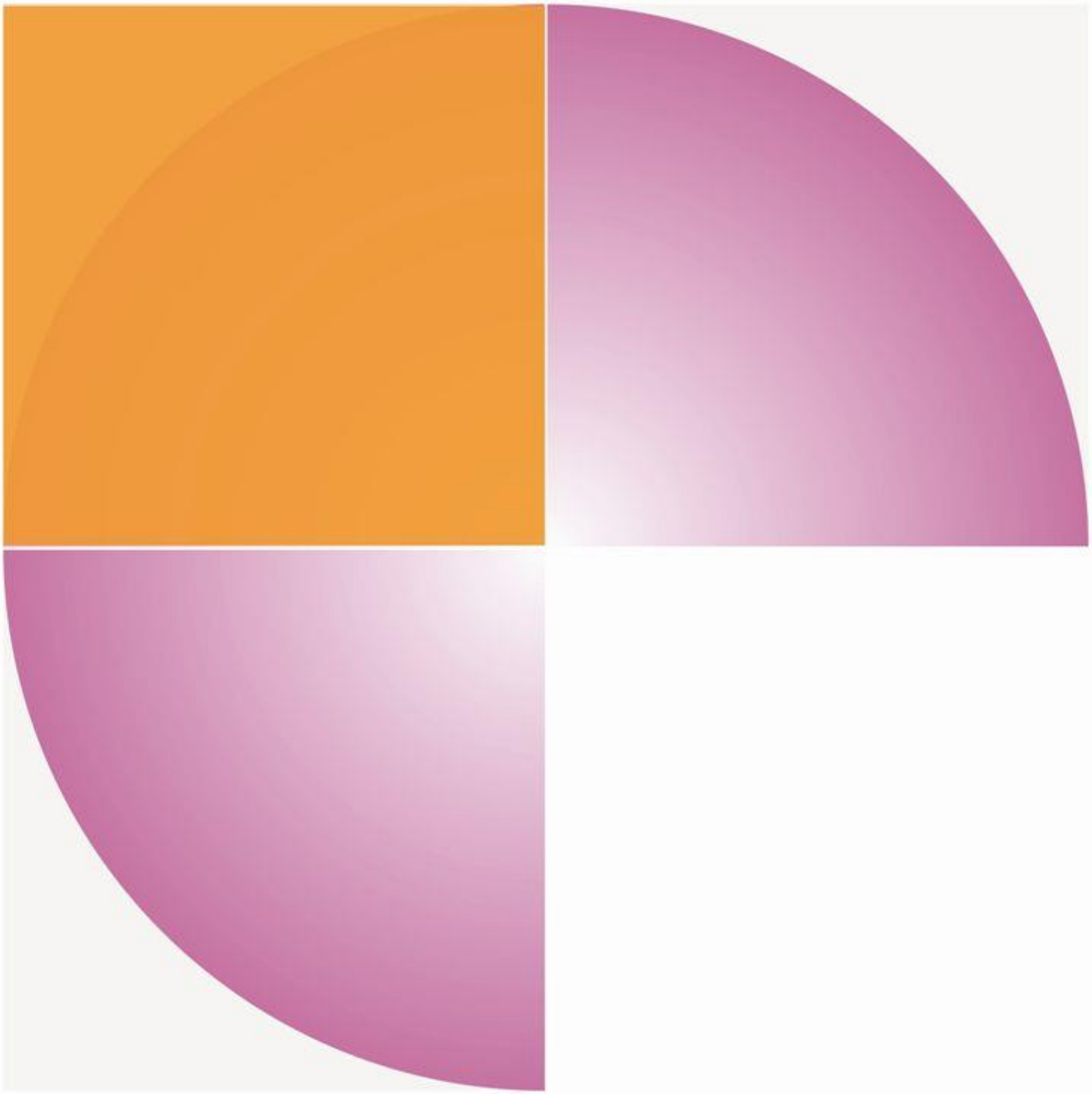
Guide to Interoperability between XDS Affinity Domains 2015

INTEROPERABILITY

Better healthcare
through better IT

Nictiz



Guide to Interoperability between XDS Affinity Domains 2015

INTEROPERABILITY

Better healthcare through better IT

Nictiz

Date

21 July 2015

Original title: “Handreiking Interoperabiliteit tussen XDS Affinity Domains”

Version: 0.9 (draft)

Authors

Vincent van Pelt (Nictiz)

Robert Breas (MedicalPHIT)

GERRIT

UPZuid

Stichting RijnmondNet Zorg door communicatie

ZorgNetOost

sleutelnet

EZDA Amsterdam

SDSK Digitale Snelweg Kennemerland

Betere zorg door betere informatie Nictiz

rzcc

Stichting Transmurale Zorg Den Haag en omstreken

Zorgnetwerk Midden-Brabant

Foreword

The *Guide to Interoperability between XDS Affinity Domains* is the result of an ambition of the Regional Cooperation Organisations (RCOs) in the Netherlands to facilitate the secure, reliable and interoperable exchange of medical images and documents between different XDS infrastructures and Affinity Domains. In the Netherlands there are more than 10 regional organizations who use XDS infrastructures for sharing images, reports, letters, summaries, assignments, workflows and other patient-related information between healthcare organizations within these XDS infrastructure. But since patients have a tendency not to stay within regional boundaries, there is a real need for the exchange of medical information between different XDS infrastructures. IHE has defined a profile for the connection and seamless accessability of information from other XDS infrastructures, Cross-Community Access (XCA). However, more agreements have to be laid down, at all levels of interoperability, to enable truwe interoperability between these different XDS Affinity Domains. guarantee things like a comparable degree of security, the uniform approach towards the recording of patient consent, compatible metadata, reliable infrastructures and controllable quality of information transfer in each region.

The *Guide to Interoperability between XDS Affinity Domains* consists of an extensive set of principles, preconditions, agreements, guidelines, methods and sample contracts, which can be used by the regional organisations to set up their organisation and infrastructure. It has been laid out as a *'cookbook'* for organising XDS Affinity Domains. The Guide forms the basis for verifiable quality of XDS infrastructures in the Netherlands.

Revision management

Version	Date	Author	Details	Status
0.1	6-6-2014	Robert Breas	First concept version	Concept
0.2-0.4	27-6-2014	Robert Breas Vincent van Pelt	Addition 1.1, 1.2, 1.3.2, 2.4, 2.5, 2.6, 2.7, 2.8 addition of appendices, textual changes	Concept
0.5	20-7-2014	Vincent van Pelt, Robert Breas	Version for review by the Regional Platform	First Concept for comments
0.6	7-11-2014	Robert Breas, Vincent van Pelt	Version for review by Interoperability Workgroup	Concept
0.7	1-12-2014	Robert Breas, Vincent van Pelt	Version for review by RAP (Regional Architecture Platform)	Concept
1.0	26-01-2015	Robert Breas, Vincent van Pelt	Version after input from: • Haga Ziekenhuis • Medisch Centrum Haaglanden • St. RijnmondNet • UP Zuid • Vivia • ZMBR	Concept
1.1, 1.2	11-02-2015	Robert Breas, Vincent van Pelt	Version after extra input from: • EZDA • St. Gerrit • RZCC	For approval by the workgroup
1.3	19-06-2015	Vincent van Pelt	Version after input from suppliers	Concept
1.4	15-07-2015	Vincent van Pelt	Textual changes	Definitive

Please contact Nictiz Interoperability Project Leader Vincent van Pelt if you have any questions, comments or additions.

Table of contents

Table of contents 6
1 Introduction to the Guide 9
1.1 Introduction 9
1.1.1 Questions 11
1.1.2 Assignment 11
1.1.3 Objective 11
1.1.4 Target group 12
1.1.5 Guiding principles 12
1.1.6 Use of international open standards and profiles 12
1.1.7 Expected advantages of the Guide 13
1.1.8 Further development of the Guide 14
1.2 Background Information 14
1.2.1 Interoperability – Agreements at several levels 14
1.2.2 Exchange within Affinity Domains - XDS 19
1.2.3 Exchange between Affinity Domains - XCA 22
1.3 Explanation of the agreements in the Guide 28
1.3.1 Governance, organisation structure 28
1.3.2 Security and privacy 29
1.3.3 Legislation and regulations 31
1.3.4 Policy organisation 34
1.3.5 Work processes 34
1.3.6 Information 37
1.3.7 Applications 39
1.3.8 Infrastructure 41
2 Interoperability Agreements between Affinity Domains 2015 43
2.1 Governance-level Agreements, Organisation Structure 43
2.1.1 Governance 43
2.2 Security and Privacy-level Agreements 44
2.2.1 Security 44
2.2.2 Privacy 47
2.2.3 Safety 48
2.2.4 Certificates for communicating systems 48

2.2.5 Certification 48
2.3 Legislation and regulation-level Agreements 48
2.3.1 Legislation – Medical Treatment Agreement Act, Personal Data Protection Act, Use of Citizen Service Number Act 48
2.3.2 Standards – NEN 7510, 7512, 7513 49
2.3.3 Guidelines - Electronic Data Exchange in Healthcare 49
2.4 Policy organisation-level Agreements 50
2.4.1 Framework agreement / Covenant 50
2.4.2 Data processing agreement 50
2.5 Work process-level Agreements 50
2.5.1 Notification when new data becomes available 50
2.5.2 Support of multi-disciplinary workflow 50
2.5.3 Logging and monitoring 51
2.6 Information-level Agreements 51
2.6.1 XDS Metadata 51
2.6.2 Value lists in the XDS metadata set 52
2.7 Application-level Agreements 52
2.7.1 Use of standards and profiles 53
2.7.2 Actors and transactions to be used (IHE) 53
2.7.3 Configuration for exchange within an Affinity Domain 53
2.7.4 Configuration for exchange between Affinity Domains 53
2.7.5 Patient ID 53
2.8 Infrastructure-level Agreements 54
2.8.1 Affinity Domain network 54
2.8.2 Network design 54
2.9 Standard and profile Agreements, certification 54
2.9.1 Standards and profiles, certification 54
2.9.2 Administration and support 54
2.9.3 Tests 56
2.10 Dot on the horizon 57
2.10.1 Use of standards and profiles 57
2.10.2 Additional dots 57
3 Appendices with sample documents 59
3.1 Governance Level, Security and Privacy 59

3.1.1 Object Identifiers of organisations 59
3.1.2 Applying for an UZI Pass 59
3.2 Legislation and Regulations Level 59
3.3 Work Processes Level 59
3.4 Information Level 59
3.4.1 BPPC Policy Object Identifiers 59
3.5 Application Level 59
3.5.1 Overview of IHE actors and transactions used 59
3.5.2 Overview of IHE actors and transactions per Affinity Domain 62
3.6 Infrastructure Level 62
3.6.1 IDs, Affinity Domains and healthcare institutions, services (example) 62
3.6.2 IP numbers matrix, firewall settings, clients (example) 63
3.6.3 Application Entity Titles (AET) table 63
3.7 Implementation Level, administration and support 64
3.7.1 Tests 64
3.7.2 Tests on Connectathon 64
3.7.3 Central infrastructure tests 65
3.7.4 Technical tests 65
3.7.5 Functional tests 66
3.7.6 Acceptance tests 66
3.7.7 Operational test 67
3.7.8 Implementation of roadmap 67
3.8 Steps for plan of Approach for implementation 67
4 General appendices 70
4.1 Glossary 70
4.2 Concise explanation of IHE profiles 71
4.3 Landscape of regional infrastructures in the Netherlands 73

1 Introduction to the Guide

Reading guide

This is version 1.4 of the ***Guide to Interoperability between XDS Affinity Domains****.*

A number of other documents are also referred to within this document, sometimes via hyperlinks.

The Guide to Interoperability between XDS Affinity Domains consists of the following chapters:

- ***Chapter 1.1*** *contains a definition of the problem, assignment, objective and principles for the Guide.*
- ***Chapter 1.2*** *describes relevant aspects concerning (interregional) interoperability and an explanation of the XDS and XCA IHE profiles.*
- ***Chapter 1.3*** *is an explanation of the agreements set out in detail in Chapter 2. Knowledge of the content of these chapters is required to be able to understand and apply the agreements.*
- ***Chapter 2*** *describes the agreements themselves, arranged in the same order as in the interoperability model.*
- ***Chapter 3*** *consists of appendices with sample documents and templates, arranged in the same order as in the interoperability model.*
- ***Chapter 4*** *contains general appendices such as an explanatory glossary.*

1.1 Introduction

In various regions in the Netherlands, so-called Regional Cooperation Organisations (RCOs) have been set up by cooperating healthcare institutions in order to exchange medical information. These RCOs provide reliable infrastructures on which this information (images, documents) can be shared; this is often done by using various technical infrastructures.
An increasing number of RCOs provide an infrastructure for exchanging images and documents based on XDS (Cross-enterprise Document Sharing). XDS is one of the 'profiles' which has been set up by IHE (Integrating the Healthcare Enterprise). A profile describes the preconditions which an application has to comply with to be able to exchange information in a standardised way with other profiles. Different suppliers can build applications on the basis of the profile requirements, which, as a result, are always able to communicate with each other.
RCOs that use XDS can also exchange information with each other, even when the infrastructures come from different suppliers.
In the first place, it is mainly hospitals that use the possibility to exchange information. However, more and more different healthcare organisations, such as radiotherapy centres, laboratories, GPs, chemists, paediatric healthcare (JGZ), mental healthcare (GGZ), nursing homes, residential homes and home care organisations (VVT), are also following suit. Patients will also be able to gain access at a later stage to images and documents via XDS infrastructures.

An XDS infrastructure makes it possible for healthcare institutions to exchange medical images and documents within a so-called *Affinity Domain*. An Affinity Domain can be seen as an environment /

infrastructure within which medical information can be shared quickly and securely. An XDS Affinity Domain makes it possible for all affiliated healthcare institutions to access information which has been registered in the network.

One of the advantages of this standardised architecture is that solutions by different suppliers are able to interact automatically, because the components which make up the infrastructure work according to standard communication protocols. In addition, XDS is a profile which is used throughout the world to set up similar infrastructures.

During the setting up of an Affinity Domain, all kinds of agreements are made between different participating healthcare organisations, and with the RCO which takes care of (the smooth operation of) the infrastructure. These include legal, management, organisational, logistical healthcare, medical and technical agreements. These agreements are laid down by the participating health institutions, usually in cooperation with an RCO, and include a number of principles, contracts, guidelines, sample contracts and connection requirements. These must be adhered to by the parties which exchange information within the Affinity Domain. A secure and reliable environment for sharing medical images and documents emerges within an Affinity Domain on the basis of these mutual agreements.

Interregional exchange– the problem
Information also needs to be made accessible when patients receive care outside their own region, and it then becomes necessary to connect several Affinity Domains. This has led to the development of the IHE profile XCA (Cross-Community Access), by which Affinity Domains can be linked to one another in a standardised way. This allows for cross-affinity domain acess to medical documents. However, when several Affinity Domains become linked together, a new problem arises as the affinity domains may be organised in different ways. Although many issues have been laid down in the XDS profile description, there are issues that the IHE does not mention, partly because they may be organised differently in different countries, for instance due to legislation and regulations. IHE profiles are implementation guidelines, but they still allow for a large degree of freedom, resulting in possible differences in the final implementations of the XDS infrastructures. In a situation in which several Affinity Domains have to be interoperable, the degree of freedom should be limited and overarching agreements should be made.

But the setting up of an Affinity Domain entails more than just the technical side. Agreements must be made on how the legal liability, responsibilities, governance, access control, malfunction procedures, arrangement of metadata and so forth should be organised between the regions / Affinity Domains as well. If this is not organised properly, it can lead to security and quality problems.

Interregional exchange – the solution
By laying down the agreements at all interoperability levels, XDS networks can be organised according to the same rules. As a result, the different Affinity Domains can rely on a standard level of quality and security.

An elegant way to achieve reliable and secure interregional exchange is to lay down a common set of principles, agreements, sample contracts, configurations and templates for all levels of interoperability, which have to be used by all the Affinity Domains: interoperability between systems consists for a large part of uniform organisation within the systems. As a result, exchanging patient details is no longer bound to only one particular Affinity Domain, and XDS becomes scalable.

This document, the *Guide to Interoperability between XDS Affinity Domains,* is a first version of this common set of agreements. It has come about by the Interoperability Workgroup of the Regional Architecture Platform commissioned by the Regional Platform, a network of the Regional Cooperation Organisations (RCOs) in the Netherlands. It forms the practical basis for the development of a secure and efficient exchange of medical information within and between XDS networks and for a verifiable quality assessment of the networks.

1.1.1 Questions

The RegioPlatform has formulated the following questions:

→ Which agreements have to be made at management and organisation level between XDS Affinity Domains to be able to guarantee interoperability and the secure exchange of data?

→ How can we arrive at a common and broadly supported set of agreements, methods and contracts, which is used by all the regions to design their infrastructure?

→ Which set of agreements are required between all the Affinity Domains in the Netherlands for a comprehensive Dutch (XDS) infrastructure to emerge?

1.1.2 Assignment

The RegioPlatform has commissioned the development of a common, overarching set of principles, preconditions, agreements, guidelines, methods and sample contracts, which can be used by the regional organisations to design their organisation and infrastructure in order to achieve a consistent, coherent and secure exchange of medical information between different XDS Affinity Domains. The Regional Architecture Platform has formed a workgroup for this purpose, the Interoperability Workgroup, which has executed this assignment. The Interoperability Workgroup consists of members of the Regional Architecture Platform and of Nictiz (National IT Institute for Healthcare in the Netherlands).

1.1.3 Objective

With the project 'Guide to Interoperability between XDS Affinity Domains', the Interoperability Workgroup has set itself the objective of compiling a document in which interoperability between XDS networks (based on IHE profiles) can be realised in an unequivocal way.

The Guide forms the basis of a verifiable set of connection requirements that an Affinity Domain needs to meet. It may be used as a quality criterion of an XDS Affinity Domain itself, and for the design of an interregional infrastructure.
The Guide is not a statement of requirements as such, but it can form the basis for this.

1.1.4 Target group

This document is meant for executives, managers, information architects, analysts and technicians who are involved in setting up, designing and /or maintaining XDS Affinity Domains. As the Guide highlights management, organisational, healthcare and technical aspects, this document can be consulted by several target groups. Nictiz's multi-layer model is used for the arrangement of chapters and provides an overview of the different parts of the document. It also points out that to set up an XDS Affinity Domain, cooperation between different parties with different expertise is needed and that attention should be paid to this on all interoperability levels.
An integral and multidisciplinary approach is needed for the implementation to succeed.

