Integrating the Healthcare Enterprise

IHE IT Infrastructure Technical Framework Supplement

Advanced Patient Privacy Consents (APPC)

Rev. 1.1 – Trial Implementation

Date: August 5, 2016

Author: IHE 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.

Foreword

This is a supplement to the IHE IT Infrastructure Technical Framework V13.0. 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 August 5, 2016 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 X.X by the following:

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

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

Information about the IHE 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.

CONTENTS

Introduction to this Supplement

The Advanced Patient Privacy Consents (APPC) Profile defines a structural representation of a privacy consent policy. The definition allows for privacy consent policies that can include individualized parts, based on the patient's choices.

This profile is intended to allow an unspecified enforcement mechanism, potentially within an existing access control system, to use the structured policy representation to automatically determine and enforce those policies.

Open Issues and Questions

APPC-3: Are there limitations on what metadata or content attributes not defined by the profile can be communicated using a Privacy Consent Document? How are these attributes limited? What does the content consumer with the Structured Policy Processing Option have to understand/support?

APPC-4: The human readable consent representation in the XACML document doesn't contain formatting. The profile addresses this by specifying a linking mechanism (using associations). Is this sufficient or do we need to address this differently?

APPC-5: Should coded values be expressed in a string (or URI format) instead of a structured HL7®[1]v3 based data type? Which solution helps implementers dealing with code equivalency issues (e.g., ICD-10 vs. ICD-9 representations of the same concept)?

APPC-7: Should the profile define a policy-combining and a rule-combining algorithm? Or would picking a fixed combining-algorithm be too restrictive?

APPC-8: DateTime conversion algorithm from partial dates (i.e., dates with uncertainty, e.g., "200904" meaning some point in time in April 2009) loses the information that the metadata contained a partial date. Could this negatively impact authorizations? Please suggest language to address this.

APPC-10: Should we continue to use a string for the XdsFolder.uniqueId and the XdsSubmissionSet.uniqueId, although they are OIDs? The alternative would be an anyURI data type, but that doesn't work for document entries. The downside of using the anyURI data type for two of three attributes (which all share the resource-id URN): The data type would then be dependent on whether the resource is a DocumentEntry, a Folder or a SubmissionSet.

APPC-11: Should the document/folder/submissionSet title be available for authorization checks? Does it introduce significant risk of abuse (e.g., regex matching of user entered titles)?

APPC-12: The profile doesn't address how to control access to a document based on the metadata or identity of another document. E.g., policy writers cannot express a rule where users

[1] HL7 is the registered trademark of Health Level Seven International.

are allowed to access a document if they were allowed to access the document it replaced. This restriction applies to all document associations. Is this restriction critical to achieve the goals of the profile?

APPC-14: Are the examples that can be found at ftp://ftp.ihe.net/TF_Implementation_Material/ITI/examples/APPC useful to implementors? Please suggest other examples or corrections/improvements to the current ones.

APPC-17: Author information from multiple authors cannot be correlated in a policy. This means that it is currently not possible to have a policy that requires an author to have, e.g., a specific identifier and a specific authorRole. The profile mitigates this by limiting author metadata to the authorPerson ID and the authorInstitution ID. Is this restriction to prohibitive?

Closed Issues

APPC-1: Do we need to have an APPC Enforcement Option in XDS?

- We have given the development of an Enforcement Option for APPC in the XDS Profile (similar to what BPPC did) a very low priority – we will at most attempt to address this at the end, if time allows (Dec 1st 2015 Call)

APPC-6: Is there a need for a catch-all action ID that means “any kind of retrieve” (including generic FHIR®[2]-based data access)?

- We will only define action IDs for the IHE Document Sharing transactions to avoid scope creep

APPC-2: Should we include a list of supported metadata attributes in volume 1?

- Adding such a table would create maintenance issues

APPC-9: How to distinguish between the user’s name and the user’s identifier? The identifier doesn’t have an URN in XUA. The name URN on the other hand has two variants which are supposed to be semantically equivalent but use two different definitions in XUA and SeR.

- The subject’s real name has been removed, as it is not suitable for authorization checks

APPC-13: Appendix P for Vol 2x has not been modified yet and was included in its current (revision 12) final text form. Are extensive updates necessary? Please suggest specific sections that would benefit from updates regarding APPC.

- Removed Appendix P from the supplement, will be added through a separate CP.

[2] FHIR is the registered trademark of Health Level Seven International.

APPC-15: Should the XACML content be wrapped in a CDA®[3]?

- Wrapping the content in a CDA has been considered and rejected. The overhead of CDA wrapping (less space efficient, more complicated creation and consumption) was considered too high for the perceived benefit (better human readable representation, additional structured metadata describing who consented and how/when) when compared to using a linked document instead.

APPC-16: Should we define Obligations (e.g., inform the patient via email when "break-glass" access occurs) to be used in the policies?

- XACML2 does not define standard obligations. Defining new obligations for this profile is difficult without knowing the enforcement environment and therefore, also considered out of scope. Content Creators are free to include obligations in their policies, but APPC does not define these obligations.

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary and in the Volume 1 GLOSSARY:

Glossary Term	Definition
Privacy Consent Document	A document containing a structured policy used to express a patient's privacy preference
Structured Policy	A machine-processable set of access rules that enables the receiving system to enforce the patient's privacy preferences without requiring human interpretation.

Replace the definitions for the following glossary terms in the IHE Technical Frameworks General Introduction Glossary and in the ITI TF-1: GLOSSARY:

Glossary Term	Definition
Patient Privacy Policy	A Patient Privacy Policy will identify who has access to information, and what information is governed by the policy (e.g., under what conditions will a document be marked as containing that type of information). The policy may also describe the patient's rights to specify their consent preferences, notifications, complaints, or requests as well as the mechanism that allows them to do so.
Patient Privacy Policy Identifier	A Patient Privacy Policy Domain-assigned globally unique identifier that identifies the Patient Privacy Policy.

[3] CDA is the registered trademark of Health Level Seven International.

Glossary Term	Definition
Patient Privacy Policy Domain	The domain for which a Patient Privacy Policy applies. When using XDS this would likely be equivalent to the XDS Affinity Domain.

Volume 1 – Profiles

Copyright Licenses

Add the following to the IHE Technical Frameworks General Introduction Copyright section:

NA

Domain-specific additions

NA

Add Section 43

43 Advanced Patient Privacy Consents (APPC) Profile

Advanced Patient Privacy Consents is a content profile that describes the semantics necessary to enable patient consent(s) to be captured, managed, and communicated between systems and organizations. This profile enables the capturing of consent(s) that cannot be adequately expressed using the Basic Patient Privacy Consents (BPPC) Profile.

43.1 APPC Actors, Transactions, and Content Modules

A product implementation using this profile must group actors from this profile with actors from a workflow or transport profile to be functional. See Section 43.6.

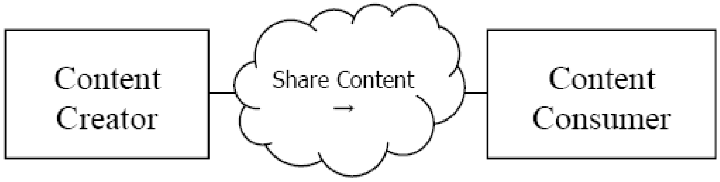


Figure 43.1-1: APPC Actor Diagram

Table 43.1-1 lists the content module(s) defined in the APPC Profile. To claim support with this profile, an actor shall support all required content modules (labeled “R”) and may support optional content modules (labeled “O”).

Table 43.1-1: APPC Profile - Actors and Content Modules

Actors	Content Modules	Optionality	Reference
Content Creator	Advanced Patient Privacy Consents Content Module	R	ITI TF-3: 5.6.1
Content Consumer	Advanced Patient Privacy Consents Content Module	R	ITI TF-3: 5.6.1

43.1.1 Actor Descriptions and Actor Profile Requirements

See PCC TF-1: Appendix A.

43.2 APPC Actor Options

Options that may be selected for each actor in this profile are listed in Table 43.2-1.

Table 43.2-1: APPC - Actors and Options

Actor	Option Name	Reference
Content Creator	No options defined	--
Content Consumer	View Option[Note 1]	Section 43.2.1
	Structured Policy Processing Option [Note 1]	Section 43.2.2

Note 1: Content Consumer shall implement at least one of View Option or Structured Policy Processing Option

43.2.1 View Option

The requirements for the View Option defined in PCC TF-2: 3.1.1 apply.

43.2.2 Structured Policy Processing Option

The Content Consumer that supports the Structured Policy Processing Option shall be able to process and interpret the structured policy contained in the APPC document. The option does not require the ability to enforce the rules contained in the structured policy.

43.3 APPC Required Actor Groupings

An actor from this profile (Column 1) shall implement all of the required transactions and/or content modules in this profile ***in addition to*** all of the transactions required for the grouped actor (Column 2).

Section 43.5 describes some optional groupings that may be of interest for security considerations and Section 43.6 describes some optional groupings in other related profiles.

Table 43.3-1: APPC - Required Actor Groupings

APPC Actor	Actor to be grouped with	Reference	Content Bindings Reference
Content Creator	none	--	--
Content Consumer	none	--	--

43.4 APPC Overview

The Advanced Patient Privacy Consents (APPC) Profile defines a structural representation of a patient-specific Privacy Policy. The Privacy Policy is considered patient-specific because it includes individualized parts based on the patient's choices.

The content of a Privacy Consent Document is designed to allow an unspecified enforcement mechanism, potentially within an existing access control system, to use the structured policy representation contained within the consent document to automatically determine and enforce those policies. Such an enforcement mechanism could collect and organize the structured policies to allow for efficient access decisions and enforcement.

43.4.1 Concepts

Healthcare providers utilize many different sets of data to carry out treatment, billing, and other related operations. This information may include patient demographics, contacts, insurance information, dietary requirements, general clinical information, and sensitive clinical information. This information may be published as independent documents, e.g., by means of the Document Sharing profiles. When using these profiles, each document has a clearly defined set of metadata attributes including coded values denoting the document type, the medical specialty involved, and one or more sensitivity labels (i.e., confidentialityCodes). Healthcare providers also have attributes, such as a functional role, the organization that they work for, which Affinity Domain they belong to, etc.; the Cross-Enterprise User Assertion (XUA) Profile defines one set of such attributes.

This profile enables attribute-based security at the document level using the Document Sharing metadata. Documents and accessing providers each have a set of attributes that are clearly defined when using Document Sharing profiles and XUA. Attribute-based security arrives at an access decision (i.e., whether a specific user is authorized to access a specific document) by using a set of rules that compare attributes to each other or against value constraints. To understand attribute-based security conceptually, the specific values, and who determines them, is not critical.

Different healthcare providers will have different needs to access these documents. For example, administrators may need to be able to access patient demographics, billing and contact documents. Dietary staff will need access to the dietary documents but would not need access to insurance documents. Patients' assigned doctors will need access to all clinical documents, whereas other providers from the same facility will need access to fewer clinical documents. These statements form one basic Patient Privacy Policy. The policy can be expressed as a set of access rules in an attribute-based security system. Note that such a policy contains nothing that is specific to a particular patient, and only consists of general rules.

IHE Document Sharing profiles allow for the publication and use of clinical documents associated with a patient. Privacy Consent is an important attribute of Document Sharing. The IHE Basic Patient Privacy Consents (BPPC) Profile allows the patient to choose from a set of predefined Patient Privacy Policies, without modifications. The APPC Profile allows a Patient Privacy Policy Domain (e.g., an XDS Affinity Domain) to have a number of Patient Privacy Policies that can be individualized and customized.

This profile allows Patient Privacy Policy Domains to give patients choices that are more granular by creating access rules that add constraints on top of the rules defined in an underlying

Patient Privacy Policy. A patient may not want to give all physicians access to her clinical documents and may therefore limit the Patient Privacy Policies to only apply to a specific healthcare provider organization (see Section 43.4.2.1) or to a specific episode of care (see Section 43.4.2.2). The patient-specific access rules are transmitted in a structured policy as a part of the consent document.

