure generated by the sending side. Typically, there is an agreement on a set of document formats which must or may be supported. This could include unstructured content like PDF or text documents. Or a more structured format like CDA or a specific implementation guide applied to CDA for a particular purpose. The key is to ensure that whatever type of content is shared, the receiving system is able to interpret the content in an appropriate way, either through human review or machine processing.
- **Coding within documents**: Structured documents often include coded data derived from a given coding system. Agreeing on which coding systems to use for which data is often covered by an implementation guide for the structured document. Agreeing to an implementation guide, or a general guideline for coding systems to use, is necessary to enable semantic understanding of the document received.
- **Coding of metadata**: Metadata are data that provide information about one or more aspects of the document. In the case of IHE-defined document exchange, specific metadata are coded within the structure of the content being exchanged. See Section 50.7.2.6 where the metadata defined by IHE are introduced. Some of that metadata have values chosen from a coding system defined by the governance of the sharing community. Because IHE profiles can be applied in many parts of the world where coding systems are different, IHE has not specified which code sets to use and this decision must be made among the systems exchanging documents.

The purpose of this aspect of governance is to enable semantic interoperability among participating partners.

50.7.2.3 Distinction between Documents and Messages

The HL7 standard for Structured Documents Section 1.2 describes the document vs. message distinction as follows "A document is designed to be persistent for long periods of time, whereas messages are more often expected to be transient. There is a place for both of these constructs in healthcare." HL7 characterizes a document by the following properties:

- *Persistence* – Documents are persistent over time. The content of the document does not change from one moment to another. A document represents information stored at a single instance in time.
- *Wholeness* - A document is a whole unit of information. Parts of the document may be created or edited separately, or may also be authenticated or legally authenticated, but the entire document is still to be treated as a whole unit.
- *Stewardship* –A document is maintained over its lifetime by a custodian, either an organization or a person entrusted with its care.

 Copyright © 2020: IHE International, Inc.

- *Context* - A clinical document establishes the default context for its contents
- *Potential for authentication* - A clinical document is an assemblage of information that is intended to be legally authenticated.

Health messages, on the other hand, are not expected to be persistent, but represent a unit of information at a moment in time where the context is often implied by the transaction partners. The content is not always whole, where context may exist in the messaging environment rather than inside the message itself. The distinction between message and documents can get blurry at times, as messages sometimes can be persisted and can contain all necessary context. In fact, messages can be converted to documents and can carry documents within their content. But documents are expected to be persistent, relevant over time and having the same meaning regardless of environment. And messages need not be any of those things.

The scope of 'document' in the MHDS Profile and other IHE Document Sharing Profiles would prefer that documents have the above "Document" properties, but does not require that documents have these properties. The only property required is that there is a mime-type for the document.

50.7.2.4 Longitudinal Patient Record

Building on the document concepts described above in Section 50.7.2.3 of persistence, wholeness, stewardship and context, we can identify the principle of the longitudinal patient record which is foundational and central to health document sharing. Document Sharing Communities are patient centric, and the patient identity is associated with every document shared.

Care providers, which may support a broad variety of healthcare facilities: private practice, nursing home, ambulatory clinic, acute care in-patient facility, etc., are typically the sources or creators of health documents. Typically, a patient will go through a sequence of encounters in different care settings over the course of his/her lifetime. With each encounter there is the potential that a provider will produce a health document that can be shared with the community. Documents shared by the provider and tracked by a centralized registry (see Section 50.7.3.2) or federation of communities (see Section 50.7.3.3) form a longitudinal record for the patients that received care among those providers within the community. Longitudinal records, therefore, are expected to last over the span of many decades, just as the documents that comprise them are expected to have persistence, wholeness, stewardship, context, and potential for authentication. As a health information exchange is adopted it is a common practice to use an historical bulk data load, or comprehensive patient summary to initialize the electronic patient record with data for historical purposes.