1.1.5 Guiding principles

This document has been compiled on the basis of the following guiding principles:

- Interoperability between XDS Affinity Domains can be best guaranteed when the XDS Affinity Domains use the same agreements for their design. For this purpose, a common set of connection requirements and design principles must be laid down in a document.
- For information exchange between different Affinity Domains, agreements must be made on several organisational levels. The Nictiz interoperability model is used as the basis for this.
- The agreements are formulated at the initiative of and in cooperation with the participating parties.
- The agreements should use open, international standards and profiles which have been proven in practice as much as possible.
- Each participating organisation is responsible for its own Affinity Domain.
- New agreements with regard to exchanges between Affinity Domains should be made at the level of the participating RCOs (or other administrators of the Affinity Domain).
- This document serves as a design principle for an RCO (or other Affinity Domain administrator) for an Affinity Domain and for an interoperable exchangeability with other XDS Affinity Domains.

1.1.6 Use of international open standards and profiles

One of the guiding principles is the use of open, internationally accepted standards and profiles. This has a number of advantages:

- Quality – Standard Developing Organisations (SDOs) provide an opportunity to record information in an unequivocal way. Above all, the SDOs often make standardised quality assessment and certification possible.

- Security – in solutions based on standards, it is also possible to organise the security in a uniform way by laying down uniform agreements and using special integration profiles set up for this purpose.
- Reusability – standardised parts / modules can be used for several purposes and in several countries.
- Efficiency – combining international standards and profiles makes it possible to use work which is carried out internationally.
- Sustainability – combining and using international initiatives.
- Scalability – many SDOs provide a range of connected functionalities with which healthcare ICT can be supported. International standardisation also makes it possible to use international software, and to realise communication across borders.
- Controllability – the possibility of standardised testing and the awarding of quality hallmarks.
- Freedom of choice – software based on profiles and standards can be procured from different suppliers – less chance of vendor lock-in.
- Future-proof – broadly supported, international and open standards and profiles ensure continuity of the solution, and make it possible to benefit from further international development of these standards and profiles.

1.1.7 Expected advantages of the Guide

The *Guide to Interoperability between XDS Affinity Domains*:

- Is the result of a request from the RCOs themselves; because of this there is broad support.
- Forms a practical implementation guide for XDS Affinity Domains at all levels of interoperability. It forms the basis of agreements between Affinity Domains on design and configuration. This increases the quality and consistency of the systems.
- Makes use of existing international standards and profiles, as well as laying down sections at national level. This prevents confusion and 'local' solutions, which better guarantees the quality of the solution.
- Makes better agreements between suppliers and system designers possible. By referring to the Guide, long specification routes no longer need to be followed, consistent quality levels develop and there is a possibility of realising new functionalities on the basis of the same infrastructure (request pooling).
- Makes procurement transparent, verifiable and ensures clear agreements. By employing a standardised approach, lower implementation and running costs are realised.
- Forms the basis of a verifiable quality assessment of the different XDS infrastructures.
- Sections of the Guide can be introduced internationally in the long term (such as the design of the XDS metadata), making broader support and joint development possible.

1.1.8 Further development of the Guide

This is the first version of the Guide, in which the basic conditions for interoperability between XDS Affinity Domains are laid down. These conditions will be expanded upon and refined in the following versions, which will be published on a yearly basis.

1.2 Background Information

In this chapter, a number of relevant aspects concerning the concept of interregional interoperability are discussed.

1.2.1 Interoperability – Agreements at several levels

The term 'interoperability' is comprehensive. It describes all measures which need to be taken, by several stakeholders, to achieve secure, reliable and efficient exchange of information. One of the definitions of interoperability:

> Interoperability is the possibility of different autonomous, heterogeneous systems, equipment or other units (for example organisations or countries) to communicate with one another and interact. In order to achieve this, standards, protocols and procedures are needed to harmonise the different entities. (Wikipedia)

Interoperability is a concept which is often interpreted by different parties from their own perspective, and, as a result, they often do not realise that other organisational and knowledge levels are necessary for a successful implementation.

1.2.1.1 Model for Interoperability

The Nictiz multi-layer model has been set up in order to gain a good insight into different aspects which are relevant when setting up interoperability between systems. The multi-layer model, which has meanwhile also been adopted at European level[1] as the standard model (eHealth Network[2]), shows different areas of attention which are involved when creating interoperable systems. Different designs and models are possible, but this model avoids technical terms and makes it clear that agreements have to be made on and between all levels, and that there has to be harmonisation between all the parties involved.

[1] Antilope – see http://www.antilope-project.eu/wp-content/uploads/2013/05/D1.2a-Educational-material-presentation-v1_4.pdf
[2] eHealth Network – see http://ec.europa.eu/health/ehealth/docs/ev_20151123_co03_en.pdf

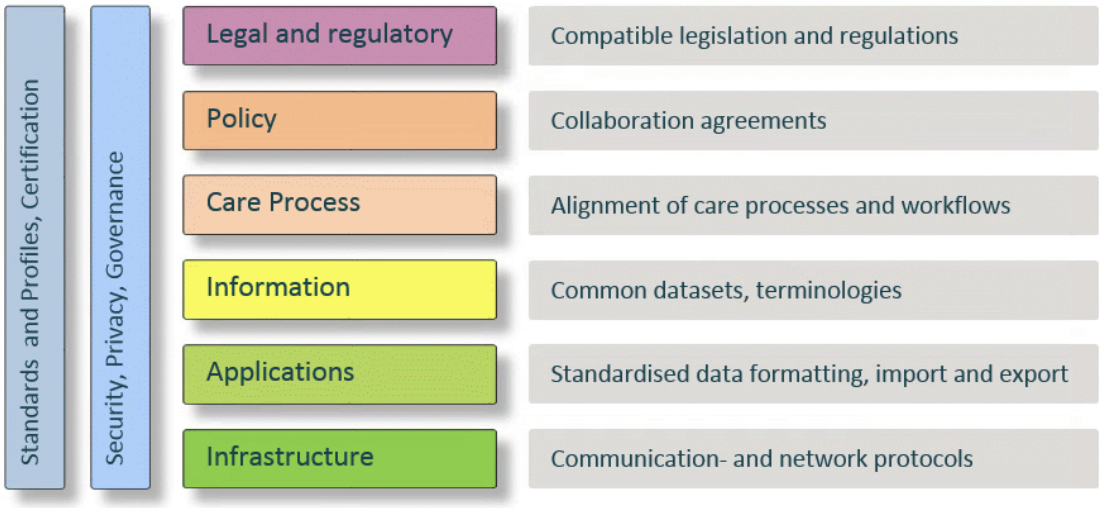


Figure 1 - Antilope and eHN interoperability model

In the figure below, the different stakeholders are indicated at the different interoperability levels they are involved in:

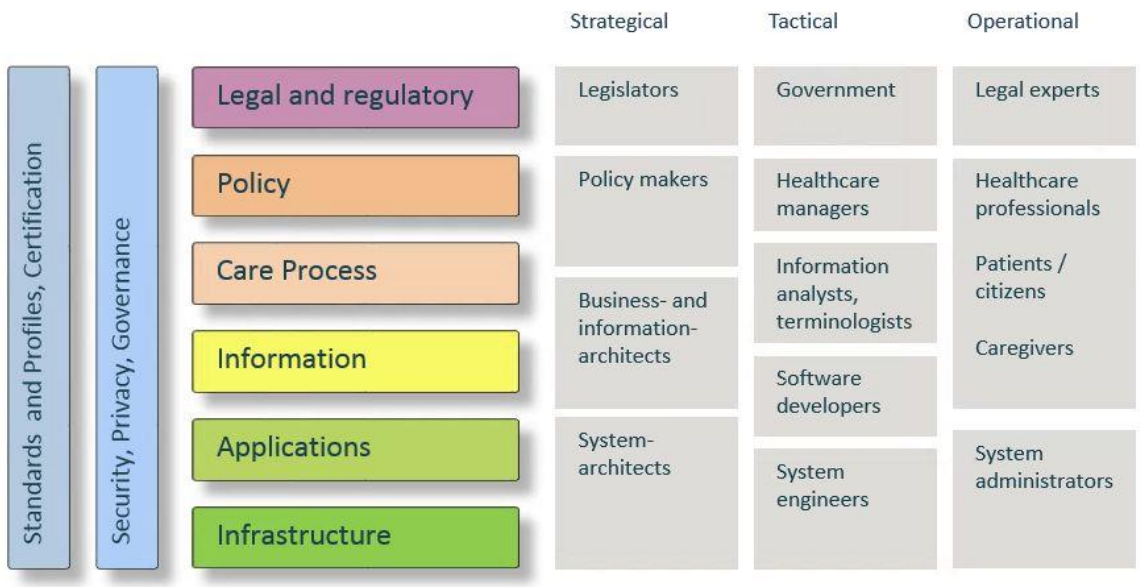


Figure 2 - Interoperability – different stakeholders

The different interoperability levels of the model are described briefly below:

Legislation and regulatory
Legislation and regulations indicate the limits which apply to the exchange of medical information. Agreements are made at this level on the interpretation of the relevant legislation and regulations. This mainly concerns laying down the agreements on the implementation of the legislation and regulations (in a number of design principles). At an international level, this layer is used to harmonise legislation and regulations in different countries.
NB: as the legislation and regulations are the same for all parties in a country, this layer is often left out for local, regional and national projects, particularly in projects in which the legislation and regulations play a smaller role.

Organisation policy
In this layer, agreements are made at management level between cooperating organisations: organisation of the governance, cooperation contracts, framework and data processing agreements, as well as agreements on privacy and security, patient consent, uniform design of the infrastructure and so forth.

Healthcare processes
Harmonisation and cooperation are vital in every healthcare route, but in particular in integrated care, multidisciplinary treatment teams and other partnerships. An overview of the patient's whole healthcare route, insight into the status of the process, and access to the results generated by different healthcare institutions and healthcare professionals, improves the quality and efficiency of the healthcare. In this layer, logistical aspects of healthcare are organised: How medical staff keep each other informed on the progress of the healthcare process, which information is generated, and what the following steps are. In short: how one gains an insight into the whole healthcare process, as well as into the information that is generated at different locations in the process. Processes are analysed at this level and we look at how parts of the process can support each other more efficiently. At this level, use cases are described, workflows are defined, information transfer is harmonised and insight into the logistical processes of healthcare is made possible.

Information
At this level, the information to be transferred is given a functional description. This means that healthcare professionals indicate which information elements at the very least need to be exchanged and to which level of detail. The possible values which may be assigned to a particular term are also laid down here. Although information can be transferred as free text, it is desirable to structure and code the information to be transferred, both for recording information at source and - when exchanging information - for viewing and importing it by the recipient party. By structuring (part of) the information, it can also be imported by the recipient ICT systems if required. For this to be done, agreements have to be made on the following matters:

- Dataset - Which information is transferred in a structured way? And which data elements and value lists are used for this?

- Terminology – this couples the terms, and the values they may hold, with standardised terms (terminology). In principle, this enables systems to 'understand' which terms and values are concerned. Coded terms can for example be coupled to translation tables, decision support systems and so on.

When transferring information, more and more use is made of standardised, generic data blocks (see also healthcare information building bricks), which can be used in different combinations as standardised sections to fill in a transfer document or message, along with the more specific information which is often transferred as text.

Functional specifications are laid down at the Information level. These form the basis for the technical specifications, which are described at the Application level. This disconnects the generic specifications from the technical 'packaging' of the information.

Applications
At this level, agreements have to be made within both the delivering and recipient organisations regarding the integration of various applications between which information is exchanged. Agreements on the technical exchange format of the information to be transferred (such as HL7 CDA, FHIR or other formats) determine how the information to be transferred is structured. ICT systems on the recipient side can import the structured data elements automatically into their own system through a mutually agreed-upon format in which the information is 'packaged'.
In addition, at this level, agreements on system configurations and, if necessary, on the user interface, are laid down.
Which data in a document or message is transferred depends on the context, including, for example, a transfer document, dismissal letter, medication overview, multidisciplinary meeting, patient summary, et cetera. The context therefore determines the packaging format (application layer), while the content of the healthcare information building bricks remains the same in as far as possible (information layer).

Infrastructure
The technical infrastructure determines in what way the information systems involved exchange data. This layer takes care of the infrastructure for the communication between systems in the different healthcare organisations. At this level, agreements are laid down on the design of the infrastructures, networks, IP numbers, SAML tokens and other parts which connect the systems with one another technically. In this layer, the XDS networks can be found, for instance.

1.2.1.2 Governance

One of the most important characteristics of an Affinity Domain is that use is made of a single index (Registry in XDS terms) from where all available documents can be accessed. The management of this Registry and the systems that go with it (for example for logging, security, patient consent and so forth) lies in the hands of a single party. In many cases, an RCO will be the logical party to run and exploit these central components, but a healthcare institution or a specialist organisation can also play

this role. For exchange between Affinity Domains, agreements need to be made at this level. The governance concerns the organisation, the management and the maintenance of the systems.

1.2.1.3 Security, privacy

Security and privacy are organised on several levels; this is shown by the fact that this bar is vertical. Among other things, it concerns agreements on the legislation to be followed, norms and guidelines, the protection of information which the patient has not released for exchange, the quality of the information itself, transfer of information, the security of the information itself (encryption) and the security of communication lines and the ICT systems. The patient's consent is also relevant here, in whichever way and at whatever level of detail.

1.2.1.4 Certification of standards and profiles

Agreements on the standards and profiles to be used (implementation manuals) must also be made on several levels of interoperability. The diagram below gives an illustration of the different organisations, standards and profiles which can be used at different levels of interoperability.
NB: Besides this, the selection of standards and profiles to be applied depends on the use case which has to be supported: in nursing, different specialism standards are used than in cardiology, surgery, radiology et cetera.

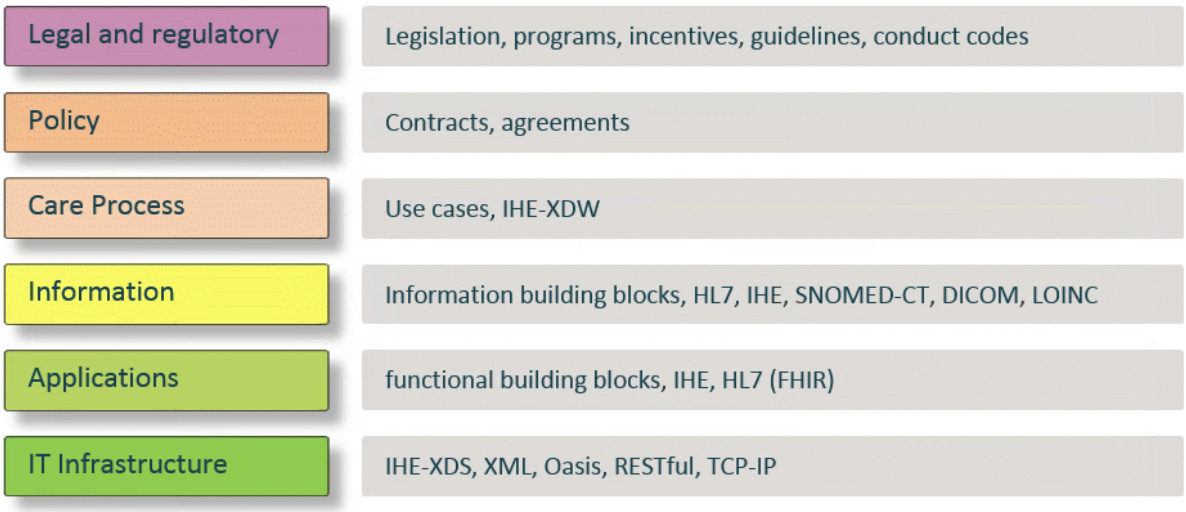


Figure 3 – Interoperability – examples of use of standards and profiles

By using standards and profiles, it is also possible to use standardised test possibilities, which are provided by standardisation organisations like IHE and Continua Health Alliance (CHA). This means the quality of testing, and the possibility of certifying parts of the software is better organised.

The testing and certifying is dealt with at this level.

NB: The vertical layers are often left out because implicitly they are considered to be part of every layer.

1.2.2 Exchange within Affinity Domains - XDS

1.2.2.1 Organisation

On the XDS page of the IHE Wiki-site, a definition of an Affinity Domain is given: "*An XDS Affinity Domain is a group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure*." This emphasises that when an Affinity Domain is set up, there has to be a willingness to cooperate in the first place.

In practice, an XDS Affinity Domain often consists of cooperating healthcare institutions in a certain region, in cooperation with an RCO (Regional Cooperation Organisation) which designs the shared infrastructure.
An Affinity Domain can be organised at different levels:

- Local (within a hospital or a group of merged hospitals)
- Regional (several healthcare institutions within a certain geographical area)
- National (there are currently no examples of this)
- Specialist (concerning a certain illness or certain functionality).

An example of a specialist network is the Dutch breast cancer screening programme, MammoXL.
This XDS Affinity Domain is specifically designed to exchange data on breast cancer screening and is organised nationally.
In addition, other initiatives may design XDS Affinity Domains for a specific functionality, such as an infrastructure for Multidisciplinary Consulting. XDS infrastructures can therefore be organised on several organisational and geographical axes.

1.2.2.2 Technology - XDS

The exchange of medical images and documents between healthcare institutions by regional networks has increased in recent years and is rapidly spreading. The infrastructure used for this regional exchange is **XDS** (Cross-enterprise Document Sharing), an infrastructure based on open and international standards which are defined by the IHE.

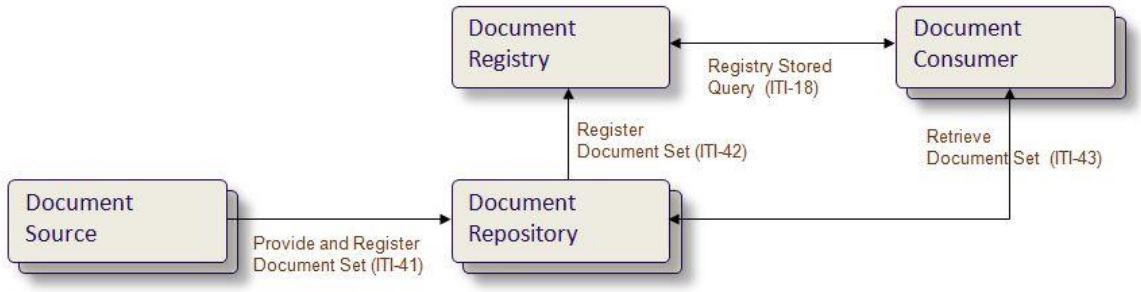


Figure 4 - XDS flowchart: actors and transactions

XDS defines *Transactions* (formal interfaces, message exchanges) between *Actors* (functional modules), using already existing standards. So XDS is not software, but a set of implementation guidelines which is used by different suppliers to build modules which can communicate with each other because of their predefined message patterns (transactions). This means that a Document Source from supplier A can exchange information with a Document Repository from supplier B, et cetera. This results in a standardised, supplier-independent environment.