The Patient Privacy Policy Domain determines the available policy customizations. For example, one particular domain may only support blocking of (otherwise permitted) document access to specific care providers, while another domain may allow specific care providers access to certain (otherwise blocked) documents from a specific date range.

Neither staff members that digitize paper consent forms, nor patients using a portal to fill out a digital consent form, can be expected to have the knowledge or training to write a consent document with a structured policy from scratch. Therefore, the Patient Privacy Policy Domain must determine a set of foundational, re-usable Patient Privacy Policies defining access patterns (e.g., “full access”, “summaries only”), and clearly define the ways the patient (or other participants) can further make them specific to the patient’s circumstances (e.g., by adding which healthcare provider organization it applies to, by limiting it to documents related to a particular episode of care). When designing the foundational Patient Privacy Policies and the degree of patient-specific adjustments, the Patient Privacy Policy Domain must take many factors into account: the applicable legal framework, medical ethics, the types of data exchanged, the characteristics of the patient population (e.g., age, level of utilization of healthcare services), the capabilities of the IT systems involved, and the exchange participants’ existing access management policies and procedures. Additional factors may be present. Patient Privacy Policy Domains may look to national or regional bodies to assist them in identifying and addressing all relevant factors.

A foundational Patient Privacy Policy should identify what the acceptable use and re-disclosure uses are, which functional roles may access which document, and under which conditions. Other representations may exist, e.g., a “patient-friendly” explanation. A unique Privacy Policy Identifier identifies each foundational Patient Privacy Policy. The Patient Privacy Policy Domain has one set of Privacy Policy Identifiers.

Along with the normative text, there might be a machine-readable, structured representation of the foundational Patient Privacy Policy, which can be combined with the machine-readable, structured representation of the patient-specific constraints that are included in the Privacy Consent Documents defined in this profile. Combining them enables automatic enforcement of the patient’s privacy choices. How to combine these different sets of access rules is not in scope for this profile.

Combining Patient Privacy Policies from different Patient Privacy Policy Domains might be difficult. An exchange of foundational Patient Privacy Policies using a structured policy format between different Patient Privacy Policy Domains might allow automatic enforcement of Privacy Consent Documents from other Patient Privacy Policy Domains, but this is not part of the APPC Profile.

43.4.2 Use Cases

The following use cases illustrate the capabilities enabled by this profile. They are not meant to be an exhaustive list of supported patient consent / access control schemes, nor are they intended to imply any particular implementation. The use cases all share a level of complexity that would be challenging to implement using BPPC and therefore are a better fit for this profile.

43.4.2.1 Use Case #1: Facility-specific Disclosure

In this use case, the patient grants access to his data to the staff of a specific facility. The extent of access and any accompanying restrictions are condensed into an access patterns that the patient selects for this facility.

43.4.2.1.1 Facility-specific Disclosure Use Case Description

Pre-Condition:

This use case takes place in an opt-in XDS Affinity Domain, where access to PHI is only granted if the patient explicitly agreed to share documents.

The XDS Affinity Domain – acting as the Patient Privacy Policy Domain – has defined three foundational Patient Privacy Policies, which may be referenced in a Privacy Consent Document. The XDS Affinity Domain consists of 50 separate facilities.

The facilities providing care for the patient (a hospital and a post-surgical care facility) can exchange data via an HIE using a common patient ID and these facilities are listed in the HIE's Healthcare Provider Directory.

Main Flow:

A patient visits a hospital because he needs a hip replacement. After the procedure, the hospital wants to arrange post-discharge care at another facility. The hospital uploaded all relevant data regarding the procedure to their HIE. A staff member asks the patient to sign a consent form that authorizes the HIE to grant access to the patient's health data to the target facility. The patient has a choice between three access patterns, which are listed on the form: "summary-only" access, "general" access, and "full" access. The patient selects "general" access, which includes most notes, labs and images, but excludes particularly sensitive documents (e.g., psychiatric evaluations). The patient signs the form.

The staff member selects the patient in the EHR, searches for the post-surgical care facility in the connected Healthcare Provider Directory, selects the facility, and then selects the access pattern ("general"). The EHR creates a Privacy Consent Document and transmits it to the central XDS Document Repository in the HIE. After discharge from the hospital, the patient visits the post-surgical care facility. The HIE's enforcement mechanism (acting as a APPC Content Consumer with the Structured Policy Processing Option) uses the structured and coded policy from the consent document to decide to grant access to the longitudinal patient record for users from the post-surgical care facility.

Post-Condition:

The longitudinal patient record in the HIE contains a consent document.

The doctors and care providers in the post-surgical care facility can access the patient’s longitudinal record in the HIE.

The doctors and care providers in facilities not involved in the patient’s care cannot access the patient’s longitudinal record in the HIE.

43.4.2.1.2 Facility-specific Disclosure Process Flow

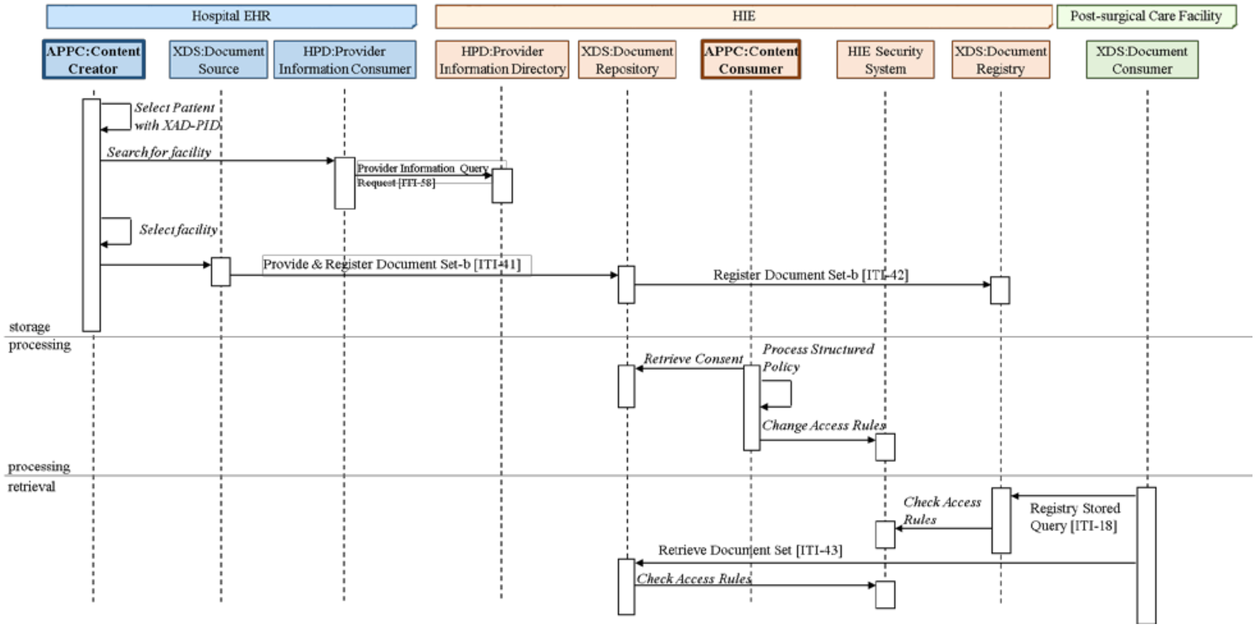

Hospital EHR
HIE
Post-surgical Care Facility
APPC:Content Creator
XDS:Document Source
HPD:Provider Information Consumer
HPD:Provider Information Directory
XDS:Document Repository
APPC:Content Consumer
HIE Security System
XDS:Document Registry
XDS:Document Consumer
Select Patient with XAD-PID
Search for facility
Provider Information Query Request [ITI-58]
Select facility
Provide & Register Document Set-b [ITI-41]
Register Document Set-b [ITI-42]
storage
processing
Retrieve Consent
Process Structured Policy
Change Access Rules
processing
retrieval
Check Access Rules
Registry Stored Query [ITI-18]
Retrieve Document Set [ITI-43]
Check Access Rules

Figure 43.4.2.1.2-1: Facility-specific Disclosure Process Flow in APPC Profile

43.4.2.2 Use Case #2: Consent for an Episode of Care

In this use case, the patient allows a care team consisting of healthcare providers from multiple organizations to exchange data related to a specific episode of care. All care team members have the same level of access.

The detailed access rules for the care team members are defined independently of the patient’s consent by the HIE.

43.4.2.2.1 Consent for an Episode of Care Use Case Description

Pre-Conditions:

This use case takes place in an opt-in XDS Affinity Domain, where all patient data is organized as episodes of care. The episode of care is summarized by a diagnostic code and always has an (expected) end date.

The patient is identified using a common patient ID.

The participating providers and organizations are listed in the HIE's Healthcare Provider Directory.

Main Flow:

A patient has completed an inpatient treatment for depression at a mental health treatment center. A staff member of the center recommends a care team consisting of a psychiatrist, the patient's primary care physician, and an occupational therapist. The staff member initiates a new episode of care in her information system to allow the care team to exchange all relevant documentation (i.e., documents regarding the inpatient treatment, psychiatric evaluations, occupational therapy progress notes, and intervention plans).

In the information system, the staff member selects the patient, then the diagnostic code that best summarizes the episode of care and enters the expected duration of the episode. She searches in the provider directory to find the care team members and adds them in her information system to the episode of care. The system prints out a consent form containing this data. The patient signs it and the nurse confirms the signature in her system.

The treatment center's system creates an XDS Folder representing the episode of care and a Privacy Consent Document referencing the Folder. The system sends these objects via its XDS Document Source to the central XDS Document Repository. When a care team member tries to access the episode of care, the HIE's security system (acting as an APPC Content Consumer with the Structured Policy Processing Option) extracts the structured and coded policy representation and makes an access decision.

Post-Condition:

The longitudinal patient record in the HIE contains the consent document.

The care team can upload and access any documents in the record that are linked to an XDS Folder that has the episode's diagnostic code in its folder codeList.

Other healthcare providers do not have access to the documents in the record that are linked to an XDS Folder that has the episode's diagnostic code in its folder codeList.

490 43.4.2.2.2 Consent for an Episode of Care Process Flow

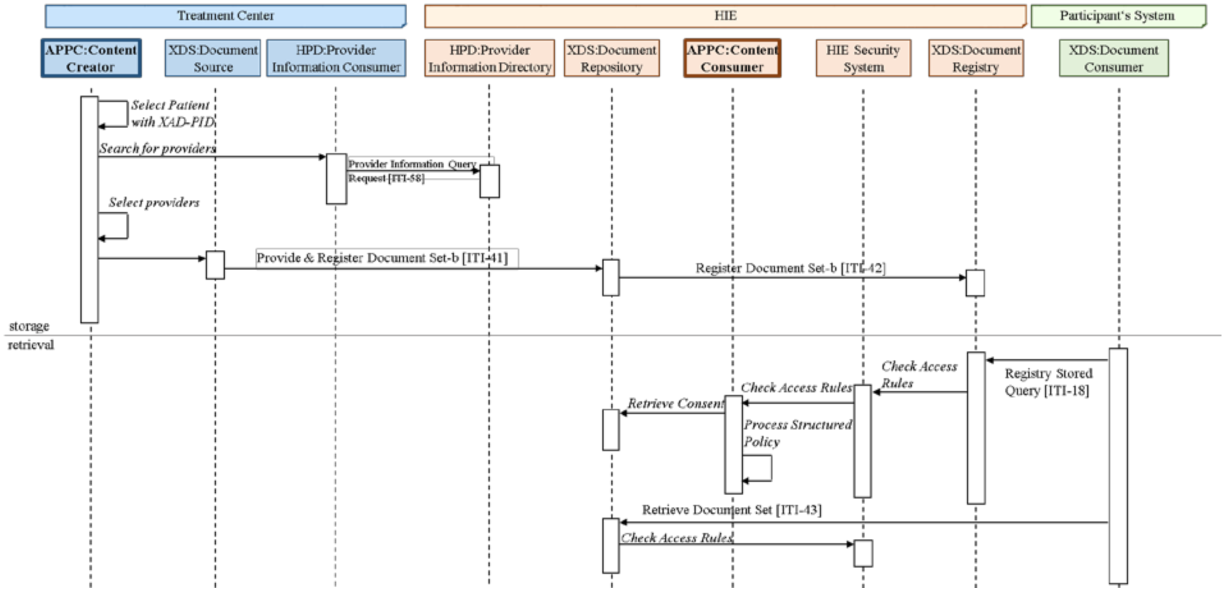


Figure 43.4.2.2.2-1: Consent for an Episode of Care Process Flow in APPC Profile

43.4.2.3 Use Case #3: Consent to Collect from a Specific Service Delivery Location 495

This use case describes a situation where the patient wishes to provide consent for an organization to collect information from one or more specific provider locations for multiple purposes.

