

**DOCUMENT 27:  
THE IT INFRASTRUCTURE TECHNICAL FRAMEWORK WHITE  
PAPER**

**HIMSS, RSNA, and ACC  
Integrating the Healthcare Enterprise**



**IHE IT Infrastructure Technical Framework  
White Paper  
2007-2008**

**Template for XDS Affinity Domain Deployment Planning**

**< Version for Trial Implementation >**

## Contents

1	Introduction.....	2
1.1	Expected Knowledge and References.....	2
2	Goals .....	2
2.1	Request for Feedback.....	3
2.2	Open Issues and Questions .....	3
3	Overview.....	3
	Appendix X: XDS Affinity Domain Definition Template .....	4
X.1	Introduction.....	4
X.2	Glossary .....	4
X.3	Reference Documents .....	5
X.4	Organizational Rules.....	5
X.5	Operational Rules.....	6
X.6	Membership Rules .....	8
X.7	Connectivity to the XDS Affinity Domain from External Systems .....	9
X.8	System Architecture.....	9
X.9	Terminology and Content .....	10
X.10	Patient Privacy and Consent .....	15
X.11	Technical Security .....	17

## 1 Introduction

The concept of an XDS Affinity Domain is defined in ITI TF-1:10 and Appendix K. It is clear that many regulatory/professional organizations will need to define policies regarding coded terminology, privacy, document format and content, language support, etc. for an XDS Affinity Domain. In addition, there will be the need to define such policies on a national or regional basis for all XDS Affinity Domains within a geographic region. These policy decisions, necessary for successful implementation, may result in refinements of the XDS Profile itself.

This White Paper proposes a new template that should be used when defining policies for either an individual XDS Affinity Domain, or multiple XDS Affinity Domains within a particular nation or region. This template provides a consistent documentation format for specifying implementation decisions, policies, and possible refinements of XDS and related Profiles. Additionally, its' outline provides a comprehensive list of all relevant topics that XDS Affinity Domain implementers may find helpful in planning for deployment.

### 1.1 Expected Knowledge and References

It is assumed that the reader has a working knowledge of the IHE ITI XDS Profile and its dependent Profiles which can be downloaded from the IHE web site:

[http://www.ihe.net/Technical\\_Framework/index.cfm](http://www.ihe.net/Technical_Framework/index.cfm)

The key Integration Profiles and section number in the above document are:

- XDS – Section 10
- PIX – Section 5
- PDQ – Section 8
- ATNA – Section 9

In addition, the existing Cross Community Information Exchange and the Cookbook for the Security Sections of IHE Profiles White Papers, as well as Basic Patient Privacy Consents Supplement provide useful information regarding areas that should be addressed when implementing an XDS Affinity Domain. These can all be found using the IHE web site link above.

## 2 Goals

This paper addresses the following goals:

- Describe the issues to consider when planning the deployment of XDS Affinity Domains.
- Define the areas of the XDS and related Profiles to consider refining for XDS Affinity Domains.

- Provide a standardized document template to be used when specifying the deployment policies for a single XDS Affinity Domain, or for multiple XDS Affinity Domains that are in a particular nation or geographic region.

## 2.1 Request for Feedback

The IHE IT Infrastructure Technical Committee requests feedback on the concepts described in this White Paper. In particular, we would like your thoughts on whether this paper addresses all the issues involved and what you think of the proposed organization of this template.

Comments arising from Trial Implementation may be submitted to

<http://forums.rsna.org> under the forum:

**“IT Infrastructure Technical Framework ”**

Select the sub-forum:

**“Template for XDS Affinity Domain Deployment Planning”**

The IHE ITI Technical Committee will address these comments and publish a Trial Implementation version of this template in August 2007.

## 2.2 Open Issues and Questions

## 3 Overview

Currently, ITI TF Appendix L provides an informative checklist for the key policies that need to be addressed in order to deploy an EHR-LR document sharing environment for an XDS Affinity Domain. However, it has been recognized that this existing checklist is incomplete. Many additional implementation details may need to be defined, depending upon the scope of the XDS Affinity Domain in question and the degree to which particular rules are to be defined (i.e. for architecture, content, security, etc.). This White Paper proposes a new template that should be used when defining policies for either an individual XDS Affinity Domain, or multiple XDS Affinity Domains within a particular nation or region. It takes the form of a template rather than a checklist because it acts more as an outline for all the issues that should be considered, rather than a checklist to be used to verify the correctness of a particular implementation. It is proposed that the checklist in ITI TF Appendix L will be replaced by a brief summary of the content of this White Paper, along with a reference to it.