Within a care setting Clinical Data Repositories (CDR) or Clinical Information Model Infrastructure databases might be used to enhance Clinical Decision Support as a complement to document discovery. These databases would not be nationwide, but rather be local to the patient's care facility, like EHRs themselves, Document Sharing supports interoperability

 Copyright © 2020: IHE International, Inc.

amongst local systems and supports a longitudinal patient record that spans across many local systems potentially using multiple different database systems.

50.7.2.5 Use of Documents

IHE Document Sharing profiles are content neutral, meaning that any type of information without regard to content and representation is supported. A document is any collection of bytes, including proprietary and textual formats. It is expected that a deployment of Document Sharing will restrict the format and content of documents exchanged to those agreed to by the partners in the exchange, as stated in Section 50.7.2.2. While the format and content of a document is not restrictively defined, it is expected to be a coherent set of healthcare data that includes enough context to be useful to a practitioner. A document should have the characteristics as described in Section 50.7.2.3 namely, persistence, wholeness, stewardship, context and potential for authentication.

IHE Document Sharing profiles assume that a patient identity is associated with every document shared (see Section 50.7.2.4).

The most common document content standards that are profiled by IHE are HL7 Clinical Document Architecture (CDA), and an emerging HL7 FHIR Document. These standard formats support the coding of the clinical content which allows for use of the content both for display purposes as well as machine processing. Although IHE encourages the use of CDA or FHIR as the document content type of choice, it does not restrict the content of a document in any way. Many times, a document will be encoded in PDF or simple text (e.g., U.S. Department of Veterans Affairs "Blue Button" program). Images and manifest documents may also be exchanged using the same infrastructure. By defining a document so liberally, IHE enables a common health record sharing infrastructure that is flexible enough to handle the content types agreed to by the partners in the exchange.

IHE and other organizations have profiles which define document content for specific, commonly occurring cases. For example, the IHE Laboratory domain has defined an XD-LAB content profile to support sharing laboratory reports. Likewise, the IHE Patient Care Coordination (PCC) domain has defined various content profiles including a Medical Summary (XDS-MS) content profile and an Emergency Department Referral (EDR) content profile. XDS-MS supports a patient's transfer of care from one care setting to another, and EDR supports the situation where a physician determines that a patient should proceed directly to an emergency department for care. In each of these cases, it is useful for IHE to profile (define) both the transport and the content of the documents so that true interoperability can more easily be achieved throughout the healthcare continuum.

The IHE Content Profiles utilize two abstract actors "Content Creator" and "Content Consumer", utilizing an abstraction of "Share Content"; where "Share Content" can be any of the Document Sharing infrastructures including MHDS, XDS, XDR, XCA, etc.

 Copyright © 2020: IHE International, Inc.

Figure 50.7.2.5-1: MHDS Actor Diagram

IHE Content Profiles can be found:

- CDA https://wiki.ihe.net/index.php/Category:CDA
- FHIR-Document https://wiki.ihe.net/index.php/Category:FHIR-Doc

50.7.2.6 Value of Metadata

Another key principle leveraged by IHE Document Sharing is the use of metadata. As defined in Section 50.7.2.2, metadata are data that provides information about one or more aspects of the document. While a document may be any collection of bytes, IHE defines a collection of metadata about the document that aid its identity, discovery, routing, security, provenance, privacy, authenticity and electronic pre-processing. The set of metadata is defined to facilitate interoperability, so that receiving systems can manage, route and administer documents even if they are unable to interpret the contents of the document. IHE metadata are defined in such a way that additional metadata, defined outside of IHE, can be sent. Of course, systems not enabled to understand the additional metadata will ignore them, but this capability allows the set of metadata defined by IHE, which is already extensive and robust, to be extended when local needs arise.