43.4.2.3.1 Consent to Collect from a Specific Service Delivery Location Use Case Description 500

Pre-Condition:

This use case takes place in an opt-in XDS Affinity Domain, where collection of protected health information is only granted if the patient explicitly agreed to it. The patient has the right to specify which providers and service delivery locations can be included in that consent.

505 A clinic has an EMR system that has the capability to transmit clinical documents to an XDS Affinity Domain.

The clinic and the organization managing the HIE have agreements in place which allow the exchange of clinical information for certain purposes specified within the patient's signed consent document.

Main Flow:

The patient goes to a Family Practice Clinic for his annual checkup and is provided with a pamphlet describing the associated HIE and the potential advantages of having his healthcare information readily available to other healthcare providers in his area should the need arise.

After reading the material and discussing the advantages and potential risks with his physician, the patient decides to allow his records from the Family Practice Clinic to be registered with the HIE. He is presented with, and signs, an electronic consent form indicating that documents from the specific facility are permitted to be shared with the HIE.

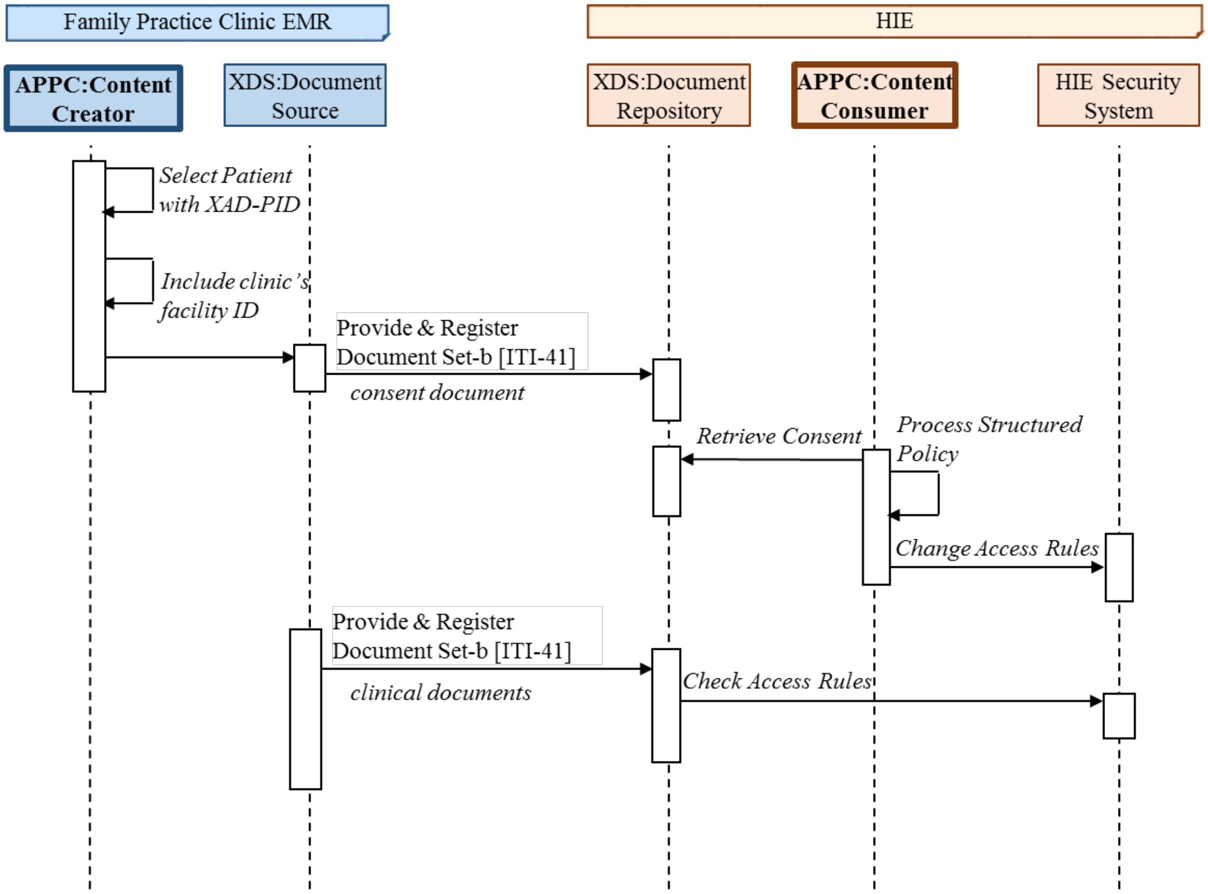
The receptionist saves the signed consent form in the clinic's EMR system and has the EMR transmit the document to the HIE for processing before sending the patient's clinical records that were a result of today's appointment. The consent document is stored in the HIE's XDS Document Repository and is used by the HIE's security system to confirm that the patient's clinical documents may be collected.

Post-Condition:

The longitudinal patient record in the HIE contains a consent document.

The longitudinal patient record in the HIE contains the documents resulting from the appointment in the Family Practice Clinic.

43.4.2.3.2 Consent to Collect from a Specific Service Delivery Location Process Flow



530

Figure 43.4.2.3.2-1: Consent to Collect from a Specific Service Delivery Location Process Flow in APPC Profile

43.4.2.4 Use Case #4: Withhold Consent for Information Related to a Specific Order 535

This use case describes a situation where the patient wishes to restrict the disclosure of the fact that a specific order was made as well as any information resulting from that order.

43.4.2.4.1 Withhold Consent to Disclose Information Related to a Specific Order Use Case Description

540 **Pre-Condition:**

The patient lives in a jurisdiction that has a central lab information repository where all lab orders and results are kept.

The jurisdiction uses an implied consent model for the provision of care, which means that the document would be visible by default.

Main Flow:

The patient goes to his primary care provider for screening for sexually transmitted diseases. He is a nurse in a local hospital and is concerned that his colleagues may have access to the order and test results.

The primary care provider would like to order a battery of tests in order to confirm a diagnosis. The patient indicates that he would like to withhold his consent for the disclosure of the battery order and the subsequent results. After some discussion, the provider enters the order into her lab's online order form and indicates that the patient has withheld consent for disclosure. This withholding of consent does not affect potential disclosure for public health reasons.

The lab information repository generates a lab order, and a consent document specifying that the patient wishes to deny access to the order, except to the ordering physician.

Later, a colleague attempts to view the patient's record and issues a request to list all lab records. Because of the information in the consent document, the lab information repository eliminates the order and result records from the colleague's search results.

Post-Condition:

The ordering physician has access to the lab order and result.

Other healthcare providers do not have access to the specific lab order and result, but may still have access to the patient's other lab orders and results.

43.4.2.4.2 Withhold Consent for Information Related to a Specific Order Process Flow

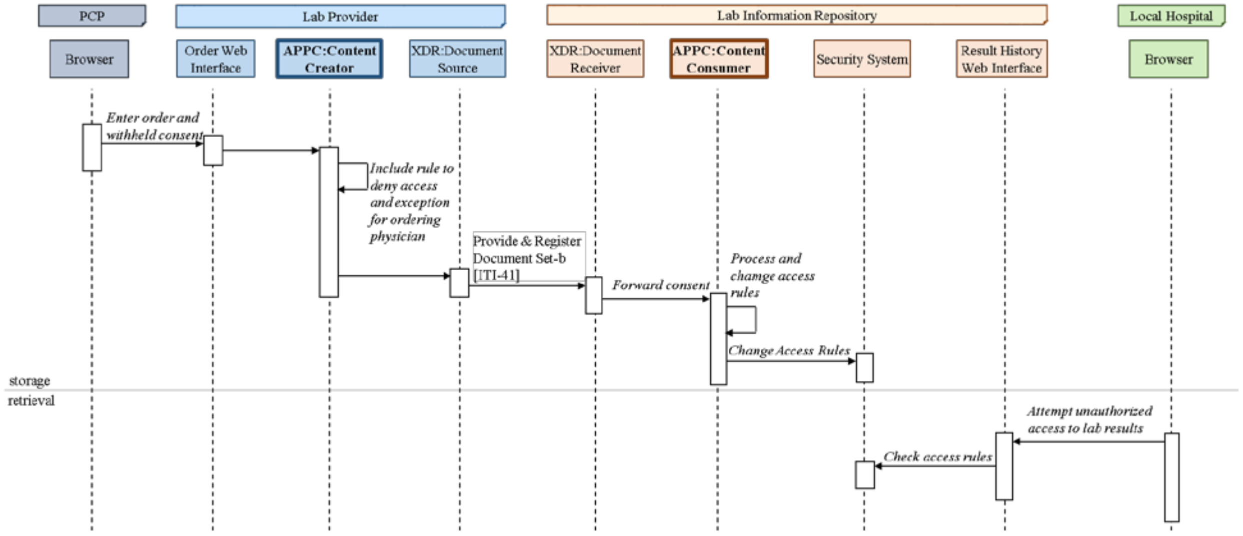

PCP
Lab Provider
Lab Information Repository
Local Hospital
Browser
Order Web Interface
APPC:Content Creator
XDR:Document Source
XDR:Document Receiver
APPC:Content Consumer
Security System
Result History Web Interface
Browser
Enter order and withheld consent
Include rule to deny access and exception for ordering physician
Provide & Register Document Set-b [ITI-41]
Forward consent
Process and change access rules
Change Access Rules
storage
retrieval
Attempt unauthorized access to lab results
Check access rules

Figure 43.4.2.4.2-1: Withhold Consent for Information Related to a Specific Order Process Flow in APPC Profile

43.4.2.5 Use Case #5: Withhold Consent to Disclose to a Specific Provider Organization

This use case details a scenario where the patient does not wish any of her health information disclosed to a particular organization.

43.4.2.5.1 Withhold Consent to Disclose to a Specific Provider Organization Use Case Description

Pre-Condition:

The jurisdiction uses an implied consent model for the provision of care, which means that the document would be visible by default.

The jurisdiction uses technical and governance mechanisms outside of the scope of this profile to ensure that the operators of the connected systems respect the patient's choices reflected in the consent documents.

Main Flow:

The patient is a nurse at a local hospital. He has been diagnosed with an STD, and is beginning treatment at a family practice clinic. The patient previously withheld his consent so that nobody but the ordering physician would be able to see the initial lab order and results. Now that he is beginning treatment, he does not wish to disclose any of his health information to the local hospital that he works at.

There is a jurisdictional consent repository (maintaining only consents) where the patient lives, so he calls the consent service desk to have his records blocked when accessed from the local hospital. After the client service representative establishes the patient's identity, she creates a new consent document, and saves it to the repository.

Later, a colleague tries to view the patient's records and issues a request in the hospital's EMR to list all of the patient's documents in the connected HIE. The EMR checks the jurisdictional consent repository before querying the HIE and processes the returned consent document. The EMR does not send the request to the HIE, since it is able to determine that access should be blocked for the local hospital.

Post-Condition:

The jurisdictional consent repository contains a consent document.

Healthcare providers in the local hospital do not have access to the patient's documents in the HIE.

Other healthcare providers still have access to the patient's documents in the HIE.

