Annex B
to
eHealth-INTEROP Report

Patient and health practitioner identifiers

in response to
eHealth Interoperability Standards Mandate

(SA/CEN/ENTR/000/2007-20 eHealth Mandate M/403 – Phase 1)

http://www.ehealth-interop.eu

Document History:

Annex B, Patient and health practitioner identifiers, to SA/CEN/ENTR/000/2007-20 eHealth Mandate M/403 – Phase 1 Report

Document Location: *http://www.ehealth-interop.eu*
Validity: *From date of publication until approval by ESOs, EC and EFTA*.
File name: *ESO_eHealth-INTEROP_AnnexB_v1000.doc*

Change History:

Date	Version (n.Nrr)	Changes file name format: ESO_eHealth-INTEROP_B0Nnn_CCYYMMDD.doc
2008-06-013< 2008-06-24	0.001 – 0.003	ID Annex in interim draft form.
2008-06-24	0.200	interim draft a) as background information to Wider Co-ordination Group meeting on 2008-07-09 and b) for general comment.
2008-08-25	0.370	Interim draft Including professional ID section, to PT for review.
2008-08-26	0.400	Consolidated draft of WGC review
2008-09-19	0.500	Added CALLIOPE in response to comment.
2008-11-26	0.600	Post comment editing started.
2008-12-22	0.900	Post-comment editing completed
2009-02-10	1.000	Final version approved by CEN, CENELEC and ETSI

Editorial project team:

Pantelis Evangelidis,
Georg Heidenreich,
Charles Parisot,
Melvin Reynolds (lead editor).

Please submit any comments on this document to:

Ms Mary van den Berg Standardization administrator	mary.vandenberg@nen.nl Tel.+ 31 152 690390 Fax + 31 152 690190	NEN-Healthcare Vlinderweg 6 NL-2623 AX Delft
Ms. Shirin Golyardi Standardization consultant	shirin.golyardi@nen.nl Tel.+ 31 152690313 Fax + 31 152690563	

Contents

Main Report, Summary of Report and Annexes A, C & D available from http://www.ehealth-interop.eu

1 Patient and health practitioner identifiers

1.1 General background

It is fundamental that patients are primarily citizens, to put it in other words every citizen is potentially a (future) patient. Thus, at least at a Member State level, the patient identification is usually mapped to another identity, the insurance and national identities being the two predominant ones. Therefore, it is true to say that at MS levels identity management systems are high profile projects with significant political stakes and involve huge investments. For these reasons every Member State developed its national/insurance/patient identity management system with a vision to achieve specific goals.

The interoperability aspect between national identity management systems and health identity management systems has not necessarily been taken into consideration or has been explicitly excluded while sketching the details of individual solutions. Identity management solutions in most cases were developed in silos, without useful exchange of information, and thus resulted in solutions across the EU, which are lacking the interoperability aspect between them. In many cases identity solutions within a given State is usual not to support common standard solutions. At the individual enterprise level issues are even more complicated and divergent.

In general, a citizen from one Member State cannot use their electronic identification (eID) token in another Member State for private or public services, whereas the non-electronic ID can in most cases be used.

The Member States, however, were quick to realize that interoperability in eID projects is a requirement and therefore significant progress has been made recently. At the EU level, a road map has been agreed upon by Member States that indicates an interoperable eID system by 2010 [1]. At the healthcare/insurance area interoperability at European level was kicked-off by Decisions 189 and 190 for the European Health Insurance Card (EHIC) [2] targeting to develop a means of identification for the European migrant worker (as well as tourist) and his entitlement to receive healthcare services while visiting another MS of its original residence either permanently or temporarily. An electronic version of this card (eEHIC) is currently under investigation for an interoperable solution across Europe. [3]

The EU has been funding several projects that are tackling the issue of identification from different dimensions. There is also work in progress in CEN with the European Citizen Card standards (15480 series) producing already a wealth of information. CEN has also contributed heavily on the patient and administrative healthcare data ISO standards (21549 Parts 5&6) which are consider as the base today not only for health cards but also in general for identification tokens.

In the healthcare domain IHE has provided implementation guidelines under its PIX/PDQ integration profiles, based on HL7 standards that provide solutions for a number of pragmatic use cases for cross-enterprise and intra-enterprise identification. [4]

Beyond the citizen/patient identification may refer to the healthcare professional, enterprise or device. Again, a number of approaches are currently in existence and are implemented in a bigger or limited success.

We outline here the current situation in terms of identity management interoperability and discuss a framework for working out a plan for internationally driven interoperability at European level as required by the Mandate.