Metadata serve multiple purposes. They allow systems to perform:

- automated management of the documents – like assigning priorities or work tasks
- automated patient identification – adding the new information to the correct patient's local record
- support for provenance management – making decisions based on authority of creator of content
- support for episodic searches – by type, date of service
- support relationships between documents
- support privacy/authorization controls – enabling access to content only where appropriate
- support security and integrity controls

 Copyright © 2020: IHE International, Inc.

Any metadata element may support overlapping purposes, but the combination of metadata elements provides a robust understanding of the document and enables automated and manual management of the document without the requirement access to the detailed clinical information contained within the document.

50.7.2.7 Document Relationships

The metadata defined in the IHE Document Sharing model encompasses more than just characteristics of documents. In fact, the metadata model is very rich, encompassing the relationships between documents through use of folders, submission sets, and associations. For a complete list of document metadata, refer to ITI TF-3: Section 4.1 – "Abstract Metadata Model". This abstract metadata model has two representations: Section 4.2 "ebRIM Representation" used by XDS and XCA; and Section 4.5 "FHIR Representation" used by MHDS and MHD.

Documents: Each document shared using IHE-defined constructs comes with a collection of metadata which describes the document. The metadata describing the document includes things like: document identifier, patient identifier and demographics, document author, class of document, confidentiality of document, creation time, and events causing creation of document, document format and several more.

Folders: Metadata shared using IHE-defined constructs can also describe folders and document's membership in folders. A folder may be used to collect documents for many purposes, like ease of access or describing a functional purpose.

Submission Set: When documents are published or pushed using IHE transactions they are collected into submission sets to reflect the collection of documents sent at a given moment. Since a submission set reflects a collection of documents it shares some of the same metadata as a document, like patient identifier and author, and adds metadata reflecting the collection like identifier of the source, intended recipient and submission time.

Document Associations: The document sharing metadata supports the description of associations between documents. The associations supported are: append, replace, transform, transform with replace, and signs (i.e., digital signature). The append, replace, and transform associations support representation of document lifecycle events, where a document is associated with documents which are created as part of lifecycle events related to the original document.

50.7.2.8 Document Sharing Models

IHE has enabled three distinct Document Sharing Models that share the principles in this section. Because the principles are the same it is relatively simple to implement more than one model to accomplish multiple objectives. The three models are:

- **Direct Push** – in this model, clinical content in the form of documents and metadata is sent directly to a known recipient, or published on media for delivery

 Copyright © 2020: IHE International, Inc.

- **Centralized Discovery and Retrieve** – in this model, a centralized locator is used to discover the location of documents which enables a retrieval of the document from a custodian who has registered existence of the document with the centralized locator
- **Federated Discovery and Retrieve** – in this model, a collection of peer entities is enabled to query each other to locate documents of interest, followed by retrieval of specific documents.

These models share the common definition of a document and metadata describing documents, folders, submission sets and document associations. Each requires some level of governance structure in order to operate, although there is some difference in the governance needs. For instance, the centralized model requires knowledge only of the centralized locator which can then provide connections with distributed document repositories. For Direct Push and Federated approaches, a detailed directory of participating entitles is typically used to ensure that the push or query transactions are sent to the proper place. All include strong support for authenticity and encryption on transport. Privacy requirements vary especially between the Direct Push, where privacy policy is generally determined prior to initiation of the action, and Discovery mechanisms where privacy policy is most often determined prior to responding to the request. So, while the issues that need to be resolved through governance are largely the same, the resolutions will sometimes vary depending on the model chosen.

It is expected that most communities of exchange will start with one of the three forms of document exchange and, if needed, adopt the others later. The addition of a new model to an existing deployment is relatively simple because the IHE profiles are based on common principles.

50.7.2.9 Patient Identity Management

The Document Sharing mechanisms enabled through IHE assume that a patient is associated with every document shared. That patient is described within the metadata describing the document.

In the Discovery models the document query requires the specification of a patient identifier as known by the query recipient. So, in these models it is necessary to resolve the patient prior to searching for documents. In fact, the query does not carry any patient demographic data beyond the patient identifier.

