PD CEN/TR 15872:2014

BSI Standards Publication

Health informatics — Guidance on patient identification and cross-referencing of identities

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 15872:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 64182 4
ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2014.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 15872

March 2014

ICS 35.240.80

English Version

Health informatics - Guidance on patient identification and cross-referencing of identities

Informatique de santé - Guide relatif à l'identification des patients et au référencement croisé des identités

Medizinische Informatik - Leitfaden für die Patientenidentifikation und Kreuzreferenzierung von Identitäten

This Technical Report was approved by CEN on 17 February 2009. It has been drawn up by the Technical Committee CEN/TC 251.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TR 15872:2014 E

Contents

Page

Foreword

This document (CEN/TR 15872:2014) has been prepared by Technical Committee CEN/TC 251 “Health informatics”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

1 Scope

This Technical Report addresses the issue of multiple identifiers that may refer to the same person. It describes the management of patient identification and cross-referencing of identities and provides some practical guidance for addressing implementation of standards, reports, guidelines, methods, etc. The need to identify a person unambiguously is an important component for the interoperability of health information systems.

Within healthcare there is an essential requirement for good quality information, not least to uniquely identify an individual to ensure that the appropriate and relevant care can be delivered irrespective of geography, time and situation. To ensure that health care providers have access to information about an individual patient, it is vital that the patient can be reliably identified within a Health Care Information System. Currently, a given patient may have several identifiers corresponding to different geographical locations, different health care organisations or various specialities. The allocation of multiple identifiers and related processes increases the risk of identification error within one or more information systems and as a result, might compromise the safety of a patient.

The quality of identification ensures that health care providers have access to patient information, facilitating closer coordination and continuity of care, improving service in terms of prevention and follow-up. Quality will be pursued within the framework of:

— medical care in a hospital information system (HIS): covering all the stages from patient identification to admittance to the health care organization or directly to the care unit or emergency care, through to the issuing of reports by the different health care services (medical and medico-technical services);

— continuity of care;

— patient mobility.

Because electronic heath care records may be updated by several and various healthcare providers over a long period of time, the patient identification needs to be formalized in such a way to ensure that the correct patient's healthcare record is being accessed.

In the regions or the countries where a national unique patient identifier is not used, the patient is identified by using patient identifiers for each healthcare system, wherever the patient is registered. Even within an individual healthcare organization, the patient may be identified by a specific identifier for an individual ward or a medical support unit. To ensure the continuity of care and the sharing of patient information, it is necessary to reliably link together the different patient identities within what we will call a "patient identifier cross-reference domain".

The need to cross-reference identities appears when a healthcare provider wants to access all the healthcare information for one patient and that information is contained in different healthcare systems managed by several healthcare professionals or organisations.

In recent years, many research studies and implementations have taken place to try to resolve this issue. This document provides an overview and proposals for the management of the patient identities and the cross referencing of identities and provides guidance for authorities, organisations, project managers and users.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/TS 22220:2011, *Health informatics — Identification of subjects of health care*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
alias
assumed name that can be specifically applied to disguise identity, which, in a healthcare situation, might be used to protect a famous person receiving treatment or an individual receiving sensitive treatment in, for example, a drug or alcohol rehabilitation unit or sexual health clinic

[SOURCE: ISO/TS 22220:2011]

3.2
collision
case in which two or more different patients are represented by the same patient identity

EXAMPLE In the cardiology service, the nurse who is consulting the record of Mr Jean Martin, finds that some data are not consistent between then (for example, in the same day, two effort trainings were done). She suspects a collision of two patients. After checking the patient identification server, she detects two Mr Jean Martin; one is born in January 25th, 1950 and the second on June 25th, 1950.

[SOURCE: IHE-PIX]

3.3
duplicate
case in which several identities represent the same patient in the same patient identifier domain

3.4
federation cross-referencing index
index that carries the federative identities within a federation cross-referencing domain

3.5
healthcare provider
person or organization who is involved in, or associated with, the delivery of healthcare to a patient, or caring for patient wellbeing

3.6
identifier
sequence of characters which is used by one or more systems to represent a person (a patient) and reference individual information within his care process and which is unique within a Patient Identifier Domain and linked to the traits of the Patient

Note 1 to entry: The identifier is called Subject of Care identifier in ISO/TS 22220.

EXAMPLE They are many types of identifiers: Person identifier, Patient identifier, Unit record Number.

3.7
linked identities
case in which, for a given patient, several identities (duplicates: see above) were created, which can lead to a clash between them

Note 1 to entry: The identification system will have the capability of keeping track of these duplicate identities. After correction, the duplicate identities are linked and one of the identity becomes the primary and the others become “ghost” identities. When new healthcare information is recorded, they will be attached to the Patient Identity Source.