1.2 Use-case requirements

1.2.1 Identity types

Identity is perceived differently in different domains; for our purposes with identity we refer to a set of (digital) data that uniquely identify a person, an organisation or an object. An identity management system (IDMS) is a system that deals with sociological, legal and technical aspects of an identity. An identity profile is a set of rules that define an IDMS process (list of actions) for a specific use case scenario.

Identity is usually used for one of the following:

- **Identification**
  'the process of using claimed or observed attributes of an entity to deduce who the entity is' [5]: e.g. *identifying an X-ray as belonging to Mr. X*
- **Authentication**
  'the corroboration of the claimed identity of an entity and a set of its observed attributes.' [5]. In simple terms authentication is the process of making sure that the claimed identity is the true one, e.g. *identifying an insured person as the person claiming to be Mr. X.*
  Authentication is based on one of the following principles:
  - Checking against something known: e.g. a password or a PIN
  - Checking against something possessed: e.g. a token (smart card for example)
  - Checking against something inherent: e.g. a biological characteristic like the fingerprint or the retina of the eye
- **Authorisation**
  the process of deciding what attributes (rights or privileges) one may have, based on a patient identity, e.g. *a cardiologist having access to their patients' medical summaries*
- A combination of the above

1.2.2 User requirements

User requirements for identification fall within the following perspectives:

Industry Perspective

Industry innovation is what usually creates gaps between standards and practice. Industry is by definition the body that gives life to standards and thus their perspective is always important. In general industrial corporations (vendors) are looking for interoperable standards. When it comes to identification the main required interoperability functions cover items like Definition of Identifiers and Verification, Patient Registry Addition and Manipulation, Resolution of Duplications, Demographics.

Policy Perspective

Member States have agreed, under the Lisbon agenda, to a clear perspective for European citizen mobility and provision of quality healthcare services across the Union. However, citizen (and thus patient) identification has left to the individual countries in a direct call for creation of interoperable solutions.

Healthcare Professional/Organisation Perspective

Healthcare providers are looking for a common language to use when it comes to identification (including authentication and authorisation). A patient identity that is standard throughout the industry, offers healthcare enterprises increased confidence and improved quality of services.

Patient Perspective

The current trend in healthcare is to provide means that enable patients to play an important role in their own healthcare. Systems that support such functionality should offer identification services that will support self-health management, and make feasible maintaining and updating their own health records and better communicating with their physicians, in a secure and quality environment. In other words, the patient doesn't really care about identity and identification. It is the legal, administrative and fiscal environment that requires identification services to provide the quality healthcare services that the patient really cares for.

More specifically patient identification[1] is needed for different purposes and applied in different environment. Identification at a country level is required for a person to receive healthcare services, but also for the organisation to receive reimbursement of these services. As facilitation for such services usually comes from a state oriented procedure a centralized (in most cases) or decentralised identity management system is usually put in place. Interoperability is strongly brought in the picture when health

[1] Refs [8]-[12] contain useful information and background material fro the interested reader

information is widely shared within one country, even more when shared across countries, a situation now appearing within the EU, representing not only a practical necessity but also a political goal. This background, or high-level overview whichever name one decides to use, such a type of identification is reflected in a set of requirements such as:

1. Interoperability (across Member States, but also across e-government services)
2. Safety (including public safety and coordinated response to epidemic threats)
3. Security (including privacy protection)
4. Quality/reliability
5. Efficiency
6. Communication
7. Demographics (including regional or cultural related wellness and hygiene)
8. Reimbursement support

The user identity that is communicated in a cross-enterprise transaction represents another source of patient identification requirement. This front office, or organisation level which ever name one decides to use, type of identification needs to include for example enough information about the user core attributes and serves as the main vehicle for document exchange. This calls for a distributed user identity management and cross-exchange of identified patient information. Requirements from this perspective are:

1. Demographics (in terms of patient orientation)
2. EHR/Summary retrieval (in a cross-enterprise environment)
3. Minimisation of (Duplication/False identification) errors
4. Secure transactions (including encryption and signatures)
5. Traceability
6. Description of the user core attributes

Unique identification of all parties is clearly essential for a number of purposes of different orientation. From the healthcare provider perspective an enterprise can impose a single identification technology and maintain a single (patient/device/personnel) directory. However, it goes without saying, that multiple enterprises that participate in an affinity domain may not be able to impose a single technology or directory. However, current standards on identification from the various SDOs used a combination of demographic attributes for identification, may solve the problem without requiring a unique identification number.

1.3 Base Standards[2]

One can arrive to four key pre-requisites necessary to achieve functional interoperability on patient identification:

1. A standardized Reference Model (namely, the id information architecture)
2. Standardized service interface models to provide interoperability between the identification services and other components such as demographics, terminology, access control and security services.
3. A standardized set of domain-specific concept models, namely, archetypes and templates for e.g. authentication, attribute determination and other domain-specific concepts.
4. An assigning “authority” or a list of those that offer unique identification to subjects of healthcare

A standard covering 1 above can be considered as a ***patient identification base standard***. Base standards, as defined in section 7.3.1 represent generic and/or very specific information.