Resolving the patient is a complex subject made more complex through historic norms, regulations, and business factors. Some regions have a universal identifier, but most regions do not. IHE provides several profiles that aid the resolution of the patient identifier. The profiles are described in Section 50.7.2.4.

50.7.2.10 Locating sharing partners

One of the challenges of Document Sharing that is not directly addressed by IHE is the identification of Document Sharing partners. Each Document Sharing model has a different type

 Copyright © 2020: IHE International, Inc.

of need: where a centralized discovery approach requires the identification of the central locater, the peer-based push and discovery mode requires identification of each of the peers. This ability to discover sharing partners can be accomplished in many different ways and a clear preference is not yet apparent. The approaches can be broadly characterized as a) locating electronic services which can provide information and b) locating patient specific source of information.

For locating electronic services which can provide information, some approaches currently used in various parts of the world are:

- Local configuration files – many organizations keep a local configuration file or address book which is managed manually whenever a new sharing partner is identified or updated.
- Service Registry – a services registry is sometimes used as a centralized service available to all participants.
- Healthcare Provider Directory – enables a directory of individual and organizational entities along with electronic services provided by those entities.

50.7.2.11 Security/Privacy

IHE addresses Privacy and Security through the use of Risk Assessment and Management. Each profile is assessed for various types of risks and the profile includes mitigations identified through that assessment in the privacy and security considerations.

IHE includes profiles specific to interoperability of security and privacy. Interoperability profiles are not enough to fully address privacy or security. Privacy and security are enabled and enforced at many levels of depth including policy, physical environment, procedures, organizational, departmental, functional, and information technology.

IHE provides profiles that support privacy and security audit logging, user and system identification and authentication, access control, encryption, data integrity, digital signatures, and privacy consent management. Security and Privacy and the profiles IHE offers are discussed in Section 50.5.

50.7.3 Document sharing profiles

The key actors in health information exchange are the document source actors – those applications or modules that create the document to be shared, and the document consumer actors – those applications or modules that retrieve the document to act on it (i.e., present it to the user, import it into the receiving system, etc.). The strength of the Document Sharing profiles is that they enable effective sharing of data among multiple, disparate systems in a way that minimizes the burden that data sharing imposes on those systems.

The three models defined in Section 50.7.2.8 are designed to support different use cases. The Direct Push model can be relatively simple, but it cannot satisfy all use cases because it relies on the source of documents to know where those documents will be needed. The Discovery models can also handle use cases like:

 Copyright © 2020: IHE International, Inc.

- Treatment of a new condition where prior conditions may be relevant
- Open Referral, where the patient is allowed to choose the specialist
- Highly mobile patient
- Emergency
- Patient with many medical conditions
- Patient with complex condition

The IHE profiles addressing these models are:

- Direct Push – Mobile access to Health Documents (MHD), Cross-Enterprise Document Reliable Interchange (XDR), and Cross-Enterprise Document Media Interchange (XDM)
- Centralized Discovery and Retrieve (XDS Affinity Domain) – Mobile Health Documents Sharing (MHDS), and Cross-Enterprise Document Sharing (XDS)
- Federated Discovery and Retrieve – Cross-Community Access (XCA)

The Mobile access to Health Documents (MHD) Profile is also an access (API) method to XDS or XCA environments. These models and other alternatives are further discussed in the White Paper on Enabling Document Sharing through IHE Profiles.

50.7.3.1 Direct Push

This exchange model is not the focus of the MHDS Profile. This function can be achieved using MHD Profile with Document Source pushing to Document Recipient.

50.7.3.2 MHDS based Centralized Discovery and Retrieve

The MHDS Profile enables centralized discovery of health documents and retrieval of those documents from distributed document repositories.

