**ACC, HIMSS and RSNA**

**Integrating the Healthcare Enterprise**

# IHE Patient Care Coordination Technical Framework

# Supplement 2005-2006

# Basic Patient Privacy Consents (BPPC)

## Trial Implementation Version

**Draft Date: August 10, 2006**

# 1 Foreword

Integrating the Healthcare Enterprise (IHE) is an initiative designed to stimulate the integration of the information systems that support modern healthcare institutions. Its fundamental objective is to ensure that in the care of patients all required information for medical decisions is both correct and available to healthcare professionals. The IHE initiative is both a process and a forum for encouraging integration efforts. It defines a technical framework for the implementation of established messaging standards to achieve specific clinical goals. It includes a rigorous testing process for the implementation of this framework. And it organizes educational sessions and exhibits at major meetings of medical professionals to demonstrate the benefits of this framework and encourage its adoption by industry and users.

The approach employed in the IHE initiative is not to define new integration standards, but rather to support the use of existing standards, HL7, DICOM, IETF, and others, as appropriate in their respective domains in an integrated manner, defining configuration choices when necessary. IHE maintain formal relationships with several standards bodies including HL7, DICOM and refers recommendations to them when clarifications or extensions to existing standards are necessary.

This initiative has numerous sponsors and supporting organizations in different medical specialty domains and geographical regions. In North America the primary sponsors are the American College of Cardiology (ACC), the Healthcare Information and Management Systems Society (HIMSS) and the Radiological Society of North America (RSNA). IHE Canada has also been formed. IHE Europe (IHE-EUR) is supported by a large coalition of organizations including the European Association of Radiology (EAR) and European Congress of Radiologists (ECR), the Coordination Committee of the Radiological and Electromedical Industries (COCIR), Deutsche Röntgengesellschaft (DRG), the EuroPACS Association, Groupement pour la Modernisation du Système d'Information Hospitalier (GMSIH), Société Francaise de Radiologie (SFR), Società Italiana di Radiologia Medica (SIRM), the European Institute for health Records (EuroRec), and the European Society of Cardiology (ESC). In Japan IHE-J is sponsored by the Ministry of Economy, Trade, and Industry (METI); the Ministry of Health, Labor, and Welfare; and MEDIS-DC; cooperating organizations include the Japan Industries Association of Radiological Systems (JIRA), the Japan Association of Healthcare Information Systems Industry (JAHIS), Japan Radiological Society (JRS), Japan Society of Radiological Technology (JSRT), and the Japan Association of Medical Informatics (JAMI). Other organizations representing healthcare professionals are invited to join in the expansion of the IHE process across disciplinary and geographic boundaries.

The IHE Technical Frameworks for the various domains (IT Infrastructure, Cardiology, Laboratory, Radiology, etc.) defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of medical information to support optimal patient care. It is expanded annually, after a period of public review, and maintained regularly through the identification and correction of errata. The current version for these Technical Frameworks may be found at www.ihe.net/Technical_Framework.

The IHE Technical Framework identifies a subset of the functional components of the healthcare enterprise, called IHE Actors, and specifies their interactions in terms of a set of coordinated, standards-based transactions. It describes this body of transactions in progressively greater depth. The volume I provides a high-level view of IHE functionality, showing the transactions organized into functional units called Integration Profiles that highlight their capacity to address specific clinical needs. The subsequent volumes provide detailed technical descriptions of each IHE transaction.

Date: August 10, 2006

Author: Keith W. Boone, John Moehrke, Lori Fourquet, Robert Horn

These”boxed” instructions for the author to indicate to the Volume Editor how to integrate the relevant section(s) into the overall Technical Framework

# Volume I – Integration Profiles

## 1 Introduction

The **Basic Patient Privacy Consents (BPPC)** profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use.

### 1.1 Open Issues and Questions

### 1.2 Closed Issues

1. *Not clear how we handle the case where a patient changes their mind on a consent. How does this affect the documents that are already published, already consumed by other enterprises in the Affinity Domain under the previous consent? The proposal is to handle all of these issues as manually.*
2. *This method does not try to communicate the meaning of the patient consent. This is expected to be a safe thing to communicate through manual configurations.*
3. *This profile does not mandate the use of digital signatures on all privacy consents. The consent is no more sensitive than other sensitive documents in XDS.*
4. *It is not clear how we handle the BPPC profile with the XDM/XDR profile. It is informative to publish the consents, but the consumption of the documents is harder to control given that the ultimate recipient may not be in the same Affinity Domain. We suggest that the importer in these cases needs to deal with this factor, but the fact that the same data is available to a browser negates any controls that might be enforceable by the importer actor.*
5. *We do not have a normative way to publish the XDS Affinity Domain – Patient Privacy Consent documents. We suggest that ITI produce a way to publish non-patient specific documents.*

## Profile Abstract

The XDS profile provides little guidance on supporting privacy policies within an affinity Domain. Documents can be marked with a confidentialityCode, but no information has been provided on how to use this information to support patient privacy concerns. This profile corrects that deficiency by describing a mechanism whereby an Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. EHR systems).

There are three key parts of the profile:

1. The profile provides a content module for capturing a patient consent to a privacy policy or policies.
2. The profile describes how the confidentialityCode attribute of the XDSDocumentEntry metadata is used to support the consent policies.
3. Finally it describes the method by which XDS Consumer Actors can enforce the privacy policies determined by the document confidentialityCode and the patient privacy consents.

# 2 Changes to Sections

## GLOSSARY

**Functional Role –** Role an individual is acting under when they are executing a function. See ISO 21298

**Structural Role** – Role of an individual within an organization. See ISO 21298

**Wet Signature** – Ink on paper signature.

**Affinity Domain Policy –** Affinity Domain Policy that clearly defines the appropriate uses of the XDS Affinity Domain. Within this policy is a defined set of acceptable use Privacy Consent Policies that are published and understood.

**Privacy Consent Policy –** One of the acceptable-use Privacy Consent Policies that are agreed to and understood in the Affinity Domain.

**Privacy Consent Policy Identifier** – An Affinity Domain assigned identifier (OID) that uniquely identifies the Affinity Domain – Privacy Consent Policy. There is one unique identifier (OID) for each Privacy Consent Policy within the Affinity Domain.

**Patient Privacy Consent –** The act of a patient consenting to a specific Privacy Consent Policy.

**Patient Privacy Consent Document** – A document that follows the BPPC profile and captures the act of the patient consenting to a specific XDS Affinity Domain defined Privacy Consent Policy.

**Privacy Consent Policy Act Identifier** – An Affinity Domain assigned identifier that uniquely defines the act of a patient consenting to a specific Affinity Domain – Privacy Consent Policy.

## 2.4 History of Annual Changes

Add the following bullet to the end of the bullet list in section 2.4

- Added the **Basic Patient Privacy Consents (BPPC)** profile that enables XDS Affinity Domains to be more flexible in the privacy policies that they support.