Parts 5 and 6 of ISO/IEC 21549, “Patient health card data”, specify a set of personal data that can be held on a general electronic patient health card for use in multiple applications. This set is derived from Logical Data Structure (LDS) set defined by the International Civil Aviation Organisation (**ICAO)** for

2 The order of sections 1.3 & 1.4 is arbitrary; the reader may choose to read them in the order it suits; as a loose recommendation the writers would suggest for the readers with a standardization orientation to read first section 1.3, while readers from the implementation arena to read first section 1.4.

machine-readable travel documents. A subpart of this set is used be the European Health Insurance Card (EHIC) set. A mapping to HL7-RIM is foreseen but not yet completed. It should be noted that the LDS defined by the ICAO for machine readable travel documents is derived from a number of ISO standards for biometric systems.

HL7 PID (Patient Identification Segment) is used within an HL7 standardised environment by all applications as the primary means of communicating patient identification. It is broader than the previous in the sense that it contains additional fields for patient identifying and demographic information, but it still refers to permanent information that, for the most part, is not likely to change frequently.

ISO/PDTS 22220 also covers the same area, but with a still broader approach that not only refers to data, but moves to data communication and linkage (messaging base) and biometrics (authentication base).

Other useful base standards on patient identification include:

- ENV 13606-1, 13606-3, 13606-4
- ENV 12967 (HISA) patient component
- RIM HL7 V3 Master Patient Index
- HL7 v2.5, Health Level Seven, version 2.5, Ann Harbor, Michigan
- EN 14484:2003 “Health Informatics – International Transfer of Personal Health Data covered by the EU Data Protection Directive – High Level Security Policy
- EN 14485:2003 “Health Informatics – Guidance for Handling Personal Health Data in International Applications in the context of the EU Data Protection Directive;

Almost every patient identification standard, including the three plus six above, or implementation guideline of those reviewed in Annex A (Inventory) refer to particular base standards that either deal with data representation (country, language, gender etc.), messaging (SAML, X.509 etc), or tokens (smartcards, biometrics etc.).The following list offers an indication of the data representation, messaging and tokens standards these patient identification base standards use (indicative not exhaustive list for proof of concept purposes, the reader is referred to the respective standards for more information)

- Data representation
  - ISO 8601:2004, Data elements and interchange formats - Information interchange - Representation of dates and times
  - ISO/IEC 8824-1:2002, Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation
  - ISO/IEC 8825-1:2002, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
  - ISO/IEC 8859 series: 1998, Information technology - 8-bit single- byte coded graphic character sets - Part 1-4: Latin alphabet No. 1-4
  - ISO/IEC 10646: 2004, Information technology - Universal Multiple-Octet Coded Character Set (UCS*)*
  - ISO 639 series: Code for the representation of names of languages
  - ISO 3166-1: :2006 With Cor1:2007 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes
  - ISO/IEC 5218:2006 Information interchange – representation of human sexes
  - ISO/IEC 7501-1:1997 Identification cards – Machine readable travel documents – Part 1: Machine readable passport
  - ISO 20302 “Numbering system and registration procedure for issuer identifiers”
- Tokens
  - ISO/IEC 7810: Integrated Circuit Cards
  - ISO/IEC 7816 series: Identification cards -- Integrated circuit(s) cards with contacts
  - **ISO/IEC JTC 1/SC 37 Standing Document 2,** Vocabulary on Biometrics
  - A new project ISO/IEC 29144 – The Role of Biometrics in Identity Management, may be of particular interest when completed.

- Communication (messaging/security)
  - W3C Recommendation: SOAP http://www.w3.org/TR/soap12-part1/
  - ebXML Business Process Specification Schema Technical Specification v2.0.1, http://docs.oasis-open.org/ebxml-bp/ebbp-2.0/2.0.3/
  - OASIS SAML: Security Assertion Markup Language
  - ITU-T X.509:1997 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
  - ITU-T X.811:1995 Information Technology -Open Systems Interconnection – Security Frameworks For Open Systems: Authentication Framework
  - ITU-T X.813:1996 Information_Technology- Open Systems Interconnection – Security Frameworks In Open Systems: Non-Repudiation Framework
  - HL7 V2 and V3 Patient Management

1.4 Profiles

Standards are necessary both for integration and for interoperability. However, any actual implementation of a standard requires some form of tailoring. Therefore, in developing practical and effective interoperability solutions, the industry relies on integration profiles which are business processes describing selected real-world use-cases. As explained in section 7.3.2 profiles represent a layer that describes how a set of (base) standards can be put into a functional order to serve an interoperable practical solution of a pragmatic use case. Here we are concerned with two use cases: (a) patient identification in the (a1) back-office and (a2) the front office, and (b) healthcare professional identification again in the (b1) back-office and (b2) the front office. A third use case usually accompanying the above two, medical device identification, is not considered here.