The following scenario describes a typical exchange of clinical information using MHDS. Dr. Suwati works for New Hope Medical Partners which provides her with an EMR system. Her patient, Mary Gomez, just explained to the doctor that she was recently hospitalized at Norwalk General Hospital. Dr. Suwati would like to review the medical records that documented Mary's hospital stay. Using her EMR, Dr. Suwati searches for recent documents for Mary Gomez created by Norwalk General Hospital's EHR. Having found several documents (lab results, radiology reports, a discharge summary, etc.), Dr. Suwati chooses first to view Mary's radiology reports. Having read the reports, she discards them. However, Dr. Suwati reads the discharge summary and then saves it to Mary's record in the local EMR.

In this scenario of health information exchange, the primary player (Dr. Suwati) has three principal objectives: find patient records available from external systems, view a selection of those records, and incorporate a select number of those records to her local system. This sequence of actions is repeated continually in the healthcare setting. To address this very

 Copyright © 2020: IHE International, Inc.

common scenario, IHE has created the MHDS Profile, a method to coordinate the authorized discovery and sharing of medical documents among disparate information systems.

MHDS minimizes the burden imposed on the document sources and consumers when sharing documents by establishing the use of two infrastructure components (the document registry and document repositories), which handle most of the effort involved in exchanging clinical data. This separation allows for minimal yet rich metadata to be centrally managed in a document registry while the full clinical details stay protected within distributed document repositories. The IHE profiles enable the automation of discovery and retrieve by more advanced health information systems.

50.7.3.2.1 Document Publishing

The MHD system acts like a Library for books. The document may be made available within the document registry or at the source organization, an organized resting place for books (i.e., medical documents) that are available to library patrons. The document registry is the library's card-catalog, a tool for locating specific books that lie on those rows and rows of shelves. Unlike a library, the bookshelves are potentially deployed within each participating organization; thus, the books are controlled by the original organization until the moment that another organization requests a copy.

It is the responsibility of the publisher to put the books (documents) on the shelf and provide the information for the card-catalog (metadata). The library will step in to update the card-catalog with the data needed to find the new book. In IHE jargon the publisher is called the document source, whereas the act of putting the book on the shelf and then cataloging it.

The actual location of the document repository will depend on the local deployment. IHE provides flexibility to enable many different deployment approaches.

- The document repository may be combined with the document registry, allowing for an integrated environment where no external “update registry” transaction is needed.
  - In this case the Document Source includes the document in a FHIR Binary Resource within the “Provide Document Bundle” [ITI-65] transaction
- The document repository could be combined with a document source allowing a large hospital system to enable its local EMR system to also act as a document repository. In this case, there is no externally recognized “provide and register” transaction, but simply the “update registry” transaction from the hospital system to the central document registry.
  - In this case the Document Source stores the document in an accessible server and includes the URL to that location in the “Provide Document Bundle” [ITI-65] transaction
- There is no restriction on how many document repositories can be associated with a single document registry. However, any document repository must be made available for

 Copyright © 2020: IHE International, Inc.

authorized retrieval of the documents contained and referenced within the Document Registry.

- There are no constraints on where a document repository is hosted, the decision is based on many implementation considerations. For instance, a hospital may want to keep its clinical content local in which case it supplies a repository hosted locally. Or a small physician office may have no ability to support a repository and will prefer to use a repository provided by an external organization, like a hospital system of an infrastructure only partner.

50.7.3.2.2 Document Discovery

To complete our analogy, we must consider the library patron (Dr. Suwati in our case), whose goal is to find specific books. The patron interacts with the catalog; sometimes searching for specific books, other times browsing what is available. Once the locations of interesting books are discovered, the patron fetches them from the shelves. In our MHDS drama, the document consumer (our library patron) interacts with the Document Registry through the Document Responder to find medical records of interest. This process is known as the "Find Document Manifests" [ITI-66], and "Find Document References" [ITI-67] transactions. The act of fetching the medical record from a Document Responder (repository) is known as the "Retrieve Document" [ITI-68] transaction. Of course, with the structured and coded metadata, this step of discovery can be highly automated.

