Integrating the Healthcare Enterprise

IHE IT Infrastructure Technical Framework Supplement

Advanced Patient Privacy Consent (APPC)

Draft for Public Comment

Date: May 27, 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 V12.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on May 27, 2016 for public comment. Comments are invited and can be submitted at http://www.ihe.net/ITI_Public_Comments. In order to be considered in development of the trial implementation version of the supplement, comments must be received by June 26, 2016.

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 within the constraints of a CDA®[1] document. 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 enforcement mechanism, potentially within an existing access control system, to use the structured policy representation contained within the consent CDA document 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 an Advanced 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®[2]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)?

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

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

APPC-12: The profile doesn't address how to control access to a document based on the metadata or identity of a document it replaced. This restriction also applies to other document associations. E.g., policy writers cannot express a rule where users are allowed to access a document if they were allowed to access the document it replaced. Is this restriction critical to achieve the goals of the profile?

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.

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.

Closed Issues

APPC-1: Do we need to have a 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®[3]-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

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary:

Glossary Term	Definition

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

Advanced Consent Document	A structured document used to express a patient's privacy preference including the structured policy and the document's metadata
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:

Glossary Term	Definition
Patient Privacy Policy	A Patient Privacy Policy further explains appropriate use of data/documents in a way that provides choices to the patient. The policy can have different representations, including a text for legal compliance, a text for easy consumption by patients and a coded representation as a Structured Policy. A Patient Privacy Policy may identify what patient information may be collected, accessed and disclosed and by whom, and how information is governed by the policy (e.g., under what conditions will a document be marked as containing that type of information). The Patient Privacy Policy may be a consent policy, dissent policy, authorization policy, etc. The policy may also describe the patient's rights to specify their consent preferences, complain or request more information as well as the mechanism which allows them to do so.
Patient Privacy Policy Identifier	A Patient Privacy Policy Domain-assigned globally unique identifier that identifies the Patient Privacy Policy.
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 XX

XX 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 if appropriate. This profile enables the capturing of consent(s) that cannot be adequately expressed using the Basic Patient Privacy Consent (BPPC) Profile.

XX.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.

Figure XX.1-1: APPC Actor Diagram

Table XX.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 XX.1-1: APPC Profile - Actors and Content Modules

Actors	Content Modules	Optionality	Reference
Content Creator	Advanced Patient Privacy Consent Content Module	R	ITI TF-3: 5.YY.1
Content Consumer	Advanced Patient Privacy Consent Content Module	R	ITI TF-3: 5.YY.1

XX.1.1 Actor Descriptions and Actor Profile Requirements

See Technical Framework General Introduction Appendix A (Actor Definitions)

XX.2 APPC Actor Options

Options that may be selected for each actor in this profile are listed in Table XX.2-1.

Update the PCC TF-2 reference, once the PCC-CP-211 is moved to final text.

Table XX.2-1: APPC - Actors and Options

Actor	Option Name	Reference
Content Creator	No options defined	--
Content Consumer	View Option (see XX.2.1) Note 1	PCC TF-2: 3.1.1
	Structured Policy Processing Option Note 1	Section XX.2.2

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

XX.2.1 View Option

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

XX.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.

XX.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 XX.5 describes some optional groupings that may be of interest for security considerations and Section XX.6 describes some optional groupings in other related profiles.

Table XX.3-1: APPC - Required Actor Groupings

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

XX.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 an Advanced 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.

XX.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 which include 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 a set of such attributes.

This profile enables attribute-based security at the document level using the Document Sharing metadata. To understand the concept of attribute-based security, it is not important who determines the acceptable values for these attributes. It is important that documents and accessing providers can be thought of as each having 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., is the user authorized to access a specific document) by using a set of access rules that compare attributes to each other or against value constraints.

Different healthcare providers will have different needs to access these documents. For example, administrators may need to be able to access the patient demographics, billing and contact documents. Dietary staff will need access to the dietary documents but would not need access to insurance documents. The patient's assigned doctor will need access to all clinical documents, whereas other providers from the same facility will need access to fewer clinical documents. This is an example of a basic Patient Privacy Policy. It can be expressed as a set of access rules in an attribute-based security system. Please note that so far these concepts contain nothing that is specific to a particular patient – these are general rules.

IHE Document Sharing profiles allow for the publication and use of clinical documents associated with a patient. The APPC Profile allows for a Patient Privacy Policy Domain (e.g., an XDS Affinity Domain) to have a number of Patient Privacy Policies that can be further constrained based on patient's individual choices. BPPC only allows the patient to choose from a limited set of Patient Privacy Policies. This profile allows Patient Privacy Policy Domains to give patients more granular choices by creating access rules that add additional 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 XX.4.2.1) or to a specific episode of care (see Section XX.4.2.2). The patient-specific access rules are transmitted in a structured policy as a part of the consent document.

While the patient's choice could be extremely detailed (e.g., determining which healthcare provider may access which document), it is the Patient Privacy Policy Domain's responsibility to determine the choices available to the patient.

Neither healthcare provider staff members that digitize consent forms, nor patients using a patient 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 levels (e.g., "full access", "summaries only"), and clearly define the ways in which the patient can further make them specific to their 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 choice, the Patient Privacy Policy Domain must take many factors into account: the applicable legal framework, 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.

This profile provides a mechanism by which a Patient Privacy Policy Domain can create a basic vocabulary of codes that identify Patient Privacy Domain managed Privacy Policy Identifiers with respect to document sharing. Each Privacy Policy Identifier uniquely identifies a foundational Privacy Policy. The Privacy Policy should identify in text that complies with the local laws (which may be separate from a "patient-friendly" explanation) what the acceptable use and re-disclosure uses are, which functional roles may access which document, and under which conditions. If used with XDS, the administration of the XDS Affinity Domain will assign all Privacy Policy Identifiers for use within the XDS Affinity Domain.

Along with the text that complies with the local laws, it is assumed that there is 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 Advanced Consent Documents defined in this profile. Combining them is necessary to enable automatic enforcement of the patient's privacy choices. How to combine these different sets of access rules is not in scope for this profile.