EXAMPLE Ms Alice Berthon got married between two stays in hospital. She prefers now to use the name of her husband Mr. Martin. It is possible that within EHRs, she has two records: one with one identifier and the name of Berthon and a second record with another identifier and the name of Martin. This is a duplication and these need to be kept track of and solved. After correction, the duplicate identities are linked and one of the identities (Miss Berthon) becomes the primary and the others becomes "ghost" identities.

3.8
Patient Identifier Domain
domain in which, in the ideal world, the patient has one and only one Patient identifier and a common identification scheme which is used between systems for sharing healthcare information within the domain, and in which the identifier is assigned by the assigned authority

EXAMPLE 1 Hospital St Vincent is a Patient Identifier Domain. The patient of the Hospital St Vincent is identified at the entrance with one and only identifier. All systems in hospital share the same patient identity delivered by one system: the Patient Identity Source.

EXAMPLE 2 The Insurance which delivers an Insurance card with identifier is an Insurance Identifier Domain. The country which delivers a citizen card is a citizen Identifier Domain.

[SOURCE: IHE-PIX]

3.9
Patient Identifier Cross-reference Domain
domain which consists of a set of Patient Identifier Domains, known and managed by a Patient Identifier Cross-reference Manager Actor who is responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains

Note 1 to entry: 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.

Two **models** of implementation of a Patient Identifier cross-reference domain can be managed:

- Federation Patient Identifier cross-reference domain, where one member of the identities in the Cross Referencing Information System is always the federative identity (the Master),

- Correlation Patient Identifier cross-reference domain, where the Cross Reference manager actor manages a list of identities defined in the cross referenced identification domains where all patient identities are in the same level.

EXAMPLE 1 In England and in the Netherlands, at the country/regional level, the NHS number or the BSN are the federative identifier. When two healthcare providers want to share medical information for a patient, they refer to the NHS number in UK or BSN in the Netherlands.

EXAMPLE 2 In a country where the national identifier does not exist, a patient who has several medical records split in several healthcare provider systems, the mechanism to link all the records is based on a correlation model where the list of all patient identifiers linked to the patient identifier domains is available.

3.10
Patient Identity
representation of a real person within a **Patient Identifier domain (called also Patient identifier Assigning Authority)**, which, by extension, could also represent a fictional person for some purposes (testing or training)

Note 1 to entry: The patient identity is composed of:

— an identifier, ID;

— a set of traits, {T}.

EXAMPLE The person named M. Jean Martin is represented in the hospital St Vincent in Paris by the record (sample): “23654, Martin, M., Jean, Male,19500125”.

3.11
Patient Identity versions
patient's traits that are changed because of events during the life and that then need to be modified or corrected

Note 1 to entry: The author of the modification will have the permission to update the record and the modification will be done in a controlled procedure and audited.

EXAMPLE 1 Ms Alice Berthon was represented in hospital St Vincent as “23478, Berthon, Miss, Alice, Female, 19800325, v1”.

She got married and now she preferred to be named Ms Alice Martin. The representation will be changed on “23478, Martin, Ms, Alice, Female, 19800325, v2”

EXAMPLE 2 Mr. Richard Louis Kerren was an outpatient in hospital St Vincent and he was represented as “43542, Kerrene, Male., Richard, Louis, Male,19540613,v1”.

When he comes back to hospital for a second visit, the administrative staff searches his name and they do not find the record. After a careful research, they discover that the name was not correctly registered. They update his name: the new representation is “43542, Kerren, Male, Richard, Louis, Male,19540613,v1”.

3.12
traits
characteristics defined in a **Patient Identifier domain**, and “commonly” used in the real world, as a part of a patient identity

Note 1 to entry: These could be criteria in the query of patient identity in the Patient. The Patient Identity Source Actor is retrieved when the criteria of the query meet the traits in the Patient Identity Source Actor.

Note 2 to entry: See *Service Functional Model for the Entity Identification Service*.

4 Patient identity management

4.1 General

In this section, we will provide the definition of the concepts used by the management process of the patient identity. It is following by a section on the cross-referencing management which completes the description by the management of patient identity between several healthcare providers within a cross reference domain.

4.2 Concepts

4.2.1 Patient Identity

Within a Patient Identifier Domain, the patient is a real person represented by an identifier and a set of identity characteristics called traits:

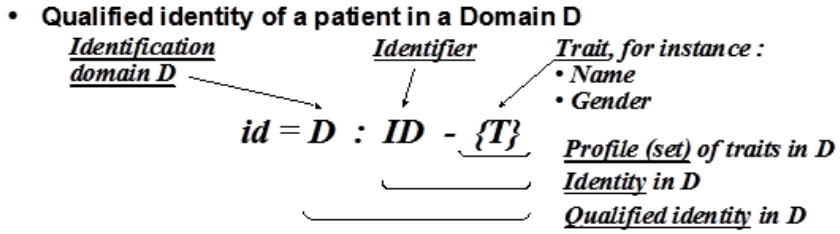


Figure 1 — Definition of the qualified identity

In the case where the identification of the domain is not explicitly given, the identity is called unqualified identity.