50.7.3.2.3 Governance

As described in Section 50.7.2: *Principles of IHE for Health Document Sharing*, the MHDS Profile is document content neutral; uses document metadata that are represented in a structured, standard format; and supports longevity of document storage.

MHDS requires a governance structure as described in Section 50.7.2.2 and defines the MHDS Community as the agent for that governance. An MHDS Community is a group of healthcare enterprises that have agreed to work together using a common set of policies and MHDS infrastructures for sharing patient clinical documents. Some examples are:

- Regional community of care
- Nationwide EHR
- Specialist (cardiology, oncology) or disease-oriented (diabetes) care networks
- Government-sponsored or federation of enterprises
- Insurance provider supported communities

The MHDS Profile is patient centric and thus requires that a patient identity is managed centrally as well. The PMIR Profile enables this patient identity management domain to use a single Patient Identification Domain so that each patient has a master identity called a PMIR Golden Domain Patient. This ensures that, for example, when submitting documents for Mary Gomez

 Copyright © 2020: IHE International, Inc.

the same unique patient identifier is associated with each document for Mary Gomez, and thus a search can reliably find all of Mary's documents by using this single unique identifier. MHDS specifies that PIXm or PDQm shall be used by document source and document consumer systems find the unique patient identifier assigned, see Section 50.7.4 "Patient Identity Management".

Further detail regarding deployment of an MHDS Community may be found in the "Template for XDS Affinity Domain Deployment Planning" IHE ITI White Paper.

50.7.3.2.4 Notifications

The MHDS environment does not yet have a Notification mechanism like found in XDS in the Document Metadata Subscription (DSUB) Profile.

50.7.3.3 Federated Discovery and Retrieve

MHDS has not yet addressed multiple communities federating. Where federation is critical the use of XDS and XCA are recommended.

50.7.4 Patient Identity Management

The Document Sharing defined in this profile is patient centric, meaning that a patient is associated with each document shared. When data related to an individual patient is exchanged among healthcare information systems it is critical to ensure that the participating systems are referring to the same patient. This requirement can be accomplished in several different ways.

One possible way would have each transaction carry enough demographic data to ensure that the partner is able to match the patient through demographic matching with locally held characteristics. The challenges of "enough" demographic data is a difficult problem. It includes issues around demographics changing over time (name changes) and other aspects of demographics matching rules. There is also concern around privacy when unnecessarily transporting patient demographics.

Thus, IHE recommends that the identification of the patient be done through patient identifiers in a common or accepted patient identification domain. Thus, prior to the exchange of healthcare information the partners agreed on a commonly known patient identifier to refer to the patient. Essentially any identifier that a patient provides can be used to correlate identities, with a Voluntary Health Identifier (VHID) being a specific example of an identifier assigned outside of treatment. This requirement, however, is often non-trivial and the patient identity management profiles serve the purpose of enabling this aspect of Document Sharing. Some regions and nations have enabled the use of a unique patient identifier that is widely available, but many places still need profiles which aid in patient identifier discovery.

Systems participating in Document Sharing frequently use locally assigned patient identifier domains. A patient identifier domain is defined as a single system or a set of interconnected systems that all share a common patient identification scheme (an identifier and an assignment process to a patient) and issuing authority for patient identifiers.

 Copyright © 2020: IHE International, Inc.

The Patient Resource Identity Management (PMIR) Profile supports the management of a master Patient record with links to patient identifiers from multiple patient identifier domains. The Patient Identity Cross-Reference for Mobile (PIXm) Profile supports a query given one identifier known to the client to request cross-referenced identifiers known to the Patient Identity Manager. The Patient Demographics Query for Mobile (PDQm) Profile supports the ability to query by a set of demographics and get in response a complete set of demographics, usually including patient identifiers in domains of interest.