## **Appendix X: XDS Affinity Domain Definition Template**

The concept of an XDS Affinity Domain is defined in ITI TF-1:10 and Appendix K. It is clear that many regulatory/professional organizations will need to define policies regarding coded terminology, privacy, document format and content, language support, etc. for an XDS Affinity Domain. This template provides a consistent documentation template for documenting implementation decisions, policies, and IHE Profile refinements, for either an individual XDS Affinity Domain, or multiple XDS Affinity Domains within a particular nation or region. In addition, it provides a comprehensive list of all relevant topics that should be considered for deployment of XDS Affinity Domains, and implementers may find it helpful in guiding their policy and refinement decisions.

It is realized that not all of the items in this template will need to be defined for every XDS Affinity Domain, or at every national or regional level. The list of items that need to be defined will depend upon the scope of the specifications, and whether they are for a particular XDS Affinity Domain, region, and/or nation.

When defining the policies and Profile refinements for an XDS Affinity Domain it is essential that these do not contradict those mandated for all XDS Affinity Domains in the particular nation or region in which the XDS Affinity Domain will exist. In addition, these specifications for a particular XDS Affinity Domain should not duplicate those defined at a larger regional or national level. Instead the documentation for the particular XDS Affinity Domain should reference the document defining the national or regional policies.

### **X.1 Introduction**

Define introductory text specifying the nature of the XDS Affinity Domain, or organization, region, or nation for which the XDS Profile extensions apply. If XDS Profile extensions are being defined at a national or regional level and are meant to be followed by all XDS Affinity Domains within them then this should be clarified here. The people and organizations involved in creating these should be specified, as well as any professional or regulatory organizations that were involved in their creation and/or have approved them.

If the XDS Affinity Domain extensions are being defined at a national level and there is an official IHE organization for the country involved then this organization must approve the extensions and this must be stated here. It is the responsibility of the national committee involved to determine whether testing of the extensions is necessary before they can be approved. It is still possible for national extensions to be defined for a nation that does not have an official IHE organization, however it will be necessary for the organization(s) proposing these extensions to demonstrate that they have the authority to actually define such extensions.

### **X.2 Glossary**

Glossary of terms specific to the XDS Affinity Domain extension.

### **X.3 Reference Documents**

List of all documents that are referenced in the XDS Affinity Domain extensions or were used as input in some way to the creation of these extensions.

### **X.4 Organizational Rules**

Describe the organizational rules for the XDS Affinity Domain. Detail the administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties, and penalties.

Provide an introduction and then describe these functions in the following sub-sections.

#### **X.4.1 Organizational Structure**

Describe the organizational structure within the XDS Affinity domain. Considerations include, but are not limited to:

- Organization of XDS Affinity domain governance (options to consider include: central point of authority, collaborative governance, distributed governance, etc.).

List the founders, controllers, administrators, etc. of the XDS Affinity Domain. Their roles and responsibilities should be clearly defined, and contact information provided. It should be made clear who someone wishing to participate in the XDS Affinity Domain should have to contact in order to obtain information regarding participation in or access to the XDS Affinity Domain.

#### **X.4.2 Organizational Roles**

Explain the general economic considerations associated with the implementation of this XDS Affinity Domain shall be provided. These considerations include, but are not limited to:

- Funding for system implementation (examples: central private/public source, taxes, documentation of general funding guidelines rather than explicit statement on funding source)
- Business model (payments from users, re-imbusement policy, role of insurance, etc.)
- Fiscal plan for system operation and maintenance

#### **X.4.3 Transparency**

Document the manner in which accurate and timely disclosure of information will be provided by the various organizations that administer, organize, provide, and use the XDS Affinity Domain. Detail the procedures to follow in order to gain access to this information.

Provide guidelines regarding the types of information that organizations and individuals using the XDS Affinity Domain must be capable of providing should an audit of their participation or access be carried out.

#### **X.4.4 Enforcement and Remedies**

Document the responsible organizations for enforcing rules regarding payment, access rights, performance requirements, security, etc. associated with the XDS Affinity Domain. Clearly differentiate the areas of responsibility for the different organizations. If it is not clear who will ultimately be responsible for certain areas then also document this here.