43.4.2.5.2 Withhold Consent to Disclose to a Specific Provider Organization Process Flow

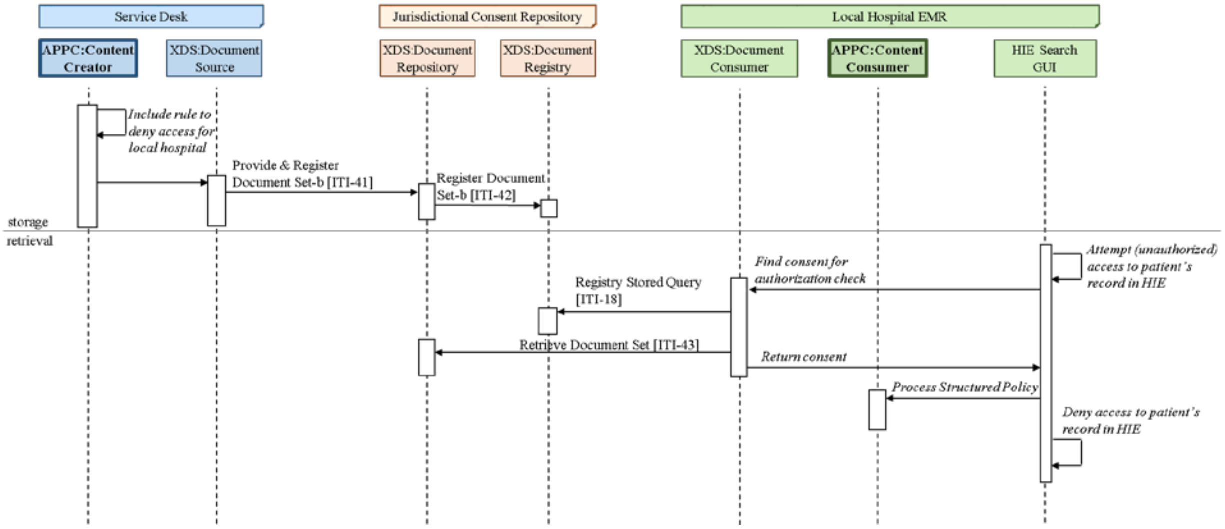

Service Desk
Jurisdictional Consent Repository
Local Hospital EMR
APPC:Content Creator
XDS:Document Source
XDS:Document Repository
XDS:Document Registry
XDS:Document Consumer
APPC:Content Consumer
HIE Search GUI
Include rule to deny access for local hospital
Provide & Register Document Set-b [ITI-41]
Register Document Set-b [ITI-42]
storage
retrieval
Attempt (unauthorized) access to patient's record in HIE
Find consent for authorization check
Registry Stored Query [ITI-18]
Retrieve Document Set [ITI-43]
Return consent
Process Structured Policy
Deny access to patient's record in HIE

Figure 43.4.2.5.2-1: Withhold Consent to Disclose to a Specific Provider Organization Process Flow in APPC Profile

43.4.2.6 Use Case #6: Withhold Consent to Disclose a Specific Document

This use case details a scenario where the patient does not wish that a specific document be disclosed to any healthcare provider.

43.4.2.6.1 Withhold Consent to Disclose a Specific Document Use Case Description

Pre-Condition:

The XDS Affinity Domain uses an implied consent model for the provision of care, which means that all documents would be accessible by default.

The patient has access to a patient portal with the ability to list and display all documents available in his longitudinal patient record.

In this jurisdiction, the patient has the right to deny access to any individual document in his longitudinal patient record. According to this jurisdiction's rules, there must be no indication in the record if the patient has decided to deny access to any documents.

Main Flow:

The patient has undergone a drug screening and the resulting document has been added automatically to his longitudinal patient record by the lab. He does not want this document to be accessible by his healthcare providers.

The patient logs into the patient portal and finds the drug screening result document. He selects the option to "hide" this document. The patient portal presents the potential risks of hiding information from healthcare providers. The patient acknowledges the warning and confirms that the document should be hidden.

The patient portal creates a Privacy Consent Document. The consent includes a structured policy that denies access to this document and to the consent document itself to anybody except the patient. The patient portal sends the document to the HIE using the Mobile access to Health Documents (MHD) Profile. The HIE extracts the structured policy and adjusts the access rights accordingly.

A healthcare provider accesses the HIE through his EMR. The provider sees the patient's other clinical documents, but does not see that there is a drug screening result document or that a document has been hidden.

Post-Condition:

The longitudinal patient record in the HIE contains a consent document.

Healthcare providers do not have access to the drug screening result document in the HIE.

Healthcare providers do not have access to the consent document in the HIE.

The patient has access to the drug screening result document and the consent document in the HIE using the patient portal.

43.4.2.6.2 Withhold Consent to Disclose a Specific Document Process Flow

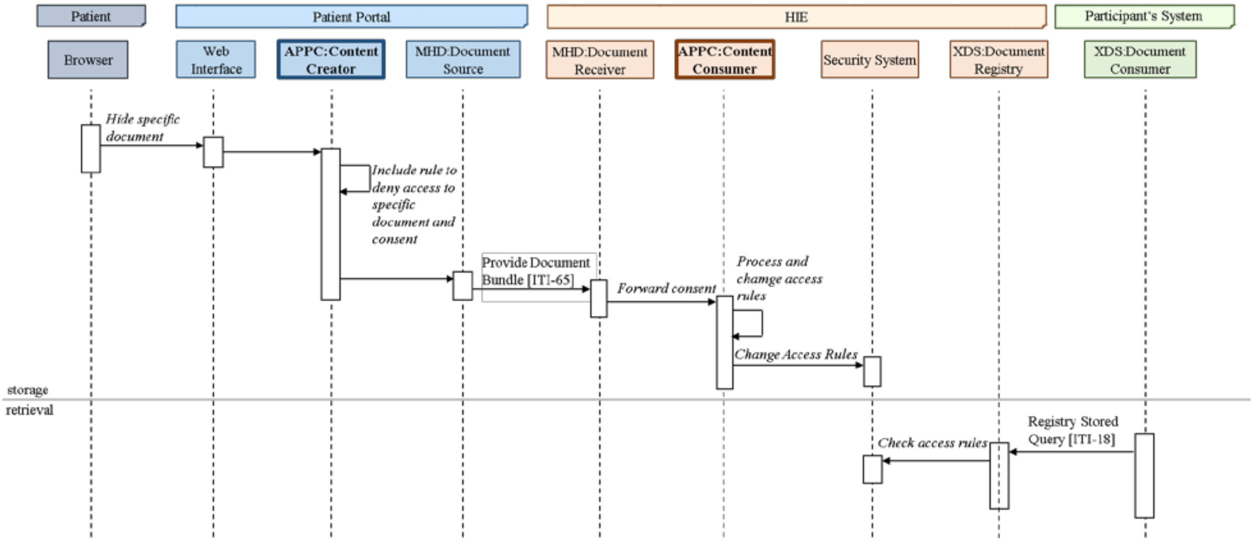


Figure 43.4.2.6.2-1: Withhold Consent to Disclose to Specific Document Process Flow in APPC Profile

43.5 APPC Privacy and Security Considerations

Like patients' clinical documents, consent documents are also governed by privacy policies. The content of a Privacy Consent Document may itself contain sensitive information. For example, a terminally ill patient may decide that his prognosis should not be shared with his family members, but that other information may be. Sharing the Privacy Consent Document with family members would potentially inform them of a negative prognosis. Thus, the confidentialityCode placed on Privacy Consent Documents must be appropriately assigned. Another solution is to include access rules in the Privacy Consent Document that specifically regulate access to the consent document itself (see Section 43.4.2.6 for an example).

The machine processing of structured policies within a healthcare environment has different considerations and risks than interpreting similar structured policies within other non-treatment environments. Policies must be crafted to prevent inappropriate disclosure while enabling appropriate access to critical healthcare information (e.g., severe allergies). The Patient Privacy Policy Domain should take care in designing the policies for its access control system including appropriate "break-glass" policies. Governance of privacy policies is concerned with instances of multiple conflicting policies and the ability to identify and retrieve all applicable policies.

One mitigation strategy that is often adopted in healthcare is to provide accountability through audit controls. Healthcare providers are trusted not to abuse their ability to access patient's private information, but that is backed up by a policy of monitoring provider access to detect if abuse has occurred. This strategy reduces the risk of death or serious injury due to lack of access to critical healthcare information, at the increased risk of disclosure of private information. The

Audit Trail and Node Authentication (ATNA) Integration Profile, which is mandated for actors in IHE Document Sharing and related profiles, describes a framework for such audit logs.

Quality identification, authentication, and authorization governance are critical components of privacy and security. A failure to provide access, or an accidental disclosure, may be caused by inaccurate document metadata, e.g., mislabeled documents, and by inaccurate Privacy Consent Documents, e.g., inserting the wrong facility identifier in a structured policy. The XDS Affinity Domain can mitigate these risks by establishing a quality control system. This includes establishing well-documented processes for manually-selected metadata and careful review of metadata automatically mapped from other formats.

43.6 APPC Cross Profile Considerations

A Content Creator or Content Consumer may be grouped with appropriate actors from document sharing profiles such as XDS, XDM, or XDR to exchange the Privacy Consent Document.

The Document Sharing metadata has specific relationships or dependencies (which we call bindings) to the content of the Advanced Patient Privacy Consent document described in this content profile. ITI TF-3: 5.6.1.2.2 defines the bindings to use when grouping the Content Creator of this profile with actors from document sharing profiles such as XDS, XDM, or XDR.

The APPC Profile and the BPPC Profile can both be used to support digital consent documents. Generally, any consent document that can be expressed via BPPC can also be expressed via APPC. Whether APPC is the best approach for a particular Patient Privacy Policy Domain depends on the complexity of the Patient Privacy Policies and the capabilities of the systems involved in the exchange. Whereas APPC allows for individualized consents that further constrain generally applicable policies, BPPC only allows a choice from a set of predefined Patient Privacy Policies. Further guidance regarding how to design Patient Privacy Policies and how to choose between APPC and BPPC can be found in Appendix P.

Appendices

This section is left blank. It is a placeholder for an updated Appendix P, which will be created by CP-ITI-948. The appendix is aiming to assist readers in creating privacy policies and in deciding when to use APPC or BPPC.

Volume 2 – Transactions

No updates to Volume 2.

Volume 3 – Content Modules

5 IHE Content Specifications

Add to Section 5 IHE Content Specifications

5.6 Advanced Patient Privacy Consents Content Module

This section defines the Privacy Consent Document.

5.6.1 References

All standards, which are referenced in this document, are listed below with their common abbreviation, full title, and link to the standard.

Table 5.6.1-1: Advanced Patient Privacy Consents - Referenced Standards

Abbreviation	Title	URL
XACML2	eXtensible Access Control Markup Language (XACML) Version 2.0	XACML Core 2.0
HL7ADTS	HL7v3 Abstract Data Type Specification - ANSI/HL7 V3 DT, R1-2004 3/19/2012	HL7v3 ADTS

5.6.2 Privacy Consent Document Specification

5.6.2.1 Content Specification

The Privacy Consent Document shall be an XML document, adhering to the specifications found in [XACML2]. Its purpose is to express unambiguously the access granted by the patient to a provider, group of providers or any other participant in a Document Sharing environment. It specifically focuses on expressing authorizations based on IHE Document Sharing Metadata and transactions, as well as attributes in the Provide X-User Assertion [ITI-40] transaction in the Cross-Enterprise User Assertion (XUA) Profile. It can also be used for expressing authorizations based on other attributes, but this requires agreement on those attributes between Content Creators and the enforcement system, possibly established by national or regional regulators or through national extensions.

Attributes that the Content Creator may use in a Privacy Consent Document are defined in sections below:

- IHE XUA attributes are defined in Section 5.6.2.1.4
- General IHE Document Sharing attributes are defined in Section 5.6.2.1.5
- DocumentEntry attributes are defined in Section 5.6.2.1.5.2
- Folder attributes are defined in Section 5.6.2.1.5.3
- SubmissionSet attributes are defined in Section 5.6.2.1.5.4

An informative schema is available. See ITI TF-2x: Appendix W.