It is important to note that Advanced Consent Documents from different Patient Privacy Policy Domains are not mutually intelligible because they will reference different Patient Privacy Policies. An exchange of foundational Patient Privacy Policies using a structured policy format between different Patient Privacy Policy Domains would allow automatic enforcement of Advanced Consent Documents from external sources, but this is not part of the APPC Profile.

XX.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.

XX.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 level that the patient selects for this facility.

XX.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 it.

The XDS affinity domain – acting as the Patient Privacy Policy Domain – has defined three foundational Patient Privacy Policies, which may be referenced in an Advanced Consent Document.

The participants (a hospital and a post-surgical care facility) can exchange data via an HIE using a common patient ID (XAD-PID) and 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 a post-surgical care facility. The hospital uploaded all relevant data regarding the procedure to their HIE. To ensure that the target facility has access to the data, 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 facility. The patient has a choice between three access levels, which are listed on the form: "summaries-only" access, "extensive" access, and "full" access. The patient selects "extensive" 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 it and then selects the access level ("extensive"). The EHR creates an Advanced Consent Document and transmits it to the central XDS Document Repository in the HIE. The HIE extracts the structured and coded policy from the consent document and adjust the access rules for the longitudinal patient record accordingly.

After being discharged from the hospital, the patient visits the post-surgical care facility. The HIE's enforcement mechanism uses the modified access rules 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.

XX.4.2.1.2 Facility-specific Disclosure Process Flow

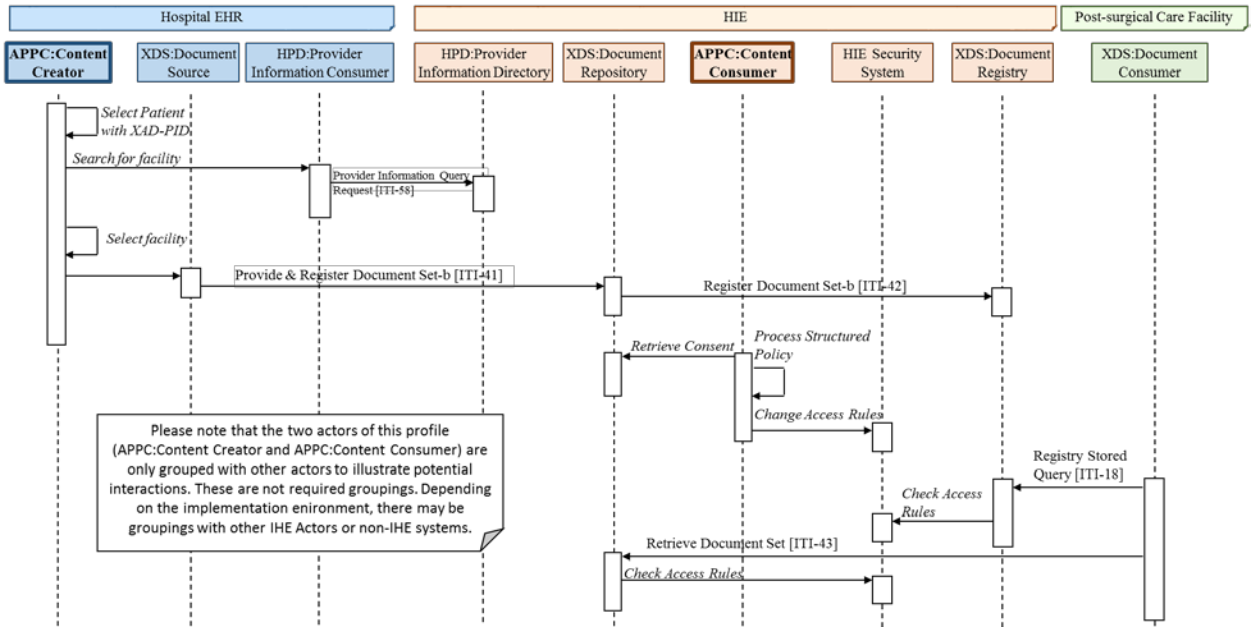

Figure XX.4.2.1.2-1: Facility-specific Disclosure Process Flow in APPC Profile

XX.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.

XX.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 (XAD-PID).

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., including documents regarding the inpatient treatment, psychiatric evaluations, occupational therapy progress notes and intervention plans).

The staff member first selects the patient. She then selects 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 center's system creates an Advanced Consent Document and a XDS Folder representing the episode of care. It sends these objects via its XDS Document Source to the central XDS Document Repository. The HIE's security system (acting as a APPC Content Consumer with the Structured Policy Processing Option) extracts the structured and coded policy representation and sets the access rights for the care team members accordingly.

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 which 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 which has the episode's diagnostic code in its folder codeList.