50.7.4.1 Patient Identity Management

Most health information systems assign to each patient an identifier (usually a string of letters and/or numbers) that is unique to the patient within only that information system. Thus, Gary Collins may be identified as 3562A at the office of his primary Care Physician (PCP) and 0320 at his specialist's clinic.

IHE utilizes the concept of Patient Identifier Domains which defines a domain of patient identifiers, like identifiers assigned within a PCP office, assigned by a single authority and an identifier for each assigning authority. For example, the PCP office identifier is unique within the assigning authority for the PCP. If the PCP's system wants to communicate with the specialist's system about Gary Collins, both systems must be able to know that 3562A assigned by the PCP offices is equivalent to 0320 assigned by the specialist's office, and that neither of those identifiers is equivalent to Garry Collin with an ID of 333 at a local Hospital. This is known as a cross-reference that links the two patient identifiers for Gary Collins.

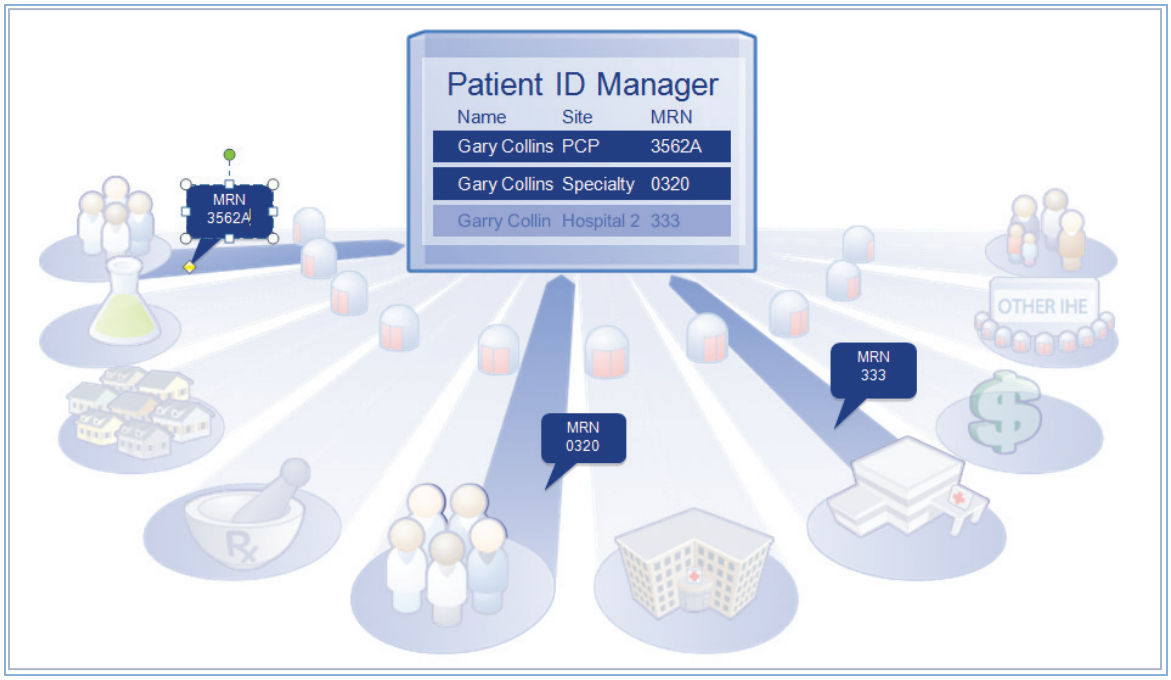

Figure 50.7.4.1-1: Patient identifier cross-referencing

 Copyright © 2020: IHE International, Inc.

The PMIR Profile is IHE's answer to the difficulty of managing an individual patient's multiple Identifiers. A PMIR Patient Identity Manager system receives feeds from multiple patient identity domains, such as the PCP and specialist offices. These feeds are coordinating a master identity for the Patient that could include many alias identifiers from each domain participating in the PMIR domain.