This section proposes a European approach for the above use cases, by reviewing relevant existing profile solutions. Three actors are identified in all cases: the patient identity source, the patient identifier manager and the patient identifier consumer.

1.4.1 Patient identification: Back-office

The European Health Insurance Card (EHIC), which replaced the paper forms E111, E110, E 128 and partly E 119 in its present phase is eye-readable only. This plastic card has been designed as a first step towards a full-blown electronic system where patients, healthcare professionals and social security institutions can communicate without paper in cross-border situations, in the same way as they would within countries.

The EHIC provides a minimum set of "eye-readable" data to be used by migrant workers of the European Union in a member state other than the Member State of the insurance or residence, in order to identify the insured person, the competent institution and the card stating the entitlement to receive health care during a temporary stay in another member state. The EHIC data elements are defined for the optical personalisation of the European health card. An official electronic data set definition does not exist yet. Table XX shows the EHIC data elements of the optical card design. All of these data elements are mandatory.

According to EU regulation 1408/71, all persons insured under the legislation of a member state are entitled to healthcare during a temporary stay in another member state. The EHIC certifies this entitlement. The DG EMPL Administrative Commission for Social Security for Migrant Workers (called CA.SS.TM) is responsible for regulating it. According to it cross-country electronic communication is centrally controlled following the EESSI guidelines. EESSI stands for “Electronic Exchange of Social Security Information". It is a project of CA.SS.TM. that is expected to use the sTESTA network.

Decision 189 [3] of CA.SS.TM prescribes that the minimum data held on the card shall consist of:

- surname and forename of the card holder,
- personal identification number of the card holder or, when no such number exists, the number of the insured person from whom the rights of the card holder derive,
- date of birth of the card holder,
- expiry date of the card,
- Member State issuing the card

- identification number and acronym of the competent institution,
- logical number of the card.

The minimum set contains enough information to identify the holder and the competent institution. In an on-line situation it can enable verification of the holder's entitlement through communication with that competent institution.

From the beginning of the introduction of the EHIC two additional steps were foreseen: electronification of the card (eEHIC) and intensification of the cross-border electronic exchanges between social security institutions. in order to fulfil these steps created an Ad-Hoc group to work upon common principles and starting points for further work on the introduction of the electronic European Health Insurance Card (eEHIC).

The electronic EHIC:

- will be electronically read in the premises of the Health Care Providers (general practitioners, pharmacists, hospitals, dentists and other health related practitioners) equipped with the appropriate card reader and
- its validity can, under certain conditions and depending on the Member States, be verified on-line.

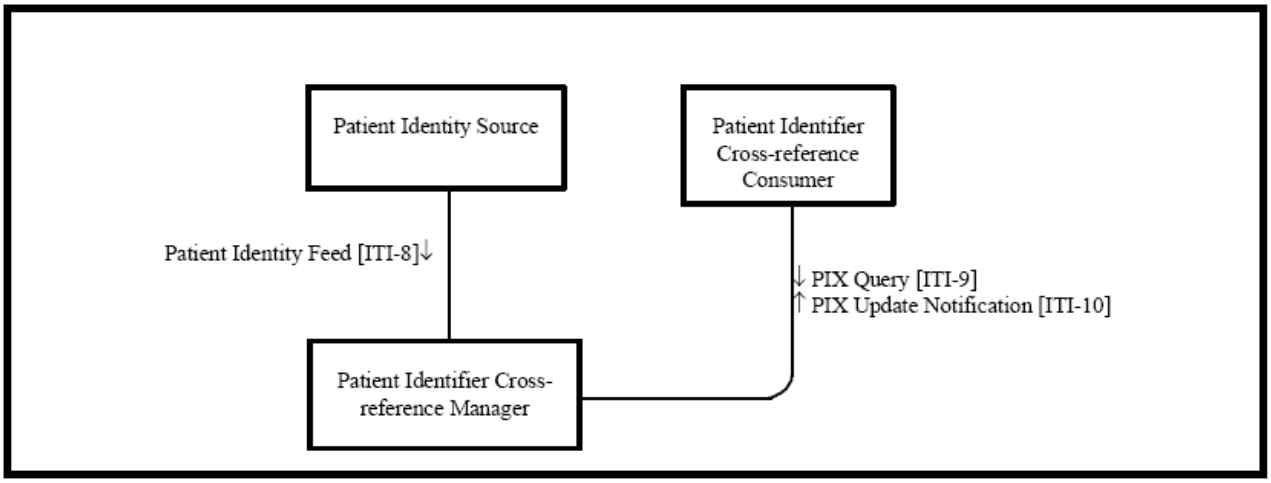
An official electronic version of the EHIC does not exist today. However CEN/ISSS/eEHIC responsible for the electronification of the EHIC is currently in an advanced state of a final CWA that describes the eEHIC as a means of electronic identification of European citizens entitled to receive healthcare services (i.e an electronic patient ID). The eEHIC in terms of data is based fully on ISO/IEC 21549-5. Furthermore, the eEHIC CWA aims at offering at least one profile for the European Citizen Card (ECC) as described in CEN 15480 series. Both the eEHIC and the ECC are exploiting the metadata interoperability middleware of ISO 24727 series. It is to be noticed that the interoperability between any future ISO 24727 compliant system and the other national or legacy pre-existing systems is also considered (taken care of) in both these standards. Thus, in an initial assessment it seems reasonable to claim that the background patient identification framework for the European Union is already (almost) in place.