XX.4.2.2.2 Consent for an Episode of Care Process Flow

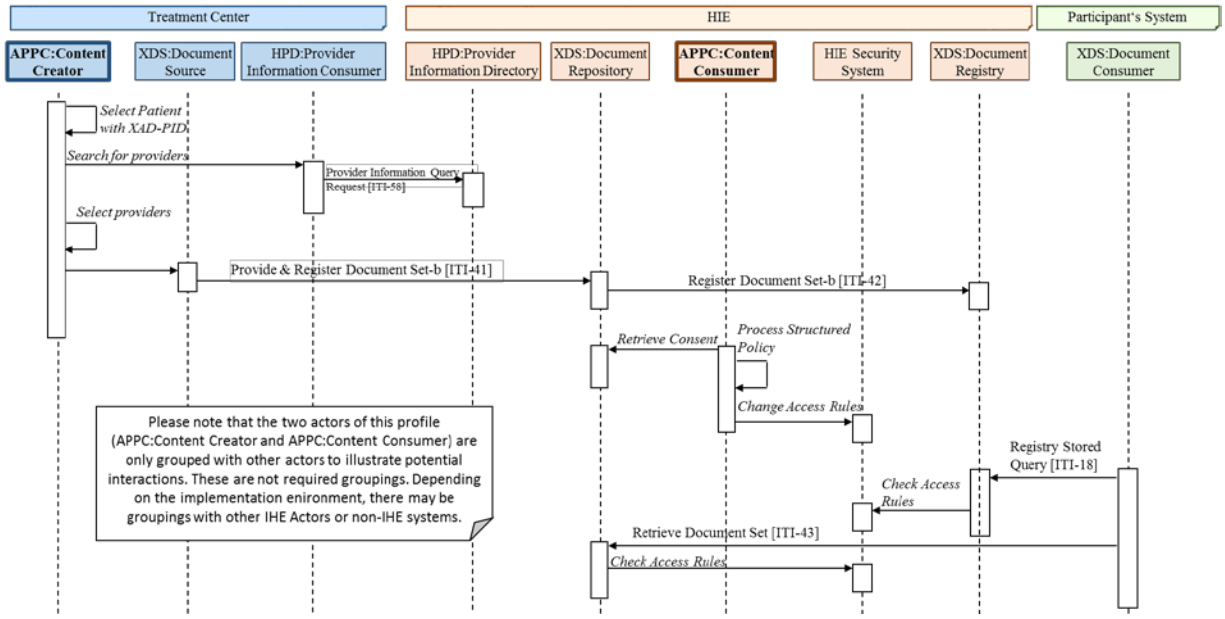

Figure X.4.2.2-1: Consent for an Episode of Care Process Flow in APPC Profile

XX.4.2.3 Use Case #3: Consent to collect from a specific service delivery location

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, including having access to all relevant clinical documents in one place.

XX.4.2.3.1 Consent to collect from a specific service delivery location Use Case Description

Pre-Condition:

This use case takes place in an opt-in XDS affinity domain, where collection of PHI 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.

The clinic has an EMR system that has the capability to transmit clinical documents to an XDS affinity domain either directly or via some other edge protocol.

The clinic and the HIE have agreements in place which allow the exchange of clinical information for purposes that are a superset of those contained 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 an electronic consent form containing the consent information, which he signs before leaving the clinic.

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 can 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.

XX.4.2.3.2 Consent to collect from a specific service delivery location Process Flow

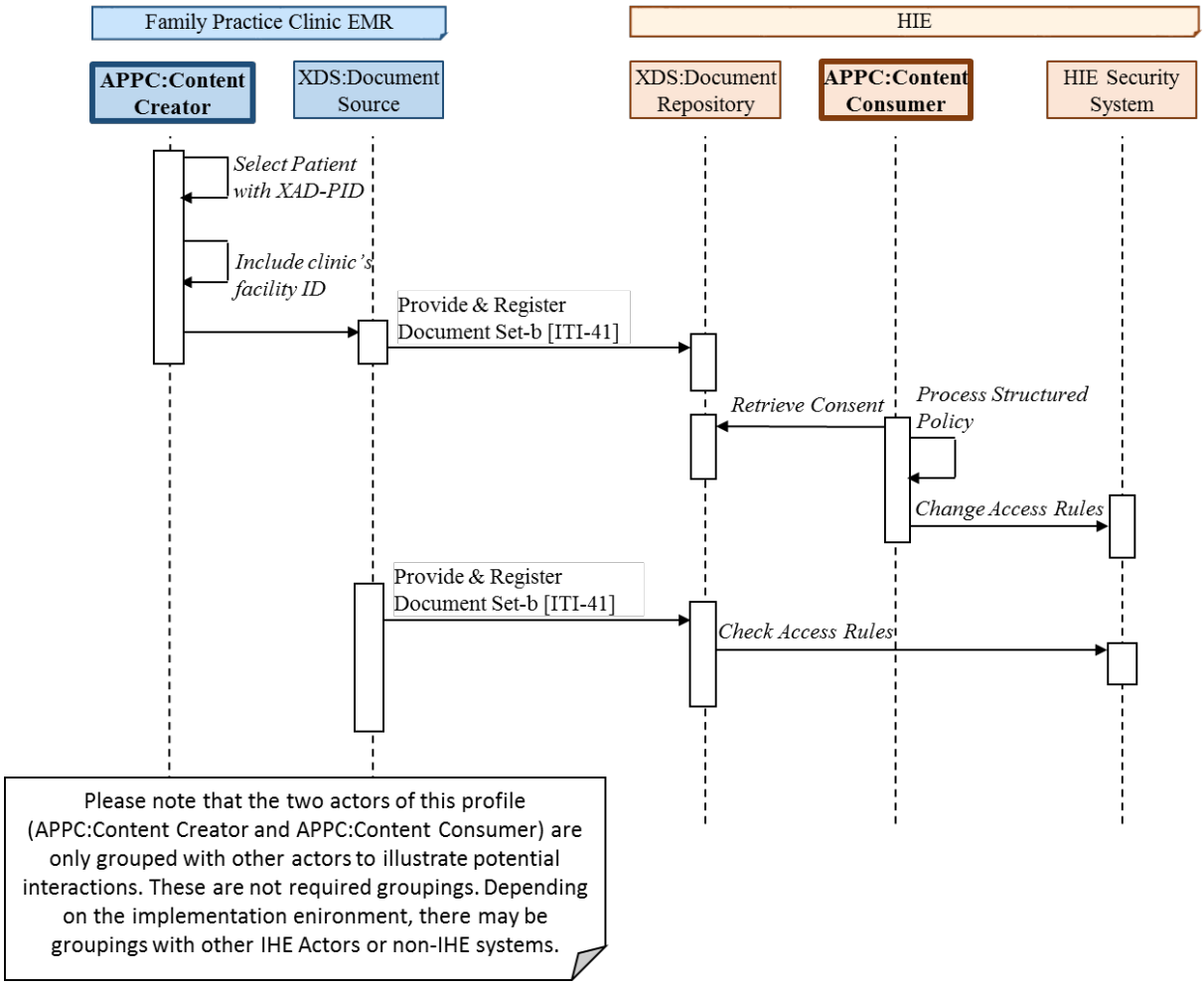

Figure XX.4.2.3-1: Consent to collect from a specific service delivery location Process Flow in APPC Profile

XX.4.2.4 Use Case #4: Withhold consent for information related to a specific order

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.