## 2.5 Patient Care Coordination Integration Profiles

IHE Integration Profiles offer a common language that healthcare professionals and vendors can use to discuss integration needs of healthcare enterprises and the integration capabilities of information systems in precise terms. Integration Profiles specify implementations of standards that are designed to meet identified clinical needs. They enable users and vendors to state which IHE capabilities they require or provide, by reference to the detailed specifications of the IHE Patient Care Coordination Technical Framework.

Integration profiles are defined in terms of IHE Actors, transactions and their content. Actors (listed in PCC TF-1: Appendix A) are information systems or components of information systems that produce, manage, or act on information associated with clinical and operational activities. Transactions (listed in PCC TF-1: Appendix B) are interactions between actors that communicate the required information through standards-based messages. Content is what is exchanged in these transactions, and are defined by Content Profiles.

Vendor products support an Integration Profile by implementing the appropriate actor(s) and transactions. A given product may implement more than one actor and more than one integration profile.

Content Profiles define how the content used in a transaction is structured. Each transaction is viewed as having two components, a payload, which is the bulk of the information being carried, and metadata that describes that payload. The binding of the Content to an IHE transaction specifies how this payload influences the metadata of the transaction. Content modules within the Content Profile then define the payloads. Content modules are transaction neutral, in that what they describe is independent of the transaction in which they are used, whereas content bindings explain how the payload influences the transaction metadata.

Figure 2.5-1 shows the relations between the Content Integration Profiles of the Patient Care Coordination Domain.

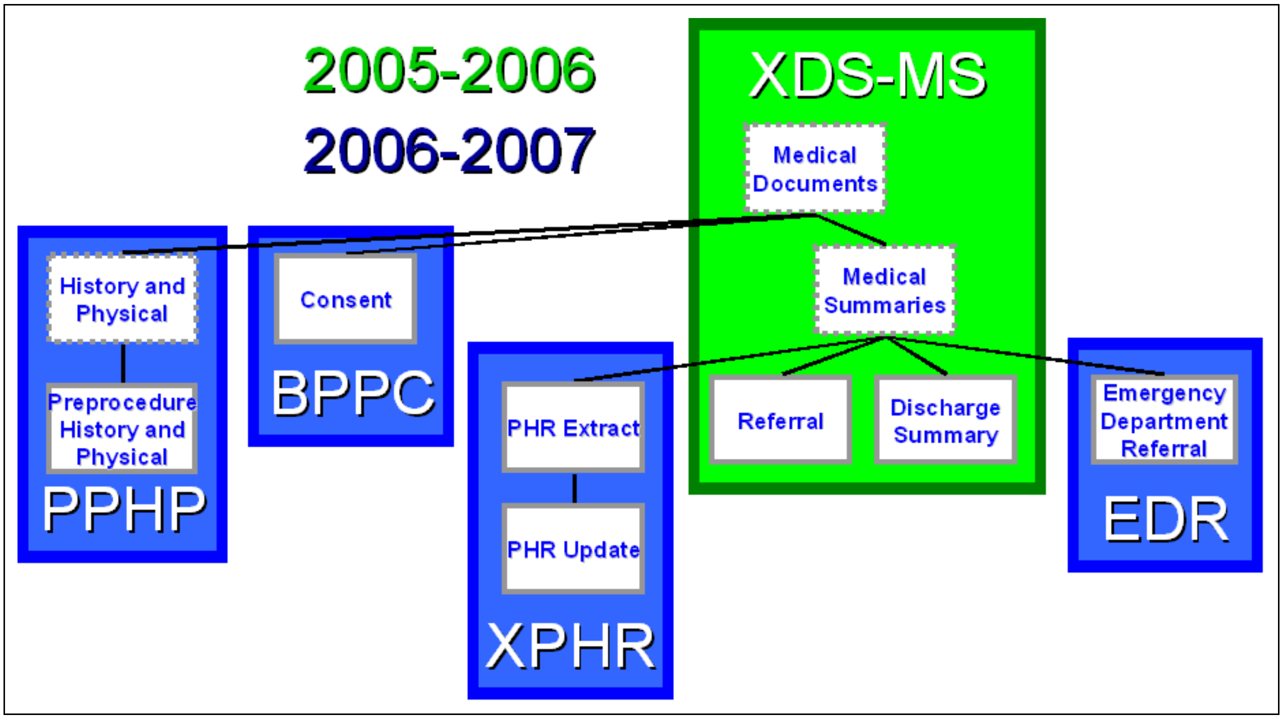


Figure 2.5-1 IHE Patient Care Coordination Content Integration Profiles

## 2.6 BPPC Integration Profile Dependencies

***Add the following section to Table 2-1 Integration Profiles Dependencies in section 2.1***

| Integration Profile | Depends on | Dependency Type | Purpose |
|---|---|---|---|
| Basic Patient Privacy Consents<br>(BPPC) | Cross Enterprise Document Sharing<br>(XDS)<br>ITI TF-1:10 | An Actor using the BPPC profile must conform to the rules of the Medical Document [PCC TF:2-4.1] to XDS Binding. | Ensures that the metadata for each shared document contains appropriate confidentially codes indicating the desired confidentiality of the document, and that the patient consent act is available to the consumer of the document. |
| | Cross Enterprise Document Media Interchange<br>(XDM)<br>ITI TF-1:16 | An Actor using the BPPC profile must conform to the rules of the Medical Document [PCC TF:2-4.1] to XDM Binding. | |
| | Cross Enterprise Document Reliable Interchange<br>(XDR)<br>ITI TF-1:15 | An Actor using the BPPC profile must conform to the rules of the Medical Document [PCC TF:2-4.1] to XDR Binding. | |
| | XDS Scanned Documents<br>(XDS-SD)<br>ITI TF-1: ? | Document Sources publishing Consent documents must use the XDS-SD profile when creating documents containing scanned images of "wet" signatures. | When the patient uses wet signatures (ink on paper), XDS-SD is used to capture the actual copy of the consent that the patient signed. |
| | Document Digital Signature<br>(DSG)<br>ITI TF-1: ? | Document Sources publishing Consent documents must digitally sign the consent document. | To ensure that the consent act is appropriately witnessed or authorized by the patient or legal guardian. |

### 2.6.1 XDS/XDR Option Requirements of the BPPC Profile

Table 2.6-2.6-1 lists the XDS and XDR options that shall be supported by Document Registry, Document Sources and Document Consumers Actors in the BPPC profile.

| Actor | Options | Vol & Section |
|---|---|---|
| Document Source | *Privacy Option* | ITI TF-2:3.15.4.1.1 |
| Document Consumer | *Privacy Option* | ITI TF-2: 3.17.4.1.1.1<br>ITI TF-2: 3.18.4.1.1.1 |
| Document Registry | *Privacy Option* | ITI TF-2: 3.14.4.1.1.1<br>ITI TF-2:3.18.4.1.1.1 |
| Document Repository | *(none)* | |

**Table 2.6-2.6-1 XDS Option Requirements**

### 2.6.2 XDM Option Requirements of the BPPC Profile

Table 2.6-2.6-1 lists the XDM options that shall be supported by XDM Actors in the BPPC profile.

| Actor | Options | Vol & Section |
|---|---|---|
| Portable Media Creator | *Privacy Option* | ITI TF-2: 3.32.4.1.1.1 |
| Portable Media Importer | *Privacy Option* | ITI TF-2: 3.32.4.1.1.1 |

**Table 2.6-2.6-2 XDM Option Requirements**

***Add the following section to section 2.7***

## 2.7 Integration Profiles Overview

### 2.7.4 Basic Patient Privacy Consents (BPPC)

This Supplement provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use.