The traits are characteristics as name or subject of care name (ISO/TS 22220), first name, sex, date of birth, address, etc. However some traits are more constant than the others. The constant traits form the strict traits.

Other traits can be categorized:

— extended traits: traits describing the patient such as Insurance number, mobile phone number, etc;

— specific traits such as food habit, medical specificities, etc;

— technical traits such as status of the patient identity, validity, indicators, etc.

4.2.2 Patient identifier domain

The Patient Identifier Domain is the context in which the identities described above are managed. It may be all or part of a single organization, or a group of organizations. The Patient Identifier Domain is associated with a Patient Identifier Assigning Authority, an organization, agency or provider that allocates patient identifier designation.

In the identification process (see Figure 2), the arrow shows that the actor A accesses the identity id = D: ID - {T} and uses it to point the patient information (e.g. the patient record) in order to consult and update it.

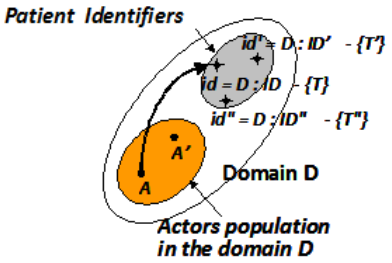


Figure 2 — Representation of the Patient Identity Source

Additionally, 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, one and only one identifier is assigned to a single patient within a given Patient Identifier Domain, though a single Patient Identity Source; generally because of errors or safety (when there is a doubt on the identity and to prevent a wrong assignment with an existing patient identity) during the process, it may assign multiple identifiers to the same patient;

— a Patient Identifier Domain Identifier 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. (From IHE-PIX.)

4.2.3 Examples of patient identifier domain

The nature of the Patient Identifier Domain can be various depending of the regulation of the country:

— Health domain with a clear separation with the insurance domain:
the patient identifier could be national or local;
— Insurance domain;
— Citizen domain: in this case, a passport or national ID card:
could be used in healthcare to identify the patient.

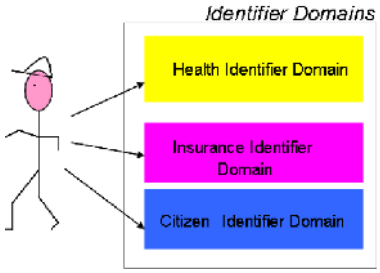


Figure 3 — Identifier domains linked to one person

When a patient travels from country to country and when he has a contact with healthcare providers, the process of identification is different. This problem is identified and addressed in this document.

4.3 Identity management process

4.3.1 General

In this section, the processes of identification are shown and illustrated by a care provision use case in hospital.

The term “Identity management process” is preferred to the term “identification process”. The Identification process is in fact a part or is included in the identity management process as the sub process of the creation or update of the patient identity.

4.3.2 Care provision use case

The interest of this use case is that many of principal actions of the identity process management are inventoried as shown below. The scenario assumes that all systems involved in it are in the same Patient Identifier Domain.

This scenario “Caring in In-Patient setting” is split into two different sub-scenarios:

— caring in ward unit;

— caring in medical-technical unit.

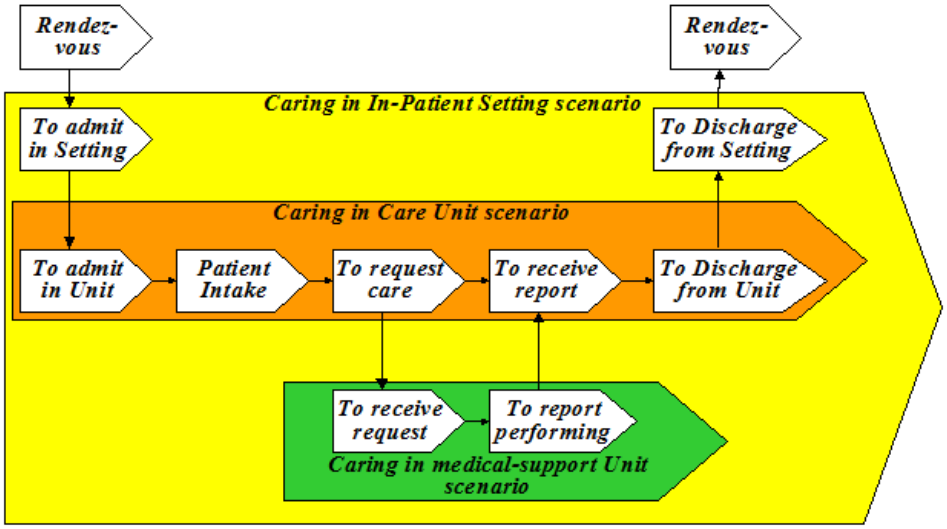


Figure 4 — Care process in hospital

Different actions are performed, related to the episode and to the services provided to the patient:

— ***To arrange an appointment for admission***: in many countries, the appointment for admission is made by telephone. At this stage, when the Admissions Clerk or the Consultants Secretary registers the patient identification; Errors can occur (when the Admissions Clerk or the Consultants Secretary has not understood the name or does not spell the name correctly and the patient information is erroneous or not complete).