The way XDS works is described as follows:

Saving documents: a **Document Source** (for example an application in a department where additional research is carried out) sends a document which has just been generated (image, report etc.), along with the metadata that goes with it, to a **Document Repository** (storage environment for images and/or documents) [ITI-41, see figure 4].
The Document Repository saves the file, and then sends the metadata (with its own additional metadata on how the file can be retrieved) to the **Document Registry** [ITI-42]. The Document Registry consists of a central index in which this metadata is saved.

Retrieving: the **Document Consumer** asks the Document Registry which files on a particular patient are available [ITI-18]. The Document Registry sends a list back with the available documents from all the affiliated locations. The user of the Document Consumer then chooses one of the files from the list, after which the Document Consumer requests the chosen document from the Document Repository [ITI-43], and then shows it to the end user.

A few comments:

- In an XDS infrastructure, there is always only one Document Registry. All other Actors can occur several times. Therefore, Storage can for example take place at several locations and on several servers; this is what makes the system so flexible. Document Consumers can be installed in different systems (such as Hospital Information Systems, Personal Heath Records).
- The different Actors in an XDS infrastructure are defined in such a way that they can come from different suppliers. As the communication between Actors is registered in Transactions, all parts of the system can communicate with one another in an unequivocal way.
- XDS is *content-agnostic,* which means that, in principle, every type of document can be stored depending on the functional or technical type, the file format, the content of the document, or the objective.

- During the implementation of the XDS profile, there are two IHE profiles which have to be implemented obligatorily: ATNA (Audit Trail and Node Authentication) and CT (Consistent Time).
  ATNA is a profile with which all activities on the XDS infrastructure are logged (which person from which institute searched and/or viewed which data when).
  CT is a synchronisation protocol that allows different systems to be used at the same time.

XDS-i – exchange of images

Although XDS is suitable in principle for all kinds of files, an extension has been defined on XDS for exchanging images, XDS-i (XDS for Imaging). This takes specific characteristics of the DICOM standard into account. The flow chart below shows the Actors and Transactions for XDS-i:

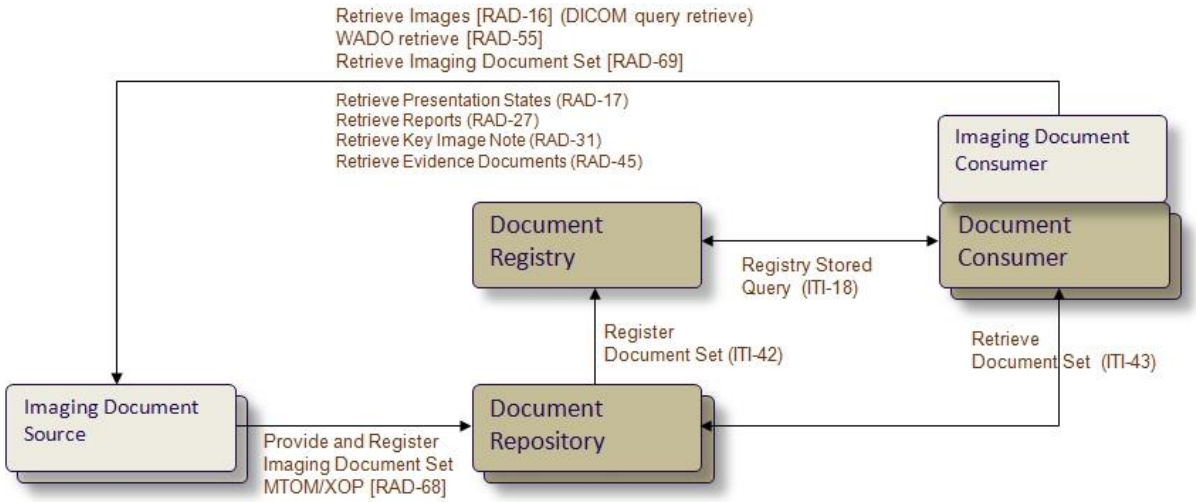


Figure 5 - XDS-i schema

Comments on XDS-i:
The retrieval of images can be done through three transactions. These are the following transactions:

- RAD-16 (DICOM query retrieve)
- RAD-55 (WADO, use of web services)
- RAD-69 (Retrieve Imaging Document Set, via SOAP).

With XDS-i, the DICOM images are not saved in the Repository, but they remain in the PACS system. In the XDS Repository, only the so-called KOS objects (Key Object Selection documents) are stored, which act like a kind of index file to give access to the images belonging to a certain study. The DICOM images therefore are physically in the PACS, but can be accessed from the XDS infrastructure. For more technical information on XDS-i, see the IHE website: http://www.ihe.net/uploaded-Files/Documents/Radiology/IHE_RAD_TF_Vol1.pdf

1.2.3 Exchange between Affinity Domains - XCA

1.2.3.1 Organisation

Although most of the information exchanges between healthcare institutions take place within an Affinity Domain, there is also cooperation with healthcare institutions outside the region, and therefore outside their own Affinity Domain. A patient's information can be stored in several systems, and in several Affinity Domains. How can this information be accessed from someone's workspace? For XDS infrastructures this is organised via a different IHE profile: Cross-Community Access (XCA).

1.2.3.2 Technology - XCA

There is an increasing demand to connect Affinity Domains, opening opportunities to expand transparent information exchange across several XDS networks.
In order to exchange data between regions, there is a possibility of connecting Affinity Domains to one another via the IHE profile Cross-Community Access (XCA). XDS systems which are expanded using XCA have a 'gateway' system which, put simply, acts as a portal when a different region requests images and documents. The XCA gateway is an extra functionality in addition to the XDS infrastructure; this means that healthcare institutions can use the XDS infrastructure which is already present. This is shown in the flow chart below:

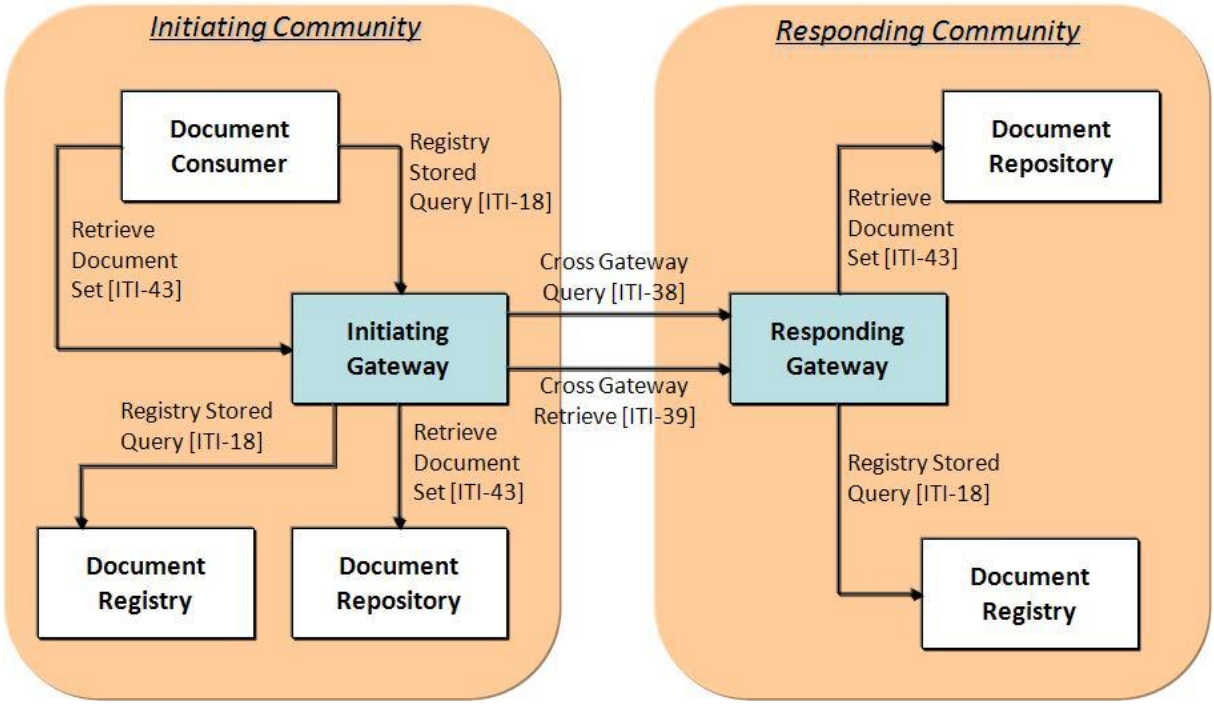


Figure 6 - XCA flow chart

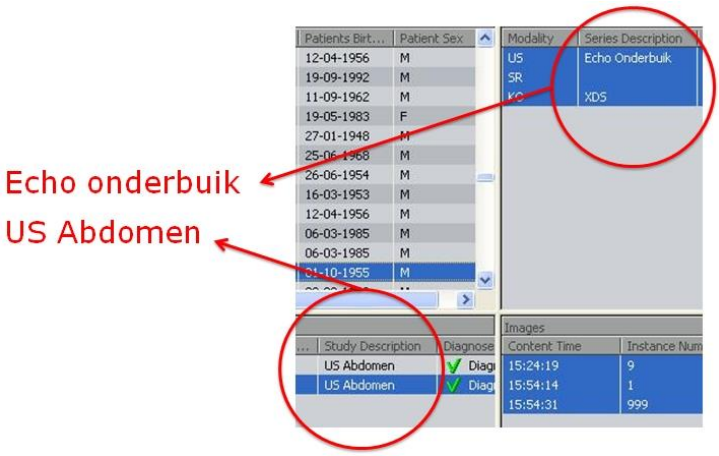
The following describes the effect of exchanging patient data via XCA:
A *Document Consumer* asks whether certain documents or images are available [ITI-18]. This produces a list of available files. This request, however, is no longer sent to the Registry of the XDS Affinity Domain, but it goes to the Initiating Gateway of the Affinity Domain [ITI-38]. The gateway is responsible for passing (routing) this request on to its own Registry, and to connected Responding Gateways of other Affinity Domains. The search request enters another Affinity Domain, and the Responding Gateway then sends the request on to the Registry of another Affinity Domain. In this way, a list is compiled of available documents from all the affiliated Affinity Domains.
When the end user chooses a document from another Affinity Domain from this list, it can be retrieved using the transaction ''Cross-Gateway Retrieve" [ITI-39].

Within an Affinity Domain, a system is needed which is able to play the part of this gateway. This system can for example be managed by an RCO.

Exchange between Affinity Domains however, brings a number of preconditional changes with it which have an impact on the interregional exchange.
These preconditional matters concern the following subjects:

- Identification and authentication of users
- Authorisation of users
- Patient consent
- Logging
- Used metadata and value lists

As well as being harmonised within an Affinity Domain, these matters also have to be harmonised between Affinity Domains, and therefore have to be organised uniformly in all the affiliated Affinity Domains. An example is the use of the same metadata and value lists. When different metadata sets are used in Affinity Domains, it is possible that a certain type of document is not found when it is requested, for example when one Affinity Domain saves a certain study in the category of 'lower abdomen echo' and another uses the category 'US abdomen' (see chapter 2.5.1 for more information.)



Another example concerns patient consent rules allowing the exchange of his/her medical details. It must be clear to the patient that their consent is also needed for their details to be viewed in a different region (see also chapter 2.4.1 for more information).

XDS-i and XCA

Images are retrieved from the 'Imaging Document Consumer' Actor by a RAD-69 transaction via the gateway. The WADO (Web-Access to DICOM Objects, = RAD 55 transaction) and the DICOM Query Retrieve (=RAD-16) transactions are not included in the XCA profile.

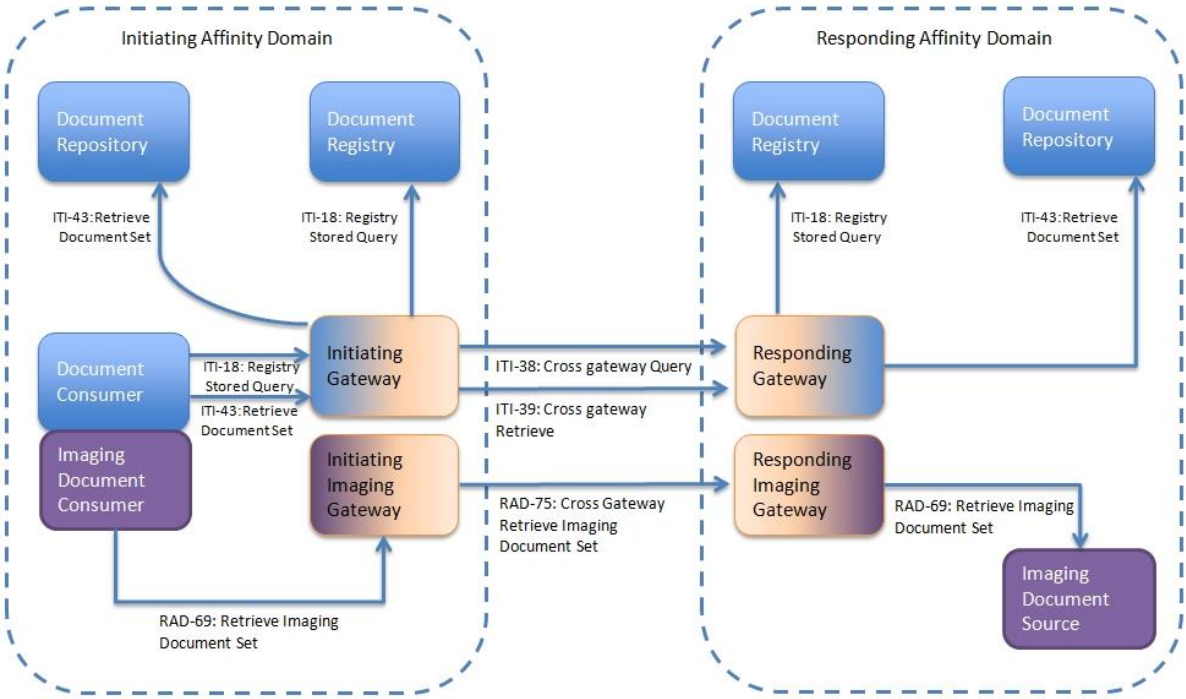


Figure 7 - XCA and XCA-i. Blue actors are always used when exchanging data (documents and images), the purple actors are only used when images are exchanged **(XDS-i)**

In practice, the 'Initiating Gateway' and the 'Initiating Imaging Gateway' actors are often grouped in a single system. Both are responsible for passing on the search query; the first is responsible for retrieving the documents and the second for retrieving DICOM images.

For more information on XCA, see the IHE Wiki:
http://wiki.ihe.net/index.php?title=Cross-Community_Access and
http://wiki.ihe.net/index.php?title=Cross-Community_Access_for_Imaging

1.2.3.3 Different architectures possible

There are several possibilities available for setting up exchanges between Affinity Domains using XCA. These are partly dependent on the strategic choices of the regions, and partly on existing infrastructures or initiatives.

When exchanging information between different Affinity Domains, several different topologies are possible. The flow charts below show the most important ones.

NB: the 'circles' in the flow charts represent XDS Affinity Domains, in which one Registry (list) and two health organisations (H) are shown. Of course, more than two healthcare institutions per Affinity Domain can be connected.

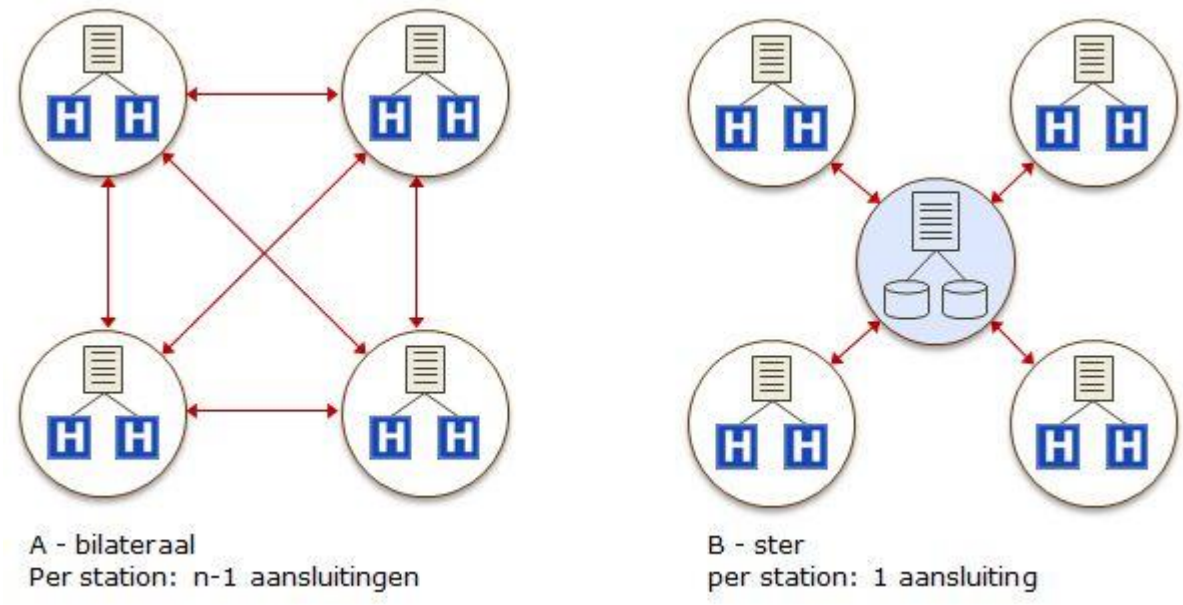


Figure 8 – Topologies of information exchange between Affinity Domains

It is not necessary to choose a certain topology straight away. In the illustration on the right, there is a central Responding Gateway, which can be connected to the other Affinity Domains. This has the advantage that a healthcare institution only has to set up one outgoing Gateway. However, this raises the question of who should manage the central gateway. Until something has been set up to resolve this, a point-to -point configuration (option A) between the different XDS Affinity Domains seems to be preferable, since (up to now) no central Gateway has been set up in the Netherlands. Please note: the diagrams above show that exchange between different healthcare institutions in different Affinity Domains takes place at regional level, and therefore not directly between hospitals. An example: Hospital A in Affinity Domain 1 communicates via its own regional Affinity Domain 1 with Affinity Domain 2 in order to retrieve information from Hospital B. This limits the proliferation of possible connections, and thereby better guarantees security.

NB: this issue will be developed in more detail in the next Guide.