***The section shall be added to Vol 1***

# 3 BPPC Integration Profile

The document sharing infrastructure provided by XD* [1]allow for the publication and use of clinical documents associated with a patient. The XDS/XDR system requires that the Affinity Domain create and agree to a single policy (See IHE-ITI Vol 1:Appendix L). The Affinity Domain Policy is enforced in a distributed way through the inherent access controls of the systems involved in the Affinity Domain. This profile will use terms consistent with ISO 22600 - Privilege Management and Access Control (PMAC), but is not restricted to systems that implement PMAC. The systems involved in XDS are expected to support sufficient Access Controls to carry out the Policy of the Affinity Domain.

Today this single Affinity Domain Policy restriction means that much of the useful data is not entered into the XDS, or that the access to this data is too liberally allowed. This profile allows for the Affinity domain to have a small number of privacy consents. This allows for more flexibility to support some patient concerns, while providing an important and useful dataset to the healthcare provider.

Healthcare providers utilize many different sets of data to carry out treatment, billing, and normal operations. This information may include patient demographics, contacts, insurance information, dietary requirements, general clinical information and sensitive clinical information. This information may be published to XDS as independent documents under different privacy consent policies.

Healthcare providers in different functional roles 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.  General care providers will want access to most clinical documents, and direct care providers should have access to all clinical documents.

This profile provides a mechanism by which an affinity domain can create a basic vocabulary of codes that identify affinity domain privacy consent policies with respect to information sharing.  Each privacy consent policy should identify in legal text what are the acceptable re-disclosure uses, which functional roles may access a document and under which conditions. Each privacy consent will be assigned a unique XDS Affinity Domain wide OID by the administration of the XDS Affinity Domain with care to respect any inheritance of previous privacy consent policies. Future profiles may include structured and coded language that can be used to support dynamic understanding of the patient’s directives (see HL7 and OASIS).

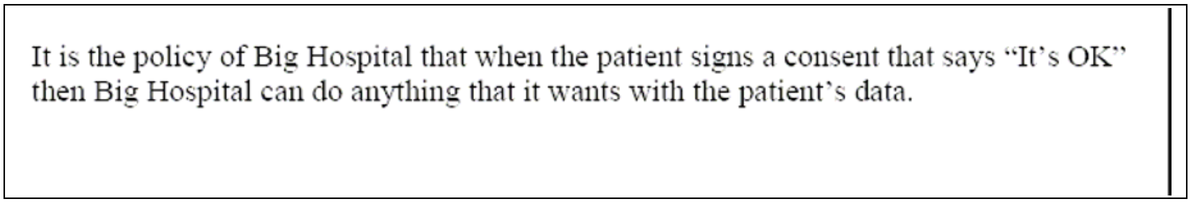
[1] XD* is used to represent the XDS, XDM, and XDR profiles. Where XD* is used it should be understood that similar functionality exists in all XDS, XDM, and XDR Profiles. Where this is not true the specific profiles will be called out independently.

## 3.1 Basic Patient Privacy Consent Use-Cases

This section gives examples of some possible patient privacy consent policies and how the systems publishing documents and using documents might act. This is an informative section and should not be interpreted as the only way to implement the BPPC profile.

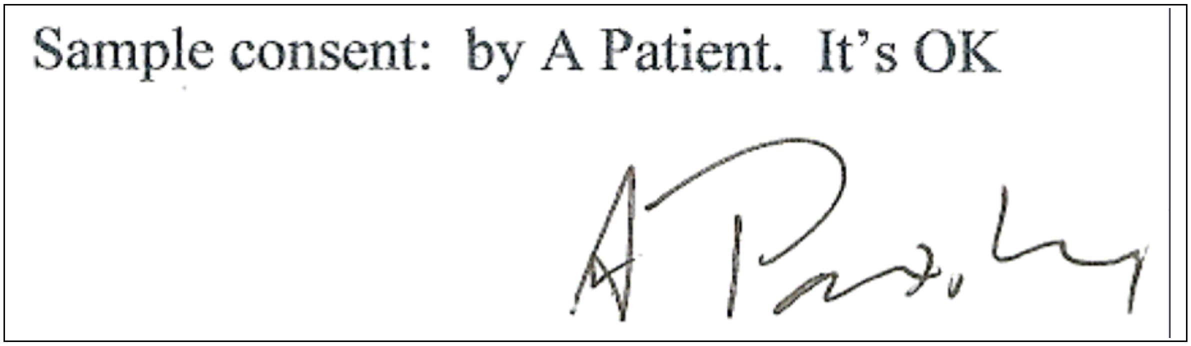
### 3.1.1 Wet Signature

Big Hospital has not yet fully digitized their patient consents process. They have a paper document that describes their Privacy Consent Policy. In our example this Privacy Consent Policy will be referenced as policy 9.8.7.6.5.4.3.2.1. Our example is ridiculous, but points out that the content of the policy is legal text, and that we provide no structured or coded way to interpret. This policy looks like:



It is the policy of Big Hospital that when the patient signs a consent that says "It's OK" then Big Hospital can do anything that it wants with the patient's data.

Big Hospital has the patient acknowledge this consent through ink on paper. This act produces the Patient Privacy Consent, For Example:



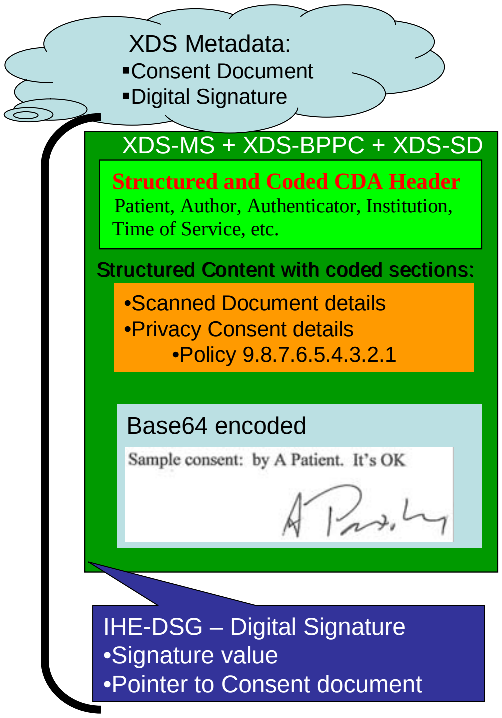
Sample consent: by A Patient. It's OK

This acknowledgement is captured according to the XDS-SD profile, with the additional parameters specified in the BPPC profile also applied to the CDA wrapper. This is registered with the XDS as proof that the patient has consented to policy 9.8.7.6.5.4.3.2.1. This acknowledgement will have its own OID as any document registered in XDS will have, but this instance OID is not further used.

This example is available on the IHE wiki for educational purposes.