XX.4.2.4.1 Withhold consent to disclose information related to a specific order Use Case Description

Pre-Condition:

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

The jurisdiction uses an implied consent model for the provision of care.

Main Flow:

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

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

The LIS generates a lab order and a consent document that specifies that the patient wishes to deny access to the order, except for the ordering physician.

At some later point, one of the patient's colleagues decides to snoop into his records and issues a request to list all lab records. 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.

XX.4.2.4.2 Withhold consent for information related to a specific order Process Flow

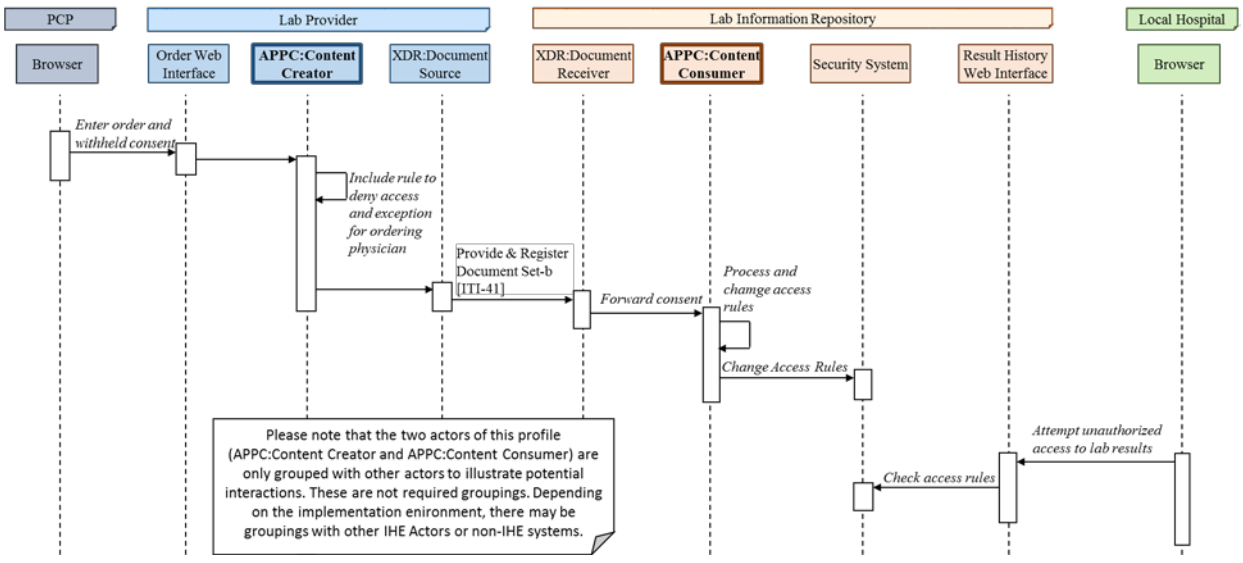

Figure XX.4.2.4.2-1: Withhold consent for information related to a specific order Process Flow in APPC Profile

XX.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.

XX.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.

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 and is beginning his treatment for an STD 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 government service desk to have his records blocked if 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 after verifying its correctness.

At some later point, one of the patient's colleagues decides to snoop into his 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 the consent blocks access 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.

XX.4.2.5.2 Withhold consent to disclose to a specific provider organization Process Flow

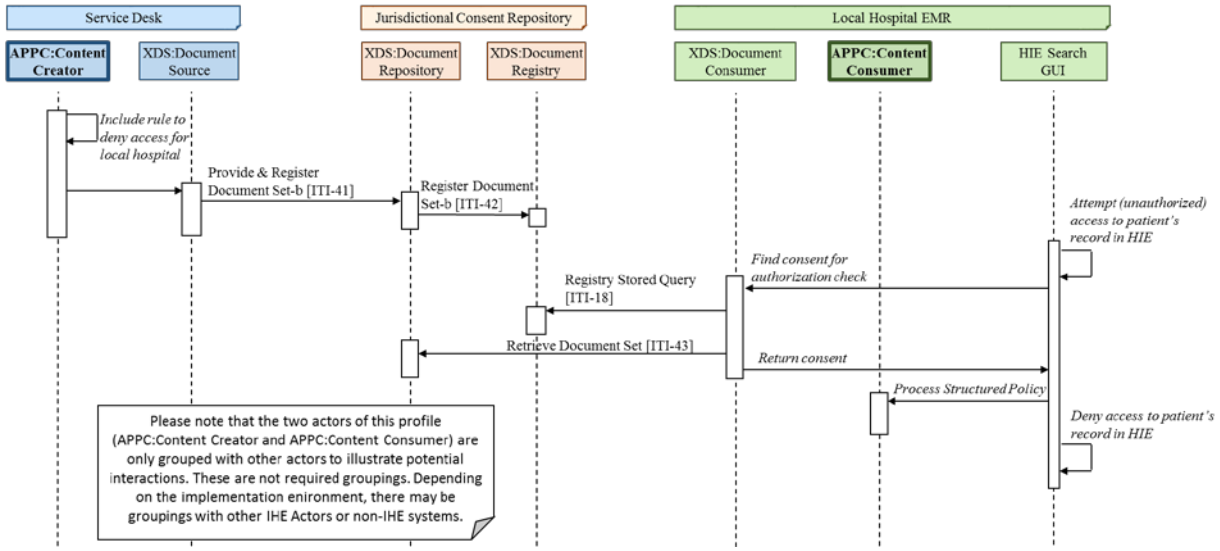

Figure XX.4.2.5.2-1: Withhold consent to disclose to a specific provider organization Process Flow in APPC Profile

XX.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 is disclosed to any healthcare provider.

XX.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 the document would be visible 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 informs the patient of potential risks of hiding information from his healthcare providers. He acknowledges the warning and confirms that the document should be hidden.

The patient portal creates an advanced 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 MHD. 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.