#### **X.4.5 Legal Considerations**

##### **X.4.5.1 Legal Governance**

Define policies regarding the governance of legal issues related to users, publishers, IT staff, and vendors involved in the XDS Affinity Domain or within XDS Affinity Domains of the region or nation for which these policies are defined.

##### **X.4.5.2 Liability and Risk Allocation**

Distinguish any policies regarding liability issues and risk allocation for the XDS Affinity Domain. Document any policies regarding the provision of liability insurance for those publishing documents to, or using documents from, the XDS Affinity Domain.

##### **X.4.5.3 Indemnification**

Describe how indemnification is dealt with in this XDS Affinity Domain implementation. To give the reader a better idea of what to include in this section, we provide a few guiding scenarios:

- Indemnification of providers against lawsuits for data they publish that is misused by a user from a consuming system.
- Mechanism to isolate financial responsibility to a particular provider when a patient sues another for misuse of his/her data.
- Providers of data create indemnification agreements with all possible users of data.
- Recourse methods for providers to communicate problems with published data, rather than the use of that data.

##### **X.4.5.4 Intellectual Property Rights to Published Documents**

Define how intellectual property rights will be managed for documents published to the XDS Affinity Domain. For example, define whether property rights are maintained in any way once documents are published or if they are immediately waived.

#### **X.5 Operational Rules**

Describe the operational rules for the XDS Affinity Domain.

##### **X.5.1 Service Level Agreements**

Define how Service Level Agreements shall be created for the operational components of the XDS Affinity Domain.

### **X.5.2 Daily Governance**

Describe how the components of the XDS Affinity Domain are managed at an operational level. Considerations to comment on include, but are not limited to:

- Overall operation management (coordination of efforts)
- Sub-component division (if any)
- Day to Day operations management communication methods (meetings, summits, forums, etc.)

### **X.5.3 Management When Systems are Unavailable**

Define policies for managing cases where various types of components of the XDS Affinity Domain are unavailable. For example, what type of workarounds should be used if the PIX Manager for this XDS Affinity Domain implementation is unavailable? Other considerations include, but are not limited to:

- Notification mechanisms for scheduled system downtime and maintenance
- Notification of causes and resolutions for unscheduled system downtimes

### **X.5.4 Configuration Management**

Specify how change management issues (such as hardware upgrades, software upgrades, configuration changes, etc) are to be managed. Explain what authorization is needed in order to make changes to a component of the XDS Affinity Domain that will affect other components (such as those that will cause component downtime, require configuration changes on other systems, or effect functionality).

Define how configuration settings will be disseminated among systems in the XDS Affinity Domain.

Define the rules for DNS management and system naming conventions. Make sure to mandate the use of appropriate host names and policies that will attempt to guarantee their continued use as hardware is upgraded and replaced over time. This is important because host names are used in the <location> part of Metadata URLs, and thus URLs can be broken if host names are not maintained over time.

Note that security related configuration should be defined in the appropriate sub-sections of 0

### **X.5.5 Addition of New Components**

Specify procedures for adding new components to the XDS Affinity Domain. Explain who is authorized to grant permission for new components to be added and how are they can be contacted. Define procedures for providing the necessary configuration and security information to the managers of components that will need to communicate with a new component.

Define rules for moving of systems, particularly XDS Repositories.

### **X.5.6 Data Retention, Archive, and Backup**

Define policies regarding the responsibilities for data retention, archive, and backup for the various types of components of the XDS Affinity Domain. For example, specify how long access to documents published to an XDS Repository of the XDS Affinity Domain must be maintained, and how long their data integrity must be guaranteed. State the backup requirements for the Repository.

### **X.5.7 Disaster Recovery**

Define disaster recovery practices for the various types of components of the XDS Affinity Domain. Define procedures to follow when disaster recovery is needed, and what notification must be provided in such cases.

## **X.6 Membership Rules**

### **X.6.1 Acceptance**

Define the types of organizations and individuals that can become members of the XDS Affinity Domain so that they will be permitted access to its components and data. Specify how they can apply for membership.

If there are any different rules for handling the membership of organizations and individuals whose physical location is considered part of another XDS Affinity Domain then define these here. For example, if the XDS Affinity Domain is defined for a specific geographic region, such as a Province or State, but an organization or individual located outside of this region wants to become a member. In addition, if there are any special rules for handling the membership of organizations and individuals who are already members of a different XDS Affinity Domain then define these here also.