— ***To admit in the hospital:*** when the patient is admitted and to reduce errors, the clerk shall ask for a patient document like insurance card or citizen card at the entrance or any other document, or checking process depending of the rules in the country. The patient will be registered with the more complete information. When the patient is not able to produce any document, the patient information are not reliable and the clerk will registered the identity as temporary identity. In the emergency case, when the patient is unconscious, the registration of patient information is difficult. A temporary name is given to the patient.

— ***Admission to the ward:*** when the patient goes directly in the ward, the situation can be the same as in admissions but that the patient registration will be done by the Medical Secretary and/or the Nurse. This is treated as a Clinical Admission and not administrative admission. The patient identity is treated as temporary as professional staff does not always control Patient Registration. In the case of a VIP or a patient being admitted for sensitive treatment (e.g.de-intoxication cure) a procedure for pseudonymization or anonymization will be applied (this procedure and the usage are not described in this document). During the care, an alias (or pseudonym) is used. When the patient has an appointment in a radiology department for example, he shall have with him all the information needed to identify himself (for example a wristband with his alias and identifier, document).

— ***Discharge from the ward:*** Discharge from ward and/or hospital may require relevant information to be collated and sent to another professional / organization. This may require an identity in a different domain. This includes the identity in the insurance domain for billing purposes.

— ***Discharge from the hospital****:* When patients are being discharged in insurance-based healthcare regimes, the Admissions Clerk or the Consultant's Secretary prepares the invoice, the real patient identity is used. In the case where information about the patient identity is not available, the invoice may be delayed.

— ***Fixing a follow-up appointment following the discharge:*** the patient identity is used and the Admissions Clerk or the Consultant's Secretary should have no problems in making an appointment(s) for the patient.

During the ward episode of care, several actions are performed:

a) **in the ward**:

1) clinicians send order communications to be performed by a medical technical unit (e.g. radiology, laboratory);

2) the clinician receives reports from the medical technical unit;

b) **in the medical technical unit**:

1) the technical team receives the communications orders from the ward;

2) the radiologists or the laboratory professional reports on the procedures carried out and the outcomes.

At each stage of the process, the healthcare professionals will verify the patient identity by requesting to the patient identity source and use the identity and identifier to access to the historical or current clinical information. The principal actions are searching, consulting and updating the patient identity when necessary. The way of processing internally is not describing, depending of if the Patient identifier domain is unique for all systems in the hospital or if the hospital is composed of several patient identifier domains federated by one patient identifier domain.

4.3.3 The identity management process

Four main processes are identified as shown Figure 5:

a) the identification action, which is the action of creation of an identity for a new patient in the patient identifier domain;

b) the referencing action, which allows using an identity in order to reference a patient information using the identifier of the patient identity; actions in this process are, for example, "to stick a label carrying the patient identity (identifier, names, date of birth) on an order communication or an "act on" report;

c) the identity maintenance action, which copes with:

1) traits updates;

2) reconciliation of duplicates;

3) resolving the collision;

d) the deletion of the identity in the identification action.