1.4.2 Patient identification: Front-office

When it comes to the front office patient identification (management), the central focus is on "sharing records". To be able to exchange health records or parts of them (e.g. documents), within an enterprise, or in a cross-enterprise scenario, it is critical that each element of the record be reliably associated with the corresponding patient (Patient Id).

The IHE/PIX profile specifies how patient identifiers used in different healthcare institution could be linked to each other when verified to be related to the same patient. This profile, called Patient Identifier Cross-referencing Integration Profile (IHE-PIX) [4], supports the information exchanges for cross-referencing of patient identifiers from multiple patient identifier domains.

The figure below (from [6]) shows the actors directly involved in the Patient Identifier Cross-referencing Integration Profile and the relevant transactions between them.



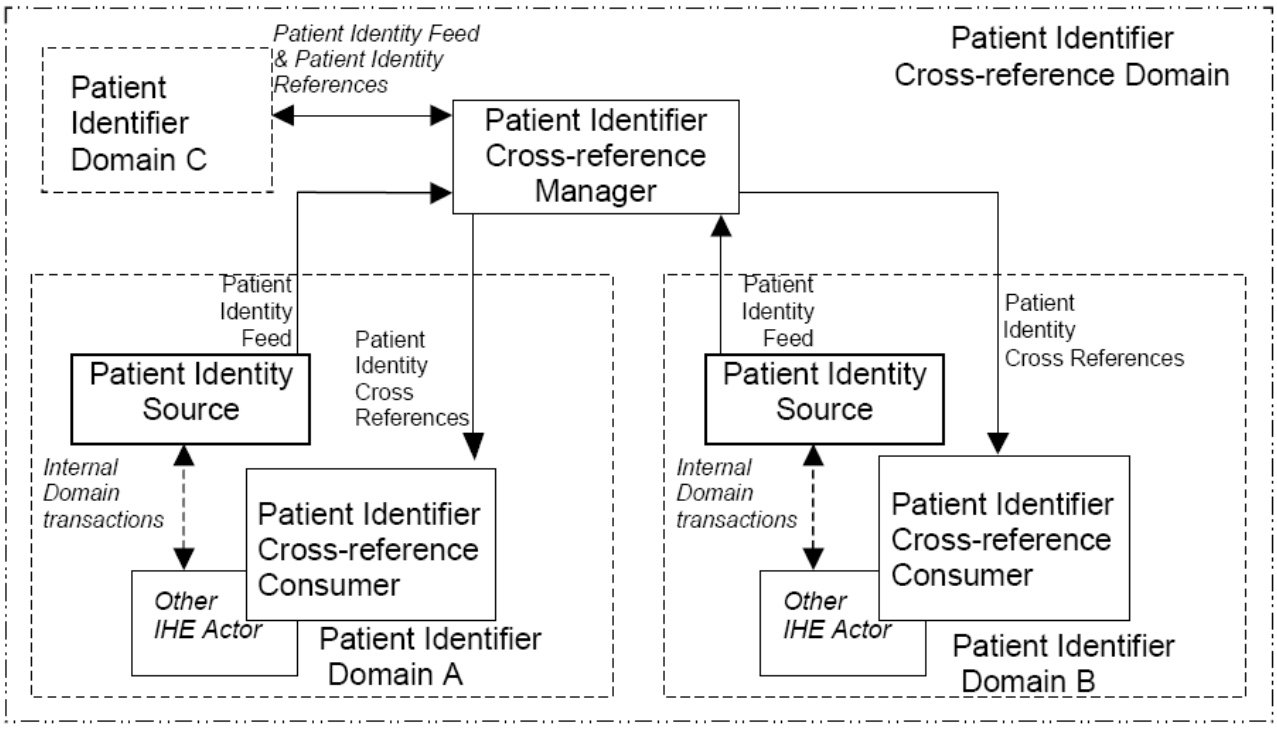
PIX therefore supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions:

- The transmission of patient identity information from an identity source to the PatientIdentifier Cross-reference Manager.
- The ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via update notification.