### **X.6.2 Types of Membership**

Are there different types of membership that define how published data can be accessed (i.e. read-only, publish-only, etc.)? How will it be ensured that members are only permitted this type of access?

### **X.6.3 Membership Policies**

Define any rules regarding management of members status. How does an individual or organization apply to no longer be a member? How is the list of members maintained and distributed? Is the list of members public? If not then what is the policy regarding requests for access to this list? Handling of membership in multiple XDS Affinity Domains.

## **X.7 Connectivity to the XDS Affinity Domain from External Systems**

### **X.7.1 Interoperability Strategy**

The Policy Agreement shall identify the procedure for how to reach the data over the domain borders. There are many ways to bring this about and it is therefore very important that this is specified in the Agreement.

## **X.8 System Architecture**

In order to secure both information retrieval and publishing, the system architecture of the applications has to be specified and understood by all parties. The Policy Agreement shall therefore contain detailed information regarding the architecture of systems supporting the various Actor/Profiles, and the supported document types and publication policies.

### **X.8.1 Global Architecture**

The XDS Affinity Domain global architecture diagram should be offered in this section indicating the stakeholders and system actors.

### **X.8.2 Affinity Domain Actors**

A number of systems implementing IHE Actors defined in the XDS Integration Profile need to be identified and configured to communicate. This includes defining addressing information and ATNA Secured Node certificate:

#### **X.8.2.1 Registry**

Identify any specific requirements for a Registry Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.2 Repository**

Identify any specific requirements for a Repository Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.3 Document Source**

Identify any specific requirements for a Document Source Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.4 Document Consumers**

Identify any specific requirements for a Document Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.5 PIX Patient Identity Source**

Identify any specific requirements for a PIX Patient Identity Source Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.6 PIX Manager**

Identify any specific requirements for a PIX Manager Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.7 PIX Consumer**

Identify any specific requirements for a PIX Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.8 PDQ Source**

Identify any specific requirements for a PDQ Source Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.9 PDQ Consumer**

Identify any specific requirements for a PDQ Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

#### **X.8.2.10 Audit Repository**

Identify any specific requirements for an Audit Repository Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. Specify any requirements for security audit logs that go beyond those specified in the ATNA Profile.

### **X.8.3 XDS Affinity Domain Transaction Support**

Specify any details required for transactions within this XDS Affinity Domain.

#### **X.8.3.1 XDS Affinity Domain Transaction Diagram**

Define the transaction diagram for the XDS Affinity Domain. In particular, it is important to detail any optional transactions that the XDS Affinity Domain extensions now define as being mandatory.

#### **X.8.3.2 Cross XDS Affinity Domain Transaction Support**

Specify any details required for transactions from this XDS Affinity Domain to any components of another XDS Affinity Domain. Explain procedures for dealing with the use of different code sets. Also explain how to deal with the validity of assigning authorities for identifiers from external systems.

## **X.9 Terminology and Content**

### **X.9.1 Introduction**

If the IHE XDS Profile or XDS Content Profiles are refined in any way then describe this here. Typically the following types of refinements are made:

- XDS Affinity Domains can refine the use of many attributes of XDS Profile Transactions and attributes of the contents of the supported XDS Content Profiles. Frequently this involves restricting attributes to using certain defined sets of values, or mandating the manner in which the fields of an attribute’s data type are used. In the case of Metadata attributes, their values are explicitly defined as being “XDS Affinity Domain specific” by the XDS Profile itself.
- In addition, XDS Affinity Domains can refine the attributes of XDS Transactions or Content so they are required to be supported rather than optional as stated in the XDS Profile or the definition of the Content for the XDS Content Profile.

Such refinements must not break conformance with the XDS Profile or to the defined Content of the XDS Content Profiles being supported. For example, it is not acceptable to lower the requirement of an attribute to be optional when it is defined to be required for XDS Metadata or Content.

This introductory section explains any principle areas of terminology and content that are refined by the XDS Affinity Domain. In addition, if there is any overall philosophy followed in defining these then this should also be explained here.

For example if there is some overall way in which any object identifier value (i.e. for patient ids, practitioner id, etc.) must be created then this should be specified as part of the introduction to this terminology section.