XX.4.2.6.2 Withhold consent to disclose a specific document Process Flow

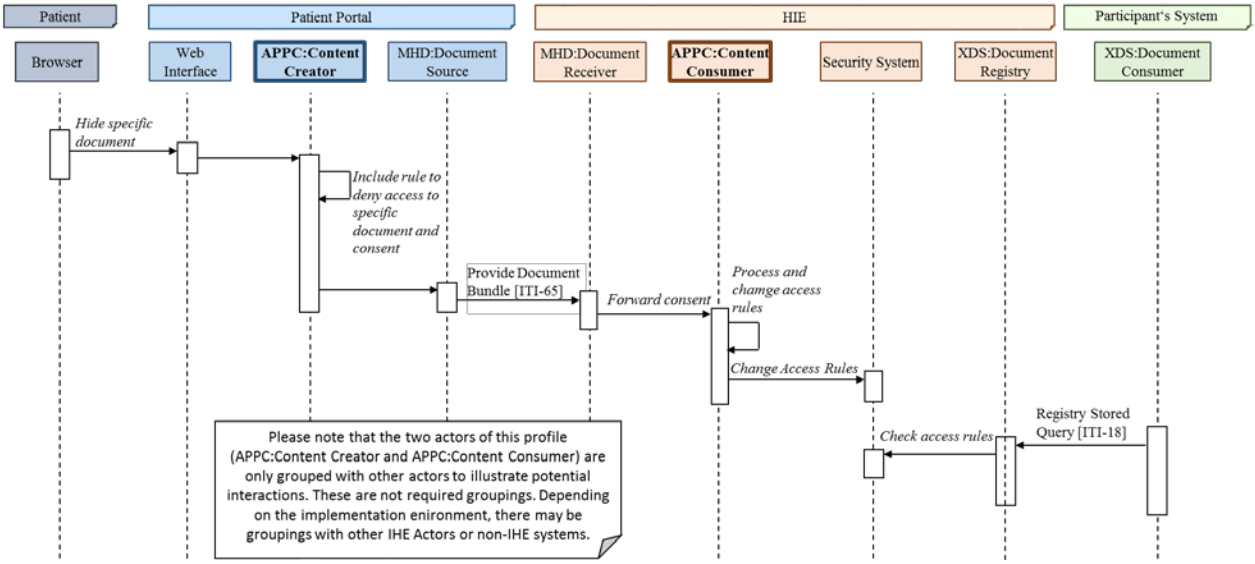

Figure XX.4.2.6.2-1: Withhold consent to disclose to specific document Process Flow in APPC Profile

XX.5 APPC Security Considerations

Consent documents are also governed by privacy policies. The content of an Advanced 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 Advanced Consent Document with family members would potentially inform them of a negative prognosis. Thus the confidentialityCode placed on Advanced Consent Documents must be appropriately assigned (e.g., most will be assigned the broadest use confidentialityCode). Another solution is to include access rules in the Advanced Consent Document that specifically regulate access to the consent document itself.

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. This is for the simple reason that failing to provide access to critical healthcare information (e.g., severe allergies) can be a risk to patient safety. This risk must be balanced against the risk of prosecution or lawsuit due to accidental or malicious disclosure of private information. The Patient Privacy Policy Domain should take care in designing the policies for their access control system to avoid this.

One mitigation strategy that is often adopted in healthcare provides accountability through audit controls. That is to say that the healthcare providers are trusted not to abuse their access to private information, but that this is followed up by a policy of monitoring healthcare provider accesses to private information to ensure that abuse does not occur. This strategy reduces the risk of serious death or injury due to lack of access to critical healthcare information, at the increased risk of disclosure of private information. This is why the ITI Technical Committee created the Audit Trail and Node Authentication (ATNA) Integration Profile, and furthermore, why that profile is a requirement of XDS and related profiles.

A failure to provide access, as well as accidental disclosure, may also be caused by inaccurate document metadata, e.g., mislabeled documents, and by inaccurate advanced 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.

XX.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 Advanced 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 the content profile. ITI TF-3: 5.YY.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.

Appendices

No updates to Volume 1 appendices.

Volume 2 – Transactions

No updates to Volume 2.

Volume 2x – Volume 2 Appendices

Updated ITI Volume 2x as follows.

Appendix P: Privacy Access Policies (Informative)

This Appendix provides information about when consent could be automated and consequently when the BPPC Profile could be used. Privacy consent can be summarized as: "I agree on my personal data being disclosed to someone under specific conditions".

Conditions are based on various factor(s) for example:

- type of person the data is disclosed to;
- type of data disclosed;
- type of access (normal access, emergency access...);
- security level in which the disclosure takes place (weak authentication vs. strong authentication);
- type of purpose for which the data is disclosed;
- timeframe (period of validity of the consent, window of disclosure...);

BPPC could be used when conditions can be described with a limited number of factors and when the factors can be defined and be easily interpreted by a Document Consumer implementing the Basic Patient Privacy Enforcement Option.

The XDS Affinity Domain Privacy Consent Policies could result in various actions, for example:

- limitation of the display of the existence of specific documents to the users of a Document Consumer
- limitation of the access to specific documents by the users of a Document Consumer
- display of a warning note (either concerning this access or to inform that further disclosure is not allowed, limited to some defined population, needed further consent...)
- collection of new consent (oral consent, patient authentication, electronically signed consent, paper consent...)

P.1 Consents in a sensitivity labeled and role based access control environment

One possible implementation may have a collection of policies and sensitivity markers that would form an access control matrix. An example simple access control matrix is shown in the table below.

Table P-1: Sample Access Control Policies

Sensitivity / Functional Role	Billing Information	Administrative Information	Dietary Restrictions	General Clinical Information	Sensitive Clinical Information	Research Information	Mediated by Direct Care Provider
Administrative Staff	X	X					
Dietary Staff		X	X				
General Care Provider		X	X	X			
Direct Care Provider		X	X	X	X		X
Emergency Care Provider		X	X	X	X		X
Researcher						X	
Patient or Legal Representative	X	X	X	X	X		

Each instance of the matrix results in a single Patient Privacy Policy. This vocabulary must then be configured in the XDS Affinity Domain. Thus configuring each application in the XDS Affinity Domain to recognize for each Patient Privacy Policy identified, and which sensitivity (confidentialityCode); what types of accesses are allowed. Using the example above, the Patient Privacy Policy might look like.