5.6.2.1.1 Policy Structure

The Privacy Consent Document shall contain exactly one `PolicySet` root element. As defined in [XACML2], it may contain other `PolicySet` elements as child elements of the root. The `PolicySet` root element may also contain `Policy` child elements. The `PolicySetId` attribute of the `PolicySet` root element is known as the Root Policy Set ID and must be a URN encoded globally unique identifier as defined by ITI TF-2x: Appendix B.

The `PolicySet` root element may contain references to other `PolicySet` or `Policy` elements, using the `PolicySetIdReference` or the `PolicyIdReference` elements respectively. This allows the Patient Privacy Policy Domain to define foundational Patient Privacy Policies, which are applied to specific individuals and situations by the Privacy Consent Document. E.g., a referenced foundational Patient Privacy Policy defines what kind of access a healthcare provider receives; the Privacy Consent Document applies this to one specific provider, patient, and purpose of use. How external references are resolved is out of scope for this profile.

The `PolicySet` root element shall contain at least one //`Target/Resources/Resource/ResourceMatch/ResourceAttributeDesignator` element with AttributeId `urn:ihe:iti:ser:2016:patient-id`, which restricts its applicability to one or more patient IDs belonging to one patient (see Section 5.6.2.1.5.1.5). When using IHE Document Sharing profiles, the patient ID in the Privacy Consent Document should be identical to the patient ID in the Document Sharing metadata. Note that patient merge events can change the patient ID in the Document Sharing metadata and that this may necessitate changes of the patient ID in the structured policy as well.

5.6.2.1.1.1 Human Readable Representation

The `PolicySet` root element shall contain a `Description` child element. This `Description` element shall contain a plain text description (i.e., no markup) of the contents of the Privacy Consent Document. It may hold information on who signed the consent form, when it was signed and what person or organization is responsible for this document.

Other elements in the Privacy Consent Document may contain additional `Description` elements that explain the relevant aspects of that `PolicySet`, `Policy`, or `Rule`.

The Description element has a limited ability to carry human readable representation. Therefore, Content Creators may create a separate document containing the human readable representation of the Privacy Consent Document. The document may be a BPPC consent acknowledgment document (see ITI TF-3: 5.1), a PDF (e.g., following the XDS-SD Profile – see ITI TF-3: 5.2), or any other appropriate format. When transmitting such an additional representation using IHE Document Sharing profiles, the Content Creator shall register the human readable representation as a separate document entry and add a transformation (XFRM) association linking the Privacy Consent Document and the human readable document. The XDS Affinity Domain may decide whether the Privacy Consent Document is considered a transformation of the human readable document or whether the human readable document is considered a transformation of the Privacy Consent Document (i.e., the direction of the association between the two).

When the human readable representation is a BPPC consent acknowledgment document, the Root Policy Set ID of the Privacy Consent Document and the BPPC Patient Privacy Policy Identifier shall be identical.

5.6.2.1.1.2 Example Document

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet PolicySetId="urn:uuid:e3585197-9e3d-4ca3-9583-4540a3a5b64b"
  PolicyCombiningAlgId=
    "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:hl7="urn:hl7-org:v3"
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os ihe-appc-
xacml-combined-schema-1.0.xsd">
    <Description>The patient agrees to grant access to the identified
facility. The extent of access is defined by the referenced policy.
    </Description>
    <Target>
        <Subjects>
            <Subject>
                <SubjectMatch
  MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <AttributeValue
  DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                        urn:oid:2.999.2.1.1.35
                    </AttributeValue>
                    <SubjectAttributeDesignator
  DataType="http://www.w3.org/2001/XMLSchema#anyURI"
  AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization-id" />
                </SubjectMatch>
            </Subject>
        </Subjects>
        <Resources>
            <Resource>
                <ResourceMatch MatchId="urn:hl7-org:v3:function:II-equal">
                    <AttributeValue DataType="urn:hl7-org:v3#II">
                        <hl7:InstanceIdentifier root="2.999.1.1.1"
                          extension="78901234" />
                    </AttributeValue>
                    <ResourceAttributeDesignator DataType="urn:hl7-org:v3#II"
                      AttributeId="urn:ihe:iti:ser:2016:patient-id" />
                </ResourceMatch>
            </Resource>
        </Resources>
    </Target>
    <PolicySetIdReference>
        urn:example:policy:extensive-access
    </PolicySetIdReference>
</PolicySet>
```

5.6.2.1.2 Data Types

The Privacy Consent Document relies on data types derived from HL7v3 (see [HL7ADTS] Section 2.9 and 2.17) to represent complex data types such as coded values and instance identifiers. These data types utilize the XACML extensibility described in chapter 8 of [XACML2]. If the name of the XML attribute or element matches a property name in the HL7v3 Data Types Abstract Specification then the semantics of the content will be as described in the HL7v3 Data Types Abstract Specification, otherwise the narrative will explain the use of the attribute or element.

Coded Values Data Type

Data type URI: `urn:hl7-org:v3#CV`

Specification:

A CV shall have the XML element `codedValue` with the XML attributes `code` and `codeSystem`. `code` may be any string. `codeSystem` shall be an OID. A CV may also have the XML attributes `codeSystemName`, `codeSystemVersion`, `displayName` and the XML child element `originalText`. `codeSystemName`, `codeSystemVersion`, and `displayName` may be any string.

Example:

```
<CodedValue code="1" codeSystem="1.0.14265.1" />
```

Instance Identifier Data Type

Data type URI: `urn:hl7-org:v3#II`

An Instance Identifier shall have the XML element `InstanceIdentifier` with the XML attribute `root` and may have the XML attribute `extension`. `extension` may be any string. `root` shall be an OID. An Instance Identifier may also have the XML attribute `assigningAuthorityName` and `displayable`. `assigningAuthorityName` may be any string. `displayable` must be either `true` or `false` if it exists.

Example:

```
<InstanceIdentifier extension="11231" root="2.16.840.1.113883.19" />
```

5.6.2.1.3 Functions

The use of HL7v3-derived data types in Privacy Consent Documents necessitates the use of custom functions to compare attributes with those data types. These functions utilize the XACML extensibility described in chapter 8 of [XACML2].

Coded Value Comparison Function

Function URI: `urn:hl7-org:v3:function:CV-equal`

This function shall take two arguments of data-type `urn:hl7-org:v3#CV` and SHALL return an `http://www.w3.org/2001/XMLSchema#boolean`. The function shall return `True` if and only if the `code` attribute of both of its arguments are equal according to the function `urn:oasis:names:tc:xacml:1.0:function:string-equal` AND the `codeSystem` attribute of both of its arguments are equal according to the function `urn:oasis:names:tc:xacml:1.0:function:string-equal`. Otherwise, it shall return `False`.

Instance Identifier Comparison Function

Function URI: `urn:hl7-org:v3:function:II-equal`

This function shall take two arguments of data-type `urn:hl7-org:v3#II` and shall return an `http://www.w3.org/2001/XMLSchema#boolean`. The function shall return `True` if:

- the `extension` attribute is empty and the `root` attribute of both of its arguments are equal according to the function `urn:oasis:names:tc:xacml:1.0:function:string-equal`; or,
- the `extension` attribute of both of its arguments are equal according to the function `urn:oasis:names:tc:xacml:1.0:function:string-equal`, and the `root` attribute of both of its arguments are equal according to the function `urn:oasis:names:tc:xacml:1.0:function:string-equal`.

Otherwise, it shall return `False`.

5.6.2.1.4 Attribute Definitions – Subject

5.6.2.1.4.1 User ID

IHE XUA Definition	ITI TF-2b: 3.40.4.1.2 as "Subject" - "logical identifier of the principal performing the original service request"
SAML Attribute Name	not an attribute in SAML, but communicated in `<Subject>/<NameID>`

SAML Example	`<saml:Subject>`
	`    <saml:NameID>user1</saml:NameID>`
	`    <saml:SubjectConfirmation`
	`      Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>`
	`</saml:Subject>`

XACML Target Section	subject

XACML Attribute ID	`urn:oasis:names:tc:xacml:1.0:subject:subject-id`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#string`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string">`
	`    <AttributeValue>user1</AttributeValue>`
	`</Attribute>`

5.6.2.1.4.2 User Organization

IHE XUA Definition	ITI TF-2b: 3.40.4.1.2 as "Subject Organization" - "plain text description of the organization"
SAML Attribute Name	`urn:oasis:names:tc:xspa:1.0:subject:organization`

SAML Example	`<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">`
	`    <saml:AttributeValue>Family Medical Clinic`
	`    </saml:AttributeValue>`
	`</saml:Attribute>`

XACML Target Section	subject
XACML Attribute ID	`urn:oasis:names:tc:xspa:1.0:subject:organization`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#string`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization" DataType="http://www.w3.org/2001/XMLSchema#string">`
	`    <AttributeValue>Family Medical Clinic</AttributeValue>`
	`</Attribute>`

5.6.2.1.4.3 User Organization ID

IHE XUA Definition	ITI TF-2b: 3.40.4.1.2 as "Subject Organization ID" - "a unique identifier for the organization that the user is representing in performing this transaction"
SAML Attribute Name	`urn:oasis:names:tc:xspa:1.0:subject:organization-id`

SAML Example	`<saml:Attribute`
	`Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">`
	`    <saml:AttributeValue>http://familymedicalclinic.org`
	`    </saml:AttributeValue>`
	`</saml:Attribute>`

XACML Target Section	subject
XACML Attribute ID	urn:oasis:names:tc:xspa:1.0:subject:organization-id
XACML Data Type	http://www.w3.org/2001/XMLSchema#anyURI
XACML Attribute Value Content	The organization ID shall be one of: a) Object Identifier (OID), using the urn format (i.e., "urn:oid:" followed by the OID); b) a URL assigned to that organization.

XACML Example	`<Attribute AttributeId=`
	`"urn:oasis:names:tc:xspa:1.0:subject:organization-id"`
	`DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>http://familymedicalclinic.org`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.4.4 User Home Community ID

IHE XUA Definition	ITI TF-2b: 3.40.4.1.2 as "Home Community ID"
SAML Attribute Name	`urn:ihe:iti:xca:2010:homeCommunityId`

SAML Example	`<saml:Attribute`
	`Name="urn:ihe:iti:xca:2010:homeCommunityId">`
	`    <saml:AttributeValue>`
	`        urn:oid:2.16.840.1.113883.3.190`
	`    </saml:AttributeValue>`
	`</saml:Attribute>`

XACML Target Section	subject
XACML Attribute ID	urn:ihe:iti:xca:2010:homeCommunityId
XACML Data Type	http://www.w3.org/2001/XMLSchema#anyURI
XACML Attribute Value Content	The identifier shall be an Object Identifier (OID), using the urn format ("urn:oid:" followed by the OID)

XACML Example	<Attribute AttributeId=
	"urn:ihe:iti:xca:2010:homeCommunityId"
	  DataType="http://www.w3.org/2001/XMLSchema#anyURI">
	    <AttributeValue>
	        urn:oid:2.16.840.1.113883.3.190
	    </AttributeValue>
	</Attribute>

5.6.2.1.4.5 National Provider Identifier (NPI)

IHE XUA Definition	ITI TF-2b: 3.40.4.1.2 as "National Provider Identifier"
SAML Attribute Name	urn:oasis:names:tc:xspa:1.0:subject:npi

SAML Example	<saml:Attribute
	Name="urn:oasis:names:tc:xspa:1.0:subject:npi">
	   <saml:AttributeValue>1234567890</saml:AttributeValue>
	</saml:Attribute>

XACML Target Section	subject
XACML Attribute ID	urn:oasis:names:tc:xspa:1.0:subject:npi
XACML Data Type	urn:hl7-org:v3#II
XACML Attribute Value Content	When the SAML attribute contains a value in the string format instead of the HL7 CE format, the Content Creator may need to select an appropriate instance identifier root representing the namespace of the national provider identifier.

XACML Example	<Attribute
	    AttributeId="urn:oasis:names:tc:xspa:1.0:subject:npi"
	    DataType="urn:hl7-org:v3#II">
	    <AttributeValue>
	        <hl7:InstanceIdentifier extension="1234567890"
	            root="2.16.840.1.113883.4.6" />
	    </AttributeValue>
	</Attribute>

5.6.2.1.4.6 User Role

IHE XUA Definition	ITI TF-2b: 3.40.4.1.2.1 as "Subject-Role"
SAML Attribute Name	urn:oasis:names:tc:xacml:2.0:subject:role

SAML Example	<saml:Attribute
	Name="urn:oasis:names:tc:xacml:2.0:subject:role">
	    <saml:AttributeValue>
	        <Role xmlns="urn:hl7-org:v3"
	          xsi:type="CE" code="46255001"
	          codeSystem="2.16.840.1.113883.6.96"
	          codeSystemName="SNOMED_CT"
	          displayName="Pharmacist"/>
	      </saml:AttributeValue>
	</saml:Attribute>

XACML Target Section	subject
XACML Attribute ID	urn:oasis:names:tc:xacml:2.0:subject:role
XACML Data Type	urn:hl7-org:v3#CV
XACML Attribute Value Content	No restrictions

XACML Example	<Attribute
	AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
	DataType="urn:hl7-org:v3#CV">
	    <AttributeValue>
	        <hl7:CodedValue code="46255001"
	          codeSystem="2.16.840.1.113883.6.96" />
	    </AttributeValue>
	</Attribute>

5.6.2.1.4.7 Purpose Of Use

IHE XUA Definition	ITI TF-2b: 3.40.4.1.2.3 as "PurposeOfUse"
SAML Attribute Name	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse

SAML Example	<saml:Attribute
	  name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
	    <saml:AttributeValue>
	        <PurposeOfUse xmlns="urn:hl7-org:v3" xsi:type="CE"
	          code="12"
	          codeSystem="1.0.14265.1"
	          codeSystemName="ISO 14265 Classification of Purposes for processing personal health information"
	          displayName="Law Enforcement"/>
	   </saml:AttributeValue>
	</saml:Attribute>

XACML Target Section	subject
XACML Attribute ID	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse
XACML Data Type	urn:hl7-org:v3#CV
XACML Attribute Value Content	No restrictions

XACML Example	<Attribute AttributeId=
	"urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
	DataType="urn:hl7-org:v3#CV">
	    <AttributeValue>
	        <hl7:CodedValue code="12"
	          codeSystem="1.0.14265.1" />
	    </AttributeValue>
	</Attribute>

5.6.2.1.5 Attribute Definitions – Resources

5.6.2.1.5.1 Attribute Definitions – General Document Sharing Attributes

This section describes how to express IHE Document Sharing metadata in XACML for metadata attributes used in multiple resource types (DocumentEntries, Folders, or SubmissionSets).

5.6.2.1.5.1.1 Author Institution ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.1 as "authorInstitution"; this attribute can be used to restrict access based on the authorInstitution identifier. Note that the identifiers might belong to multiple, separate authors. When including both an authorPerson ID and an authorInstitution ID in a policy, policy writers need to take into account that they might belong to different authors in the IHE Document Sharing metadata.
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:author-institution:id`
XACML Data Type	`urn:hl7-org:v3#II`
XACML Attribute Value Content	If XON.10 is an OID, use XON.10 as root with no extension. If XON.10 is not an OID, use XON.6.2 as root and XON.10 as extension
Used in Resource Type	DocumentEntry, SubmissionSet

XACML Example	`<Attribute`
	`AttributeId="urn:ihe:iti:appc:2016:author-institution:id"`
	`DataType="urn:hl7-org:v3#II">`
	`    <AttributeValue>`
	`        <hl7:InstanceIdentifier root="1.2.3.9.1789.45"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.1.2 Author Person ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.2 as "authorPerson"; this attribute can be used to restrict access based on the authorPerson identifier. Note that the identifiers might belong to multiple, separate authors. When including both an authorPerson ID and an authorInstitution ID in a policy, policy writers need to take into account that they might belong to different authors in the IHE Document Sharing metadata.
XACML Target Section	Resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:author-person:id`

XACML Data Type	`urn:hl7-org:v3#II`
XACML Attribute Value Content	If XCN.1 is an OID, use XCN.1 as root with no extension. If XCN.1 is not an OID, use XCN.9.2 as root and XCN.1 as extension.
Used in Resource Type	DocumentEntry, SubmissionSet

XACML Example	`<Attribute`
	`AttributeId="urn:ihe:iti:appc:2016:author-person:id"`
	`DataType="urn:hl7-org:v3#II">`
	`    <AttributeValue>`
	`        <hl7:InstanceIdentifier extension="11375"`
	`          root="1.2.840.113619.6.197"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.1.3 Availability Status

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.2 as "DocumentEntry.availabilityStatus" ITI TF-3: 4.2.3.3.2 as “SubmissionSet.availabilityStatus” ITI TF-3: 4.2.3.4.1 as “Folder.availabilityStatus”
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:availability-status`
XACML Data Type	http://www.w3.org/2001/XMLSchema#anyURI
XACML Attribute Value Content	"`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" or "`urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated`" or any other valid availabilityStatus
Used in Resource Type	DocumentEntry, Folder, SubmissionSet

XACML Example	`<Attribute`
	`AttributeId="urn:ihe:iti:appc:2016:availability-status"`
	`DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>`
	`      urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.1.4 Community ID

IHE Document Sharing Metadata Definition	An Object Identifier (OID) that uniquely identifies the community holding the resource in question (e.g., a XDS Affinity Domain holding a document). This is often identical to the homeCommunityId (ITI TF-3: 4.2.3.2.12 as "DocumentEntry.homeCommunityId" and ITI TF-3: 4.2.3.3.6 as "SubmissionSet.homeCommunityId"), but may differ from it in complex cross-community scenarios with proxy gateways. For example, a policy writer may use this to restrict access to all data held in a specific community.
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:community-id`
XACML Data Type	http://www.w3.org/2001/XMLSchema#anyURI
XACML Attribute Value Content	The identifier shall be an Object Identifier (OID), using the urn format ("urn:oid:" followed by the OID)
Used in Resource Type	DocumentEntry, Folder, SubmissionSet

XACML Example	`<Attribute`
	`  AttributeId="urn:ihe:iti:appc:2016:community-id"`
	`  DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>urn:oid:2.999.1.1.12345`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.1.5 Patient ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.16 as "DocumentEntry.patientId" ITI TF-3: 4.2.3.3.8 as "SubmissionSet.patientId" ITI TF-3: 4.2.3.4.7 as "Folder.patientId"
XACML Target Section	Resource
XACML Attribute ID	`urn:ihe:iti:ser:2016:patient-id`
XACML Data Type	`urn:hl7-org:v3#II`

XACML Attribute Value Content	Use CX.4.2 as root and CX.1 as extension
Used in Resource Type	DocumentEntry, Folder, SubmissionSet

XACML Example	`<Attribute`
	`  AttributeId="urn:ihe:iti:ser:2016:patient-id"`
	`  DataType="urn:hl7-org:v3#II">`
	`    <AttributeValue>`
	`        <hl7:InstanceIdentifier extension="6578946"`
	`          root="1.3.6.1.4.1.21367.2005.3.7"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.1.6 Source System ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3.9 as "SubmissionSet.sourceId"; in the IHE Document Sharing metadata, the sourceId is only defined for SubmissionSets. To enable source-dependent policies, this attribute is also attached to the XACML representations of DocumentEntries and Folders.
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:source-system-id`
XACML Data Type	http://www.w3.org/2001/XMLSchema#anyURI
XACML Attribute Value Content	The attribute shall contain the sourceId of the system which originally submitted the object; for a SubmissionSet this is the sourceId, for a DocumentEntry, and for a Folder this is the sourceId of the SubmissionSet used to initially register the object.
Used in Resource Type	DocumentEntry, Folder, SubmissionSet

XACML Example	`<Attribute`
	`  AttributeId="urn:ihe:iti:appc:2016:source-system-id"`
	`  DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>`
	`        1.3.6.1.4.1.21367.2005.3.7`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2 Attribute Definitions – DocumentEntry Resource

5.6.2.1.5.2.1 Class Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.3 as "DocumentEntry.classCode"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:class-code`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId=`
	`"urn:ihe:iti:appc:2016:document-entry:class-code"`
	`DataType="urn:hl7-org:v3#CV">`