If the hospital wants to further provide authenticity protections they may apply a DSG digital signature to the whole package with the appropriate purpose and signed by an appropriate signing system/person.

The following shows this graphically:


XDS Metadata:
▪Consent Document
▪Digital Signature
XDS-MS + XDS-BPPC + XDS-SD
Structured and Coded CDA Header
Patient, Author, Authenticator, Institution, Time of Service, etc.
Structured Content with coded sections:
•Scanned Document details
•Privacy Consent details
•Policy 9.8.7.6.5.4.3.2.1
Base64 encoded
Sample consent: by A Patient. It's OK
IHE-DSG – Digital Signature
•Signature value
•Pointer to Consent document

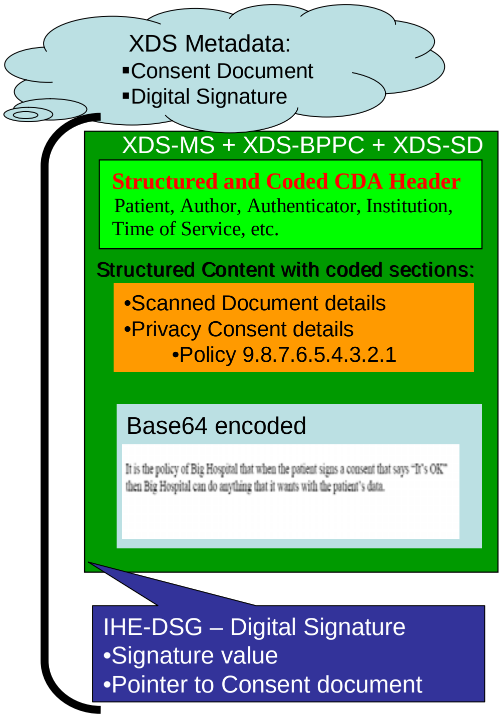
### 3.1.2 Implied Consent vs Explicit Consent

This profile supports both Implied Consent as well as Explicit Consent environments. In order to provide a profile with global appeal we have supported both environments. In an implied consent environment a Document Consumer will not find an instance of a Patient Privacy Consent document in the XDS, as capturing the act of consenting would not be required. This may be true in an Explicit Consent environment as well in cases where getting the explicit consent is delayed due to medical reasons (e.g. emergency).

In an implied Consent environment, the clinical documents submitted to the XDS would need to be marked with the general use consent, where other documents may have additional explicit consents.

### 3.1.3 Electronic Patient Consent

In this use case we move forward to a XDS Affinity Domain where the patient has a unique Public Certificate. This use case has the patient digitally signing the consent. In this case we don't capture a wet signature. For this example we include the PDF of the consent text, and this is what the patient signs. The patient's digital signature is captured using the IHE Digital Signature (DSG) profile, as shown below:


XDS Metadata:
▪Consent Document
▪Digital Signature
XDS-MS + XDS-BPPC + XDS-SD
Structured and Coded CDA Header
Patient, Author, Authenticator, Institution, Time of Service, etc.
Structured Content with coded sections:
•Scanned Document details
•Privacy Consent details
•Policy 9.8.7.6.5.4.3.2.1
Base64 encoded
IHE-DSG – Digital Signature
•Signature value
•Pointer to Consent document

It is the policy of Big Hospital that when the patient signs a consent that says "It's OK" then Big Hospital can do anything that it wants with the patient's data.

### 3.1.4 Administrative Use

Healthcare providers utilize many different sets of data to carry out the treatment, billing, and normal operations. When a patient presents, often the patient must fill out volumes of information used for patient demographics, contacts, and insurance.

For this example we might illustrate a registration system that captures a scanned image of the patient's insurance card. This scanned image can be submitted to the XDS using the confidentiality code indicating that it is available for administrative uses. This registration system could additionally capture the typical demographics and such in a form of coded clinical document that is also published as available for administrative use. Both of these documents don't have clinical information and thus wouldn't need to be restricted to direct care providers.

Now that we have shown how this information can be captured. We can see cases where the patient presents at a different clinic in the same XDS Affinity Domain. The administrative staff can now query the XDS and simply confirm that the information is the same.

### 3.1.5 Clinical Support Staff Use

The patient when staying for a few days might have special dietary needs based on their conditions. These dietary needs could be documented in the XDS and marked as for clinical support staff. This document could be accessed by the dietitian when preparing the meals.

### 3.1.6 Mixed Patient Privacy Consents

As can be seen by the use-cases shown already over time an XDS Affinity Domain may have a mixture of implied consent, wet signature consents and patient digital signature consents. The XDS Affinity Domain will also have multiple generations of patient consents.

### 3.1.7 Policies in an environment with comprehensive access controls

An Affinity Domain may have jurisdictional or organizational policies that require support for more complex patient privacy consent policies. These privacy policies may require that a patient explicitly consent to disclosure of protected or sensitive health information to specific entities. The BPPC profile provides a starting point for implementing these types of privacy consent policies, but does not explicitly specify how additional information needed to enforce the policy would be conveyed.

For example, in a jurisdiction that requires explicit patient consent to disclose psychotherapy notes:

1. The Affinity Domain would define sufficiently explicit functional roles as well as contextual and user specific role information to support these policies in the consent provided.

2. The Affinity Domain would include a sensitivity marker for psychotherapy notes and may only permit access by the functional role

(1) “named entity”, where the named entity identifier must match the identifier of the named entity in the patient’s associated consent document associated with the patient’s health document;

(2) an “unnamed entity” based on a time limited and non-transferrable “shared secret key” supplied to the entity by the patient and authenticated by some algorithm the informaiton in the patient’s associated consent document; or

(3) an emergency provider who submits a “break the glass key” administered by the Affinity Domain that has an appropriate audit trail with documentation of the provider’s reason and context for use per Affinity Domain policy.

The psychotherapy notes would then be submitted to the XDS using the confidentiality code indicating that it is available only to these entities.

In addition to document type level sensitivity markers, e.g., psychotherapy notes, an Affinity Domain might also support sensitivity markers for types of health information that might be included in documents of many types. There may be sensitivity markers for any document that includes diagnosis, procedure, medication, location, or provider information which the patient believes may indicate that the patient has genetic, substance use, HIV-AIDs, mental health or other conditions, which the patient wishes to mask. Another use for sensitivity markers is for victims of abuse who wish to mask all records containing their demographic information.

## 3.2 Privacy Access Policies (Informative)

One possible implementation may have a collection of policies and sensitivity markers form an access control matrix. A simple access control matrix is shown in Table 3.2-1.

| Sensitivity<br>Functional Role | Billing Information | Administrative Information | Dietary Restrictions | General Clinical Information | Sensitive Clinical Information | Research Information | Mediated by Direct Care Provider[2] |
|---|---|---|---|---|---|---|---|
| Administrative Staff | √ | √ | | | | | |
| Dietary Staff | | √ | √ | | | | |
| General Care Provider | | √ | √ | √ | | | |
| Direct Care Provider | | √ | √ | √ | √ | | √ |
| Emergency Care Provider | | √ | √ | √ | √ | | √ |
| Researcher | | | | | | √ | |
| Patient or Legal Representative | √ | √ | √ | √ | √ | | |

**Table 3.2-1 Access Control Policies**

The matrix can be sliced vertically. By slicing the matrix vertically (by sensitivity marker), a single patient consent policy (aka. sensitivity marker) vocabulary can be established. This vocabulary must then be configured in the XDS Affinity Domain.