A few comments:

- Exchange takes place between Affinity Domains, not directly between healthcare institutions.
- The optimal architecture depends on the number of Affinity Domains to be connected.
- As the number of Affinity Domains grows, model B becomes more efficient. As the number of regions to be connected increases, the importance of a meta-index becomes relevant.

- Impact analysis of switching from one model to the other: in cases where, up to now, only one XCA gateway has been set up (with a different Affinity Domain), switching appears to be relatively simple, as you only have to switch to another Affinity Domain.
- As the number of affiliated Affinity Domains grows, the implementation of a meta-index can be useful. This makes it possible to look up which Affinity Domains have information for a particular patient, so that only these Affinity Domains are consulted. In general, patients know at which hospitals they have been treated; in addition, the number of affiliated Affinity Domains is still too small at present to justify a meta-index.
- Some hospitals intend to set up a local XDS infrastructure alongside the regional one, for the management of their own documents and images. This is possible, but then it is necessary to find out whether it needs to be included in the regional network. In most cases, it is necessary for use to be made of the regional XDS connection for information exchange with other healthcare institutions (connecting with the RCO Affinity Domain).
- An XDS infrastructure can only be used to share documents to be transferred (by which it is used as a kind of *push* system with notification), or to make all relevant documents available in the Affinity Domain. The latter possibility provides an overview of the patient's whole healthcare route, and also provides an opportunity to access all medical documents at the same time, for example via a Patient Health Record for the patient / citizen.

1.2.3.4 *Scalability and flexibility*

As the number of Affinity Domains increases, the bilateral model becomes redundant due to the multiple connections which have to be realised per Affinity Domain: n-1 connections.

This leaves two models:
1. Star model (more Affinity Domains)

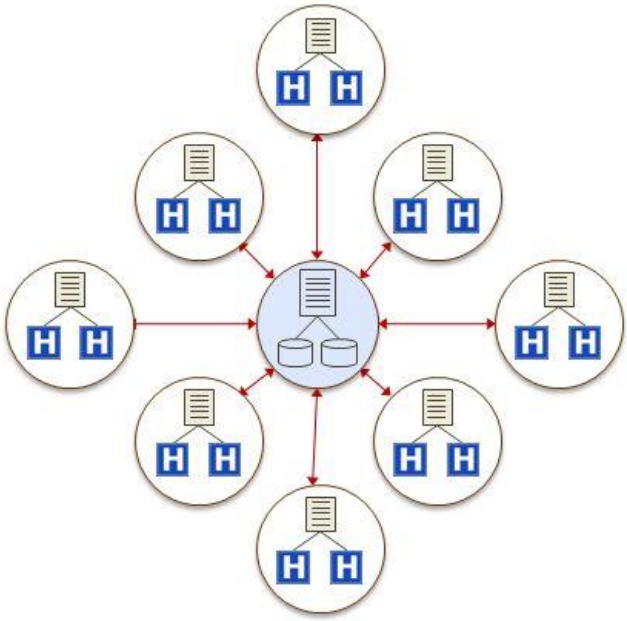


Figure 9 – Star model, extended

In this model, all Affinity Domains are connected to one central 'hub'. The advantage is that each Affinity Domain only has one external connection. Then the central hub can also fulfil extra duties, such as services in the area of national lists, a high-quality authentication and authorisation, and other services. Disadvantages may be: dependency on one central hub, many connections which have to be served from one hub, and legal and organisational matters which are easier to organise at regional level.

2. Multi-star model

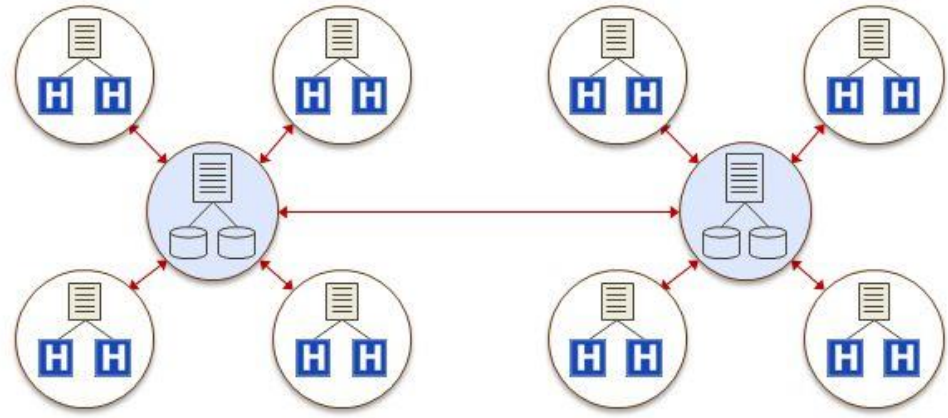


Figure 10 - Multi-star model

There are going to be several 'hubs' which are connected to one another, so there will be several 'central' Affinity Domains.
Advantages: this model is flexible, and can be built up with the retention of the Affinity Domains which are currently present. The principle is that a number of Affinity Domains in a somewhat bigger region all connect to a (super) regional Affinity Domain. This 'hub' forms the connecting point for a limited number of Affinity Domains with other hubs. Disadvantages: the hubs have to be interoperable, and there is no central point from which extra services can be delivered. On the other hand, several hubs can duplicate each other's functionality and data, which means in emergencies they can take over each other's function.

Frequency of exchange
Most information exchange takes place inside the same healthcare organisation. A small percentage is exchanged between organisations, of which most takes place between organisations inside the same Affinity Domain. An even smaller percentage is exchanged between Affinity Domains. International exchange makes up just a small part of this.
These frequencies may also have an influence on the choice of model. If there is relatively little traffic between regions, then one XDS Affinity Domain may be sufficient in quite a large region across which these documents are exchanged. The flexibility of the IHE architecture makes it possible to develop and adapt solutions along the way.

1.3 Explanation of the agreements in the Guide

The agreements / connection conditions of the Guide are listed item by item in chapter 2. This chapter forms the explanation of these items. Both chapters use the same lay out, which is based on the multi-layer model.

1.3.1 Governance, organisation structure

1.3.1.1 Governance of the Affinity Domains and the interregional infrastructure
An Affinity Domain can be defined as a group of healthcare institutions which have made agreements to work together in the area of data exchange and make use of the same infrastructure on the basis of a common set of agreements. This set of agreements includes, for example, items in the area of privacy, patient consent, security, display of clinical data etc. Besides this, there is, of course, also a more technical definition.

Functionally speaking, one important characteristic of the Affinity Domain is that there is one central index (Registry) which contains information on all the documents which are registered in the Affinity Domain. The management of this Registry and the systems which belong to it, for example, for logging, lies in the hands of one party. In many cases, an RCO will be the logical party to manage and exploit these central components. This role can also be fulfilled by a healthcare institute or, as in the

case of a specialist Affinity Domain for example, by the Dutch National Institute for Public Health (for screening programmes).
Therefore, it has to be established which party is responsible for managing the central infrastructure within an Affinity Domain.

NB: In the rest of this document, we use the term RCO, but this may be understood to stand for any central organisation structure.

1.3.1.2 Governance of the Guide

The Guide contains requirements and recommendations for exchanging information between XDS Affinity Domains (this document). The RegioPlatform orders additions / alterations to the document. Nictiz takes care of the publication of new versions.

1.3.1.3 Governance of testing and certification

For the testing and certifying XDS Affinity Domains which are designed on the basis of the Guide, no agreements have been laid down in the current version of the Guide (version 1.4). These will be described in more detail in the next version.

1.3.2 Security and privacy

In order to gain access to medical data, it is necessary to follow the identification, authorisation and authentication process. During identification, the user indicates who he or she is. The identity provided is checked during the authentication step. Once the user has been authenticated, it is determined what information he or she has access to in the authorisation step, depending on the rights which have been entered / configured for the user.
This is partly determined by the rules laid down in the *patient consent*, and partly by the roles and rights which apply to the healthcare institution.

For exchanges within the Affinity Domain, as well as between Affinity Domains, clear agreements are necessary to organise authentication and authorisation. Firstly, this has to happen within the Affinity Domain. However, there also have to be agreements when exchanging information between Affinity Domains. The aim being that a lack of properly aligned security measures does not lead to users gaining access to data which they are not entitled to see.
In the area of authentication, agreements have to be made about the minimal conditions the joint ´systems´ (i.e. the combination of two Affinity Domains) have to meet.
There is a chance that data may 'leak' from more secure organisations to less secure organisations.

1.3.2.1 Authentication - XUA

The Cross-enterprise User Assertion (XUA) profile has been developed within the IHE architecture in the area of authentication. The XUA profile provides various possibilities for authentication and authorisation of the end user, partly by making use of sending authorisation tokens. After authentication of the user has taken place, it can be determined which data the user is given access to on the basis of these tokens.

In the XUA profile, there are three attributes available to arrange this access. This can be done via:

- Role-Based Access Control (RBAC). A certain role is allocated to a user, such as the role of Gastro-enterologist. Certain permissions are connected to this role which determines access to this data.
- Authorisation/Consent. For example, authorisation is determined on the basis of a consent form which is handed in by the patient (see also chapter 1.3.4.1).
- Purpose of Use. The envisaged use of the data, for example, for research objectives, determines whether the user has access to this data.

The XUA profile is suitable to use in combination with other IHE profiles such as XDS for the exchange of data, ATNA for logging user data when executing different transactions, BPPC in which the consent (permission) of the patient is registered. When RBAC (Role-Based Access Control) is applied, the roles, used within and between Affinity Domains, must be well-defined. The coupling of the right permissions to a role requires clear agreements.

NB: at present, agreements on the use of XUA have not yet been described in detail; this may be done in the next version of the Guide.

1.3.2.2 Authorisation – Patient Consent, BPPC

When exchanging medical data outside the healthcare institution, it is obligatory to register the consent of the patient for sharing his/her information with other healthcare institutions. This permission, also known as patient consent, means documents and images can be published so that they can be requested via the reference index by healthcare workers from other institutes. In the near future, in addition to registering permission to be allowed to share patient data, permission from the patient is needed to request this data. (This was not yet legally required at the time this version was written.) By registering the patient consent, it makes it possible to guarantee the proper access to these documents by healthcare workers.

To make this possible, the IHE has developed the **BPPC** profile. The 'Basic Patient Privacy Consent' profile provides a mechanism to register permission(s) ('consent') of the patient. The agreements for being allowed to share patient data are laid down in permission rules, or the so-called *privacy policies*. These privacy policies apply within the Affinity Domain. Implementations with BPPC can take place together with roles based on access control mechanisms such as Role-Based Access Control (RBAC) or Policy Based Access Control (PBAC).

The BPPC profile does not actually maintain or control anything. It 'merely' lays down in digital form which 'consent policy or policies' have been granted by a patient. The maintenance and control takes place on the basis of agreements made within the Affinity Domain, mostly at the level of consultation of the Registry.

Healthcare institutions are obliged to inform patients about the existing privacy policies. In addition, the patient has to be capable of making such choices.

When a healthcare provider, or another person appointed by the healthcare provider such as an assistant doctor, has been given permission by the patient, registration has to take place here. The way in which the permission of the patient has to be registered is, however, not prescribed by law. The law does stipulate that:

- Every healthcare provider must ask permission from the patient;
- The registration must be traceable for the purpose of control.

When registering permissions, it is important that this is done without much ado for either the patient or the healthcare provider. In particular, it should not cost the healthcare provider much time to register patient consent.

When interregional exchange takes place, the consent policies used must be harmonised. In this case it is such that the more complex the policies or the greater the number of possible policies, the more difficult it is to harmonise them. For instance, policies may refer to each other resulting in 'deadlocks' and in healthcare providers being refused access. Or vice versa, when one policy is very specific and the other much more general, a healthcare provider can gain access to medical data which he or she has not been given rights to.

The enforcement of BPPC policies should take place at Registry level, by using the *BPPC enforced option* of the XDS profile. Putting the focus on these sorts of policies results in a number of important decisions:
- Changes in the available BPPC policies only have an impact on the Registry rather than on all the Consumers.
- Authorisation is imposed in one location and therefore is easier to verify.
- BPPC policies are imposed within the same Affinity Domain; other Affinity Domains therefore do not need to have knowledge of the BPPC policies which apply.

More information on BPPC can be found in the Nictiz White Paper "Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken" (Guideline for implementation of permission profiles within XDS networks).

1.3.3 Legislation and regulations

Which laws are relevant, and which norms and guidelines form the basis of the connection requirements? The legislation and regulations set requirements with regard to the rights and duties of different parties, the security of the medically sensitive information and the governance.
The most important laws in the area of healthcare information exchange in the Netherlands are:

- WBGO Medical Treatment Agreement Act
- Wbp Personal Data Protection Act
- Wbsn-z Use of the Citizen Service Number (the Dutch National Insurance Number) in Healthcare Act
- Zvw Health Insurance Act

- Wmg Healthcare Market Regulation Act

The following Nictiz publication provides a broader overview of all specific legislation and regulations in healthcare "Wet- en regelgeving in de zorg, een overzicht voor ICT en eHealth". (Legislation and regulations in healthcare, an overview for ICT and eHealth)

All relevant legislation and regulations which apply to (inter)regional exchange are listed in the Code of Conduct for Electronic Data Exchange in Healthcare ("Gedragscode Elektronische Gegevensuitwisseling in de Zorg"). The Code of Conduct for Electronic Data Exchange in Healthcare code is the basis for implementation of the legal aspects of exchange.

1.3.3.1 Practical realisation of legislation and regulations.

The responsible party (in the sense of the Personal Data Protection Act) should take suitable technical and organisational measures to protect personal data against loss or any form of unlawful processing. In this context, suitable means that the latest technology is utilised to meet the security measures.
The security obligation is quite broadly formulated in the Personal Data Protection Act. For this purpose, the guidelines in the Code of Conduct for Electronic Data Exchange in Healthcare should be followed.

1.3.3.2 Development in legislation

The legislation and regulations for ICT in healthcare are constantly changing. On 1 July 2014, the Patients' Rights in Healthcare bill for electronic data processing was adopted by the Lower House. The bill contains preconditions for the use of electronic exchange systems by healthcare providers for the protection of the privacy of citizens. At the time of writing, the debate on this bill, which was due to take place on 1 July 2015 in the Dutch Senate, has been postponed until further notice.

The bill has important consequences for the way in which these systems are organised and used.
It contains important changes to:

- the Personal Data Protection Act
- the Use of the Citizen Service Number in Healthcare Act
- the Health Insurance Act
- the Healthcare Market Regulation Act.

When the bill comes into force, the Use of the Citizen Service Number in Healthcare Act will be referred to as the Supplementary Provisions for Processing Personal Data in Healthcare Act (Wabvpz).
The reasons for the bill are a number of motions by the Upper House. These motions have largely come about as a result of the debate on the bill for the Framework for a National Electronic Patient Record, which was rejected by the Upper House on 5 April 2011.

1.3.3.3 Standards

The **NEN 7510**[3] standard is a standard developed by the Netherlands Normalisation Institute for Information Security in the healthcare sector in the Netherlands. The standard is based on the Code for Information Security. A modified version of the code has been formulated for the healthcare sector. The reason for this is because there are additional matters specific to the healthcare sector which require attention, such as the protection of privacy. The NEN 7510 for the healthcare sector has been modified as follows:

- **NEN 7512**: The basis of trust for data exchange.
    - In the NEN 7510, risk classification has been developed in more detail. In the NEN 7512, minimal requirements have been laid down with regard to authentication and identification for the different risk categories. Here the pros are weighed against the cons. The requirements concern the following: the sender (entity: person, organisation or the information systems with which the information is sent)
    - the medium
    - the recipient
    - There is an authentication process within this chain: the source must show his or her identity and the recipient must be able to check his or her identity. The security level of the whole chain determines the level of security used to exchange the information.
- **NEN 7513**: Logging.
    - The recording of activities using the Electronic Patient Record, so that it can be traced to who has had access to the record.
    - The patient record plays a key role in the safe care of the patient. For safe care, it is essential that data in the record is treated with integrity. Due to the nature of it being a registration, the record contains data that is very privacy-sensitive. For these two reasons, laid down in legal provisions, it is important to be able to trace who has access to the record at any time, according to which rules he or she has been given access and which activities he or she has carried out.

NB: the Electronic Data Exchange in Healthcare Code of Conduct show which standards are used in practice.

1.3.3.4 Guidelines

Many questions about the interpretation of the Personal Data Protection Act and the standards in the *Medical Treatment Agreement Act* arise when using ICT in healthcare. That is why these standards have been described in more detail in the Electronic Data Exchange in Healthcare Code of Conduct, which has been jointly compiled by the umbrella organisations of the healthcare providers and

[3] The documentation of the NEN 7510, 7512 and 7513 have been "bought free" by the Dutch government. Please contact Nictiz if you wish to get these documents

different regional (ICT) healthcare provision joint organisations. Once again, we refer to the guidelines set out in the Electronic Data Exchange in Healthcare code.

1.3.4 Policy organisation

At this level, agreements are laid down at the level of the participating organisations.
This may begin with a joint vision on information exchange in healthcare, with shared principles and objectives. A covenant, in which all the parties involved indicate the desire for and the necessity of exchanging patient data, is an important point of departure for this. In addition, agreements and contracts have to be drawn up at this level in which responsibilities, roles, financial and legal agreements of the participating organisations are laid down.

1.3.4.1 Framework agreement

In a framework agreement, agreements at RCO level are laid down. In the framework agreement, all participating organisations are listed and their roles and responsibilities are laid down. References are made in this document to data processing agreements, in which separate agreements between healthcare institutions and the RCO have been laid down.

1.3.4.2 Data processing agreement

In an Affinity Domain, the exchange of privacy-sensitive medical patient information takes place. In order to process this data, the parties involved should enter a data processing agreement with one another in which the responsibilities of processing this data have been laid down in line with the Personal Data Protection Act. Issues such as processing, security, and secrecy are laid down in the Data Processing Agreement.
The data processing agreement does not just lay down how the Affinity Domain parties have access to personal data during the agreement; it also stipulates for example that after the agreement has ceased, a party may no longer have access to personal data.
All parties within the Affinity Domain should enter this data processing agreement. An RCO (or the administrator of the central Registry) should also enter sub-data processing agreements with third parties when they carry out tasks for the RCO or the administrator of the central Registry.

1.3.5 Work processes

1.3.5.1 Notification when new data becomes available

The XDS exchange model assumes the user plays an active role when requesting patient data. A retrieval starts with posting a search query in the Registry.
There are two ways to find out whether new patient data has been entered in the Registry. These are as follows:

- **Choosing from a list of available documents from the patient in question**.
  an end user consults the Registry to see if the necessary data is already available. This may happen, for example, when a test has been carried out and the results of the test are expected the next day, after requesting an X-ray, or when viewing the available documents after selection of the patient in the user's own EPR (Electronic Patient Record).
- With this method, it is possible that the user receives a message that the patient's data is available, by, for example, telephone or email, or via the XDR IHE profile. The end user can consult the Registry on the basis of this.