The profile may be implemented by using one of the Patient Identity Source Actor as the authoritative source of Patient Identifiers (master patient ID) for the record sharing domain (e.g. an XDS Affinity Domain) and a Patient Identifier Cross-Reference Manager Actor for managing cross-reference identities across different Patient Identifier Domains (master or not).

A Patient Identifier Domain is defined as a single system or a set of interconnected systems that all share a common identification scheme (an identifier and an assignment process to a patient) and issuing authority for patient identifiers.

All these are shown in the figure below (from [6]).



A Patient Identifier Domain has the following properties:

- A set of policies that describe how identities will be defined and managed according to the specific requirements of the domain.
- An administration authority for administering identity related policies within the domain.
- A single system, known as a patient identity source system, that assigns a unique identifier to each instance of a patient-related object as well as maintaining a collection of identity traits.
- Ideally, only one identifier is uniquely associated with a single patient within a given Patient Identifier Domain.
- An “Identifier Domain Identifier” (known as assigning authority) that is unique within a Patient Identifier Cross-reference Domain.
- Other systems in the Patient Identifier Domain rely upon the identifiers assigned by the patient identity source system of the domain to which they belong.

The Patient Identifier Cross-reference Domain embodies the following assumptions about agreement within the group of individual Identifier Domains:

They have agreed to a set of policies that describe how patient identities will be cross-referenced across participating domains:

- They have agreed to a set of processes for administering these policies;
- They have agreed to an administration authority for managing these processes and policies.
- All these assumptions are critical to the successful implementation of this profile.

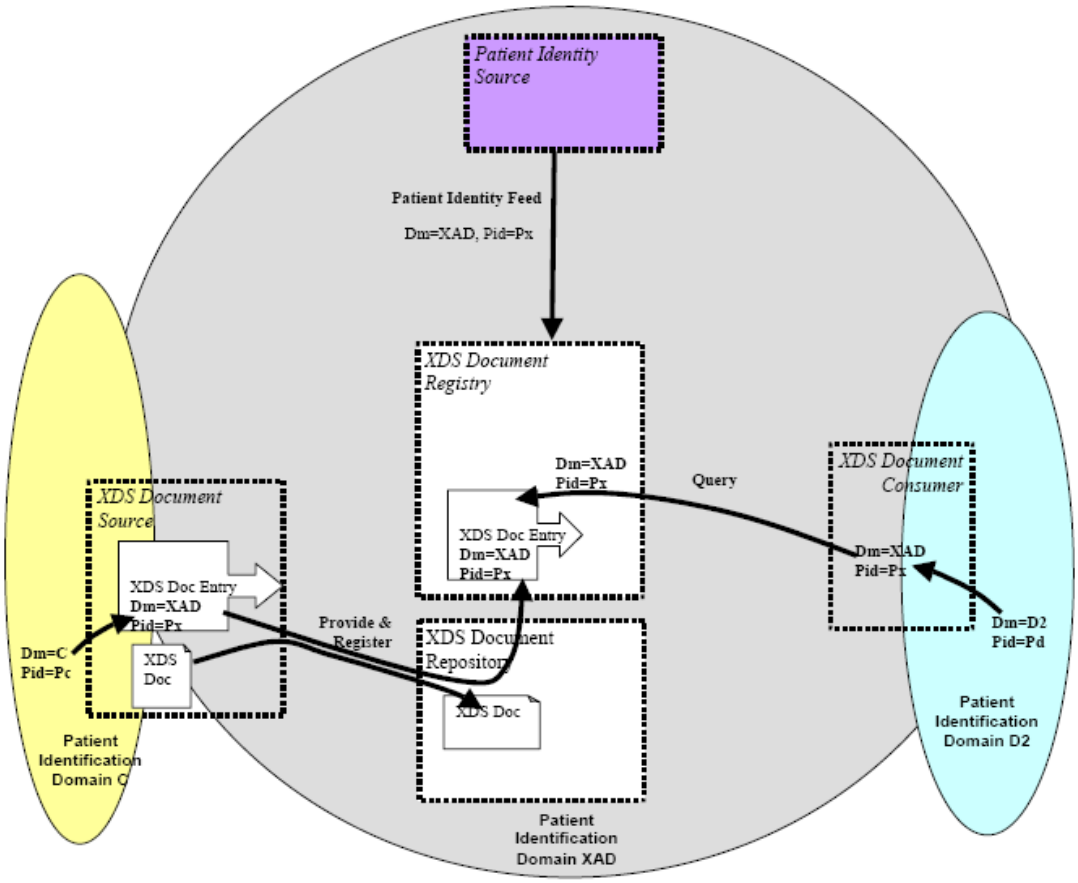
In regards to health records sharing, one may use the example of document sharing, where the following principles are defined:

1. The Patient Identifier Domain managed by the Patient Identity Source Actor in the Affinity Domain is the source of patient identifiers used by the XDS Document Registry to link Documents to a specific Patient. This Patient Identifier Domain is called the XDS Affinity Domain Patient Identification Domain (XAD-Pid Domain).