Table P-2: Patient Privacy Policies When Expressed by Document Sensitivity

Privacy Consent Policy	Description
Billing Information	May be accessed by administrative staff and the patient or their legal representative.
Administrative Information	May be accessed by administrative or dietary staff or general, direct or emergency care providers, the patient or their legal representative.
Dietary Restrictions	May be accessed by dietary staff, general, direct or emergency care providers, the patient or their legal representative.
General Clinical Information	May be accessed by general, direct or emergency care providers, the patient or their legal representative.
Sensitive Information	May be accessed by direct or emergency care providers, the patient or their legal representative.

Privacy Consent Policy	Description
Research Information	May be accessed by researchers.
Mediated by Direct Care Provider	May be accessed by direct or emergency care providers.

Other divisions of the access control matrix are possible, so long as a Patient Privacy Policy covers each layout of the matrix.

The following list of references is provided as good references to understand the terms and concepts presented here. These references are not required by this profile.

- ISO/TS 21298 "Health informatics – Functional and structural roles".
- ISO/TS 22600 "Health Informatics – Privilege Management and Access Controls".
- CEN prEN 13606-4 "Health informatics — Electronic health record communication — Part 4: Security requirements and distribution rules"

P.2 Possible checklist for implementations

General (before anything else)

- Granularity of confidentiality implementation:
  - Granularity of document: all documents, document type, each document.
  - Granularity of user: all users, user type, each type.
- Depth of confidentiality implementation:
  - Is the existence (metadata) about a document that can't be read by the user shown in a list of available documents for this patient?
  - Is the user informed there are / might be not shown documents and how much?
  - Is there the possibility to manage different depth of confidentiality depending on users or document type?
- How to identify users, documents and policy?
- Does confidentiality management spread through further use (once the document is downloaded by a user)

While implementing

- Definition of default codes depending on site / hardware, document type, author, patient...
- Implementing options:
  - possibility of a list to choose from and how the list is constituted (out of all the possible value, out of the value acknowledged by patient...)

- possibility to change default codes prior to publication
- possibility to use different format depending on the confidentiality policy (only non-downloadable image, pdf, word...)

- Later modification of policy (possible directly when requesting a document or have to be validated before)

Prior to publication

- What elements should be checked before publication:
  - existence of a policy
  - existence of the policy used
  - existence of a consent for that policy
  - What additional information should be given (general consent policy, patient's specific consent policy...?)

Prior to allowing access to a document

- What elements should be checked before publication:
  - accessing user role
  - existence of the policy used vs. accessing user
- Specific accesses and impact on confidentiality policy:
  - emergency (specific policy, short cut of confidentiality policy...)
  - break glass
- What additional information should be given (general consent policy, patient' specific consent policy...)

P.3 Potential obligations

Possible things that the BPPC policies might include are not fully known at this time. The following is a list that has been discovered through use by researchers, health information exchanges, and vendors. The following are some thoughts of things that might be orchestrated by BPPC Policies.

General

1. Is the existence (metadata) about a document that can't be read by the user shown in a list of available documents for this patient
2. Map local role codes into some Affinity Domain defined role codes

Prior to implementation

3. the specific Document Source is configured with one site specific “normal” code to publish all of that Document Source documents against. For example an automatic blood-pressure device being used by one specific patient.
4. prompt user for the code to apply to the document (drop-down-list)
5. document-type based codes

Prior to publication

6. validate that the code to be published against has been acknowledged
7. support for a XDS Affinity Domain Patient Privacy Policy that forbids the publication and/or use of documents in the XDS Affinity Domain (aka Opt-Out).

Prior to allowing access to a document

8. should documents with unrecognized codes be shown?
9. prompt the user with some site defined text "do you really want to do this?"
10. allow the user to review the base consent policy
11. allow the user to review the patient's specific Patient Privacy Policy Acknowledgement Documents
12. allow the user to override a consent block (break-glass)
13. require that a new consent be acquired from the patient before using the documents in the XDS Affinity Domain
14. support for a XDS Affinity Domain Patient Privacy Policy that forbids the publication and/or use of documents in the XDS Affinity Domain (aka Opt-Out).
15. validate that the code on the document has been acknowledged
16. confidentialityCode that would indicate that the Document can only be viewed, it cannot be incorporated or copied.
17. use of this document shall result in an ATNA emergency access audit event

P.4 Dynamic Use Models

It has also been suggested that documents should simply be published with the expected codes, and that only on use of a document that ALL current Patient Privacy Policy Acknowledgements are evaluated against with the code on the document. In this way revocation is more dynamic.

Volume 3 – Content Modules

5 IHE Content Specifications

Add to Section 5 IHE Content Specifications

5.YY Advanced Patient Privacy Consent Content Module

This section defines the Advanced Consent Document.

5.YY.1 References

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

Table 5.YY.1-1: Advanced Patient Privacy Consent - 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 11/29/2004	HL7v3 ADTS

5.YY.2 Advanced Consent Document Specification

5.YY.2.1 Content Specification

The Advanced Consent Document is an XML-encoded plain text document, adhering to the specifications found in [XACML2]. Its purpose is to unambiguously express the level of access granted by the patient to a provider, group of providers or any other participant in a document sharing environment. It specifically focusses on expressing authorizations based on IHE Document Sharing Metadata and transactions, as well as IHE XUA Attributes. 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.

5.YY.2.1.1 Policy Structure

The Advanced Consent Document shall contain exactly one `PolicySet` root element. As defined [XACML2], it may contain other `PolicySet` elements as child elements of the root. The `PolicySet` root element may also contain `Policy` child elements.

The PolicySet root element may contain references to other `PolicySet` or `Policy` elements, using the `PolicySetIdReference` or the `PolicyIdReference` elements. This allows the Patient Privacy Policy Domain to define base policies which are applied to specific individuals and situations by the Advanced Consent Document. E.g., a referenced base policy defines what kind

of access a healthcare provider receives and is applied to one specific provider, patient and purpose of use by the Advanced Consent Document.