#### **X.9.1.1 Common Rules for Identifier Construction (example)**

This terminology sub-section serves as an example of where general rules for constructing any identifier for this XDS Affinity Domain should be specified. For example, this sub-section could specify rules for creating OIDs to be used in this XDS Affinity Domain.

#### **X.9.2 XDS Registry Metadata**

Define all ways in which the XDS Affinity Domain refines Metadata attributes of an XDS Submission Set or an XDS Folder. It must specify any refinements to the way these attributes are used or to the sets of values that can be assigned to them. In addition, it may be useful for it to provide a translation to the language(s) of the XDS Affinity Domain of ITI TF-2: Table 3.14.4.1-6 Submission Set Metadata Attribute Definitions.

##### **X.9.2.1 Submission Set Metadata**

If the language used in the XDS Affinity Domain is not english and a translation of the entire IHE ITI Technical Framework has not been done then this section should provide a translation of the ITI TF-2: Table 3.14.4.1-6 Submission Set Metadata Attribute Definitions, to one of the languages. If more than one language exists in the XDS Affinity Domain then this entire section and its sub-sections should be repeated for each of these languages.

If a translation is not provided here then the following table should list all of the Submission Set Metadata Attributes from ITI TF-2: Table 3.14.4.1-6 whose use is refined in any way.

In either case, there should be a comment for each listed Attribute indicating if the use of the Attribute is refined in any way for the XDS Affinity Domain. If so then the comments must

indicate how this is done. Unless this can be explained very briefly then it should provide a link to a following sub-section that includes text describing how the attribute’s use is refined. For example, if the XDS Affinity Domain restricts an attribute so that it can only use a set of values that is not already specified in the XDS Profile, then this set should be specified in the sub-section for this attribute.

**Submission Set Metadata Attribute Definitions**

<b>XDS Document Entry Attribute</b>	<b>Refinement of Attribute</b>	<b>Source/Query (Bold and Underline if refined)</b>	<b>Data Type</b>
authorInstitution	<p>Provide a translation if necessary.</p> <p>Define whether or not the XDS Affinity Domain refines the use of this Attribute in any way. If not then it is not mandatory to list the attribute here. Otherwise, point to the sub-section of <a href="#">X.9.2.1</a> explains the refinement of this Attribute for the extension. If the Attribute is refined by defining a Source or Query value that is different from the Technical Framework (i.e. by requiring a value whereas it is optional in the Framework) then bold and underline the altered value and provide an explanation in the sub-section.</p> <p>Same applies for the remaining Attributes.</p>	R2/R	<p>Provide a reference to the sub-section of <a href="#">X.9.2.1</a> that specifies the list of permitted XON data type authorInstitution values for the of this attribute.</p> <p>For this example, “Refer to <a href="#">X.9.2.1.1</a> for the XDS Affinity Domain specification of this Attribute”.</p>

Create a sub-section for each Submission Set Metadata Attribute that is refined for the XDS Affinity Domain.

**X.9.2.1.1 Refinement of authorInstitution (example)**

This sub-section for the authorInstitution Metadata Attribute should state how the values for this attribute are specified for this XDS Affinity Domain.

For example, authorInstitution, has an HL7 Data Type of XON so the authorInstitution sub-section could specify the sets of permitted values for each field of the XON Data Type for authorInstitution.

**HL7 V2.5 Component Table – XON – for authorInstitution**

SEQ	DT	OPT	COMPONENT NAME	COMMENTS
1	ST	O	Organization Name	Specify whether or not the XDS Affinity Domain refines this component in any way for authorInstitution. If not then the comment "No Refinement" will suffice. Otherwise, point to the subsection of 0 that specifies how values for this component should be specified. If only a defined set of values should be used then this list should be specified. Same applies for each of the following XON components.
2	IS	O	Organization Name Type Code	—
3	NM	B	ID Number	—
4	NM	O	Identifier Check Digit	—
5	ID	O	Check Digit Scheme	—
6	HD	O	Assigning Authority	—
7	ID	O	Identifier Type Code	—
8	HD	O	Assigning Facility	—
9	ID	O	Name Representation Code	—
10	ST	O	Organization Identifier	—

#### **X.9.2.1.1.1 Specification of Organization Name component (example)**

This sub-section for the authorInstitution Metadata Attribute should state how the Organization Name component is specified for this XDS Affinity Domain.