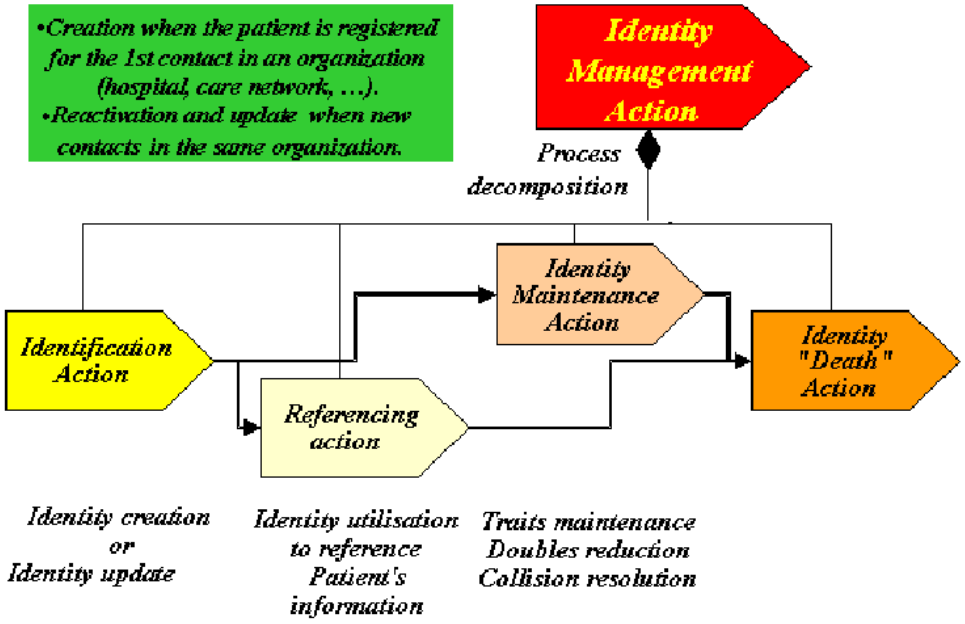


Figure 5 — Patient identity management process

The identity management process shall be described in the identification policy.

4.3.4 Patient Identifier Domain Policy

The Patient Identification Policy defines how the patient identity should be managed throughout all the procedures which are written in the identity policy charter. The principles of the Patient Identification Policy and process rules are written and saved in the Charter. Training and education need to be provided for all users, particularly for those actors authorized to create patient identities.

The Patient Identifier Domain Policy defines:

— the scope of the Patient Identifier Domain;

— the Patient Rights and Regulation over such information: this should be available for the patient on a separate and specific document which is given to the patient at their first visit; for application within the European Union Member States, the disclosure and use of personal information about health are regulated by laws on privacy, confidentiality and data protection[1)];

— the organisations holding such information and with whom it is shared (e.g. General Practitioner Practice);

— the profiles and the roles of the actors concerned and their actions, for example four categories of actors can be defined: patient, administrative staff (e.g. admissions clerks, medical secretaries, medical records staff), practitioners and clinical staff (e.g. nurses);

— the patient management systems and other healthcare systems which are direct users of the patient identity;

— identification authorities: two authorities shall be defined: the management authority and the patient identity vigilance authority; the first structure has the responsibility to define the patient policy and the management and the second will check the quality of the patient identity in the patient identifier domain;

1) See European Standards on Confidentiality and Privacy in healthcare.

— definition of the profile of the patient identity based on the pertinent traits of the patient (for example, groups of names, first name, date of birth, sex);

— definition of the different status and version management;

— security of the patient identity management: privacy, availability, integrity, audit trail;

— the management and quality indicators: e.g. number of patient identities created per month, numbers of duplicates, number of updates, etc.

For more detailed information, see Annex A.

4.3.5 Basic process actions

4.3.5.1 General

Two basic process actions are used in the sub-processes presented above:

— search on the patient identifier;

— search on the patient traits.

These basic process actions can take place in the four sub-processes described above, with different contexts for the initial and final events. They highlight actions where human beings participate in such process actions and can pose risks for the process.

4.3.5.2 Search on the object identifier

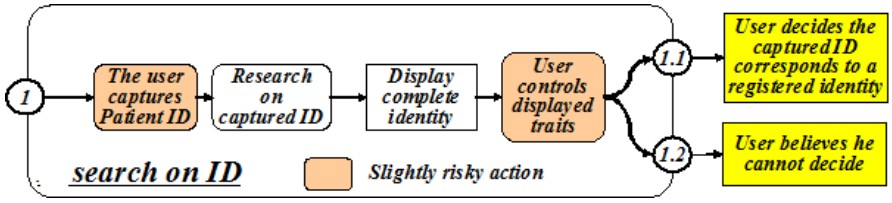


Figure 6 — Search of Patient identity process based on Identifier

(1) In this process action, the user (admissions or ward clerk, healthcare professional) captures the patient ID in the identification domain D on a healthcare system. A search on identifier ID is launched on the index and the complete unqualified identity (ID and traits) are displayed. The user should confirm that the displayed data (defined by the identification policy) correlate to the patient's identity (using documentation produced by the patient, e.g insurance card, identity card or other relevant documentation.

Two events should occur:

(1.1) The user decides that the displayed traits correspond (exactly or only slight variation) to those referenced by the healthcare system: The user then determines if the produced identification documentation corresponds to the identity registered on the healthcare system.

(1.2) The user considers that the discrepancies between the displayed traits and those referenced by the produced identification documentations too variable to be able to determine the identity of the patient to complete the processes without further investigation.

Several risks appear due to human actions:

A user error can alter the captured identifier and particularly if the user does not take care at the displayed traits, the user wrongly decides that the identity matches to the captured identifier. A

collision is created.

Some traits can have changed, and then, the now displayed traits can be different from those captured.

The risks of these occurring are in fact low: the procedures for capturing such information are usually sound or are automated through positive methods e.g. bar code, smart card,.