5.YY.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 Advanced Consent Document. It may hold information on who signed the consent form, when it was signed and a person or organization responsible for this document.

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

Additionally, Content Creators may include a human readable representation of the Advanced Consent Document in a separate document. The document may be a BPPC consent acknowledgment document, a PDF (e.g., following the XDS-SD Profile), 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 transformation of the original Advanced Consent Document using the XFRM association.

When linking a BPPC consent acknowledgment document to an Advanced Consent Document, the PolicySetId of the PolicySet root element shall be included in the BPPC document's eventCodeList.

5.YY.2.1.1.2 Example Document

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet PolicySetId="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.YY.2.1.2 Data Types

The Advanced Consent Document relies on data types derived from HL7v3 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].

Coded Values Data Type

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

Specification:

The data type is based on the HL7v3 "Coded Value" data type (see [HL7ADTS] section 2.9). 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`, but these may be safely ignored.

Example:

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

Instance Identifier Data Type

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

The data type is based on the HL7v3 "Instance Identifier" data type (see [HL7ADTS] section 2.17). 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`, but these may be safely ignored.

Example:

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

5.YY.2.1.3 Functions

The use of HL7v3-derived data types in Advanced 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` a) if and only 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 b) if and only if 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.YY.2.1.4 Attribute Definitions – Subject

5.YY.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.YY.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>`

945 **5.YY.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.YY.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.YY.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:2.0:subject:npi`
SAML Example	`<saml:Attribute Name="urn:oasis:names:tc:xspa:2.0:subject:npi"> <saml:AttributeValue>1234567890</saml:AttributeValue> </saml:Attribute>`
XACML Target Section	subject
XACML Attribute ID	`urn:oasis:names:tc:xspa:2.0: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:2.0:subject:npi"`
	`DataType="urn:hl7-org:v3#II">`
	`<AttributeValue>`
	`<hl7:InstanceIdentifier extension="1234567890"`
	`root="2.16.840.1.113883.4.6" />`
	`</AttributeValue>`
	`</Attribute>`

5.YY.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	

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.YY.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	
XACML Example	<Attribute AttributeId= "urn:oasis:names:tc:xspa:1.0:subject:purposeofuse" DataType="urn:hl7-org:v3#CV"> <AttributeValue> <hl7:CodedValue code="1" codeSystem="1.0.14265.1" /> </AttributeValue> </Attribute>

5.YY.2.1.5 Attribute Definitions – Resources

5.YY.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 two or more of the following: DocumentEntries, Folders, and SubmissionSets.

5.YY.2.1.5.1.1 Author Institution Name

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.1 as "authorInstitution"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:author-institution:name`
XACML Data Type	`http://www.w3.org/2001/XMLSchema#string`
XACML Attribute Value Content	Use XON.1 of the authorInstitution
Attribute ID used in	DocumentEntry, SubmissionSet

XACML Example	`<Attribute AttributeId=`
	`  "urn:ihe:iti:appc:2016:author-institution:name"`
	`  DataType="http://www.w3.org/2001/XMLSchema#string">`
	`  <AttributeValue>NY Mercy Hospital</AttributeValue>`
	`</Attribute>`

5.YY.2.1.5.1.2 Author Institution ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.1 as "authorInstitution"
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	Use XON.6.2 as root and XON.10 as extension or (if XON.10 is an OID) use XON.10 as root
Attribute ID used in	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.YY.2.1.5.1.3 Author Person ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.2 as "authorPerson"
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	Use XCN.9 as root and XCN.1 as extension or (if XCN.1 is an OID) use XCN.1 as root
Attribute ID used in	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.YY.2.1.5.1.4 Author Role

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.3 as "authorRole"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:author-role`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	Use CX.4.2 as codeSystem and CX.1 as extension; if it is not coded as a CX data type, a local codeSystem shall be defined for the affinity domain
Attribute ID used in	DocumentEntry, SubmissionSet
XACML Example	`<Attribute AttributeId="urn:ihe:iti:appc:2016:author-role" DataType="urn:hl7-org:v3#CV"> <AttributeValue> <hl7:CodedValue code="PCP" codeSystem="2.16.840.1.113883.19.9"/> </AttributeValue> </Attribute>`

5.YY.2.1.5.1.5 Author Specialty

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.4 as "authorSpecialty"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:author-speciality`
XACML Data Type	`urn:hl7-org:v3#CV`
XACML Attribute Value Content	Use CX.4.2 as codeSystem and CX.1 as extension; if it is not coded as a CX data type, a local codeSystem shall be defined for the affinity domain

Attribute ID used in	DocumentEntry, SubmissionSet

XACML Example	`<Attribute`
	`  AttributeId="urn:ihe:iti:appc:2016:author-speciality"`
	`  DataType="urn:hl7-org:v3#CV">`
	`  <AttributeValue>`
	`  <hl7:CodedValue code="Cardiology"`
	`  codeSystem="2.16.840.1.113883.19.10"/>`
	`  </AttributeValue>`
	`</Attribute>`

960 **5.YY.2.1.5.1.6 Author Telecommunication**

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.1.4.4 as "authorTelecommunication"
XACML Target Section	resource
XACML Attribute ID	`urn:ihe:iti:appc:2016:author-telecommunication`
XACML Data Type	`urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name`
XACML Attribute Value Content	If XTN.3 has the value “Internet”, use the email address in XTN.4 as the value of the attribute
Attribute ID used in	DocumentEntry, SubmissionSet

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

5.YY.2.1.5.1.7 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 defined by an extension or by a new profile
Attribute ID used in	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.YY.2.1.5.1.8 Community ID

IHE Document Sharing Metadata Definition	An Object Identifier (OID) which 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, 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)
Attribute ID used in	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.YY.2.1.5.1.9 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 as root and CX.1 as extension
Attribute ID used in	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.YY.2.1.5.1.10 Source System ID

IHE Document Sharing Metadata Definition	ITI TF-3: 4.2.3.3.9 as "SubmissionSet.sourceId"
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 (i.e., the DocumentEntry, Folder, or SubmissionSet)
Attribute ID used in	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>`