- **'Subscribing' to certain kinds of (new) patient files**.
  an end user has 'subscribed' to certain types of files, such as a referral of the patient to the user's healthcare institution, a request for a laboratory test or endoscopy results. The possible choices are determined by the XDS metadata elements (see 1.3.6.1, XDS metadata). As soon as new data is registered in the Registry, the subscriber receives an automatic message after which the new documents and/or images can be retrieved. This mechanism is defined in the DSUB IHE profile (Document Metadata Subscription). The DSUB profile is also applicable in an interregional setting for exchange between Affinity Domains.

1.3.5.2 Support of the multi-disciplinary workflow

For the multi-disciplinary parts of medical information between healthcare institutions, the XDS infrastructure plays a key role, as information is made available to all affiliated locations via this infrastructure.
In some cases, it is enough to make medical information available, such as a simple referral, or a request for additional tests. However, there are also situations in which several healthcare institutions and healthcare providers are jointly involved, such as care paths, chain care, oncology treatment, cardiology treatment or in the case of Multi-Disciplinary Consultation (MDC). In these cases, there is usually a central coordinator of the care process, and different healthcare providers make decisions at different moments in the workflow. The progress of such a process depends on the treatment or treatments carried out or decisions made by different healthcare providers in the chain.

The XDW IHE profile (Cross-enterprise Document Workflow) provides an opportunity to exchange logistical healthcare information between healthcare organisations or departments.
The basic principle consists of a meta-document which is available to all healthcare providers via the XDS infrastructure. In the XDW document, references are included to different steps in the healthcare process and to relevant documents which have been used or generated per step. This way, an overview of available documents is created within the context of the patient's healthcare route. In the case of multi-disciplinary consultation in oncology, these include the relevant CT images and reports, lab results of blood values, a pathology report and the final MDC report. XDW documents provide structure to the list of medical documents by coupling them to a workflow: XDW gives the context of the process to the information.

An XDW document is also for workflows which run across several Affinity Domains. For this, agreements need to be made on the location of the XDW document. In most cases, this is the location where the XDW document was first created.

The alternative is that an update of an XDW document takes place in the Affinity Domain where the patient is located at that time. In this case, a message must be sent to the other Affinity Domain that ensures the 'old' XDW document is declared obsolete and therefore will no longer appear when a search query is entered. In both cases, the right to register or make changes to a document in a different Affinity Domain plays an important role. Which of the two alternatives should be chosen depends on the choice which is being compiled by IHE International. This will be detailed in more depth in a later version of the Guide (see also the Points of Discussion document).

Example of an XDW profile

In the figure below, a schematic overview is given of an XDW document which supports the MDC process:

XTB-WD – Cross-enterprise Tumour Board – Workflow definition

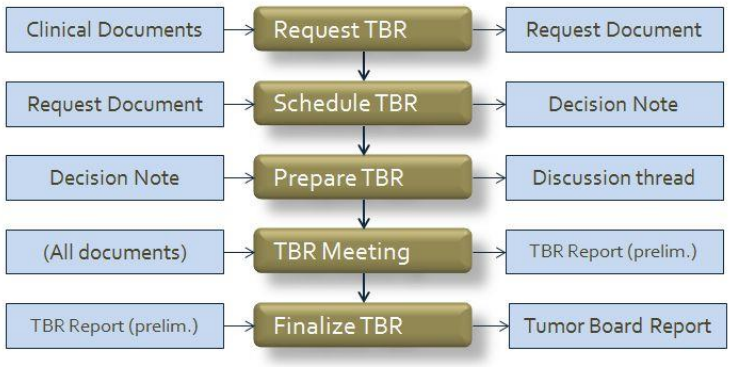


Figure 11 – Example of an XDW workflow definition profile (XTB-WD)

1.3.5.3 Logging and monitoring

All transactions which take place with regard to (inter-)regional exchange are registered for the purpose of auditing. This is in compliance with the specification of IHE, and makes use of the ATNA IHE profile (Audit Trail en Node Authentication). This concerns the logging of matters such as which user has registered, requested or downloaded what and when.
The administration of the logging lies with administrator of the Registry. In many cases, this is the RCO, but it can also be another (healthcare) institution.

In addition, a healthcare institution is obliged to keep its own 'local' logging of all transactions (including non-IHE transactions). (See Electronic Data Exchange in Healthcare code of conduct article 10: logging). These are transactions of all kinds of systems which are used in the healthcare institution. There is no obligation to include all transactions centrally in the logging (of the Affinity Domain).

In a setting with several Affinity Domains, there are no changes to agreements on logging data. This is treated in the same way as within the XDS Affinity Domain; the only difference is that a search query can come from a different Affinity Domain. The processing of such a transaction is done in the same way, with the proper treatment of user data. Logging of a search transaction takes place in the

central log of both Affinity Domains, and also in the 'local' logging of transactions by the systems active in the healthcare institutions.

The central log of an Affinity Domain, usually under the control of an RCO, is defined in the ATNA profile. The recorded data can be used to find out which person from which institution has searched and/or viewed which data at what time. RCOs must make agreements on this with one another in order to be able to check data from the logging in cases of (alleged) abuse; for more information see chapter 2.5.3.

Agreements must be made between Affinity Domains on which (extra) transactions and metadata are registered in the central log. All the Affinity Domain's healthcare institutions must comply with this and register logging data of the transactions in the ATNA index of its own Affinity Domain.

It has been agreed that each healthcare institution appoints one person who has access to the central log. The objective of this access is to ascertain whether technical malfunctions can be seen when data exchange does not work. This only applies to being able to view logging data from the same institution. In order to ascertain possible abuse on the basis of logging data, or a request to view it by a patient, agreements are necessary within and between the Affinity Domains. An example of this is a description for running through a procedure with regard to a request for an overview of certain logging data within the Affinity Domain, determining where you start, as well as the procedure in the case of interregional exchange.
An example is the document "*Procedure Auditlogging template V1_0"*, (Audit logging procedure template) originally laid down by *ZorgNetOost*[4].

1.3.6 Information

1.3.6.1 XDS Metadata

The use of metadata plays an important role in setting up and managing proper storage of images and documents via XDS. Metadata describes the following things:

- Date and time of creation
- Who has created the data
- Subject (patient)
- The kinds of data (functional and technical)
- System or equipment which created the data

The application of the use of metadata focuses on simply being able to find data, such as an X-ray image file. In addition, stored data can easily be placed in a certain context.
Metadata plays an important role within an Affinity Domain or in exchanges between Affinity Domains. To realise interoperability within the information layer, agreement is needed to ensure the consistent use of the metadata. When this is not the case, it is possible documents or images which

[4] One of the RCOs in the Netherlands

have been requested will not be found. An example is when there are two different metadata terms in use that describe the same procedure, such as 'lower abdomen echo' and 'US abdomen'.

A section has also been added on the use of metadata in the XDS standard. The XDS Registry contains a number of metadata elements (and the accompanying value lists for filling in the elements). Some parts in the standard are obligatory. These are, for instance, the metadata which tell us about: demographic data of the patient, the author of the document, the identification number of the document, the mime type etc. More information on this can be found in the IHE Technical Framework of ITI in Volume 3, chapter 4.
In addition, for a number of elements, more general instructions are given on how to fill them in. The IHE standard has been set up at a global level; the filling in of certain elements should be done per country. For the Dutch setting, it is necessary to fill in all metadata elements, even elements which are not specified or only at a level which is too abstract. In order for the exchange between Affinity Domains to run smoothly, it is necessary for XDS metadata to be organised uniformly.

To achieve this, a national metadata set has been developed. For the purpose of the Guide, a new version of the XDS Metadata set is underway. In it, things that have not been specified up to now, such as the metadata elements classCode, typeCode, practiceSettingCode and eventCodeList, are described in more detail.
NB: the agreements in this area are laid down in ART-DÉCOR, and in an older Nictiz document "Dataset XDS voor digitale beeld- en documentuitwisseling"[5] (XDS Dataset for digital image and document exchange) and the accompanying "Handleiding dataset XDS-metadata" (XDS metadata dataset manual). This document sets out how this should be organised for 2015. New versions of these documents are underway for 2016, and references will be made to the current update when the time comes.

1.3.6.2 Value lists in the XDS metadata set

So-called value lists have been included in the national set of metadata. These are lists of terms which fall under a joint category, such as the value list for *modalities* (equipment for X-ray or other image files). This value list contains different sorts of diagnostic equipment, such as CT, MRI, PET, etc. The value lists brings uniformity to the different sorts of supplementary tests.

The elements of a value list are also coupled to a unique code from a classification or terminology system where possible. This ensures uniformity of language, unequivocality, simpler processing by systems and international harmonisation. Nictiz maintains the relevant value lists, including the value lists which are used in the XDS metadata.

[5] These documents are under construction!

Agreements on the use of these value lists must be made both within and between Affinity Domains. In addition to existing value lists, there are also value lists imaginable at present which do not yet exist, but which are desirable. An example of this is a healthcare provider guide, a structured list in which healthcare providers can be looked up.
One of the advantages of a healthcare provider guide is that authorisation is easier to organise than it is at present. In the future, it is to be expected that patients will be able to determine which healthcare data they wish to make available for exchange.
A healthcare provider guide therefore, ensures that the patient can give a specific healthcare provider access to medical data or indeed refuse such access. The healthcare provider guide does not need to be organised at national level, it can also be done at the level of an Affinity Domain.

1.3.7 Applications

1.3.7.1 Use of standards and profiles

The Guide focuses mainly on the use of IHE profiles when realising a standardised infrastructure for the exchange of medical information. The main principle is that as much use as possible is made of IHE profiles, as they match one another ('family of standards').

1.3.7.2 Integration, coupling to healthcare applications

The wishes of users are important for integrating and coupling the healthcare applications they work with daily. The extra functionalities which XDS provides must be able to be used transparently by a user within the same application. Integration in the same EPR avoids the need for separate login procedures or having to select the right patient. The integration of XDS actors is important to support continuity in the working methods.

1.3.7.3 Interim solutions

In practice, however, it turns out that integration in EPRs is not always possible. This makes it necessary to use a separate viewer or another 'interim application', which is integrated in the main application (visual integration). In this case, the user does not need to start a separate programme, nor log in separately (Single Sign On), and when the patient context is changed, the integrated application changes with it. The 'viewer' of an XDS supplier (a Document Consumer) can also be visually integrated in the main application. This means that the application can be called up using the correct parameters by the main application.

The use of a (central) viewer, however, may be an interesting step towards full XDS functionality within the Affinity Domain. A viewer (Document Consumer) is relatively simple to use to retrieve data within an Affinity Domain. In addition, once this viewer is connected to the gateway, it is also possible to request interregional data. It is important, of course, to make good agreements on security to protect access to documents and images. For example: the national breast cancer screening

programme (MammoXL) requires Unique Healthcare Provider Identification (UZI) passes for users when they request data via a webviewer.

1.3.7.4 Patient ID

A unique identification ID is required to find a specific patient. It is possible within the Netherlands to identify a patient uniquely via the Citizen Service Number (BSN). Agreements have been made to use the Citizen Service Number both within an Affinity Domain and for interregional exchange.

In addition, many healthcare institutions use a local patient identification number. The healthcare institutions will have to link this number to the Citizen Service Number or add the Citizen Service Number when they register medical data. In these cases, the Hospital Information System or EPR needs to be coupled so that a Citizen Service Number can be linked to the data to be registered.
NB: In the current version of the Guide, no recommendations have been made with regard to patients without a Citizen Service Number; this may be described in more detail in the next version.

1.3.7.5 Unique IDs of Affinity Domains, repositories and documents

After consulting a Registry, the Consumer system receives data back concerning availability of a document. In response to a search query, a Consumer receives the metadata of the document concerned and a number of unique IDs from the Registry. The Consumer needs these unique IDs to retrieve the required document from the right Repository.
There is an ID for the document, the *DocumentUniqueID*, and an ID for the Repository where the document is located, the *RepositoryUniqueID*. The third ID is the ID of the Affinity Domain, the *HomeCommunityID*. See figure 11 below. Based on this HomeCommunityID, the consulting Consumer can retrieve data from the right Affinity Domain and the right Repository. For exchanges within an Affinity Domain, this ID is not obligatory but it may be sent along optionally.

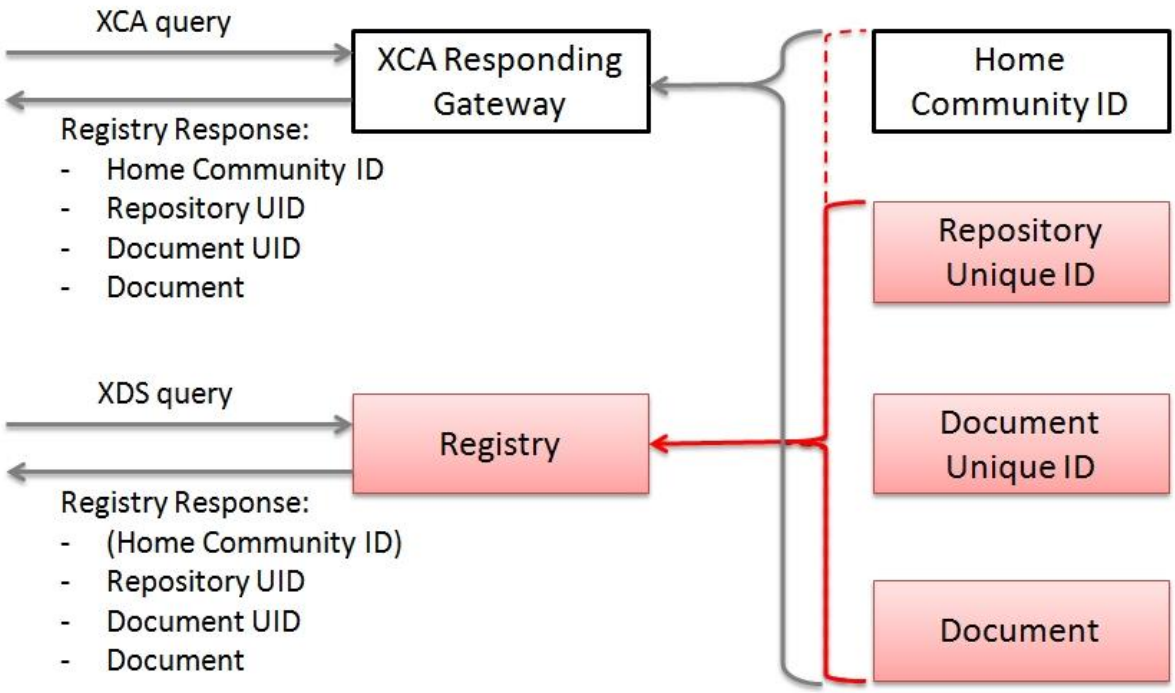


Figure 12 - XCA and Home Community ID

For exchange between Affinity Domains, the HomeCommunityID is obligatory otherwise it is not possible to retrieve the right document from another Affinity Domain. For the purpose of the Guide, the HomeCommunityID needs to be filled in as much as possible.

1.3.8 Infrastructure

Agreements on the use of the networks, Virtual Private Networks (VPNs) and so forth are dealt with further in chapter 2.7. In general, the idea is to strive for a design with as much network compatibility as possible, although it is not strictly necessary. However, comparable designs of communication networks make harmonisation and problem solving simpler (at least in theory).

1.3.8.1 Affinity Domain network

The creation of an infrastructural ICT network for exchanging medical data within an Affinity Domain can be done in several ways. The main two ways are described below.

One way is to set up a closed network. In this option, a physical (glass fibre) network (ZSP network) is laid down in a region and the cooperating healthcare institutions connect to it. Examples of this are the EZDA region, Gerrit Zorgnet and the RijnmondNet region. Each of them has set up a closed network to which only specific users and healthcare institutions have access.

Another possibility works using links on a secure connection (VPN). This makes it possible to set up secure connections to the RCO and other healthcare institutions using your own provider.

These connections can also be used by a healthcare institution outside an Affinity Domain to make direct contact with another Affinity Domain.

1.3.8.2 Network design

A configuration document has to be created per Affinity Domain in which the following data has been laid down:

- IP addresses
- Port numbers
- AE titles
- (WADO) URL
- OIDs
- Firewall configuration settings

For connection with other Affinity Domains the following needs to be laid down:

- HomeCommunityID

It is necessary for this set of configuration data to be known within the Affinity Domain. The network administrators of the healthcare institutions are the people who can organise the incoming and outgoing traffic. They need to become involved in the XDS project at an early stage to ensure quick lead times.
An example document of this configuration data can be found in appendix 3.6.2.

In the case of interregional exchange, it is essential for the Gateways of the different Affinity Domains to be able to find one another. Other traffic, for instance the search query or the retrieval of documents, can take place via the usual XDS methods within the Affinity Domain.

2 Interoperability Agreements between Affinity Domains 2015

Reading guide
This chapter describes the agreements which the regions have laid down from the different interoperability levels which have been explained in chapter 1.3, with the same arrangement of chapters. Chapter 3 contains a number of appendices with (links to) sample documents; chapter 3.8 contains a step-by-step plan for the implementation of an XDS Affinity Domain.
Chapter 4 contains a number of general appendices.

2.1 Governance-level Agreements, Organisation Structure

2.1.1 Governance

2.1.1.1 Governance of the Guide

This is the first version of the Guide. A number of sections and aspects of the Guide will be explained in more detail in subsequent versions. The Interoperability Workgroup has compiled a document, *"Discussiepunten Handreiking Interoperabiliteit tussen Affinity Domains"* (Issues for discussion of the Guide to Interoperability between Affinity Domains) which will serve as input for further development of the Guide. [6]
For the governance of the Guide itself, of the standards and profiles which have been mentioned in it and of the infrastructure, agreements have been made on multiple levels in the document *"Governance Handreiking Interoperabiliteit tussen Affinity Domains"* (Governance of the Guide to Interoperability between Affinity Domains).
In the next version of the Guide, agreements shall be laid down on version management, testing and certification methods. The functional management of the Guide is currently being carried out by the RegioPlatform; the technical management is being carried out by Nictiz.

2.1.1.2 Governance of standards and profiles

In general, the content management of standards, profiles, connection conditions, et cetera is the terrain of the expert parties, such as the SDOs (Standards Developing Organisations) involved, Nictiz, and the RegioPlatform. For the management of each aspect, separate agreements may be made. When exchanges take place between different Affinity Domains, it is necessary to lay down the use of XDS metadata at interregional level, so that they can be exchanged between different regions. The following agreements have been made with regard to this:

[6] This part has not been translated in English bas it is a working document.