4.3.5.3 Search on the traits

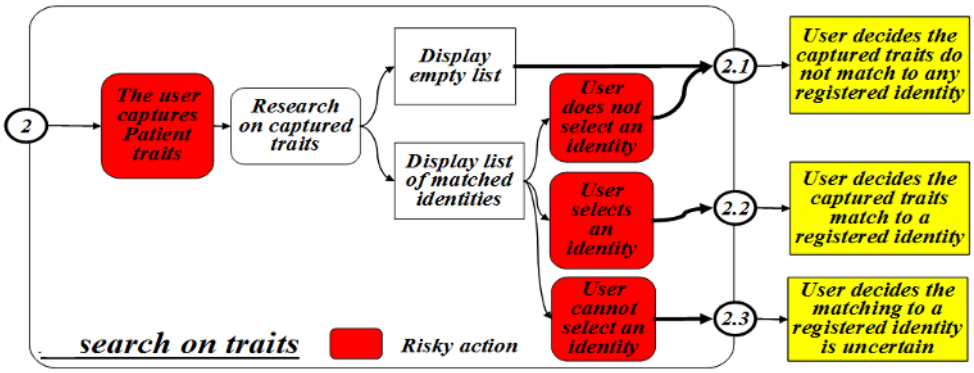


Figure 7 — Search of patient identity process by traits

The user captures the patient traits as search criteria in the healthcare system indexes to retrieve matching identities. The results of such action could be:

— no candidate identity matches are found within the captured data;

— several candidate identity matches are available.

The user usually decides that no identity corresponds to the captured traits; in the second case one or more patient identities are displayed and the user selects one of the identities on the patient list:

The user does not select any identity because he/she decides that none of the traits match exactly to any displayed patient traits. Such decision should be made after checking all the pertinent traits which are described in the policy.

4.3.6 Identity utilization or referencing action

The use process is enacted when the patient's identity is active, then he/she is known by his identifier ID, which can be available on labels, cards, etc. or with automatic reading (bar-coding, RFID, etc.). The process uses the ID to reference the patient's data existing in an order, an act report, a patient record element, etc.

It is an exception when the user cannot reference the information with the ID. Then he performs a search on traits to obtain the ID and references the information.

4.3.7 Identity maintenance action

The traits of individual patients are generally not stable for their whole life; for example, a woman using the surname of her husband may use a pseudonym, may have had a different name at birth and use other identifiers e.g. insurance identifier, medical identifier, etc.; it is the reason why the need of a maintenance of the identity is required.

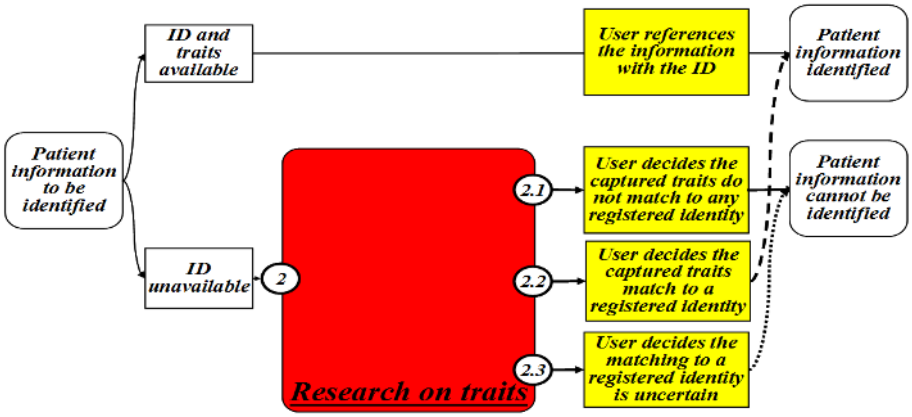


Figure 8 — Maintenance process

When the identity of the patient already exists, the user shall check the data with the patient in the referencing process, where:

1) The traits are not the same: after checking the user shall update the traits and creates a new version of traits and/or patient identity.

2) A list of candidates is available and some of them corresponds to the patient; after checking all the data, the user decides to merge patient identities and selects them in the Patient Identity Source. The other patient identities are de-activated and linked to the source. They become “ghosts” (see Figure 9).

3) The identity that the user has selected corresponds in fact to one or more patients: the resolution of the collision is more complex regarding to the medical records already existing. In that case the medical records shall be spilt into two patient medical records linked to two patient identities. It is the role of the relevant healthcare professionals to separate medical data (see Figure 9).