#### **X.9.2.1.1.2 Etc.**

Sub-section for specification of each remaining XON Data Type component for authorInstitution.

#### **X.9.2.1.2 Refinement of Further Submission Set Metadata Attributes (example)**

Define a sub-section for each remaining Submission Set Metadata Attribute that the XDS Affinity Domain refines the use of. Explain how the value for each of these attributes must be specified. If a defined set of values should be used and this is not defined in the XDS Profile itself, then this list of values should be specified here.

#### **X.9.2.2 Folder Metadata**

If the language used in the XDS Affinity Domain is not english and a translation of the entire IHE ITI Technical Framework has not been done then this section should provide a translation of the ITI TF-2: Table 3.14.4.1-7 Folder Metadata Attribute Definitions, to one of the languages. If more than one language exists in the XDS Affinity Domain then this entire section and its sub-sections should be repeated for each of these languages.

If a translation is not provided here then the following table should list all of the Folder Metadata Attributes from ITI TF-2: Table 3.14.4.1-7 whose use is refined in any way for this XDS Affinity Domain.

In either case, there should be a comment for each listed attribute indicating if the use of the attribute is refined in any way for the XDS Affinity Domain. If so then the comments must indicate how this is done. Unless this can be explained very briefly then it should provide a link to a following sub-section that includes text describing how the attribute’s use is refined. For example, this could require defining the set of possible values that can be used for the attribute.

**Folder Metadata Attribute Definitions**

XDSFolder Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type
codeList	Provide a translation if necessary. Define whether or not the XDS Affinity Domain refines the use of this Attribute in any way. If not, then it is not mandatory to list the attribute here. If it is, then point to the sub-section of <a href="#">X.9.2.2 Folder Metadata</a> that explains the refinement of this Attribute. If the Attribute is refined by defining a Source or Query value that is different from the Technical Framework (i.e. by requiring a value whereas it is optional in the Framework) then bold and underline the altered value and provide an explanation in the sub-section. Same applies for the remaining Attributes.	R/R	Provide a reference to the sub-section of <a href="#">X.9.2.2.1</a> . Create a sub-section for each Folder Metadata Attribute that is refined for the XDS Affinity Domain. that specifies the list of codes that can be used to specify the type of clinical activity that resulted in placing the XDS Documents in an XDSFolder. For this example, “Refer to <a href="#">X.9.2.2.1</a> for the XDS Affinity Domain refinement of this Attribute”.

Create a sub-section for each Folder Metadata Attribute that is refined for the XDS Affinity Domain.

**X.9.2.2.1 Refinement of codeList (example)**

This sub-section for the codeList Folder Metadata Attribute should state how the values for this attribute are specified for this XDS Affinity Domain.

For example, the codeList sub-section could specify the set of permitted values (Code Value, Display Name, and Coding Scheme Designator):

**Permitted Clinical Activity codeList Values**

CODING SCHEME DESIGNATOR	DISPLAY NAME	CODE VALUE
—	—	—
—	—	—

### X.9.3 Supported Content

#### X.9.3.1 Supported Content Profiles

**Supported XDS Content Profiles**

Code	Comment
XDS-MS	Comment explaining if the XDS Affinity Domain has any guidelines or rules for this type of content beyond those defined in the ITI Technical Framework. If there are then a reference to a following subsection explaining these, or to another document that does this must be provided. Same applies for all listed XDS Content Profiles.
XDS-SD	—
XDS-I	—
XDS-BPPC	—

#### X.9.3.2 Document Content Specialization

This section should specify any specialization of attributes and terminology to be used in the actual document content. This should be only for those attributes that are not defined as being part for Metadata.

## X.10 Patient Privacy and Consent

### X.10.1 General Guidelines Regarding Document Access and Use

Specify the general guidelines to be followed regarding the access and use of medical information in the XDS Affinity Domain. The Privacy Access Policies (Informative) section of the IHE BPPC Profile provides several examples of the ways this can be expressed, such as the example table below:

**Access Control Policies**

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 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.

If access control policies are tied to specific user roles then an access control matrix should be specified here that links specific user roles to the types of documents that these users are permitted to access. The means for actually defining, and assigning these user roles should be specified in the 0 X.11.1.1 Role Management section.

## **X.10.2 Patient Consent**

The rules for patient consent have to be harmonized or agreements have to be defined on how differences shall be bridged when harmonization is not possible. Both parties shall agree to this in the Policy Agreement.