2. Submission Requests for Documents related to Patients with IDs not registered in the XDS Affinity Domain Patient Identifier Domain shall be rejected by the XDS Document Registry.

3. As XDS Document Sources and Consumers may belong to different Patient Identification Domains, these systems need to cross-reference their own local Patient ID to the XAD-Pid Domain, using the IHE Patient Identifier Cross-referencing Integration Profile (PIX) for this purpose.

The figure below (from [7]) depicts an example of an XDS Affinity Domain with its Patient Identifier Domain (called XAD) and two local health IT systems (e.g. EHRs) where the cross-referencing is performed internally to the Document Source and the Document Consumer Domains (Domain C and Domain D2 respectively).



From the above one can depict that patient identification in the front-office is well supported by the PIX Integration Profile and may rely on a Patient Identifier Cross-reference Domain regulated by the EU EHIC framework.

Other useful relevant profiles include:

- Service Functional Model Specification - Entity Identification Service (EIS), HSSP (joint endeavour between HL7 and OMG), Version 0.997 July 17, 2006
- Person Identification Service (PIDS), (a.k.a. Patient Identification Service), Final Submission - Revision 7, OMG CORBAmed DTF, 98-01-09

In Austria the “XCA Integration Profile” of IHE [14] has been found to be a necessary element to deal with patient IDs within the Austrian EHR. In addition to “domains” it introduces “communities”. This enables the information exchange between existing groups who use different patient ID systems.

One may choose to rely on the IHE/PIX Profile using CA.SS.TM Decisions on Clearing Institutes as Patient Identity Source for each MS and EESSI as Patient Identifier Cross-reference Manager. Base standards on data identification to be used are ISO 21549-5 and the (not yet official) CEN CWA eEHIC which is based on it.

1.5 Interoperability Workplan

It is, at the time of drafting this Report, not clear what new work on base standards or profiles needs to be undertaken. New requirements may emerge from the epSOS and CALLIOPE projects and would need to be accommodated appropriately in the latter half of Phase 2 of the mandate work programme. This could present a significant resourcing challenge.

Anchor points
(application of the Chapter 4 methodological approach to the patient identification use case): To address the front-office interoperability, between the identity management systems and the health care IT systems used in care delivery, a choice of Base Standards exist. Profiling has already been done. Europe needs to recognise one such Profile to ensure that all EU healthcare systems support the access to cross-referencing and patient demographics queries in an interoperable manner.

New requirements may emerge from the epSOS and CALLIOPE projects and would need to be accommodated appropriately in Phase 2 of the mandate work programme. This could present a significant resourcing challenge.

2 Health Professional ID

2.1 Background

The main political document behind health professional identification is the European Directive 2005/36/EC on the recognition of professional qualifications. The Directive makes reference to a unique professional card (that would implicitly mean a unique id number):

This professional card should make it possible to monitor the career of professionals who establish themselves in various Member States. Such cards could contain information, […] *on the professional's qualifications, his legal establishment, penalties received relating to his profession and the details of the relevant competent authority.*

2.2 Requirements

2.2.1 Policy

The main requirements to be met are a) free movement of health professionals in Europe, and b) protecting patients from professionals that could be subject to severe disciplinary sanctions. Other (future) requirements include validation of continuing education and access to medical records.

A special event at the European Parliament during on October 17th 2007 defined the (minimum) identification information (printed) on the card as the name and ID of the health professional, while information also useful to be found on the card include:

- The profession;
- The logo of the competent authority;
- The name and contact details of the competent authority;
- A signature area;
- A security hologram containing the letters of the country of origin.

2.2.2 Organisation

In additional to their need to be able to conform to the policy requirements the high-level organisational requirements are commonly such things as the relationship of an individual practitioner to their organisation, the relationship to one or more departments and the role(s) preformed within those departments.

Although none of these are primarily requirements of an identifier, the identification systems used must be capable of supporting these requirements in a practical way.

2.2.3 Healthcare professional

In additional to their need to be able to demonstrate conformity to the policy and organisational requirements the healthcare professional requirements are commonly such things as the relationship of an individual healthcare professional to one or more organisations, their relationship to one or more departments and the role(s) preformed within those departments, their peer relationship to colleagues within organisations and departments and their relationship to patients.