In each case, the patient identity is updated and a new version is created. The patient identity follows a life cycle and several states are defined:

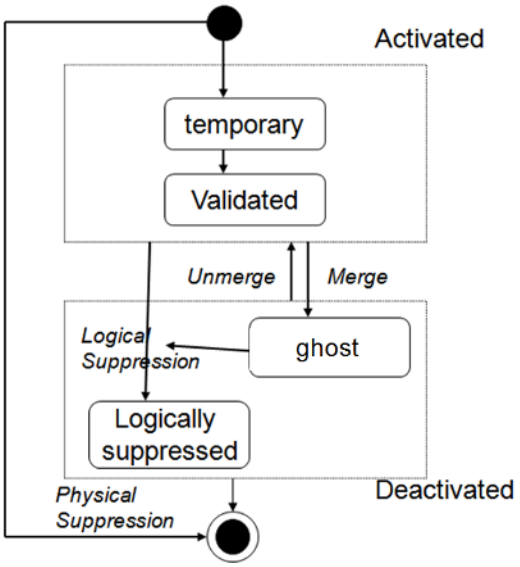


Figure 9 — Life cycle of the status of the patient identity

Identity management is supported by a Quality Policy for Identity Management. Every status update is associated with a new version of an identity.

EXAMPLE Temporary to Validated.

4.3.8 Methods of deleting patient identity

Two methods of deleting the patient identity are available:

— Logical suppression: the patient identity is de-activated. It is not possible to access to the data. The administrator is the only user authorized to manage this identity.

— Physical suppression: the patient identity is suppressed. This action is definite.

4.4 Identification anomalies

4.4.1 General

Several anomalies or exceptions may occur during the lifecycle of the patient identity. They shall also be covered by the identification policy, in order to explain to the actors how to manage them when they appear.

4.4.2 Homonymy

Where two patient identities may correspond with names and traits being identical. Normally under such circumstances the identifiers are different. The risk arising from this homonymy would be to merge the two identities by creation of the collision. To reduce the risk, the best method is to indicate (by an indicator) that the homonymy exists.

4.4.3 Duplicates

A duplicate exists when one patient has two identifiers. Generally this situation occurs when after a search and even having checked a list of patient candidates, the user with caution, decides to create a new identity with new identifier. To avoid such a situation occurring, it is necessary to educate the user to take effective action by indicating if he/she has created a new identifier and that there is the potential for a duplicate.

To prevent and to reduce a number of duplicates occurring, the user needs to be vigilant and to check frequently (daily, weekly) for potential duplicates by analysing the patient database.

After selecting a list of potential duplicates, the decision of merging patient identities is the responsibility and within the role of medical staff, who are best placed to conduct an analysis of the medical records.

4.4.4 Collision

A collision occurs when two or more patients have the same identity within the Patient Identity Source. A collision is created when after a search and even having checked a list of patient candidates, one patient identity is chosen by default (for example in the case of homonymy) and the criteria for the search are not rigorous or the user simply decides to go ahead and use this identity. The result is that information for different patients are being recorded using the same identifier that denotes the identity.

When this situation is suspected and where after a period of time the medical records are confused the following actions need to be taken to correct this situation:

— identity the type of collision;

— freeze any further action on the patient identity;

— create two identifiers;

— define two medical records;

— warn the wards/clinics responsible for the patients to split the medical data into the two medical records.

4.5 Exceptions

4.5.1 General

Exceptions are often met in the care provision process. Some of them are presented in this section.

4.5.2 Non-identified patient

In some cases, the identity details of the patient are not known and the patient identity cannot be registered. In such cases a temporary identity should be used. When the patient identity details become available, the patient identity should be updated, validated and merged with the temporary identifier.

EXAMPLE The patient arrives in an emergency and is unconscious.

4.5.3 Patient with uncertain traits

Under circumstances where all the pertinent traits for a patient are not available or uncertain (for example date of birth of foreign patients) an indicator is added to prevent errors when the professional consults that patient information.

4.5.4 New-born

A new born is generally registered with the mother's name when no other is known. The patient identity is updated when all the patient data becomes available.

Also in frequent cases, the child is not given a forename immediately following birth and therefore appears in healthcare systems as "baby" until after the child has been named or the child's birth is registered. Sometimes, it is necessary to add the father's surnames when several babies born in the same day with the same mother.

EXAMPLE In England and Wales, NHS Connecting for Health introduced the allocation of NHS Numbers to babies soon after birth as part of the statutory birth notification process. A baby's NHS number will be used to match test results, monitor quality of care, improve neonatal research… The following categories are babies born in NHS trusts, overseas visitors, armed forces babies, babies born in England and Wales, though normally residents in Scotland or Northern Ireland, still births (after 24 weeks gestation), births in non NHS hospitals, babies adopted at birth, home births and births overseas by independent midwives.

This NHS Number allocated at birth is link to the civil registration process so that the name can be added when known.

4.5.5 Identification under anonymity

Some patients do not want to be registered with their real identity (for reasons of being a VIP, healthcare professional, patient in specific health care episode). Two methods for dealing with this can be considered:

— the data are registered in the system but they are not communicated (confidentiality of the information);

— the traits are never registered and all data for this patient are fictitious.

EXAMPLE A patient attending a sexual health clinic at a hospital is given an “alias” to conceal their real identity, particularly where the hospital may be in that patients own local community of residence. The patient then requires an X-ray, but before it is safe to do so their health record needs to be checked for previous history of X-rays.