Patient privacy is a key issue in trans-border information exchange.

In order to gain a patient's full confidence with the information transactions it is of utmost importance that the rules are clear and easily understood by the patients.

### **X.10.2.1 BPPC**

Specify whether or not support of the IHE XDS Basic Patient Privacy Consents Content Profile is mandatory or not for systems connecting to this XDS Affinity Domain.

Define the rules for the use of BPPC in the XDS Affinity Domain. Refer to the IHE ITI BPPC Profile for a thorough discussion of these rules. Some examples of the rules to define are:

- Where are the set of common consent agreements going to be published.
- How are the Policy OIDs going to be distributed to and used by systems in the XDS Affinity Domain.
  - The configuration of the Document Consumers and Sources on the appropriate behaviours when specific consent OIDs are used or referenced.
  - Document Sources should select the appropriate OIDs when documents are published.
  - Document Consumers should enforce the policies associated with the OIDs when documents are queried and retrieved.
- Specify if on a patient by patient basis Consent documents will be published into the XDS Affinity Domain.
  - If Consent documents are published then specify whether “wet” signatures (thus requiring support for XDS Scanned Documents), or electronic patient consents will be used.
  - If “wet” signatures are used then specify whether or not the Scanned Documents must be digitally signed or not.
  - If electronic patient consents are used then define how the certificates are obtained for the patient digital signatures.
  - Note that in XDS Affinity Domains where implied consent is used, Consent documents are not likely to be published.
- Define all the conditions that can be used for defining a patient’s privacy consent (type of data, type of access, etc.).

### **X.10.3 Privacy Override Guidelines**

This section should specify those conditions (emergency mode, break-glass, system failure mode, etc) under which privacy restrictions can be over-ridden. This should specify any special procedures that must be followed and how such cases of privacy override must be documented and reviewed.

## **X.11 Technical Security**

This section details the technical aspects of security for the XDS Affinity Domain.

It is most likely that each domain will have its own security rules. It would be ideal of course if the involved domains can commit themselves to one and the same security model. This is the primary goal and the security standards defined in both CEN and ISO shall be the primary tools to achieve this.

If this is not possible it shall be specified in the Agreement which security level in one domain corresponds with which security level in another domain and authority for the users has to be designed for the various levels in both domains.

Refer to the “HIE Security and Privacy through IHE White Paper” for further details on the issues that should be considered when implementing an XDS Affinity Domain.

### **X.11.1 Authorization**

The authorization process shall be defined in the Policy Agreement both internally in the domain and externally in the other jurisdiction domains.

#### **X.11.1.1 Role Management**

Specify the Roles defined for users in the XDS Affinity Domain.

#### **X.11.1.2 Authentication of Users/Role**

Specify the minimal user and role authentication strength (password rules, 2-factor, certificates, etc)

##### **X.11.1.2.1 User/Role Certificates Management**

Specify how user authentication security certificates will be managed for the XDS Affinity Domain. For example, it should state which certificate provider(s) will be allowed and how the certificates can be obtained. It should also specify whether or not user certificates will also incorporate information regarding their role, etc.

#### **X.11.1.3 Attestation rights**

The Policy Agreement shall name the individuals in the organization who have the right to assign roles and attestation authority to employees. An employee with attestation authority has the right to attest medical information.

#### **X.11.1.4 Delegation rights**

Delegation is often necessary in daily operation. In order to be able to keep this under control delegation rights have to be specified in the Agreement since it is particularly difficult to know who has which rights inside and between the domains.

#### **X.11.1.5 Validity time**

Authorization, roles, attestation rights, delegation rights shall have a well defined and specified time period for the access rights to information both within the domain and across domain borders. These time periods shall be notified in the Agreement.

### **X.11.2 Node Authentication**

Specify what mechanisms of node authentication will be used.

#### **X.11.2.1 Node Certificates Management**

Specify how node security certificates will be managed for the XDS Affinity Domain. For example, it should state which certificate provider(s) will be allowed and how the certificates can be obtained.

### **X.11.3 Information Access**

How access to the information should be controlled in the XDS Affinity Domain, depending upon whether it is contained on a computer system, removable media, or being transferred over a network.

#### **X.11.3.1 Security Audit Log Access**

Specify how access to the security audit logs will be managed.