XDS metadata governance

- The agreements in this area have been laid down in the Nictiz document "Dataset XDS voor digitale beelduitwisseling"[7] (XDS Dataset for digital image exchange) (and the *"Handleiding dataset XDS-metadata"* (XDS metadata dataset manual) which goes with it). A new version of this existing document will be published when all XDS metadata definitions have been completed. When a new version has been published, the parties involved will be informed.
- Within an Affinity Domain, a procedure has to be designed which ensures that everyone is using the same version of the metadata set in order to prevent any possible exchange problems with other Affinity Domains.
- This procedure will also describe how to deal with any alterations to the XDS metadata set. The main principle is that updates will be planned periodically, which are implemented within a certain amount of time, for example 3 months, on the basis of the new version of the *XDS metadata Dataset* document.

2.1.1.3 Governance of the interregional exchange

The governance with regard to the interregional exchange is also detailed in the *"*Governance Handreiking Interoperabiliteit tussen Affinity Domains" (Governance of the Guide to Interoperability between Affinity Domains) document.

Governance of standards and profiles

In general, the content management of standards, profiles, connection conditions et cetera is the terrain of the expert parties. This is the responsibility of the RegioPlatform. Nictiz is responsible for the technical management.

XDS metadata governance

- Within an Affinity Domain, a procedure has to be designed which ensures that everyone is using the same version of the metadata set in order to prevent any possible exchange problems with other Affinity Domains.
  This procedure will also describe how to deal with any alterations to the XDS metadata set. To design the metadata infrastructure of the XDS Registry, the most up-to-date Nictiz XDS metadata set for designing the metadata within the Affinity Domain must been adhered to. It is not allowed to adhere to anything older than one version behind the most current published version.

2.2 Security and Privacy-level Agreements

2.2.1 Security

The following rules with regard to security apply to exchanging data between Affinity Domains:

[7] These two document are unbder construction

Policy/Organisation

- An RCO (or other registry administrator) has made a framework agreement with each affiliated healthcare institution, which also includes a data processing agreement.
  The framework agreement is the overarching agreement. The data processing agreement is one of its appendices.
- Once a year, an RCO has a so-called *penetration test* carried out, or has an independent party do so.
- Once every two years, an RCO has an *IT audit* carried out, or has an independent party do so. A penetration test is part of this. The scope entails testing a chain consisting of the Registry, the connecting of healthcare institutions to the Registry, and the gateway between two Affinity Domains.
- An RCO and its affiliated healthcare institutions carry an audit out of their own systems and procedures once a year. NB: this applies to the systems which are coupled with the regional Registry.
- Physical access: the "server" systems (a registry, for example) for the users are located in a secured room and cannot be accessed without supervision of an authorised person. All access to the room is registered.
- Data exchange of healthcare institutions in an Affinity Domain is preferably carried out via a direct connection (often under the control of an RCO) with the central infrastructure. Alternatively, it is also possible for non-affiliated healthcare institutions to set up a secure connection, a VPN (with an interim solution such as a webclient). A healthcare institution itself is always responsible for the connection and its related costs.

NB: Healthcare portal RijnmondNet has compiled a document concerning the Architecture and Control Framework. See "*Zorgportaal Rijnmond Architectuur en Control Framework*"[8]. (Architecture and Control Framework of Rijnmond Healthcare Portal)

Healthcare processes

- Available security updates of all relevant software, anti-malware and the necessary updates from operating systems are to be installed as quickly as possible. The Change Advisory Board (CAB) coordinates these and informs the healthcare institutions concerned.

Information

- MIME types: the MIME document types which absolutely must be supported are located in the implementation roadmap in Chapter 3.7.8.
- Encryption: encryption of the data files themselves have not yet been specified in this Guide. This will be described in more detail in a later version of the Guide.

Applications

- Authentication:
  - Authorised users require either a UZI healthcare workers pass, a UZI pass with their name or a similar smartcard solution to access to the Registry. Registration of the UZI pass or smartcard data is carried out by the administrator of the registry.
    In 2015, it was agreed that healthcare institutions are allowed to continue using user name/password methods. In principle, STORK level 3 security level, and the identification and other security methods which go with it, applies.

[8] This document is in Dutch and has not been translated

NB: these rules will be expanded upon as soon as there is more certainty about the exact legislation with regard to authentication and authorisation.

  - Policy with regard to user name and password falls under the responsibility of the healthcare institution. A mutual relationship of trust is required for exchanges with other parties. The use of a user name/password falls under the creation of a "circle of trust". In other words: the cooperation relationship between parties.
  - Group passes or anonymous passes are not permitted.
  - Mandating users is permitted in the current version. Mandating gives approval to other (personal) UZI passes.

- Authorisation:
  - Who is given access to the XDS infrastructure is determined by the software in which the XDS application runs (usually the ZIS/EPR). When the XDS software runs independently, access to the healthcare institution concerned needs to be arranged.
  - For access to the registry, a roles and rights structure is being worked on whereby authorised users are given exclusive access to the parts of the application they are entitled to enter. They are only shown the information patients have given consent for.
  - For access from outside the Affinity Domain, access rules to the Responding Gateway are also applied. It is the responsibility of the requesting Affinity Domain to check access rules for the query being made. Only when XUA has been implemented and the identification and roles have been harmonised will the responding Affinity Domain be in a position to make access decisions at the same level.

- Logging:
  - Registration of all transactions which take place within the Affinity Domain are registered for auditing using the help of the ATNA IHE profile. This is in accordance with the IHE specifications. This concerns the logging of matters such as which user registered, requested and/or downloaded what and when. The organisation which controls the registry also controls the logging (in an ATNA log file).
  - Registration of transactions between Affinity Domains is also logged in ATNA.
  - A healthcare institution is also obliged to record the local logging of transactions.
- Audit logging:
  - Logging provides an overview of all processing activities which have taken place with regard to personal data. Audit-logging enables regular control of the overview, so that it can be established whether these activities took place lawfully according to the legislation and regulations. It is the regions which are responsible for setting up this process.
    See sample procedure ZorgNetOost: *Auditlogging Procedure V1 0.docx*
  - Random checks of transactions for auditing are also possible for transactions between Affinity Domains.

Infrastructure

- Systems which communicate within the Affinity Domain do so on the basis of two-way authenticated TLS connections and only on the basis of UZI server certificates.
  The specifications with regard to TLS connections are elaborated upon in the IHE ATNA profile.
  Requesting an UZI server certificate is done via the UZI register. For more information see:
  http://www.uziregister.nl/servercertificaat/[9]

[9] This is the Dutch register for the IDs of healthcare organizations.

- Firewall:
  - IP address filtering: The configuration of IP addresses for the RCO and the affiliated healthcare institutions takes place inside the firewalls concerned. This means that communication from an unknown IP address will be blocked. For use within the Affinity Domain, healthcare institutions provide IP configurations. This data is centrally available in a list for other healthcare institutions. (see chapter 3.6.5)
  - Only one access point (chokepoint) is available for access to the Registry.
  - Uses redundancy ('Defence in Depth').
  - Using different sorts of security measures ('Diversity of Defence').
  - When one security measure fails, no further access is given ('Failure Mode').
  - Use of 'tasteful inspection': this limits access to certain parts of the system and means the system can only dispense of its information in a certain way.

2.2.2 Privacy

In order to protect the privacy of the patients and to meet legal requirements, RCOs and healthcare institutions must satisfy a combination of security measures. These are dealt with later in this document with the different layers of interoperability: see also chapters 2.1.3, 2.4.1, 2.4.4.

2.2.2.1 Patient consent

At present, we recommend keeping the model of these policies as simple as possible, especially with regard to interregional exchange, to make sure the BPPC model remains manageable in the long term. This makes maintenance and management of the policies easier and more orderly. At the same time, this will make it more practical for healthcare providers by reducing the administrative burden on them.

In addition, we recommend being practical when working with the BPPC, so that when a patient gives permission, he or she gives permission for regional exchange.

If the patient refuses, he or she can still be asked to give 'Break-Glass' permission to the healthcare institution. Asking the patient for national consent is not yet recommended due to the (political) sensitivity surrounding this matter.

In order to gain interregional permission for exchanging data, agreements between RCOs are necessary. The permissions policy document for the interregional exchange in question is laid down jointly. An example is the document "*Advies invoering patiënttoestemming en BPPC voor de Beeld- en Documentenservice Regio Rijnmond*"[10]. (Recommendations for registering patient consent and BPPC for the Image and Document service in the Rijnmond Region).

For the design of permission profile using BPPC, see the Nictiz document:
" Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken". (Guideline for implementation of permission profiles within XDS networks).

[10] (and 11) This document is in Dutch and has not been translated

2.2.3 Safety

NB: this section has not yet been developed in this version of the Guide.

2.2.4 Certificates for communicating systems

Certificates which authenticate the systems are needed to exchange data. To do this, these systems have to have UZI server certificates installed. Two communicating systems within an Affinity Domain can set up secure connections using server certificates, which means other systems cannot gain access. For more information and to apply for an UZI server certificate, see: http://www.uziregister.nl/servercertificaat/ [11]

2.2.5 Certification

The agreements mentioned in Chapter 2 serve as conditions for certification, which is one of the basic principles of the Guide. However, the governance and design of certification have to be described in more detail in a separate process. The RegioPlatform intends to turn the agreements laid down in the Guide into the connection conditions for establishing an Affinity Domain.
XDS Affinity Domains that want to exchange interregional information will have to meet the connection conditions.
The RegioPlatform proposes that Nictiz takes care of the testing and certification: Nictiz checks whether an XDS Affinity Domain meets the set requirements / connection conditions, and provides a certification document. Nictiz can also call in the help of third parties who are qualified to audit the connection conditions.

2.3 Legislation and regulation-level Agreements

2.3.1 Legislation – Medical Treatment Agreement Act, Personal Data Protection Act, Use of Citizen Service Number Act

Legislation, regulations and guidelines
For the exchange of healthcare information, the regions involved adhere to the Electronic Data Exchange in Healthcare Code and the legislation and agreements included in it.

Agreements on the legislation and regulations, guidelines/covenants can be found in the following documents:

- Agreements on the interpretation of legislation are laid down in the Electronic Data Exchange in Healthcare Code (Code of Conduct for Electronic Data Exchange in Healthcare, see Chapter 2.3.3). The further harmonisation of the code of conduct within the region is required to elaborate on the Electronic Data Exchange in Healthcare Code agreements.

[11] Dutch registration of IDs of healthcare organizations

- A region must sign a covenant for cooperation with other parties involved in order to cooperate with data exchange. The ZorgNet Oost covenant is used as a starting point: *"Raamovereenkomst template"*. (Framework agreement template).

2.3.2 Standards – NEN 7510, 7512, 7513

The following standards apply both within as well as between the XDS Affinity Domains.

NEN 7510

- The organisations cooperating within an Affinity Domain should keep the legislation and regulations which apply in mind. If applicable, the organisation must satisfy NEN 7510 in order to carry out NEN7512 and NEN7513.
- Healthcare providers that will connect to the electronic exchange system are to sign an agreement that meets the stipulations in NEN 7510 in advance, along with the responsible parties and possible third parties such as healthcare service providers.

NEN 7512

- the organisation responsible for an electronic exchange system also must ensure that the network connections used and the criteria for the a healthcare service provider satisfy the stipulations in NEN 7512;
- the responsible party and the healthcare provider ensure secure and careful use of the electronic exchange system, in accordance with the stipulations in the information security standard NEN 7512;
- data exchange takes place exclusively via a healthcare service provider that has been authorised by the responsible party in accordance with the aforementioned criteria/set classification;
- network connections which are used for transferring data to or from the healthcare information system, or for transferring data within the healthcare information system, satisfy the stipulations in NEN 7512. (NB: this concerns the electronic systems of the healthcare provider itself, not an electronic exchange system).

NEN 7513

- the healthcare provider as responsible party for the healthcare information system, as well as the responsible party for an electronic exchange system, ensure that the system's logging satisfies the stipulations in NEN 7513. The logging concerns the registration of a) who has made certain data available and on what date and b) who has viewed or requested certain information and on what date (see article 15e of the bill).

2.3.3 Guidelines - Electronic Data Exchange in Healthcare

When using ICT in the healthcare sector, many questions arise related to the interpretation of the Personal Data Protection Act and as well as the standards of the Medical Treatment Agreement Act. These are described in more detail in the Code of Conduct for Electronic Data Exchange in Healthcare (Electronic Data Exchange in Healthcare Code of Conduct, July 2013):

The Electronic Data Exchange in Healthcare Code and its explanatory document can be found in the following documents:

- Gedragscode Elektronische Gegevensuitwisseling in de Zorg - EGiZ (2013) Electronic Data Exchange in Healthcare Code of Conduct
- Samenvatting Gedragscode Elektronische Gegevensuitwisseling in de Zorg - EGiZ (2013) Summary of the Electronic Data Exchange in Healthcare Code of Conduct

2.4 Policy organisation-level Agreements

2.4.1 Framework agreement / Covenant

In appendix A "*Raamovereenkomst template V1_0*"[12] (Framework agreement template), a sample template is available.

2.4.2 Data processing agreement

In appendix a "*Bewerkersovereenkomst Affinity Domain template V1_0*"[13] (Affinity Domain Data Processing Agreement), a sample template is available.

2.5 Work process-level Agreements

2.5.1 Notification when new data becomes available

We **recommend** using the DSUB (Metadata Subscription Document) profile for planning notifications when new documents become available, such as lab reports or a CT scan. It is preferable to wait until the profile has been declared the standard. We recommend including the implementation of this profile in the strategy.

2.5.2 Support of multi-disciplinary workflow

We recommend using XDW profiles to support multi-disciplinary workflows.
Our **Recommendation** is to include the implementation of this profile in the strategy.
We **recommend** refraining from implementation of a XDW metadocument interregionally for the time being. We shall examine in how far this issue has been detailed by IHE International in a subsequent version issue.

[12] This document is currently unavailable It will be in the next version of the Guide
[13] This document is currently unavailable It will be in the next version of the Guide

2.5.3 Logging and monitoring

The agreements with regard to logging and monitoring of data are:

- The ATNA profile overrules other profiles for the design of regional logging.
- The last version of the Nictiz XDS metadata set overrules other versions for logging data.
- The RegioPlatform determines which additional transaction(s) have to be registered in the central log (of the Affinity Domain); this concerns transaction(s) which are mentioned in addition to those in the ATNA profile (for example registration of an image viewing in the logging).
- All transactions between the Initiation (such as a query) and the Responding Gateway (such as a response to a query) are audited in the Affinity Domain where the transaction takes place. This enables the correlation of transactions between Affinity Domains. The ATNA specifications work interregionally in the same way within the region.
- One person is appointed per healthcare institution to have access to the central log of the Affinity Domain.
- A procedure is set up per Affinity Domain determining how to consult logging data within the Affinity Domain and between Affinity Domains in the case of (alleged) abuse or a request by a patient to view their own logging data. See "*Procedure Auditlogging template v1_0*"[14] (Auditlogging Procedure template), originally compiled by *ZorgNetOost*[15].
- A healthcare institution is obliged to ensure its own local log is up to date. (See Electronic Data Exchange in Healthcare Code of Conduct article 10, logging).

2.6 Information-level Agreements

2.6.1 XDS Metadata

- To guarantee uniformity of language, it is obligatory to follow the Nictiz metadata set.
- To design the metadata infrastructure of the XDS Registry, the most up-to-date Nictiz XDS metadata set for designing the metadata within the Affinity Domain must be followed. Using a version which is older than the previous version is not permitted.
- Nictiz manages the metadata standard and will deliver an update for this metadata set twice yearly at the most.
- Proposals for additions or modifications to the metadata set (value lists) should be directed to Nictiz. This process is carried out via the RCO Change Advisory Board (CAB) and steering group/Regioplatform. Any modifications will be published in the new version of the XDS metadata set.
- Within an Affinity Domain, a procedure to ensure that the latest version of the metadata set is in use must be in place in order to prevent possible exchange problems with other Affinity Domains. Nictiz will indicate in this procedure when a new version is expected and announce in advance which modifications are underway.

---

[14] This document is currently unavailable It will be in the next version of the document
[15] One of the Dutch RCOs

The latest metadata set can be found here:
https://art-decor.org/art-decor/decor-valuesets--ihexds-

Note: in the current version of the ART-DÉCOR data definition, there are some national extensions:

Geslacht	(gender of the patient)
Rolcodemodel NL – Zorgaanbiedertype	(healthcare organization)
Rolcodemodel NL – Zorgverlenertype	(healthcare professional)
Taal	(language spoken by the patient)

Note: Also available is a Dutch document "Handleiding dataset XDS-metadata" (XDS metadata dataset Manual). This has not been translated yet, and is an older version. We await the results of the adoption of the proposed XDS metadataset on the European and international level.

This manual explains the field definitions of the metadata which belong to the **XDS** profile. This is the profile by which images and reports can be communicated extramurally.

- To design the metadata infrastructure of the XDS Registry, follow the latest Nictiz XDS metadata set for designing the metadata within the Affinity Domain.
- Within an Affinity Domain, a procedure must be in place to ensure that the latest version of the metadata set is in use. This is in order to prevent possible exchange problems with other Affinity Domains, when the latter uses a later version of the set of metadata. Nictiz will indicate in this procedure when a new version is expected and will announce in advance which modifications are underway.
- Proposals for additions or modifications to the metadata set (value lists) should be directed at Nictiz. Any modifications will be published in the new version of the XDS metadata set, which will then be reported back to the RegioPlatform.
- Nictiz has filled in the valuesets for the following metadata elements that were not defined by IHE:
  - classCode
  - typeCode
  - eventCodeList

The result can be found at the ART-DÉCOR website page.

2.6.2 Value lists in the XDS metadata set

- See agreements in Chapter 2.5.1 (XDS metadata).

2.7 Application-level Agreements

2.7.1 Use of standards and profiles

In the table of appendix 3.5.2, the actors and transactions for an XDS and XCA infrastructure are listed respectively. It is indicated per transaction whether this is compulsory or optional for a regional or interregional setting.

2.7.2 Actors and transactions to be used (IHE)

The tables of appendix 3.5.3 can be found in the implementation roadmap in Chapter 3.7.8.
This contains the actors and transactions for an XDS (regional) and an XCA (interregional) infrastructure, respectively.