Using the example above, the privacy consent policies would be.

| 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. |
| Research Information | May be accessed by researchers. |
| Mediated by Direct Care Provider | May be accessed by direct or emergency care providers. |

[2] This classification might be used for information about the patient's prognosis or diagnosis that has not yet been shared with the patient.

The access control matrix can also be sliced horizontally by functional role. This requires that a separate vocabulary for document Privacy Consent Policy be configured in the XDS Affinity Domain.

| Privacy Consent Policy | Description |
|---|---|
| Administrative Staff | May access documents that describe their sensitivity with the Billing Information or Administrative Information code. |
| Dietary Staff | May access documents that describe their sensitivity with the Administrative Information or Dietary Restrictions codes. |
| General care providers | May access documents that describe their sensitivity with the Administrative Information, Dietary Restrictions or General Clinical Information codes. |
| Direct care providers | May access documents that describe their sensitivity with the Administrative Information, Dietary Restrictions, General Clinical Information, or Sensitive Clinical Information codes. |
| Emergency care providers | May access documents that describe their sensitivity with the Administrative Information, Dietary Restrictions, General Clinical Information, or Sensitive Clinical Information codes. |
| Researchers | May access documents that describe their sensitivity with the Research Information code. |
| Patient (or legal representative) | May access documents that describe their sensitivity with the Administrative Information, Dietary Restrictions, General Clinical Information, or Sensitive Clinical Information codes. |

Other divisions of the access control matrix are possible, so long as a Privacy Consent Policy covers each cell granting access in the matrix.

### 3.2.1 References

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”

## 3.3 Creating Privacy Consent Policies

A Privacy Consent Policy shall identify who has access to information, and what information is governed by the policy (e.g., under what conditions will a document be marked as containing that type of information). The XDS Affinity Domain shall publish privacy Consent Policies. The mechanism for publishing these policies is not described by this profile. The Privacy Consent Policies written by the XDS Affinity Domain must be able to be implemented by the technologies in all of the systems that have access to the XDS Affinity Domain. This means that the Privacy Consent Policies must be created with great care to ensure they are enforceable.

The implementation of Privacy Consent Polices under this profile makes it strongly advisable that policies describe under what situations a functional role shall have access to information, and do not include situations in which a functional role is not granted access. Take care when writing access control policies. The two policy statement examples below illustrate the problem.

1. A Researcher may >>only<< access documents that describe their sensitivity with the Clinical Trial 1 code.
2. A Researcher may >>only<< access documents that describe their sensitivity with the Research Project 1 code.

The first policy grants access to a researcher to one class of documents (those marked with the Clinical Trial 1 code), and due to the word "only", effectively revokes access to all other documents. The second policy does the same thing (for Research Project 1), and revokes access to all other documents. These two policies cannot be applied at the same time, as they are incompatible with each other. The solution is to strike the word >>only<< and thus the two Privacy Consent Policies are able to be aggregated.

An XDS Affinity Domain may have legacy documents that were published prior to all systems supporting the BPPC Profile, and thus will have confidentiality codes not defined under the BPPC Profile (e.g. For example, "N" from 2.16.840.1.113883.5.25). The XDS Affinity Domains will need to provide Privacy Consent Policies for granting access to documents that use these non-BPPC confidentiality code values.

Affinity domains should also determine their strategy for addressing the changing of Privacy Consent Policies and the policy vocabularies.

Finally, Privacy Consent Policies used within an XDS Affinity Domain will very likely be different than those used with the XDM or XDR Profiles. The patient may provide a consent given to share information on media to the provider creating the media for specific use, rather than for more general sharing within an XDS Affinity Domain. When transferring information that originated in an XDS Affinity Domain to media (XDM), the Privacy Consent Policies found in the XDS Affinity Domain might be changed during the publication process. There are also differences in the sensitivity that should be considered for consents shared on media or transmitted through XDR and those shared in an XDS affinity domain. See the section 3.10 Security Considerations later in this volume for more details.

## 3.4 Implementation of Access Control

Consumers of documents that implement this profile are required to enforce access control based on the policies described by the Affinity Domain. This is because the consumers of the documents are best aware of the functional role, how the data will be used, the relationship between provider and patient, the urgency of access, etc. The mechanism by which consumers associate individual users with functional roles is not within the scope of this profile. However it does allow for mechanisms to be used that take into account the structural role of the user, their association with the patient, the functional role that they are assigned with the session in which they are accessing data, and the declared sensitivity of the data being protected.

## 3.5 Actors/ Transactions

There are two actors in this profile, the Content Creator and the Content Consumer. Content is created by a Content Creator and is to be consumed by a Content Consumer.

The sharing or transmission of Consents to Share Information between actors is addressed by the use of appropriate IHE profiles described by the section **Error! Reference source not found.** below.

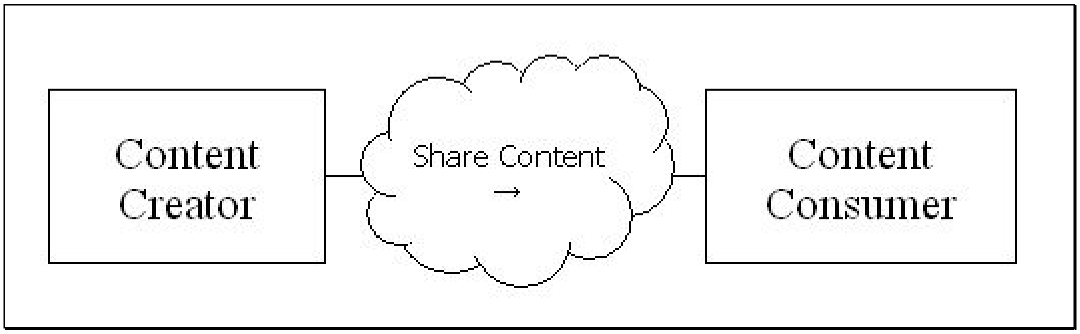


**Figure 3.5-1 BPPC Actors**

## 3.6 BPPC Bindings

It is expected that the sharing of consents will occur in an environment where the physician offices and hospitals have a coordinated infrastructure that serves the information sharing needs of this community of care. Several mechanisms are supported by IHE profiles:

- A registry/repository-based infrastructure is defined by the IHE Cross-Enterprise Document Sharing (XDS) and other IHE Integration Profiles such as patient identification (PIX & PDQ), and notification of availability of documents (NAV).
- A media-based infrastructure is defined by the IHE Cross-Enterprise Document Media Interchange (XDM) profile.
- A reliable messaging-based infrastructure is defined by the IHE Cross-Enterprise Document Reliable Interchange (XDR) profile.
- All of these infrastructures support Security and privacy through the use of the Consistent Time (CT) and Audit Trail and Node Authentication (ATNA) profiles.