965 **5.YY.2.1.5.2 Attribute Definitions – DocumentEntry Resource**

5.YY.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	
Attribute ID used in	DocumentEntry

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.YY.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	
Attribute ID used in	DocumentEntry

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.YY.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	This point in time shall be transformed 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 incomplete creationDates into dateTime instances the implementor 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 also allows only for UTC as the timezone, therefore no transformation is necessary.
Attribute ID used in	DocumentEntry

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.YY.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	
Attribute ID used in	DocumentEntry

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>

970 **5.YY.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	
Attribute ID used in	DocumentEntry
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.YY.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	Use XCN.9 as root and XCN.1 as extension or (if XCN.1 is an OID) use XCN.1 as root
Attribute ID used in	DocumentEntry
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.YY.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	
Attribute ID used in	DocumentEntry
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.YY.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)
Attribute ID used in	DocumentEntry

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.YY.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-list`
XACML Data Type	`urn:hl7-org:v3#II`
XACML Attribute Value Content	Use CXi.4 as root and CXi.1 as extension or (if CXi.1 is an OID) use CXi.1 as root; CXi.5 is not used
Attribute ID used in	DocumentEntry

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>`

975 **5.YY.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	This point in time shall be transformed 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 incomplete serviceStartTimes into dateTime instances the implementor 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 also allows only for UTC as the timezone, therefore no transformation is necessary.
Attribute ID used in	DocumentEntry

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.YY.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	This point in time shall be transformed 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 incomplete serviceStartTimes into dateTime instances the implementor 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 also allows only for UTC as the timezone, therefore no transformation is necessary.
Attribute ID used in	DocumentEntry

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.YY.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 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.*
Attribute ID used in	DocumentEntry

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.YY.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	
Attribute ID used in	DocumentEntry

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>`

5.YY.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	
Attribute ID used in	DocumentEntry

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>`

980 **5.YY.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	There shall be one attribute containing the Folder.uniqueId for each unique folder 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 they are entered into the context as attributes of the document entry.
Attribute ID used in	DocumentEntry

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.YY.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	There shall be one attribute for each unique Folder.codeList entry for each folder 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 they are entered into the context as attributes of the document entry.
Attribute ID used in	DocumentEntry

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.YY.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`"
Attribute ID used in	DocumentEntry, Folder, SubmissionSet

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.YY.2.1.5.3 Attribute Definitions - Folder Resource

5.YY.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	
Attribute ID used in	Folder

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>`

985 **5.YY.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	This point in time shall be transformed 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 document sharing metadata DTM data type also allows only for UTC as the timezone, therefore no transformation is necessary.
Attribute ID used in	Folder

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.YY.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	
Attribute ID used in	DocumentEntry, Folder, SubmissionSet

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.YY.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"
Attribute ID used in	DocumentEntry, Folder, SubmissionSet

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.YY.2.1.5.4 Attribute Definitions - SubmissionSet Resource

990 #### 5.YY.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	
Attribute ID used in	SubmissionSet

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.YY.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, use XCN.9 as root and XCN.1 as extension or (if XCN.1 is an OID) use XCN.1 as root For organizations, use XON.6.2 as root and XON.10 as extension or (if XON.10 is an OID) use XON.10 as root
Attribute ID used in	SubmissionSet

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.YY.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	If XTN.3 has the value “Internet”, use the email address in XTN.4 as the value of the attribute

Attribute ID used in	SubmissionSet

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.YY.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	
XACML Attribute Value Content	This point in time shall be transformed 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 incomplete submissionTimes into dateTime instances the implementor 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 also allows only for UTC as the timezone, therefore no transformation is necessary.
Attribute ID used in	SubmissionSet

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.YY.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	
Attribute ID used in	DocumentEntry, Folder, SubmissionSet
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>`

995 **5.YY.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`"
Attribute ID used in	DocumentEntry, Folder, SubmissionSet

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.YY.2.1.6 Attribute Definitions – Action

5.YY.2.1.6.1 Action URIs

The Content Creator of an Advanced 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-41	`urn:ihe:iti:2007:RegisterDocumentSet-b`
ITI-42	`urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b`
ITI-43 Response	`urn:ihe:iti:2007:RetrieveDocumentSetResponse`

5.YY.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

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.YY.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.YY.2.1.7 Attribute Definitions – Environment

No additional constraints.

5.YY.2.2 Document Sharing Metadata

When Advanced 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.YY.2.2.1 XDS DocumentEntry Metadata

5.YY.2.2.1.1 XDSDocumentEntry.classCode

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.YY.2.2.1.2 XDSDocumentEntry.eventCodeList

An Advanced Consent Document can reference previously defined policies using the PolicySetIdReference or the PolicyIdReference elements. This allows the Patient Privacy Policy Domain to define base policies which are applied to specific individuals and situations by the Advanced Consent Document. The referenced PolicyId or PolicySetId shall be used as the code, with a coding scheme defined by the Affinity Domain, unless the referenced element is defined in the same document.

5.YY.2.2.1.2 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.YY.2.2.1.4 XDSDocumentEntry.uniqueId

The PolicySetId of the root PolicySet in the Advanced Consent Document shall be used as the XDSDocumentEntry unique ID.

5.YY.2.2.2 XDS SubmissionSet Metadata

No additional constraints.

5.YY.2.2.3 XDS Folder Metadata

No additional constraints.

Volume 3 Namespace Additions

Add the following terms to the IHE Namespace:

URN	Reference to Description
urn:ihe:iti:appc:2016:author-institution:name	ITI TF-3: 4.2.3.1.4.1 authorInstitution (XON.1)
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:author-role	ITI TF-3: 4.2.3.1.4.3 authorRole
urn:ihe:iti:appc:2016:author-speciality	ITI TF-3: 4.2.3.1.4.4 authorSpecialty
urn:ihe:iti:appc:2016:author-telecommunication	ITI TF-3: 4.2.3.1.4.4 authorTelecommunication
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-list	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	Reference to Description
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: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 Consent (APPC)	urn:ihe:iti:appc:2016:consent	text/xml	not applicable

1040