2.7.3 Configuration for exchange within an Affinity Domain

The following agreements apply to the exchange of data within an Affinity Domain:

- For exchanging data, the **RAD-69** transaction must be used.
- The **RAD-55** transaction (WADO, Web-Access to DICOM Objects) is accepted as an exchange mechanism as a temporary alternative until 1 January 2016.
- **RAD-16 (**DICOM Query/Retrieve) is not permitted as a transaction between Affinity Domains.

2.7.4 Configuration for exchange between Affinity Domains

The following agreements apply to the exchange of data between Affinity Domains:

- See the aforementioned agreements in Chapter 2.6.3.
- Each region needs a *HomeCommunityID* and should use it when exchanging data. See specifications in the XCA profile (see http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf.
- Each gateway must possess an updated list containing all the HomeCommunityIDs of the regions between which exchanges take place.
- Applications for HomeCommunityIDs are handled by Nictiz.

2.7.5 Patient ID

- In the Netherlands, it is obligatory by law to use a validated Citizen Service Number when exchanging medical data of a patient.
- For medical data exchange within and between regions, a local patient number, i.e. a patient number issued by a healthcare institution, may not be used as the “primary key”.

2.8 Infrastructure-level Agreements

2.8.1 Affinity Domain network

A network is necessary to exchange medical data via XDS and/or XCA.

- This network can be an (existing) closed network or a virtual network (VPN). There is no specific preference for either of these two possibilities.
- The security of the network should be organised as described in this document.
- To set up secure connections, TLS or a similar solution is compulsory. For more information, see the ATNA profile.
- Coupling a hospital to another hospital located in another XDS Affinity takes place via the gateways of the Affinity Domains involved. It is not permitted to make direct connections.

2.8.2 Network design

- Each Affinity Domain has a configuration document in which the following data is laid down:
  - IP addresses
  - Port numbers
  - AE titles
  - (WADO) URL
  - OIDs
  - Firewall configuration settings
- Per Affinity Domain, couplings must be set up with affiliated Affinity Domains.
- For connection with other Affinity Domains the following needs to be laid down:
  - HomeCommunityID

A sample document of this configuration data is to be found in appendix 3.6.2.

2.9 Standard and profile Agreements, certification

2.9.1 Standards and profiles, certification

2.9.2 Administration and support

Administration and helpdesk aspects fall outside the scope of interregional harmonisation. Each Affinity Domain is responsible for keeping its own services operational. This applies to services within the Affinity Domain, as well as to services between Affinity Domains in as far as they are connected to their own domain, such as with the operation of the Initiating and the Responding Gateways.

NB: up to now, no SLA sample is available for interregional harmonisation concerning uptime and response times in this version.

2.9.2.1 Administration

Once a healthcare institution is affiliated with an Affinity Domain infrastructure and is ready to exchange patient data, aspects of administration come into play. This concerns both functional and technical administration.

2.9.2.1.1 Maintenance of systems

NB: An SLA needs to be compiled for this. No sample document has been added to the current version of the Guide.

2.9.2.1.2 Maintenance of local systems

Responsibilities of the healthcare institution:

- The participating healthcare institution is responsible for the proper functioning of its own XDS systems and ICT infrastructure.
- Agreements on its administration are organised on the level of the healthcare institution itself.
- The participating healthcare institution is responsible for allocating and administering the roles and rights of its own staff with regard to access to its own XDS applications.

2.9.2.1.3 Maintenance of central systems

The following rules apply at central level (in the RCO):

Incident Management:

- Communication with the healthcare institution concerning incidents may only be carried out via the RCO's Helpdesk.
- Communication concerning incidents between the RCO's helpdesk and the healthcare institution is carried out via same member of staff (or his or her replacement) of the healthcare institution. The healthcare institution provides the RCO with this person's contact details.
- The central helpdesk is available 24 hours a day, 7 days a week.
- *NB: more information on reaction times and process times on the basis of priority will be given in a later version.*

Service Level Agreement (SLA)

- The 'service window' of *the Affinity Domain* is open 365 days a year and 24 hours a day.
- The availability of the RCO's Affinity Domain should be laid down in the SLA, but must be at least 99.9%.
- Security patching of the servers.
  A security patch is a piece of software designed to repair or improve/update a computer programme or its supporting data. This includes the detection of security problems and possible bugs/issues, and the improvement of usability and/or performance of systems. Although they are meant to solve problems, badly designed patches can create problems.

Suppliers should take adequate measures and carry out patch management on the infrastructure of the Affinity Domain.
Patch management is the process and governance around security patching.

- Which patches should be used on which systems at what time.
- With regard to critical issues (for example HeartBleed), adequate measures should be taken to guarantee security.

Roles and rights

- Members of staff at an RCO may be authorised to access privacy-sensitive data only to the extent that it enables them to carry out their duties.
- This access is only possible using a personal account. The following is logged each time data is accessed: date, time, name of the member of staff and which data was viewed.

2.9.2.2 Support

2.9.2.2.1 Service desk

Each Affinity Domain should have its own service desk for the purpose of supporting the healthcare institution's services. In the case of problems, members of staff should always contact their own Affinity Domain's service desk. This service desk should:

- be available 365 days a year and 24 hours a day;
- give an estimate of the expected amount of time required for a solution;
- report on the progress of the solution;
- be accessible at the times laid down in the SLA with clients;
- have fixed procedures for registering, dealing with, concluding and reporting on incidents;
- monitor progress on the processing of incidents.

The abovementioned items must be detailed in the SLA (see above).

2.9.2.2.2 Solving problems

- Each healthcare institution has set up an internal procedure for reporting (technical) problems/malfunctions to its helpdesk. Healthcare institutions must define this process themselves.
- If, after an internal report and solution of a problem, it turns out that the problem lies outside the healthcare institution, then the helpdesk can pass on the report to the helpdesk of the RCO or the administrator of the central components. A process description on the treatment of the problems/malfunctions should be compiled at this level.

Agreements

2.9.3 Tests

The agreements made must be verifiable at all levels of interoperability. This is done partly in the form of tests.

In a test process, whether with a healthcare institution, RCO or another institution, the following tests should be carried out:

- Testing on Connectathon by supplier
- Testing central infrastructure
- Technical tests
- Functional tests
- Acceptation tests
- Operational tests

In appendix 3.7.1, a step-by-step plan for these tests has been laid down in more detail.

NB: at present the Guide does not provide a simulation environment (or for example a sandbox for testing). A simulation environment is desirable for testing new developments or bringing them into use. We **recommend** designing a simulator/webapplication in which tests can be carried out. In addition it is useful to provide suppliers with a test environment so that they can develop using the same connection that will be carried out in practice.

2.10 Dot on the horizon

2.10.1 Use of standards and profiles

In the future, representatives of the Affinity Domains can decide whether to add additional or new profiles to the list of profiles, actors and/or transactions to be supported. See the overview in 3.5.1. From the point of interoperability, it is necessary to opt jointly for a standardised solution. This way future differences in implementations between Affinity Domains can be avoided. Some profiles are still under development and not yet available for implementation in daily practice.

2.10.2 Additional dots

2.10.2.1 Austria – ELGA

In the future, it will be necessary for the RCOs to agree on a joint model with a set of accompanying agreements for authentication and authorisation. Various countries have developed solutions for this, like Austria for instance.
The ELGA project in Austria has taken care of national agreements.

The following important agreements have been made in the ELGA project:
- Role-Based Access Control (RBAC) is organised at national level. The role of the healthcare provider determines whether he or she has access to a certain patient's medical details.

- The patient has electronic access to his/her details and can determine the access the healthcare professional has to these. Viewing access to data is possible at the document, healthcare professional, healthcare institution and Affinity Domain level. Moreover, it is possible for a patient to view the logging data to see who has had access to their details.
- A healthcare guide has been compiled for the exclusion and inclusion of healthcare providers with regard to viewing medical data. All active healthcare providers and their role(s) are listed in the guide.
- All actors exchanging data have implemented the XUA profile. The ELGA architecture also lists which systems register, manage, monitor, execute and allocate access to data.

The current profiles used, such as BPPC, for establishing patient consent are not adequate for organising authorisation at an acceptable level in the Netherlands (this also applies to other European countries). The Austrian model can easily be implemented in the Dutch context. However, the model cannot be adopted exactly as it is. More depth is required.

We **recommend** developing a plan in the medium term to bring authentication within and between Affinity Domains to the same level, by setting up a joint model with a set of accompanying agreements.
At present, Nictiz is occupied with setting up such a model in the area of authentication and authorisation for primary care. It will be ready in 2015. Such a set of agreements for interregional exchange will be detailed on the basis of this and of other initiatives (such as ELGA). Any agreements made will be included in the next version of the Guide.

3 Appendices with sample documents

3.1 Governance Level, Security and Privacy

3.1.1 Object Identifiers of organisations

HL7 has a file available with a list of the Object Identifiers (OIDs) of Dutch healthcare institutions, RCOs and other parties:
http://www.hl7.nl/images/downloads/openbaar/OID/HL7NL_OID_register.pdf
NB: This link always gives the most up-to-date information.

3.1.2 Applying for an UZI Pass

For more information on applying for a Unique Healthcare Provider Identification (UZI) pass, see this website:
http://www.uziregister.nl/uzipas/nieuweklant/uzipasaanvragen/

3.2 Legislation and Regulations Level

* No appendices for 2015

3.3 Work Processes Level

* No appendices for 2015

3.4 Information Level

3.4.1 BPPC Policy Object Identifiers

For more information, the Nictiz document "Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken" (Guideline for the implementation of permission profiles within XDS networks) is available.

3.5 Application Level

3.5.1 Overview of IHE actors and transactions used

Which actors and transactions in the RCO and the healthcare institution should be supported, albeit optionally, are indicated.

Legend: R = Required, O = Optional, - = not applicable

Profile	Profile name	Actors	Transactions	RCO	Healthcare institution
The profiles below apply to regional exchange					
XDS	Cross-enterprise Document Sharing	Document Registry	Register Document Set-b [ITI-42]	R	R
			Registry Stored Query [ITI-18]	R	R
			Patient Identity Feed [ITI-8]	-	-
			Patient Identity Feed HL7v3 [ITI-44]	-	-
		Document Repository	Provide and Register Document Set-b [ITI-41]	R	R
			Register Document Set-b [ITI-42]	R	R
			Retrieve Document Set [ITI-43]	R	R
		Document Consumer	Registry Stored Query [ITI-18]	R	R
			Retrieve Document Set [ITI-43]	R	R
		Document Source	Provide and Register Document Set-b [ITI-41]	-	O
		Patient Identity Source	Patient Identity Feed [ITI-8]	-	-
			Patient Identity Feed HL7v3 [ITI-44]	-	-
XDS-i	Cross-enterprise Document Sharing for Imaging	Imaging Document Consumer	Retrieve Images [RAD-16]	-	O
			Retrieve Presentation States [RAD-17]	-	O
			Retrieve Reports [RAD-27]	-	O
			Retrieve Key Image Note [RAD-31]	-	O
			Retrieve Evidence Documents [RAD-45]	-	O
			WADO Retrieve [RAD-55]	-	O
			Retrieve Imaging Document Set [RAD-69]	-	R
		Imaging Document Source	Provide and Register Imaging Document Set MTOM/XOP [RAD- 68]	-	R
			Retrieve Images [RAD-16]	-	R
			Retrieve Presentation States [RAD-17]	-	R
			Retrieve Reports [RAD-27]	-	R
			Retrieve Key Image Note [RAD-31],	-	R

			Retrieve Evidence Documents [RAD-45]	-	R
			WADO Retrieve [RAD-55]	-	R
			Retrieve Imaging Document Set [RAD-69]	-	R
ATNA	Audit Trail and Node Authentication	Audit Record Repository	Record Audit Event [ITI-20]	R	-
		Secure Node	Authenticate Node [ITI-19]	R	R
			Record Audit Event [ITI-20]	R	O
			Maintain Time [ITI-1]	R	R
		Secure Application	Authenticate Node [ITI-19]	R	R
			Record Audit Event [ITI-20]	R	R
			Maintain Time [ITI-1]	R	R
CT	Consistent Time	Time Server	Maintain Time [ITI-1]	O	R
		Time Client	Maintain Time [ITI-1]	R	R
XUA	Cross-enterprise User Assertion	X-Service User	Provide X-User Assertion [ITI-40]	-	R
		X-Service Provider	Provide X-User Assertion [ITI-40]	R	R
BPPC	Basic Patient Privacy Consents	Content Creator	Share Content	-	R
		Content Consumer	Share Content	-	R
DSUB	Document Metadata Subscription	Document Metadata Publisher	Document Metadata Publish [ITI 54]	R	-
		Document Metadata Subscriber	Document Metadata Subscribe [ITI 52]	-	O
		Document Metadata Notification Broker	Document Metadata Publish [ITI 54]	R	-
			Document Metadata Subscribe [ITI 52]	-	O
		Document Metadata Notification Recipient	Document Metadata Publish [ITI 54]	-	O
The profiles below apply to interregional exchange					
XCA	Cross-Community Access	Initiating Gateway	Cross Gateway Query [ITI-38]	R	-
			Cross Gateway Retrieve [ITI-39]	R	-
			Registry Stored Query [ITI-18]	O	R
			Retrieve Document Set [ITI-43]	O	R
		Responding Gateway	Cross Gateway Query [ITI-38]	R	-

			Cross Gateway Retrieve [ITI-39]	R	-
XCA-i	Cross-Community Access for Imaging	Imaging Document Consumer	Retrieve Imaging Document Set [RAD-69]	-	R
		Imaging Document Source	Retrieve Imaging Document Set [RAD-69]	-	R
		Initiating Imaging Gateway	Retrieve Imaging Document Set [RAD-69]	R	-
			Cross Gateway Retrieve Imaging Document Set [RAD-75]	R	-
		Responding Imaging Gateway	Cross Gateway Retrieve Imaging Document Set [RAD-75]	R	-
			Retrieve Imaging Document Set [RAD-69]	R	-

3.5.2 Overview of IHE actors and transactions per Affinity Domain

NB: As yet no inventory has been made of these in the current version. In the next version, the IHE profiles used will be shown per RCO.

3.6 Infrastructure Level

3.6.1 IDs, Affinity Domains and healthcare institutions, services (example)

Institution	Description	Host-name	Internal IP	External IP	Service	Port	Called AET
Healthcare Institution A	PACS healthcare institution A	hostname PACS A	Internal IP address of PACS A	External IP address of PACS A	RAD-69	no.	Called AET modality
					WADO	no.	Called AET modality
Healthcare Institution B	PAC healthcare institution B	hostname PACS B	Internal IP address of PACS B	External IP address of PACS B	RAD-69	no.	LUMC_SN_QR
	Viewer (optional)	Hostname viewer	Internal IP address of viewer	External IP address of viewer	WADO	no.	n/a
	Consumer (when not on PACS)	Hostname consumer	Internal IP address of consumer	n/a	RAD-69 or WADO	no.	n/a
RSO	Central registry / repository	Hostname registry/repository	internal IP registry/ repository	Ext IP registry/ repository	HTTPS	8080	n/a
	PACS (webservice) (optional)	Hostname PACS	Internal IP PACS	n/a	WADO	n/a	n/a
	Viewer (optional)	Hostname Viewer	Internal IP viewer		HTTPS		

3.6.2 IP numbers matrix, firewall settings, clients (example)

HostnameClient	Description	Internal IP	External IP client	Calling AET	Port
hostname	Viewer healthcare inst. B	n/a	external IP	Requesting AET	7070
hostname	PACS healthcare inst. C	n/a	external IP	Requesting AET	7070
hostname	Viewer healthcare inst. B	n/a	external IP	n/a	no.
hostname	PACS healthcare inst. C	n/a	external IP	n/a	no.
hostname	PACS healthcare inst. A	internal IP	n/a	Requesting AET	7070
hostname	Viewer healthcare inst. C	n/a	external IP	Requesting AET	8080
hostname	Consumer C	internal IP	n/a	n/a	n/a
hostname	PACS A	n/a	external IP	n/a	n/a
multiple users possible					
Hostname	PACS healthcare inst. A	n/a	external IP	n/a	no.
hostname	Viewer B	n/a	external IP	n/a	no.
hostname	Consumer B	n/a	external IP	n/a	no.
hostname	Viewer webservice	internal IP	n/a	n/a	no.
hostname	Viewer RCO	internal IP	n/a	n/a	n/a

3.6.3 Application Entity Titles (AET) table

Calling AET (requesting system)		Called AET (delivering system)			
		Healthcare institution A	**Healthcare institution B**	**Healthcare institution C**	
Calling AET **ext. IP** **Port**	Healthcare institution A 196.168.1.100 1230	x x x	Healthcare institution _B 196.168.1.130 1232	Healthcare institution _C 196.168.1.160 1234	**Healthcare Institution A**
Calling AET **ext. IP** **Port**	Healthcare institution B 196.168.1.130 1232	Healthcare institution _A 196.168.1.100 1230	x x x	Healthcare institution _C 196.168.1.160 1234	**Healthcare Institution B**
Calling AET **ext. IP** **Port**	Healthcare institution C 196.168.1.160 1234	Healthcare institution _A 196.168.1.100 1230	Healthcare institution _B 196.168.1.130 1232	x x x	**Healthcare Institution C**

3.7 Implementation Level, administration and support

3.7.1 Tests

The agreements made must be verified at all levels of interoperability. This is partially done in the form of tests.
Several test scenarios should be worked out in more detail, at different levels:

- At several organisational levels: within a healthcare institution, within an Affinity Domain, between Affinity Domains.
- At several interoperability levels: healthcare process, information and infrastructure.
- Functional and technical tests, including 'Connectathons'.
- Acceptation tests and operationalisation tests.

For general agreements on tests, see 'RijnmondNet foundation connection document v1.01'.
The different tests are described below.

3.7.2 Tests on Connectathon

Before the supplier can claim IHE *compliancy*, it needs to demonstrate that the software works properly on an IHE Connectathon first. Follow this link to see which suppliers have been tested for IHE profiles on the Connectathon: http://connectathon-results.ihe.net.
The details of all Connectathons can be found in the menu (see Figure 6). The results being sought are often in the most recent European Connectathon.