Although none of these are primarily requirements of an identifier, the identification systems used must be capable of supporting these requirements in a practical way.

2.3 Work in progress

In late February 2008 the European Commission decided to give a grant of almost 300Keuro to the HPRO Card working group (http://www.hprocard.eu/) in order, among other tasks, to:

- identify competent authorities of the health professional listed in the directive in each of the 27 Member states;
- study the current state of the art of health professional cards through all European Union;
- study the interoperability of the different health professional's strong authentication system.

The work on the implications of EU policy started on June 2008 and the initial results on identification are expected by the end of the year.

The organisational and healthcare professional requirements are likely to emerge with some clarity, in the context of the HPRO Card work, from the epSOS project in 2009. It is to be noticed also that the NETC@RDS project has successfully demonstrated the feasibility of patient and secure HPC identification as well as cross-border on-line verification of patient entitlement to receive medical treatment abroad but inside the EU/EEE. To this end, a strong synergy between the NETC@RDS, HPRO Card and ePSOS projects would be powerful for the implementation of some of the use cases outlined in Section 5/ Annex D and put them to the test.

Thus, in 2010 it may therefore be necessary to revisit the existing base standards so that they can be amended to address newly emergent issues, and to define necessary profiles.

2.4 Interoperability Workplan

It is, at the time of drafting this Report, not clear what new work on base standards or profiles needs to be undertaken. New requirements may emerge from the HPRO Card, epSOS and CALLIOPE projects and would need to be accommodated appropriately in the latter half of Phase 2 of the mandate work programme. This could present a significant resourcing challenge.

Anchor points
(application of the Chapter 4 methodological approach to the professional identification use case): Base Standards exist to healthcare professional identity in the health care IT systems used in care delivery. Profiling is required to recognise at least one (probably more) Profile to ensure that healthcare systems support the professional identification in an interoperable manner.

New requirements may emerge from on-going work at European level and would need to be accommodated appropriately in Phase 2 of the mandate work programme. As for patient identification, this could present a significant (though less intense) resourcing challenge.

References

The following material, specifically referenced in the body of this Annex gives supporting information.

[1] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - "i2010 – A European Information Society for growth and employment" {SEC(2005) 717}, http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

[2] 1. Decision No 190 of 18 June 2003 concerning the technical specifications of the European Health insurance card (OJ L 276 27.10.2003 p.4)
2. Decision No 189 of 18 June 2003 aimed at introducing a European health insurance card to replace the forms necessary for the application of Council Regulations (EEC) No 1408/71 and (EEC) No 574/72 as regards access to health care during a temporary stay in a Member State other than the competent State or the State of residence (OJ L 276 27.10.2003 p.1)

[3] WS/eEHIC/07/002Rev.1 CEN/ISSS Workshop on Interoperability of the electronic European Health Insurance Cards (WS/eEHIC), Adopted Business Plan (version 1.0), Brussels, 2007

[4] IHE IT Infrastructure Technical Framework, Patient Identifier Cross-referencing (PIX), by the IHE ITI Technical Committee, http://www.ihe.net/Technical Framework/index.cfm#IT

[5] MODINIS – IDM, 2008, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectDocs

[6] 1. IHE IT Infrastructure Technical Framework, Volume 1, (ITI TF-1) Integration Profiles, Revision 4.0 – Final Text, August 22, 2007, ACC/HIMSS/RSNA
2. IHE IT Infrastructure Technical Framework, Volume 2, (ITI TF-2) Transactions, Revision 4.0 – Final Text, August 22, 2007, ACC/HIMSS/RSNA

[7] IHE IT Infrastructure Technical Framework Supplement, Cross-Enterprise Document Sharing (XDS)

[8] General and detailed specifications for patient's identification, 2001-2002, GIP GMSIH (France) (french):

[9] Good practices referential for healthcare patient's identification; BP S97-723, AFNOR (France)

[10] Strategic Short Study - Names and Numbers as Identifiers (Final report version 2.0); Robin Hopkins, CEN/TC 251/N98-083 -

[11] Analysis of unique Patient Identifier Options, Final report, Soloman I. Appavu, November 24, 1997, DHHS

[12] Foundations for the future, Priorities for health informatics standardisation in Australia, 2005–2008, Information and Communications Technology Standards Committee (ICTSC) 2004

[13] Patient Identification : Concepts and recommendations , TS, CEN/TC251 – WI, Draft - Version 0.5, 2008, CEN/TC 251/WGI/N07-035

[14] XCA: IHE IT Infrastructure Technical Framework, Supplement 2007-2008, Cross Community Access XCA, Draft for Trial Implementation, August 15, 2007,