For more details on these profiles, see the IHE IT Infrastructure Technical Framework, found here: http://www.ihe.net/Technical_Framework/.

Thus, implementors of the Content Creator and Consent Consumer Actors must also implement either the ITI XDS, XDM or XDR Profiles to exchange content, using the bindings listed below in Table 3.6-1.

| Content | Binding | Actor | Optionality |
|---|---|---|---|
| *Consent to Share Information* | Medical Document Binding to XD*<br>*PCC TF-2: 4.1* | Content Creator | R |
|  |  | Content Consumer | R |

**Table 3.6-1 BPPC Bindings**

## 3.7 Consent Content Module

A consent document is a kind of medical document, and shall conform to the requirements of the Consent content module specified in this profile. The content of a consent document shall include the effective time of the consent and coded vocabulary identifying the policies consented to (OID). The content of the consent document may include a text description of what the patient has consented to, and either a facsimile of a wet signature, or a digital signature by the patient (or legal representative). The consent if signed shall use the IHE ITI DSG profile.

## 3.8 BPPC Process Flow

The BPPC profile uses the normal process flow of the XD* profiles, depending upon which bindings have been declared.

1) Administrative tasks prior to BPPC use
   a. The Affinity Domain will write and agree to the Affinity Domain Policy (lots of lawyers involved).
   b. The Affinity Domain Policy will include a small set of Privacy Consent Policies (more lawyers). These are text documents very similar to the privacy consent documents used today.
   c. Each Privacy Consent Policy will be given an XDS Affinity Domain unique identifier (OID)
   d. The Affinity Domain Policy and all of the Privacy Consent Policies will be published in a way consistent with the Affinity Domain's Policy. It is expected that this will be sufficiently public to support local regulation.
2) Patient consents to a policy
   a. The Patient will be presented with the Affinity Domain – Patient Privacy Consent Policies.
   b. The Patient will agree to one or more of the Privacy Consent Policies. In most regions the patient must be fully informed and acknowledge the

privacy consent. In some regions there is implied consent, and thus there is no need to capture a patient’s consent.

c. A system that captures patient privacy consents will capture this act in a BPPC Patient Privacy Consent Document.

i. XDS Metadata

1. authorPerson is the patient or legal guardian that is agreeing to the consent.

2. classCode indicates this is a consent document

3. confidentialityCode may indicate other consent OIDS that control this consent document

4. eventCodeList indicates the Privacy Consent Policy identifier (OID)

5. legalAuthenticator would be the digital signer if used, or the identity of the Affinity Domain representative that is confirming that the patient is agreeing.

6. serviceStartTime and serviceStopTime indicate when this consent is effective.

ii. Patient Privacy Consent Document

1. template ID = “1.3.6.1.4.1.19376.1.5.3.1.1.7 ”

2. The patient or legal guardian that is agreeing to the consent is identified as the author of the consent document.

3. Any witness to this consent may be captured (i.e. participant typeCode=‘WIT’)

4. authorization indicates that this is a consent act

5. Effective time is set

a. When the privacy consent is first effective. This effective date may be retroactive based on the XDS Affinity Domain Policy.

b. If necessary, when the privacy consent is expected to elapse

6. If wet signature is used, the XDS-SD profile will be used to scan the paper and encode it into the consent document

a. the XDS-SD CDA attributes are combined with the BPPC CDA attributes.

        iii. If digital signature is used the DSG profile will be used to sign the consent document. This is an additional document that is published. This may be published in the same submission set, or may come after based on workflow.

3) System checking on a patient's consent status
    a. When a system/individual wants to know if a specific patient has consented it can do a query for consent documents on that patient.
    b. Note if the local regulations allow, some XDS Affinity Domains may not publish the consent documents, so systems should be able to handle these configurations.
    c. Note if the local regulations allow, some patients may have documents shared before informed consent can be captured.
4) Clinical documents are published into XDS Affinity Domain
    a. When clinical documents are published into XDS an assessment must be done to determine which of the XDS Affinity Domain – Privacy Consent Policies would allow the documents to be published.
        i. In some XDS Affinity domains this may require that the system check that a patient has indeed consented to the specific policy (see 3)
        ii. This is likely based on human configuration of the document source system.
    b. The XDS Metadata – confidentialityCode - will include the OIDS of the appropriate (determined by the XDS Affinity Domain Policy) Privacy Consent Policy identifier (OID)
    c. The XDS Registry will validate that the confidentialityCode is one approved for use within the XDS Affinity Domain.
5) Clinical documents are used from the XDS Affinity Domain
    a. When a system queries the XDS Affinity Domain it should utilize the confidentialityCode in the queries to restrict the documents returned to those that the system can utilize
        i. For Example: If the system is a research application, then it should set the confidentialityCode in the query to the list of XDS Affinity Domain Policy identifiers (OIDs) that would allow for the documents to be used for the research.
    b. Even if the confidentialityCode is not specified, the system implementing the Document Consumer actor is still bound to enforce the XDS Affinity Domain Policies.

   c. The consumer system will enforce access controls based the returned metadata-confidentialityCode, system type, user, context, and any number of other factors that the system is capable of enforcing.

## 3.9 Grouping with Other Profile Actors

The capturing of the patient consenting could be futher covered by use of the IHE Digital Signature content profile (DSG). Systems should be prepared to see DSG related content associated with the Patient Privacy Consent document.

## 3.10 Security Considerations

Consents stored in an XDS affinity domain are also governed by privacy policies. The content of a Privacy Consent may itself contain sensitive information. For example, a terminally ill patient may decide that his prognosis should not be shared with his family members, but that other information may be. Sharing the Privacy Consent Act with family members would potentially inform them of a negative prognosis.

However, Privacy Consent Acts stored in the clear on media (XDM), or otherwise transmitted through XDR should not contain sensitive information. The rationale is that the receiver of the information must be able to read the consent that was used to share this information in order to understand how they must treat the information with respect to their own Privacy Consent Policies.

Implementation of Privacy Consent Policies within a healthcare environment has different considerations and risks than implementing similar access control policies within other non-treatment environments. This is for the simple reason that failing to provide access to critical healthcare information has the risk of causing serious injury or death to a patient. This risk must be balanced against the risk of prosecution or lawsuit due to accidental or malicious disclosure of private information. The XDS Affinity Domain should take care in writing their Privacy Consent Policies to avoid this.

One mitigation strategy often adopted in healthcare provides Accountability through Audit Controls. That is to say that 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.

Another risk that must be resolved by an affinity domain is how to address the issues of sharing truly sensitive information in a registry (e.g., for VIP patients, or sensitive data). One strategy that might be recommended is that truly sensitive data not be shared within the XDS Affinity Domain, directed communications using XDR or XDM may be more appropriate.