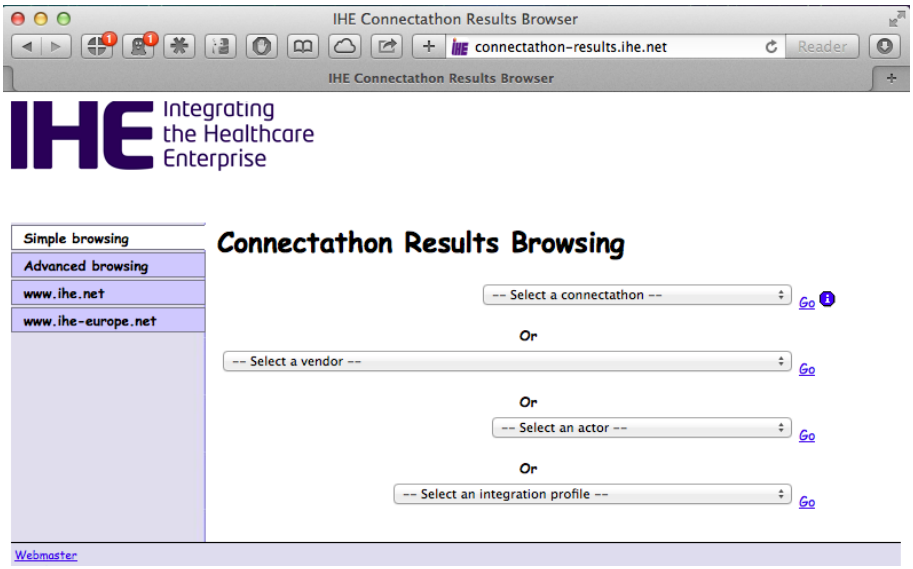


Figure 5 - selecting results of IHE Connectathons

The following requirements apply:

- A supplier must demonstrate that the software to be implemented (in accordance with the version number) has been tested successfully on a (recent) IHE Connectathon.

- Profiles which are to be newly implemented (which are to be used at a later time) should also be tested to see if they work properly on an IHE Connectathon.
- The supplier has know-how and experience with testing IHE profiles on the Connectathon so that the implementation can be carried out successfully.
- When the supplier brings out a new version of the software, it has to be tested on a Connectathon again.

The responsibility for carrying out this part lies with the supplier. The healthcare institution or RCO must check whether the Actors to be implemented (software modules) have all been successfully tested on an IHE Connectathon.

3.7.3 Central infrastructure tests

The RCO is the central hub within an Affinity Domain. The RCO facilitates central components such as the Registry. Before healthcare institutions can connect to the Affinity Domain, the infrastructural components which are provided via an RCO have to have been thoroughly tested.
It is essential that:

- New components and profiles which are rolled out within the Affinity Domain have been tested.
- Couplings with other Affinity Domain(s) should also be well tested.

The responsibility for carrying out these tests lies with the RCO and the supplier who supplies the software.

3.7.4 Technical tests

The objective of the tests is to verify whether the transactions (which apply to the healthcare institution) technically work as described in the standard. The emphasis lies on the technical realisation of the separate transactions.
Part of these tests includes testing to establish connections with the other affiliated healthcare institutions on the basis of selected use case(s).
The following agreements apply to the technical tests:

- The healthcare institution is the actionee for scheduling the testing and, if required, the attendance of the administrator from the RCO.
- An RCO provides a test environment in which tests can be tested against the conditions. This includes a Registry test, a Repository audit test, a Consumer test and a Repository test.
- An RCO provides the healthcare institution with a test set in which exchange scenarios can be tested. The Citizen Service Numbers used for this are special test Citizen Service Numbers (and not ones that have been invented; this is to avoid any possible problems).
- The healthcare institution uses test documents (including patient consent documents) and images for these test patients. These documents and images should be anonymous or given a pseudonym.
- When the supplier brings out a new version of the software, it should undergo the technical tests again.
- Testing always takes place in a test environment and not in the production environment.

The responsibility for carrying out these tests lies with the healthcare institution. An RCO only needs to provide central test Actors (such as a Registry test) for these tests and therefore does not always need to be present. The healthcare institution must be able to demonstrate to an RCO that all the required transactions have been tested successfully before the integral test can be carried out.

3.7.5 Functional tests

In addition to testing whether the technology works in accordance with the specifications, a functional test is required. The objective of this test is to establish whether the functions (lay-out, GUI etc.) are acceptable within the solution provided for the end user of the healthcare institution.

The following applies for the functional tests:

- The healthcare institution carries out this test with a selected group of end users.
- Functional changes/modifications are carried out before the acceptance test takes place.
- Functional tests can take place at the same time as the technical tests.

The responsibility for carrying out these tests lies with the healthcare institution. The healthcare institution must be able to demonstrate to the RCO that this test has been carried out successfully before the integral test can be done. An RCO administrator does not need to be involved in the functional test.

3.7.6 Acceptance tests

Once all the technical parts (the transactions) have been successfully tested for a healthcare institution, and the technical functioning and the functionality of the systems have been accepted by the end users, an acceptance test takes place.
In this test, the whole chain, with all its relevant use cases, is tested with the other healthcare institution(s) involved and the RCO (as supplier of the central infrastructure).

The following rules apply to the acceptance test:

- The healthcare institutions which exchange data are responsible for carrying out the acceptance test.
- The whole chain is run through in one go and all parts are tested one after the other.
- The acceptance test takes place in the *acceptance environment* of the RCO. The RCO is involved in the acceptance test as supplier of the central infrastructure.
- The acceptance test can take place once the supplier in question has technically tested a new version of the software with the healthcare institution and attained a successful result.
- All new profiles to be implemented, and therefore the aforementioned tests, have to undergo an acceptance test.
- An acceptance test is successful when all transactions of the use cases to be tested work according to the specifications. This applies both to transactions sent to another healthcare institution and to the central infrastructure. If it turns out that the central logging is not filled in or it is filled in incorrectly or incompletely, then the acceptance test is unsuccessful. If this is the case, the RCO cannot enter into an agreement with the healthcare institution and the acceptance test needs to be carried out once again.

A successful acceptance test means a healthcare institution can enter an agreement with the RCO, after which the latter can go into production.

3.7.7 Operational test

Once the tests have been completed satisfactorily, the healthcare institution designs the production environment according to the successfully tested configurations. After going live, the healthcare institution, along with the RCO, checks to see whether the right configurations and security measures have also been put in place in the production environment. If this is the case, the participant can start production and make use of the RCO's document and image exchange.

3.7.8 Implementation of roadmap

	In use on Aug-2014	**Aug-2015**	**Jan-2017**
Profiles	CT ATNA BPPC XDS.b XDS-I	XCA XCA-I	XUA DSUB XDW
Authentication	Username/Password	STORK 3 level Authentication (UZI pass or equivalent)	n/a
Server certification	Healthcare institution's own certificates and (solid agreements with Affinity Domain necessary)	UZI server certificates	n/a
Metadata	Current metadata set	Nictiz metadata set	n/a
Mime-types	PDF DICOM images TXT	CDA	TIFF MPEG DICOM SR
Content of reports (Codings)	Free text	CDA structure Or another standard	Codings/Terminology in message

3.8 Steps for plan of Approach for implementation

The guidelines below describe a possible step-by-step plan with regard to implementation.

1. **Starting up an XDS project team**
    a. Set up a project team
    b. Set up a workgroup (with representatives of all the interoperability layers)
    c. Request connection from the RCO
2. **Project plan**
    a. Set up a project plan and adapt it to RCO
3. **Connection to RCO infrastructure**
    a. The healthcare institution satisfies the requirements for a Well-Managed Healthcare System (GBZ)
    b. Select a provider for the data exchange if this has not been done via the provider of the RCO infrastructure
        i. Coupling with the RCO infrastructure
    c. Request UZI server certificate for security of communication with Central Infrastructure
    d. Request Smartcards (and card readers)
    e. Compile and enter an overview of the user names of the authorised users
4. **Selection of supplier, procurement of IHE compliant software**
    a. Draft a "Request for proposal" with all the required specifications for the healthcare institution, in accordance with the guiding principles of the Governance document.
    b. Request tenders from suppliers
    c. Select supplier(s)
    d. Draft SLAs
    e. Update project plan in cooperation with supplier and discuss it with RCO
5. **Covenant, data processing agreement**
    a. Enter a data processing agreement with the RCO
    b. Draft an agreement and sign it with the healthcare institutions between which patient data will be exchanged
6. **Configurations**
    a. Register IP addresses or host names of the XDS actors with the RCO
    b. Request Object Identifiers (OID) for the healthcare institution
    c. Configure URL endpoints
    d. Pass configuration settings on to RCO
    e. Implement/configure your own firewall
7. **Test plan and tests**
    a. Set up a test team
    b. Set up test plan (incl. setting up use cases)
    c. Technical tests by supplier
    d. Functional tests by healthcare institution
    e. Acceptance test in the chain (project group)
    f. Operationalisation test on production after going live
    g. Deliver test report of successful tests to RCO
8. **Operationalisation**
    a. Agree date with RCO to start production and communication with other healthcare institutions with which exchanges will take place.
9. **Management**
    a. Allocate and manage roles and rights of organisation's own staff with regard to access to the organisation's own XDS applications.
    b. Detail internal policy with regard to privacy, security, general management, workflows etc.
    c. Set up management in your own healthcare institution.
10. **Taking into use**
    a. Inform users

b. Train users, if necessary
c. Inform patients. For example, create flyers.
d. Inform healthcare institutions in the region

4 General appendices

4.1 Glossary

Affinity Domain (functional)	An XDS Affinity Domain is a group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure.
Affinity Domain) (technical)	An XDS Affinity Domain is made of a well-defined set of Document Repositories and Document Consumers that have agreed to share the clinical documents. An XDS Affinity Domain has a number of properties defined: 1. An XDS Affinity Domain does not deliver care. Only the EHR-CRs belonging to an XDS Affinity Domain as Document Sources and Consumers do. 2. An XDS Affinity Domain is managed by a single Document Registry Actor. Note: A distributed registry approach will be considered as a future and separate Integration Profile. For Document Source and Document Consumer Actors, the perception of a single Document Registry Actor hides the complexity of a distributed registry. 3. It includes any number of Document Repository Actors (a distributed configuration is the default, however, a centralised configuration with a grouped Registry/Repository is also supported). 4. It contains an explicit list of Document Consumer and Document Repository actors that participate in document sharing. The addition of a Document Repository or Document Consumer Actor is an administrative task that requires involvement of authorities maintaining the Registry and Repositories
BIG	Wet op de Beroepen in de Individuele Gezondheidszorg (Act for professions in individual healthcare)
BSN	BurgerServiceNummer (Citizen Service Number)
CAB	Change Advisory Board
EGiZ	Gedragscode Elektronische Gegevensuitwisseling in de Zorg – EgiZ (2013) (Code of Conduct for Electronic Data Exchange in Healthcare)
	Samenvatting Gedragscode Elektronische Gegevensuitwisseling in de Zorg - EGiZ (Summary of Code of Conduct for Electronic Data Exchange in Healthcare)
IHE	Integrating the Healthcare Enterprise
IHE-NL	IHE Nederland IHE Netherlands
PACS	Picture Archiving and Communication System
RfC	Request for Comments
RSO	Regionaal Samenwerkings Organisatie (Regional Cooperation Organisation (RCO))
STORK	Secure identTity acrOss boRders linked (see also: https://www.eid-stork2.eu/)
TLS	Transport Layer Security
VPN	Virtual Private Network
WGBO	Wet op de Geneeskundige Behandelingsovereenkomst (Medical Treatment Agreement Act)
Wbp	Wet bescherming persoonsgegevens (Personal Data Protection Act)

Wbsn-z	Wet gebruik burgerservicenummer in de zorg (Use of the Citizen Service Number in Healthcare Act)
Wcz	Voorstel wet cliëntenrechten zorg (Patient's rights in healthcare bill)
WGBO	Wet op de Geneeskundige Behandelingsovereenkomst (Medical Treatment Agreement Act)
ZSP	Zorg Service Provider (Healthcare Service Provider)

4.2 Concise explanation of IHE profiles

ATNA	Audit Trail and Node Authentication	Basic security through (a) functional access controls, (b) defined security audit logging and (c) secure network communications
BPPC	Basic Patient Privacy Consents	Method for recording a patient's privacy consent acknowledgement to be used for enforcing basic privacy appropriate to the use
CPMD	Community Medication Prescription and Dispense	Integrates prescription, validation and dispensation of medication in the ambulatory sector.
CT	Consistent Time	Enables system clocks and time stamps of computers in a network to be synchronised
DEC	Device Enterprise Communication	Transmits information from medical devices at the point of care to enterprise applications
DIS	Pharmacy Dispense Document	Records the dispense of medication to a patient
LCSD	Laboratory Code Sets Distribution	Distributes managed sets of clinical laboratory codes (battery, test and observation codes)
PAM	Patient Administration Management	Establishes the continuity and integrity of patient data in and across acute care settings, as well as among ambulatory caregivers
PDQ	Patient Demographics Query	Allows applications query by patient demographics for patient identity from a central patient information server
PIX	Patient Identifier Cross Referencing	Allows applications query for patient identity cross-references between hospitals, sites, health information exchange networks, etc.
RID	Retrieve Information for Display	Simple and rapid read-only access to patient-centric clinical information that is located outside the user's current application
RTM	Rosetta Terminology Mapping	Harmonises the use of existing nomenclature terms defined by the ISO/IEEE 11073-10101 nomenclature standard
SVS	Sharing Value Sets	Distributes centrally managed common, uniform nomenclatures
SWF	Scheduled Workflow	Integrates ordering, scheduling, imaging acquisition, storage and viewing for Radiology exams

XCA	Cross-Community Access	Allows to query and retrieve patient electronic health records held by other communities
XCPD	Cross-Community Patient Discovery	Supports locating communities with patient electronic health records and the translation of patient identifiers across communities.
XD-LAB	Sharing Laboratory Reports	Content (human and machine readable) of an electronic clinical laboratory report
XDR	Cross-enterprise Document Reliable Interchange	Exchanges health documents between health enterprises using a web-service based point-to-point push network communication
XDS	Cross Enterprise Document Sharing	Share and discover electronic health record documents between healthcare enterprises, physician offices, clinics, acute care in-patient facilities and personal health records
XDS-i	Cross-enterprise Document Sharing for Imaging	Update extends XDS to share images, diagnostic reports and related information across a group of care sites.
XDW	Cross Enterprise Document Workflow	Coordinates human and applications mediated workflows across multiple organisations
XPHR	Exchange of Personal Health Record	Content and format of summary information extracted from a PHR system for import into an EHR system, and vice versa
XUA	Cross-Enterprise User Assertion	Communicates claims about the identity of an authenticated principal (user, application, system...) across enterprise boundaries - Federated Identity. The '++' is an extension of the Profile attributes

4.3 Landscape of regional infrastructures in the Netherlands

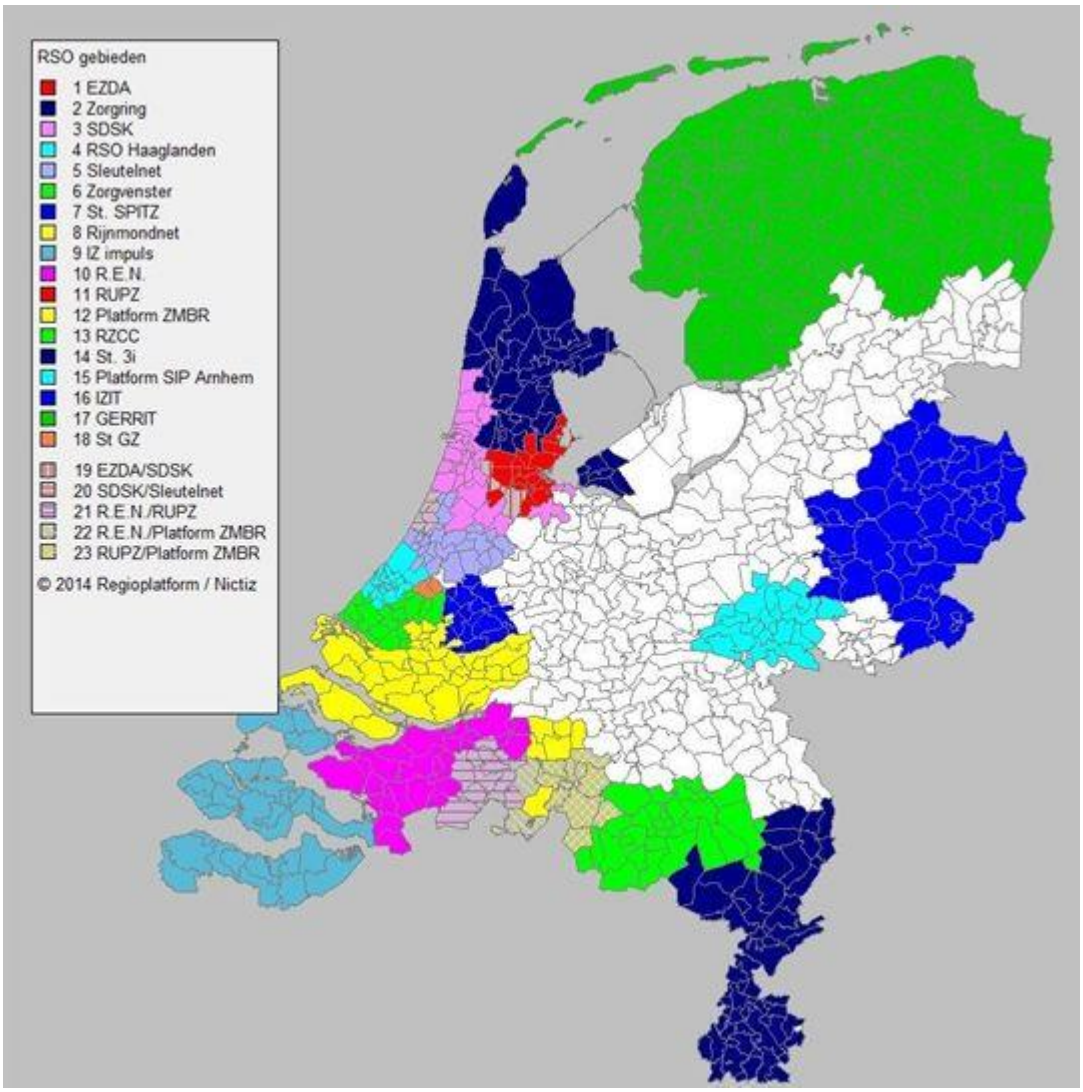


Figure 16 - RCOs in the Netherlands (2014)

Regional Cooperation Organisations which possess an XDS infrastructure:

EZDA / SIGRA	http://ezda.nl/
RZCC	http://www.rzcc.nl/
SDSK	http://www.sdsk.nl/
Stichting Gerrit	http://www.gerrit-net.nl/
Stichting Rijnmondnet	http://rijnmondnet.nl/
Sleutelnet	http://www.sleutelnet.nl/
UPZuid	
ZMBR	http://www.zorgnetwerkmb.nl/
ZorgNetOost	https://www.zorgnetoost.nl

NB: this list will be expanded in the next version.

National screening programmes

MammoXL http://www.mammoxl.nl/

*** End of document ***