#### **X.11.3.2 Network Communication Access Security Requirements**

Specify the network access security requirements for the XDS Affinity Domain. Specify the means by which network communication security will be ensured (will all Transactions have to be secured by

#### **X.11.3.3 Node Access Security Requirements**

Specify the system node access security requirements. For example, whether or not all nodes must conform to the IHE ATNA Secure Node Actor/Profile.

#### **X.11.3.4 Removable Media Access Security Requirements**

Whether or not media transfer of XDS content is permitted as part of the XDS Affinity Domain, and if so what media security is required if any. For example, must the media itself be encrypted, or the individual files?

### **X.11.3.5 Agreement validity period**

The time period for which an access Agreement is valid shall be specified in the Agreement. The Agreement shall also include a clause defining the procedure for termination of the Agreement both at the end of the Agreement period and within the Agreement period. Legitimate reasons for cancellation of the Agreement shall be defined. Economic compensations for extra costs if the Agreement is cancelled between the agreed time periods shall also be defined in the Agreement.

### **X.11.4 Information Integrity**

The integrity of the data shall be checked in order to detect corruption of data during transfer between the domains. The rules and techniques for this shall be agreed upon and specified in the Policy Agreement.

#### **X.11.4.1 Network Communication Integrity Requirements**

How will integrity of data transmitted over a (cable or wireless) network within the XDS Affinity Domain be managed? What methods for checking this integrity should be used and whether it is mandatory or not for systems acting as specific Actor/Profiles.

#### **X.11.4.2 Document Digital Signature Requirements/Policy**

Is it necessary to digitally sign any of the content in order to ensure the lifetime integrity of the data, or to allow authentication of the identity entity that created, authorized, or modified the content.

#### **X.11.4.3 Document Update and Maintenance Policies**

Detail policies regarding the modification, reading, and deletion of documents in the following sub-sections:

##### **X.11.4.3.1 Correction Policy (Modify)**

##### **X.11.4.3.2 Update Policy (Modify)**

##### **X.11.4.3.3 Document Read Policy**

##### **X.11.4.3.4 Document Deletion Policy**

#### **X.11.4.4 Folder Policy**

Explain any XDS Affinity Domain specific policies regarding Folders.

### **X.11.5 Ethics**

The rules and regulations will never cover all possible situations. Therefore ethics have to be taken into consideration and a memorandum has to be formulated to give everybody a good understanding about the framework for responsibility that everyone has to work within.

### **X.11.6 Secure Audit Trail**

<Change to only talk about ATNA>

As mentioned above, all transactions shall be logged. In most cases this will be done using the ATNA Profile. The technology used and the extent of the logging, shall be specified. If some legacy systems of the Affinity Domain do not support ATNA then how will these be supported.

Specify whether or not ATNA Audit Record Repositories will be centralized or distributed. In addition, state whether or not they will be expected to support the following, and if so how:

- Filtering
- Reporting
- Alerting
- Alarming
- Forwarding to other Audit Record Repositories

### **X.11.7 Consistent Time**

In order to be able to ensure high quality logging, time stamping is necessary. All information transactions shall have a time stamp. Specify how support for the IHE Consistent Time Profile will be implemented, and who will be responsible for providing Consistent Time servers. This may require substantial reprogramming of older system and therefore may not possible for economical reasons. In this case the parties signing the Agreement shall decide what can be done under existing circumstances and what measures shall be taken for improving the situation. An implementation plan is part of the Agreement.

### **X.11.8 Audit Check**

The agreement shall stipulate when, by whom and how the log files shall be checked and appropriate action taken.

### **X.11.9 Risk Analysis**

If risks are observed all parties have jointly to evaluate them and decide whether the risks can be accepted or not. The risks have to be documented in the Policy Agreement. If the risks can be accepted all parties shall approve it. If the risks are not acceptable a plan detailing resource requirements for risk reduction shall be included in the Policy Agreement.

What will the frequency of risk assessments be? Is recommended that they be done at least on an annual basis.

### **X.11.10 Future system developments**

The Policy Agreement shall commit all parties to develop their future system according to this and other accepted standards in order to facilitate future co-operation for information transfer between their systems.

All these functions shall be specified in the Policy Agreement. The standardized layout of the Policy Agreement is described in Annex B of this document and shall be used as a guide when Policy Agreements are established.

All information exchange functions have shall be specified in the Policy Agreement.