# Volume II

## 3 IHE Transactions

*Add the following to ITI 3.15.4.1.1 Provide and Register to explain the Privacy Option*

### 3.15.4.1.1.1 Basic Patient Privacy Consents Option

If the Basic Patient Privacy Consents Option is implemented:

1. The Document Source actor shall populate the confidentialityCode in the document metadata with the list of OID values that identify the Privacy Consent Policies that apply to the associated document. All documents submitted shall have confidentiality codes. The confidentiality codes for different documents in the same submission may be different.
2. The Document Source actor will need to be configured with the Privacy Consent Policies, Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the XDS Affinity Domain Policy. The details of this are product specific and not specified by IHE.
3. The Document Source actor may have user interface or business rule capabilities to determine the appropriate confidentiality codes for each document. The details of this are product specific and not specified by IHE. However, the information about how confidentiality codes are assigned must be part of the published policy for the XDS Affinity Domain.

*Add the following to ITI 3.14.4.1.1 Register Document Set to explain the Privacy Option*

### 3.14.4.1.1.1 Basic Patient Privacy Consents Option

If the Basic Patient Privacy Consents Option is implemented:

1. The Registry actor shall verify that the confidentialityCode in the document metadata consists of OID values that match the Privacy Consent Policies that have been defined for this XDS Affinity Domain. All documents submitted shall have confidentiality codes. The confidentiality codes for different documents in the same submission may be different.
2. The Registry actor will need to be configured with the Privacy Consent Policies, Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the XDS Affinity Domain Policy. The details of this are product specific and not specified by IHE.

*And to section ITI 3.16.4.1.1 Query Registry and ITI 3.18.4.1.1 Registry Stored Query to explain the Privacy option*

### 3.16.4.1.1.1 Basic Patient Privacy Consents Option

### 3.18.4.1.1.1 Basic Patient Privacy Consents Option

If the Basic Patient Privacy Consents Option is implemented:

1. The Document Consumer actor may populate the confidentialityCode in every query with the list of OID values that identify the Privacy Consent Policies that should apply to the documents that are returned in the query results. Note: All documents submitted have confidentiality codes.
2. The Document Consumer actor will need to be configured with the Privacy Consent Policies, Privacy Consent Policy Identifiers (OIDs and associated information necessary to understand and enforce the XDS Affinity Domain Policy. The details of this are product specific and not specified by IHE.
3. The Document Consumer shall not allow access to documents for which the Document Consumer does not understand at least one of the confidentialityCode returned.
4. The Document Consumer actor shall have user access controls or business rule capabilities to determine the details of how confidentiality codes apply to query results. For example, many EHR systems have complex role based access control (RBAC) systems that determine what information is displayed to a user. The RBAC configuration will need to know the user, the user’s role, the patient, and the confidentiality code to know whether all or only selected portions of the query results are visible to the user. The details of this are product specific and not specified by IHE. These rules shall reduce the query results to only those that are appropriate to the current situation for that actor and user.
5. The Registry shall return only documents that match the requested confidentialityCode indicated in the query according to the following rules:
    1. If the query parameter confidentialityCode is empty, then it is not considered in the filter criteria, and thus the Registry may return all otherwise matching documents.
    2. If the query contains one or more confidentialityCode, the Registry shall return all matching documents that also meet an equal’s comparison where any of the confidentiality codes on the query match any of the codes that apply to a particular document.

*Add the following to ITI 3.17.4.1.1 Retrieve Document to explain the Privacy Option*

### 3.17.4.1.1.1 Basic Patient Privacy Consents Option

If the Basic Patient Privacy Consents Option is implemented:

1. The Document Consumer actor honor the confidentialityCode in the metadata associated with the document.
2. The Document Consumer actor will need to be configured with the Privacy Consent Policies, Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the XDS Affinity Domain Policy. The details of this are product specific and not specified by IHE.
3. The Document Consumer actor is expected to have user access controls or business rule capabilities to determine the details of how confidentiality codes apply to documents. For example, many EHR systems have complex role based access control (RBAC) systems that determine what information is displayed to a user. The RBAC configuration will need to know the user, the user's role, the patient, and the confidentiality code to know whether all or only selected portions of the document are visible to the user. The details of this are product specific and not specified by IHE. These rules shall reduce the document display results to only those that are appropriate to the current situation for that actor and user.

*Add the following to ITI 3.32.4.1.1 Distribute Document Set on Media*

#### 3.32.4.1.1.1 Basic Patient Privacy Consents Option

If the Basic Patient Privacy Option is implemented:

1. The Portable Media Creator actor shall populate the confidentialityCode in the document metadata with the list of Privacy Consent Policy Identifiers (OID) values that identify the Patient Privacy Policies that apply to the associated document. All documents submitted shall have confidentiality codes. The confidentiality codes for different documents in the same submission may be different.
2. The Portable Media Creator actor will need to be configured with the Privacy Consent Policies, Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the policies. The details of this are product specific and not specified by IHE.
3. The Portable Media Creator actor may have user interface or business rule capabilities to determine the appropriate confidentiality codes for each document. The details of this are product specific and not specified by IHE.
4. The Portable Media Importer actor will need to be configured with the Privacy Consent Policies, Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the policies. The meanings of the codes on the media must be provided out of band, e.g., by telephone, fax, or email. The detail of how this is done is product specific and not specified by IHE. If the documents are transferred internally within the organization or to other members of the recipient's affinity domain, appropriate internal confidentiality codes shall be applied.

- The Portable Media Creator actor may publish at least one consent document and any applicable digital signatures that apply to the collection of content that it has created on portable media.

5. The Portable Media Importer actor shall have the ability to coerce the confidentiality code in the metadata associated with the document from the codes used by the Exporter to the codes used by the Importer.
6. The Portable Media Importer actor is expected to have user access control or business rule capabilities to determine the details of how confidentiality codes apply to query results. For example, many EHR systems have complex role based access control (RBAC) systems that determine what information is displayed to a user. The RBAC configuration will need to know the user, the user's role, the patient, and the confidentiality code to know whether all or only selected portions of the document are visible to the user. The details of this are product specific and not specified by IHE. These rules shall reduce the document display results to only those that are appropriate to the current situation for that actor and user.

# 4 Bindings

*Add the following section to the list of bindings in Section 4.*

## 4.1 Consent Binding to XDS

The consent binding to XDS is the same as the Medical Document Binding to XDS described in section 4.1, with the exception of the following XDSDocumentEntry metadata fields **highlighted** in the table below.

| XDSDocumentEntry Attribute | Optional? | Constrained? | Extended Discussion? | Source Type | Source/ Value |
|---|---|---|---|---|---|
| authorPerson | **R** | | 4.1.1.1 | | |
| classCode | R | | 4.1.1.2 | **FAD** | **Consent** |
| classCodeDisplayName | R | | 4.1.1.2 | **FAD** | **Consent** |
| confidentialityCode | R | | 4.1.1.3 | | |
| eventCodeList | **R** | | 4.1.1.4 | **CADT** | **/ClinicalDocument/authorization/consent/code/@code** |
| eventCodeDisplay NameList | **R** | | 4.1.1.4 | **CADT** | **/ClinicalDocument/authorization/consent/code/@displayName** |
| legalAuthenticator | **R2** | | 4.1.1.5 | SAT | $person <= /ClinicalDocument/ legalAuthenticator |
| serviceStartTime | **R** | | 4.1.1.6 | SA | /ClinicalDocument /documentationOf/serviceEvent /effectiveTime/low/@value |
| serviceStopTime | R2 | | 4.1.1.6 | SA | /ClinicalDocument /documentationOf/serviceEvent /effectiveTime/high/@value |

### 4.1.1 Extended Discussion

#### 4.1.1.1 author

The author is a required element, and is the person issuing the consent (e.g. the patient, guardian, or legal guardian).