A consumer system may query the PMIR Patient Identity Manager to receive the master Patient Identity based on their local identifiers or based on the identifying characteristics of the patient. In this way the PCP office can discover the master Patient Identity and know the domain specific identifier used by the specialist's system and thus can communicate with that system using a known patient identifier.

The PMIR Profile Patient Identity Manager integrates the server side of the PDQm and PIXm Profiles, so that systems needing a patient identity lookup can use PDQm or PIXm Profiles. A system that publishes documents or a system that consumes documents can implement the client PDQm Patient Demographics Consumer or PIXm Patient Identifier Cross-reference Consumer as their method of discovering patient identities. As such these clients are agnostic to the Patient Identity Management technology, which might be a PMIR Patient Identity Manager, a legacy PIX Patient Identity Manager, etc. A primary use of the PDQm and PIXm Profiles is to enable document consumers and document sources using the MHDS Profile to find the patient's identifier in that Community Patient Identifier Domain. See Section 50.7.3.2.

50.7.4.2 Patient Demographics Query for Mobile (PDQm)

Demographics (information describing the patient in general) are used to help identify the patient. With information on dates of birth and sex, information about Leslie Ramsi, a male born on May-2-1968, can be distinguished from that of Leslie Ramsi, a female born on July-23-1987. To help information systems improve their management of patient demographic information, IHE defines a profile called patient demographics query (PDQm). The premise of this profile is that some information systems will have more comprehensive and more accurate demographic information about a patient than other systems. The following paragraph describes a typical use of the PDQm Profile.

A typical use of PDQm is to discover the patient's Community Domain Patient ID. Imagine that Justin McCarthy heads to the local public health department for a vaccination. The public health department's clinical system does not assign local patient identifiers and thus cannot use the PIXm Profile to discover Justin's Community Domain Patient ID (a required element for the MHD transactions described above). The public health department can use PDQm to find matches for Justin and will receive Justin's Community Domain Patient ID as part of the demographics returned. With the knowledge of Justin's Community Domain Patient ID, the public health department can now publish his vaccination record to the community via the MHDS Profile.

 Copyright © 2020: IHE International, Inc.

50.7.5 Common Provider Directory

As with patient identity management, the management of data related to healthcare providers (both individual providers and provider organizations) is a fundamental challenge for communities. IHE has defined the Mobile Care Services Discovery (mCSD) Profile to addresses this challenge. There are two principal benefits of using the mCSD Profile. First, mCSD provides a means to disambiguate the identity of providers (i.e., allow one to distinguish between the 58 year old male pediatric nurse named Lindsay Smith and the 32 year-old female orthopedic surgeon Lindsay Smith). Second, mCSD offers a method to discover a provider's contact information (e.g., phone numbers, street address, etc., as well as an electronic endpoint and digital certificate that may be used for trusted communication).

The referral process (one provider referring a patient to the care of another provider) is one of the most common uses of the mCSD Profile. When Dr. Palov wishes to send his patient Mary Blythe to a female endocrinologist who speaks Spanish, he may query the Directory to find contact information for providers that match those criteria. Similarly, Dr. Palov may wish to refer another patient, Thomas Reed, to the local Mercy Hospital. Dr. Palov could query the Directory to discover the hospital's electronic endpoint (e.g., a secure email address or a Document Registry endpoint) so that he may forward some of Mr. Reed's medical records to the hospital in advance of his visit.

The mCSD Profile describes both how to store data regarding healthcare providers and also how to subsequently access that information. Within the directory, one may also store relationships between providers. For example, Nurse Joe may be an individual provider who belongs to the organizational provider General Hospital.

In environments where mCSD is used to manage a set of identities, these managed identities can be referenced as the author in document metadata, whereas when these identities are not managed, they must be included within the metadata as contained resources.

 Copyright © 2020: IHE International, Inc.