	`    <AttributeValue>`
	`        <hl7:CodedValue code="10160-0"`
	`          codeSystem="2.16.840.1.113883.6.1"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.2 Confidentiality Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.5 as "DocumentEntry.confidentialityCode"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:confidentiality-code`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	No restrictions

XACML Example	<Attribute
	 AttributeId="urn:ihe:iti:appc:2016:confidentiality-code"
	 DataType="urn:hl7-org:v3#CV">
	    <AttributeValue>
	      <hl7:CodedValue code="N"
	        codeSystem="2.16.840.1.113883.5.25"/>
	    </AttributeValue>
	</Attribute>

5.6.2.1.5.2.3 Creation Time

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.6 as "DocumentEntry.creationTime"
XACML Target Section	resource
XACML Attribute ID	urn:ihe:iti:appc:2016:document-entry:creation-time
XACML Data Type	http://www.w3.org/2001/XMLSchema#dateTime
XACML Attribute Value Content	The Content Creator shall transform the creationTime into a valid instance of an XML dateTime (which is based on ISO8601). This may involve adding date or time components, because in Document Sharing metadata the DTM data type allows for partial dates (see ITI TF-3: Table 4.2.3.1.7-2). To transform an incomplete creationTime into a dateTime instance, the Content Creator shall use the smallest instant covered by the partial date. E.g., "200904" would be transformed to "2009-04-01T00:00:00Z". The XACML dateTime shall be expressed as UTC using 'Z' as the timezone indicator. The DTM data type allows only for UTC as the timezone; therefore no further transformation is necessary.

XACML Example	<Attribute AttributeId=
	  "urn:ihe:iti:appc:2016:document-entry:creation-time"
	  DataType="http://www.w3.org/2001/XMLSchema#dateTime">
	    <AttributeValue>2004-12-25T21:20:10Z</AttributeValue>
	</Attribute>

5.6.2.1.5.2.4 Event Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.8 as "DocumentEntry.eventCodeList"

XACML Target Section	resource
XACML Attribute ID	urn:ihe:iti:appc:2016:document-entry:event-code
XACML Data Type	urn:hl7-org:v3#CV
XACML Attribute Value Content	No restrictions

XACML Example	<Attribute AttributeId=
	  "urn:ihe:iti:appc:2016:document-entry:event-code"
	  DataType="urn:hl7-org:v3#CV">
	    <AttributeValue>
	        <hl7:CodedValue code="45.23"
	          codeSystem="2.16.840.1.113883.6.2"/>
	    </AttributeValue>
	</Attribute>

5.6.2.1.5.2.5 Healthcare Facility Type Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.11 as "DocumentEntry.healthcareFacilityTypeCode"
XACML Target Section	resource
XACML Attribute ID	urn:ihe:iti:appc:2016:document-entry:healthcare-facility-type-code
XACML Data Type	urn:hl7-org:v3#CV
XACML Attribute Value Content	No restrictions

XACML Example	<Attribute
	AttributeId="urn:ihe:iti:appc:2016:document-entry:healthcare-facility-type-code"
	DataType="urn:hl7-org:v3#CV">
	    <AttributeValue>
	        <hl7:CodedValue code="310400000X"
	          codeSystem="2.16.840.1.113883.6.101"/>
	    </AttributeValue>
	</Attribute>

5.6.2.1.5.2.6 Legal Authenticator

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.14 as "DocumentEntry.legalAuthenticator"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:legal-authenticator:id`
XACML Data Type	`urn:hl7-org:v3#II`
XACML Attribute Value Content	If XCN.1 is an OID, use XCN.1 as root with no extension. If XCN.1 is not an OID, use XCN.9 as root and XCN.1 as extension.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:legal-authenticator:id"`
	`  DataType="urn:hl7-org:v3#II">`
	`    <AttributeValue>`
	`        <hl7:InstanceIdentifier extension="11375"`
	`          root="1.2.840.113619.6.197"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.7 Practice Setting Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.17 as "DocumentEntry.practiceSettingCode"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:practice-setting-code`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:practice-setting-code"`
	`  DataType="urn:hl7-org:v3#CV">`
	`    <AttributeValue>`

	`        <hl7:CodedValue code="213ER0200X"`
	`          codeSystem="2.16.840.1.113883.6.101"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.8 Repository Unique ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.18 as "DocumentEntry.repositoryUniqueId"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:ser:2016:document-entry:repository-unique-id`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#anyURI`
XACML Attribute Value Content	The identifier shall be an Object Identifier (OID), using the urn format ("urn:oid:" followed by the OID)

XACML Example	`<Attribute AttributeId="urn:ihe:iti:ser:2016:document-entry:repository-unique-id"`
	`  DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>`
	`        urn:oid:1.3.6.1.4.5`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.9 Reference ID List

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.28 as "DocumentEntry.referenceIdList"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:reference-id`
XACML Data Type	`urn:hl7-org:v3#II`
XACML Attribute Value Content	If CXi.1 is an OID, use CXi.1 as root with no extension. If CXi.1 is not an OID, use CXi.4.2 as root and CXi.1 as extension. CXi.5 is never used.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:reference-id-list"`
	`  DataType="urn:hl7-org:v3#II">`
	`    <AttributeValue>`
	`        <hl7:InstanceIdentifier extension="2013001"`
	`          root="2.999.1"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.10 Service Start Time

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.19 as "DocumentEntry.serviceStartTime"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:service-start-time`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#dateTime`
XACML Attribute Value Content	The Content Creator shall transform the serviceStartTime into a valid instance of an XML dateTime (which is based on ISO8601). This may involve adding date or time components, because in IHE Document Sharing metadata, the DTM data type allows for partial dates (see ITI TF-3: Table 4.2.3.1.7-2). To transform an incomplete serviceStartTime into a dateTime instance, the Content Creator shall use the smallest instant covered by the partial date. E.g., "200904" would be transformed to "2009-04-01T00:00:00Z". The XACML dateTime shall be expressed as UTC using 'Z' as the timezone indicator. The DTM data type allows only for UTC as the timezone, therefore no further transformation is necessary.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:service-start-time"`
	`  DataType="http://www.w3.org/2001/XMLSchema#dateTime">`
	`    <AttributeValue>2004-12-25T21:20:10Z</AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.11 Service Stop Time

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.20 as "DocumentEntry.serviceStopTime"

XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:service-stop-time`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#dateTime`
XACML Attribute Value Content	The Content Creator shall transform the serviceStopTime into a valid instance of an XML dateTime (which is based on ISO8601). This may involve adding date or time components, because in IHE Document Sharing metadata, the DTM data type allows for partial dates (see ITI TF-3: Table 4.2.3.1.7-2). To transform an incomplete serviceStopTime into a dateTime instance, the Content Creator shall use the smallest instant covered by the partial date. E.g., "200904" would be transformed to "2009-04-01T00:00:00Z". The XACML dateTime shall be expressed as UTC using 'Z' as the timezone indicator. The DTM data type allows only for UTC as the timezone, therefore no further transformation is necessary.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:service-stop-time"`
	`  DataType="http://www.w3.org/2001/XMLSchema#dateTime">`
	`    <AttributeValue>2004-12-25T21:20:10Z</AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.12 Source Patient ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.22 as "DocumentEntry.sourcePatientId"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:source-patient-id`
XACML Data Type	`urn:hl7-org:v3#II`

XACML Attribute Value Content	Use CX.4.2 as root and CX.1 as extension. *Note: Use of the sourcePatientId attribute of the DocumentEntry has historically been restricted to "audit and checking" purposes. The attribute contains the original local patient ID at the creating facility. It is unlikely to be meaningful or useful outside of this context. Therefore, policy writers need to take this into account.*

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:source-patient-id"`
	`  DataType="urn:hl7-org:v3#II">`
	`    <AttributeValue>`
	`        <hl7:InstanceIdentifier extension="j98789"`
	`          root="1.2.3.4.343.1"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.13 Type Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.25 as "DocumentEntry.typeCode"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:type-code`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:type-code"`
	`  DataType="urn:hl7-org:v3#CV">`
	`    <AttributeValue>`
	`        <hl7:CodedValue code="57016-8"`
	`          codeSystem="2.16.840.1.113883.6.1"/>`
	`    </AttributeValue>`
	`</Attribute>`

905 **5.6.2.1.5.2.14 Document Unique ID**

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2.26 as "DocumentEntry.uniqueId"
XACML Target Section	resource
XACML Attribute ID	`urn:oasis:names:tc:xacml:1.0:resource:resource-id`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#string`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId=`
	` "urn:oasis:names:tc:xacml:1.0:resource:resource-id"`
	`  DataType="http://www.w3.org/2001/XMLSchema#string">`
	`    <AttributeValue>`
	`        1.2.3.4.5.6.78901.2345.6.7^123456`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.15 Related Folder Unique ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.4.9 as "Folder.uniqueId"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:related-folder:id`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#anyURI`
XACML Attribute Value Content	The Content Creator may include the Folder.uniqueId for each unique folder that it requires to be associated with the document entry, i.e., folders that are associated via the hasMember association and where the folder availabilityStatus is "Approved". Note that this attribute is used to write policies regarding access to document entries. When writing policies regarding access to folders that include the Folder.uniqueId, refer to Section 5.6.2.1.5.3.3.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:related-folder:id"`
	`  DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>`
	`        urn:oid:1.3.6.1.4.1.21367.2005.3.7.3670984664`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.16 Related Folder Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.4.2 as "Folder.codeList"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:document-entry:related-folder:code`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	The Content Creator may include a Folder.codeList entry to characterize a folder that it requires to be currently associated with the document entry, i.e., folders that are associated via the hasMember association and where the folder availabilityStatus is "Approved". Note that this attribute is used to write policies regarding access to document entries. When writing policies regarding access to folders that have a specific Folder.codeList entry, refer to Section 5.6.2.1.5.3.1.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:document-entry:related-folder:code"`
	`  DataType="urn:hl7-org:v3#CV">`
	`    <AttributeValue>`
	`        <hl7:CodedValue code="EMER"`
	`          codeSystem="2.16.840.1.113883.1.11.13955"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.2.17 Resource Type

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.2 as "DocumentEntry"
XACML Target Section	resource

XACML Attribute ID	`urn:ihe:iti:appc:2016:resource-type`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#anyURI`
XACML Attribute Value Content	for document entries the value of the attribute shall be "`urn:ihe:iti:appc:2016:document-entry`"

XACML Example	`<Attribute`
	`  AttributeId="urn:ihe:iti:appc:2016:resource-type"`
	`  DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>`
	`        urn:ihe:iti:appc:2016:document-entry`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.3 Attribute Definitions - Folder Resource

5.6.2.1.5.3.1 Code

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.4.2 as "Folder.codeList"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:folder:code`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute`
	`  AttributeId="urn:ihe:iti:appc:2016:folder:code"`
	`  DataType="urn:hl7-org:v3#CV">`
	`    <AttributeValue>`
	`        <hl7:CodedValue code="EMER"`
	`          codeSystem="2.16.840.1.113883.1.11.13955"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.3.2 Last Update Time

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.4.6 as "Folder.lastUpdateTime"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:folder:last-update-time`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#dateTime`
XACML Attribute Value Content	The Content Creator shall transform the lastUpdateTime into a valid instance of an XML dateTime (which is based on ISO8601). This does not involve adding date or time components, because the last update time is set automatically by the Document Registry. The XACML dateTime shall be expressed as UTC using 'Z' as the timezone indicator. The DTM data type allows only for UTC as the timezone, therefore no further transformation is necessary.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:folder:last-update-time"`
	`  DataType="http://www.w3.org/2001/XMLSchema#dateTime">`
	`    <AttributeValue>2004-12-25T21:20:10Z</AttributeValue>`
	`</Attribute>`

5.6.2.1.5.3.3 Folder UniqueId

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.4.9 as "Folder.uniqueId"
XACML Target Section	Resource
XACML Attribute ID	`urn:oasis:names:tc:xacml:1.0:resource:resource-id`
XACML Data Type	http://www.w3.org/2001/XMLSchema#string
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId=`
	` "urn:oasis:names:tc:xacml:1.0:resource:resource-id"`
	`  DataType="http://www.w3.org/2001/XMLSchema#string">`

	<AttributeValue>
	        1.3.6.1.4.1.21367.2005.3.7.3670984664
	    </AttributeValue>
	</Attribute>

5.6.2.1.5.3.4 Resource Type

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.4 as “Folder”