#### 4.1.1.2 classCode and classCodeDisplayName

These attributes are fixed to the value "Consent" by this binding.

#### 4.1.1.3 confidentialityCode

The binding has not changed from XDS, however, note that a consent document may also be assigned a confidentialityCode, because the content of the document may be restricted to users in specific functional roles due to the possibly sensitive nature of the content of the consent document.

#### 4.1.1.4 eventCodeList and eventCodeDisplayNameList

The eventCodeList shall be populated using the codes identifying the policies that have been consented to within the document. The eventCodeDisplayNameList shall be populated using the display names for those policies.

#### 4.1.1.5 legalAuthenticator

The legalAuthenticator of a consent document shall be present if available, If the Patient Privacy Consent is digitally signed than the legalAuthenticator shall be one of the persons whose digital signature attests to the content of the consent document. If the consent is not digitally signed then the legalAuthenticator shall be the representative of the Affinity Domain that is attesting that the patient has consented.

#### 4.1.1.6 serviceStartTime and serviceStopTime

The serviceStartTime shall be present and indicates the effective start time of the consent. The serviceStopTime may be present, and if it is present, indicates the effective time at which the consent is no longer effective. If it is not present, the effectiveStopTime is assumed to be controlled by XDS Affinity Domain policy.

# 5 Content Modules

### 5.1.1 IHE PCC Template Identifiers

*Add the following row to the list of IHE PCC Template Identifiers*

| extension | Description |
|---|---|
| 1.3.6.1.4.1.19376.1.5.3.1.1.7 | The template identifier used to indicate that a CDA document conforms to the Basic Patient Privacy Consent to Share Information Module. |

*Add the following section to the IHE Content Profiles Section of Volume II of the Patient Care Coordination Technical Framework.*

## 5.7 Consent to Share Information 1.3.6.1.4.1.19376.1.5.3.1.1.7

### 5.7.1 Dependencies

A Consent document is an instance of the act of a patient signing a Patient Privacy Consent Policy and is a type of medical document, and incorporates the constraints defined for medical summaries found in section 5.3 Medical Documents above.

### 5.7.2 Standards

| | |
|---|---|
| CDAR2 | Clinical Document Architecture, Release 2.0, 2005, HL7 |
| XDS-SD | Scanned Documents |

### 5.7.3 Conformance

CDA Release 2.0 documents that conform to the requirements of this content shall indicate their conformance by the inclusion of the appropriate <templateId> element in the header of the document. This is shown below in Figure 5.7-1.

```
<ClinicalDocument xmlns='urn:hl7-org:v3'>
   <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
   <templateId root="1.3.6.1.4.1.19376.1.5.3.1.1.7"/>
      :
```

**Figure 5.7-1: Declaring Conformance**

A CDA Document may conform to more than one template, and can therefore have more that one <templateId> element. One of those <templateId> elements must appear exactly as shown above in Figure 5.7-1.

### 5.7.4 Constraints

A consent shall contain a text description of what the patient consented to, a list of codes indicating the policy(s) agreed to, a time range indicating the effective time of the consent, and shall contain a signature signifying the patient agreement to those policy(s) stated in the text description. Finally, consents must be attested to using an electronic digital signature, conforming to the ITI Digital Signature Profile.

The text description and signature shall appear as a scanned image, and it shall also conform to the constraints of the ITI Scanned Document profile.

A consent shall have one or more <authorization> elements in the header identifying the policies authorized by the document (see Section 4.2.3.4 of CDAR2). Each <authorization> element indicates informed consent to one and only one XDS Affinity Domain policy. More than one policy may be agreed to within a given consent document.

A consent shall have a documentationOf element describing a consent serviceEvent.

Consent documents shall be attested to by either the patient and/or legal guardian, or a third party assigned by the XDS Affinity Domain or its member organizations. The attestation shall be performed using the ITI Digital Signature profile. The signer may be the patient, or a third party.

#### 5.7.4.1 Authorization

Each authorization element in the CDA Header represents informed consent to one policy expressed by the XDS Affinity Domain. The consent shall have a unique identifier contained in the <id> element, representing the patient consent to that policy. The policy being consented to shall be represented in the <code> element.

```
<authorization typeCode='AUTH'>
    <consent classCode='CONS' moodCode='EVN'>
        <id root=''/>
        <code code='' codeSystem='' codeSystemName='' displayName=''/>
        <statusCode code='completed'/>
    </consent>
</authorization>
```

Policies are identified using an Affinity Domain specified coding system. Each coded value in that vocabulary represents one affinity domain specific policy.

##### 5.7.4.1.1 <authorization typeCode='AUTH'>

At least one <authorization> element must be present in a consent document. The typeCode attribute shall be present and be valued with AUTH, indicating that this is an authorization act related to the document.

##### 5.7.4.1.2 <consent classCode='CONS' moodCode='EVN'>

Each authorization element shall have one <consent> element. The classCode shall be present and be valued with CONS, indicating that the related act is an informed consent.

The moodCode shall be EVN, indicating that this element represents and act that has occurred.

#### 5.7.4.1.3 <id root=''/>

The <consent> element shall have one identifier that is used to uniquely identify the consent act. This identifier shall contain a root attribute, and shall not contain an extension attribute.

#### 5.7.4.1.4 <code code='' codeSystem='' codeSystemName='' displayName=''/>

The <consent> element shall have one <code> element that is used to identify the consent policy that was agreed to by the patient.

### 5.7.4.2 Effective Time

Within a consent document, the effective time of the consent shall be specified within the documentationOf/serviceEvent element.

```
<documentationOf typeCode='DOC'>
    <serviceEvent classCode='CONS' moodCode='EVN'>
        <id root=''/>
        <effectiveTime>
            <low value=''/>
            <high value=''/>
        </effectiveTime>
    </serviceEvent>
</documentationOf>
```

#### 5.7.4.2.1 <documentationOf typeCode='DOC'>

Only one <documentationOf> element shall exist, describing the service event of provision of consent. This element shall have a typeCode attribute with the value DOC.

#### 5.7.4.2.2 <serviceEvent classCode='CONS' moodCode='EVN'>

Only one <serviceEvent> shall exist, describing the duration of the provision of consent. This element shall have a classCode attribute set to CONS, and a moodCode attribute of EVN.

#### 5.7.4.2.3 <id root='' />

The service event shall have one <id> element, providing an identifier for the service event.

The root attribute of this element shall be present, and shall be a GUID or OID. The extension attribute shall not be present.

#### 5.7.4.2.4 <effectiveTime><low value="/><high value="/></effectiveTime>

The <effectiveTime> element shall be present, and shall indicated the effective time range over which consent is given. The low value must be provided[3]. The high value may be present. If present, is shall indicate the maximum effective time of the consent.

[3] A consent-authoring environment might assume that the low value is the creation time of the document providing consent.