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:resource-type`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#anyURI`
XACML Attribute Value Content	for folders the value of the attribute shall be "`urn:ihe:iti:appc:2016:folder`"

XACML Example	<Attribute
	  AttributeId="urn:ihe:iti:appc:2016:resource-type"
	  DataType="http://www.w3.org/2001/XMLSchema#anyURI">
	    <AttributeValue>
	        urn:ihe:iti:appc:2016:folder
	    </AttributeValue>
	</Attribute>

5.6.2.1.5.4 Attribute Definitions - SubmissionSet Resource

5.6.2.1.5.4.1 Content Type

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3.4 as "SubmissionSet.contentTypeCode"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:submission-set:content-type`
XACML Data Type	`urn:hl7-org:v3#CV`

XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId=`
	` "urn:ihe:iti:appc:2016:submission-set:content-type"`
	`  DataType="urn:hl7-org:v3#CV">`
	`    <AttributeValue>`
	`        <hl7:CodedValue code="47046-8"`
	`          codeSystem="2.16.840.1.113883.6.1"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.4.2 Intended Recipient Id

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3.7 as "SubmissionSet.intendedRecipient"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:submission-set:intended-recipient:id`
XACML Data Type	`urn:hl7-org:v3#II`
XACML Attribute Value Content	For persons, if XCN.1 is an OID, use XCN.1 as root with no extension. If XCN.1 is not an OID, use XCN.9 as root and XCN.1 as extension. For organizations, if XON.10 is an OID, use XON.10 as a root with no extension. If XON.10 is not an OID, use XON.6.2 as root and XON.10 as extension.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:submission-set:intended-recipient:id"`
	`  DataType="urn:hl7-org:v3#II">`
	`    <AttributeValue>`
	`        <hl7:InstanceIdentifier extension="11375"`
	`          root="2.999.1"/>`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.4.3 Intended Recipient Email

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3.7 as "SubmissionSet.intendedRecipient"

XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:submission-set:intended-recipient:email`
XACML Data Type	`urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name`
XACML Attribute Value Content	For telecommunications, XTN.3 has the value “Internet”. Use the email address in XTN.4 as the value of the attribute.

XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:submission-set:intended-recipient:email"`
	`DataType=`
	` "urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">`
	`    <AttributeValue>`
	`        john.doe@healthcare.example.org`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.4.4 Submission Time

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3.10 as "SubmissionSet.submissionTime"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:submission-set:submission-time`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#dateTime`

XACML Attribute Value Content	The Content Creator shall transform the submissionTime into a valid instance of an XML dateTime (which is based on ISO8601). This may involve adding date or time components, because in IHE Document Sharing metadata, the DTM data type allows for partial dates (see ITI TF-3: Table 4.2.3.1.7-2). To transform an incomplete submissionTime into a dateTime instance, the Content Creator shall use the smallest instant covered by the partial date. E.g., "200904" would be transformed to "2009-04-01T00:00:00Z". The XACML dateTime shall be expressed as UTC using ‚Z‘ as the timezone indicator. The DTM data type allows only for UTC as the timezone, therefore no further transformation is necessary.

XACML Example	`<Attribute AttributeId=`
	` "urn:ihe:iti:appc:2016:submission-set:submission-time"`
	`  DataType="http://www.w3.org/2001/XMLSchema#dateTime">`
	`    <AttributeValue>`
	`        2004-12-25T21:20:10Z`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.4.5 Submission Set Unique ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3.12 as "SubmissionSet.uniqueId"
XACML Target Section	resource
XACML Attribute ID	`urn:oasis:names:tc:xacml:1.0:resource:resource-id`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#string`
XACML Attribute Value Content	No restrictions

XACML Example	`<Attribute AttributeId=`
	` "urn:oasis:names:tc:xacml:1.0:resource:resource-id"`
	`  DataType="http://www.w3.org/2001/XMLSchema#string">`
	`    <AttributeValue>`
	`        1.2.3.4.5`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.5.4.6 Resource Type

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3 as “SubmissionSet”
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:resource-type`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#anyURI`
XACML Attribute Value Content	for submission sets the value of the attribute shall be "`urn:ihe:iti:appc:2016:submission-set`"

XACML Example	`<Attribute`
	`AttributeId="urn:ihe:iti:appc:2016:resource-type"`
	`DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`<AttributeValue>`
	`urn:ihe:iti:appc:2016:submission-set`
	`</AttributeValue>`
	`</Attribute>`

5.6.2.1.6 Attribute Definitions – Action

5.6.2.1.6.1 Action URIs

925 The Content Creator of a Privacy Consent Document shall use the action URIs in the following table when referring to the transactions in IHE Document Sharing profiles. The action URIs are used in attributes with attribute ID `urn:oasis:names:tc:xacml:1.0:action:action-id` and data type `http://www.w3.org/2001/XMLSchema#anyURI`.

Transaction	Action URI
ITI-18 Response	`urn:ihe:iti:2007:RegistryStoredQueryResponse`
ITI-38 Response	`urn:ihe:iti:2007:CrossGatewayQueryResponse`
ITI-39 Response	`urn:ihe:iti:2007:CrossGatewayRetrieveResponse`
ITI-41	`urn:ihe:iti:2007:RegisterDocumentSet-b`
ITI-42	`urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b`
ITI-43 Response	`urn:ihe:iti:2007:RetrieveDocumentSetResponse`
ITI-51 Response	`urn:ihe:iti:2009:MultiPatientStoredQueryResponse`

Transaction	Action URI
ITI-61	`urn:ihe:iti:2010:RegisterOnDemandDocumentEntry`
RAD-69 Response	`urn:ihe:rad:2009:RetrieveImagingDocumentSetResponse`
RAD-75 Response	`urn:ihe:rad:2011:CrossGatewayRetrieveImagingDocumentSetResponse`

930 5.6.2.1.6.2 Additional Action Attribute – Query ID

IHE Document Sharing Metadata Definition	ITI TF-2a: 3.18.4.1.2.3.2 Parameter Query ID
XACML Target Section	action
XACML Attribute ID	`urn:ihe:iti:2016:RegistryStoredQuery:queryId`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#anyURI`
XACML Attribute Value Content	Shall contain one of the stored query IDs defined in ITI TF-2a: 3.18.4.1.2.4 or in ITI TF-2b: 3.51.4.1.2.2.
Attribute ID used in	Attributes with action ID `urn:ihe:iti:2007:RegistryStoredQueryResponse`

XACML Example	`<Attribute`
	`AttributeId="urn:ihe:iti:2016:RegistryStoredQuery:queryId"`
	`  DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`    <AttributeValue>`
	`        urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d`
	`    </AttributeValue>`
	`</Attribute>`

5.6.2.1.6.3 Additional Action Attribute – Return Type

IHE Document Sharing Metadata Definition	3.18.4.1.2.3.1 Parameter returnType
XACML Target Section	action
XACML Attribute ID	`urn:ihe:iti:2016:RegistryStoredQuery:returnType`

XACML Data Type	`http://www.w3.org/2001/XMLSchema#anyURI`
XACML Attribute Value Content	Shall contain either `urn:ihe:iti:xds-b:2016:leaf-class` or `urn:ihe:iti:xds-b:2016:object-ref`
Attribute ID used in	Attributes with action ID `urn:ihe:iti:2007:RegistryStoredQueryResponse`

XACML Example	`<Attribute AttributeId=`
	`"urn:ihe:iti:2016:RegistryStoredQuery:returnType"`
	`DataType="http://www.w3.org/2001/XMLSchema#anyURI">`
	`<AttributeValue>`
	`urn:ihe:iti:xds-b:2016:leaf-class`
	`</AttributeValue>`
	`</Attribute>`

5.6.2.1.7 Attribute Definitions – Environment

No additional constraints.

5.6.2.2 Document Sharing Metadata

When Privacy Consent Documents are shared using IHE Document Sharing profiles, their metadata follows the requirements specified in Section 4.2.3. Only the following attributes have special rules.

5.6.2.2.1 XDS DocumentEntry Metadata

5.6.2.2.1.1 XDSDocumentEntry.typeCode

The LOINC code for these documents is “57016-8” “Privacy Policy Acknowledgement Document” and the codeSystem is 2.16.840.1.113883.6.1.

5.6.2.2.1.2 XDSDocumentEntry.eventCodeList

A Privacy Consent Document can reference previously defined policies. This allows the Patient Privacy Policy Domain to define foundational policies that are applied to specific individuals and situations by the Privacy Consent Document.

The `PolicySetIdReference` or `PolicyIdReference` values not defined in the document shall be used as the code, with a coding scheme defined by the XDS Affinity Domain.

5.6.2.2.1.3 XDSDocumentEntry.formatCode

The XDSDocumentEntry format code for this content shall be `urn:ihe:iti:appc:2016:consent`. The formatCode codeSystem shall be 1.3.6.1.4.1.19376.1.2.3.

5.6.2.2.1.4 XDSDocumentEntry.uniqueId

The Root Policy Set ID in the Privacy Consent Document shall be used as the XDSDocumentEntry.uniqueId.

5.6.2.2.1.5 XDSDocumentEntry.title

The title should reflect the human readable representation in the `/PolicySet/Description` element.

5.6.2.2.1.6 XDSDocumentEntry.serviceStartTime

The serviceStartTime shall be empty or contain the earliest point in time that parts of the Privacy Consent Document are relevant. If the serviceStartTime is empty, it is equivalent to the earliest point in time. The structured policy may contain additional date and time constraints that are not reflected in the serviceStartTime.

5.6.2.2.1.7 XDSDocumentEntry.serviceStopTime

The serviceStopTime shall be empty or contain the latest point in time that parts of the Privacy Consent Document are relevant. If the serviceStopTime is empty, it is equivalent to the latest point in time. The structured policy may contain additional date and time constraints that are not reflected in the serviceStopTime.

5.6.2.2.1.8 XDSDocumentEntry.referenceIdList

A Privacy Consent Document can reference previously defined policies. This allows the Patient Privacy Policy Domain to define foundational policies that are applied to specific individuals and situations by the Privacy Consent Document.

In an XDS Affinity Domain that supports the referenceIdList, `PolicySetIdReference` or `PolicyIdReference` values not defined in the document shall be included in the referenceIdList.

5.6.2.2.2 XDS SubmissionSet Metadata

No additional constraints.

5.6.2.2.3 XDS Folder Metadata

No additional constraints.

Add the underlined section in ITI TF Vol 3: Table 4.2.3.1.7-2:

Data Type	Source Standard	Encoding Specification
CXi	HL7 V2 Identifier	This is an identifier of a reference object, distinct from the use of CX for Patient Identifiers. HL7 Identifier type CX consists of several components. … **urn:ihe:iti:xdw:2013:workflowId** This code shall be used when the identifier is an XDW workflow identifier. The workflow identifier shall be an OID. Only the CXi.1 and CXi.5 component shall be present: For example, if the workflow identifier is “2.16.840.1” the value of referenceIdList attribute is: `2.16.840.1^^^&1.2.3.4&ISO ^urn:ihe:iti:xdw:2013:workflowId` **urn:ihe:iti:appc:2016:policyId** **This code shall be used when the identifier is a privacy policy identifier.** **For example:** **`2.999.1.3.4.5.19812371516^^^^urn:ihe:iti:xds:2016:policyId`**

Volume 3 Namespace Additions

985 *Add the following terms to the IHE Namespace:*

URN	Reference to Description
urn:ihe:iti:appc:2016:author-institution:id	ITI TF-3: 4.2.3.1.4.1 authorInstitution (XON.6/XON.10)
urn:ihe:iti:appc:2016:author-person:id	ITI TF-3: 4.2.3.1.4.2 authorPerson (XCN.1/XCN.9)
urn:ihe:iti:appc:2016:availability-status	ITI TF-3: 4.2.3.2.2 DocumentEntry.availabilityStatus or ITI TF-3: 4.2.3.3.2 SubmissionSet.availabilityStatus or ITI TF-3: 4.2.3.4.1 Folder.availabilityStatus
urn:ihe:iti:appc:2016:community-id	An Object Identifier (OID) which uniquely identifies the community holding the resource in question
urn:ihe:iti:appc:2016:source-system-id	ITI TF-3: 4.2.3.3.9 SubmissionSet.sourceId
urn:ihe:iti:appc:2016:document-entry:class-code	ITI TF-3: 4.2.3.2.3 DocumentEntry.classCode
urn:ihe:iti:appc:2016:confidentiality-code	ITI TF-3: 4.2.3.2.5 DocumentEntry.confidentialityCode
urn:ihe:iti:appc:2016:document-entry:creation-time	ITI TF-3: 4.2.3.2.6 DocumentEntry.creationTime
urn:ihe:iti:appc:2016:document-entry:event-code	ITI TF-3: 4.2.3.2.8 DocumentEntry.eventCodeList
urn:ihe:iti:appc:2016:document-entry:healthcare-facility-type-code	ITI TF-3: 4.2.3.2.11 DocumentEntry.healthcareFacilityTypeCode
urn:ihe:iti:appc:2016:document-entry:legal-authenticator:id	ITI TF-3: 4.2.3.2.14 DocumentEntry.legalAuthenticator
urn:ihe:iti:appc:2016:document-entry:reference-id	ITI TF-3: 4.2.3.2.28 DocumentEntry.referenceIdList
urn:ihe:iti:appc:2016:document-entry:practice-setting-code	ITI TF-3: 4.2.3.2.17 DocumentEntry.practiceSettingCode
urn:ihe:iti:appc:2016:document-entry:service-start-time	ITI TF-3: 4.2.3.2.19 DocumentEntry.serviceStartTime
urn:ihe:iti:appc:2016:document-entry:service-stop-time	ITI TF-3: 4.2.3.2.20 DocumentEntry.serviceStopTime
urn:ihe:iti:appc:2016:document-entry:source-patient-id	ITI TF-3: 4.2.3.2.22 DocumentEntry.sourcePatientId
urn:ihe:iti:appc:2016:document-entry:type-code	ITI TF-3: 4.2.3.2.25 DocumentEntry.typeCode
urn:ihe:iti:appc:2016:document-entry:related-folder:id	ITI TF-3: 4.2.3.4.9 Folder.uniqueId linked to a DocumentEntry through an active association
urn:ihe:iti:appc:2016:document-entry:related-folder:code	ITI TF-3: 4.2.3.4.2 Folder.codeList linked to a DocumentEntry through an active association

URN	Reference to Description
urn:ihe:iti:appc:2016:resource-type	Attribute to distinguish between different types of XACML resource, e.g., DocumentEntry, Folder, SubmissionSet
urn:ihe:iti:appc:2016:folder:code	ITI TF-3: 4.2.3.4.2 Folder.codeList
urn:ihe:iti:appc:2016:folder:last-update-time	ITI TF-3: 4.2.3.4.6 Folder.lastUpdateTime
urn:ihe:iti:appc:2016:submission-set:content-type	ITI TF-3: 4.2.3.3.4 SubmissionSet.contentTypeCode
urn:ihe:iti:appc:2016:submission-set:submission-time	ITI TF-3: 4.2.3.3.10 SubmissionSet.submissionTime
urn:ihe:iti:appc:2016:submission-set:intended-recipient:id	ITI TF-3: 4.2.3.37 SubmissionSet.intendedRecipient (XCN or XON)
urn:ihe:iti:appc:2016:submission-set:intended-recipient:email	ITI TF-3: 4.2.3.37 SubmissionSet.intendedRecipient (XTN)

Profile	Format Code	Media Type	Template ID
Advanced Patient Privacy Consents (APPC)	urn:ihe:iti:appc:2016:consent	text/xml	not applicable

990