In this case, the problem for the healthcare professional is to gain access to the historical medical information. In the case where the information is concealed, the patient has one medical record and subject access rights will control the information given to the healthcare professional. In the second case, it is possible that the same patient has more than one medical record. To resolve this problem, a recognized third party with clinical knowledge and responsibilities for the protection and privacy of patient data (for example in the UK the Caldicott Guardian) should manage the link between all patient identifiers and medical records. This action is possible if the patient has given his consent.

4.5.6 Intentional use of multiple identities

There are circumstances where a patient has expressed a wish to limit access to their medical record for personal reasons including privacy and preference.

These preferences are fundamental patient rights. Current working practice for patient identifiers in these circumstances, has grown historically from the limitations associated with managing hard copy paper records, and may include such “confidentiality protection mechanisms” as aliases or false identities for the patient. It is recognized that working practices associated with multiple alternate identities, will be difficult to eradicate (for good reason) due to a prevalence of legacy systems with limitations in confidentiality controls.

Nevertheless best practice IT systems should have no need for aliases or other such multiple identities in order to support patient preferences in controlling access to their medical records. A best practice IT system would have a regime of controls including:

— a means to limit access to the patient record to only those health care professionals with a legitimate reason for doing so – a legitimate relationships control;

— a means for a patient to express the wish to limit or prevent access to their records without expressed consent from the patient;

— a means for security-sensitive patient records to have access flagged and restricted such that a health care professional who may claim to have a legitimate relationship to a patient as a function of their role, needs further justification for accessing the individual sensitive record - a “sensitivity flag”;

— a means for the patient to decide what items of information within their electronic patient records that can be legitimately shared electronically, and those items which are to be kept private – “patient consent”.

Clearly best practice systems would deliver these patient choices and preferences by implementing systems of access control, secure access, audit trails and all other best practice security systems which can be found in the reference documents listed in chapter 2.

It is a fundamental principle of best practice systems of patient identification, that the patient has only one identity. This enables the electronic patient record to be a complete and comprehensive record of the patient's history and medical records.

Multiple identities, while for very good reasons, are not a best practice and have well known safety risks in respect of lack-of-completeness-of-patient-records.

5 Cross-reference patient identity management

5.1 General

Because of the development of medical information exchange between enterprises, the best quality of the identity management is now required. In this section we will define the concepts needed to introduce the cross reference identity management process (as we did in the previous section for identity within the healthcare enterprise). The cross reference patient identity management will permit the following requirements:

— continuity of care;

— patient safety;

— confidentiality of the medical information;

— patient consent.

5.2 Concepts

5.2.1 Cross-referencing identifier domain

5.2.1.1 General

A cross referencing identifier domain is composed by a set of patient identifier domains and is managed by a cross referencing manager actor. Two models of implementation are generally implemented:

— correlation model;

— federation model.

5.2.1.2 Federation model

In the federation model, one patient identifier domain is used by the cross referencing manager actor and the patient identity database is considered as the patient identity source actor or the main point reference. When a query occurs for the cross referencing manager actor, only the identifier coming from the source is retrieved.

EXAMPLE The NHS number which is produced by the NHS which is the assigned authority. When two healthcare providers want to exchange information for a given patient, they communicate using the NHS Number.

The process is the following:

The healthcare professional A will link the current identifier with the NHS number. He sends the NHS Number to the healthcare professional B who uses directly this number or makes a link with the local number for selecting the medical information of the patient for sending to the healthcare professional A. The question of the quality of the link is under the responsibility of every healthcare professional who is in charge of checking the validity of the Patient data and of registering the correct information.

5.2.1.3 Correlation model

In this case, all the patient identifier domains play the same role. When a query occurs to the cross reference manager actor, a list of patient identifiers should be retrieved.

EXAMPLE The student Mr John Woerth born in England is doing his high school in Amsterdam. Mr John Woerth is diabetic and is going very often to the hospital for some examinations. During his holidays, he returns to England to see his family. Because of the chronic disease, he has to go to the hospital. The healthcare professional wants to consult the last patient summary made in Amsterdam.

Mr. John Woerth has a NHS Number and a BSN Number as a student in Holland. A Cross referencing Patient manager actor will link the two numbers. When the healthcare professional in England queries to the healthcare professional in Holland, he sends the NHS Number. Because of the link between the NHS Number and the BSN, the query in Holland uses the BSN Number to obtain the Patient summary. The two numbers are at the same level.

NOTE In the example above, the responsibility of who will register the link is not described. Several options are available depending of the Cross reference Patient identification policy (see below). In the correlation model, the link is probably assumed by the two domains; each domain will correlate the two numbers for better quality. In the case where the two domains do not have the same vision of the link between two patient identifications, the patient cross-reference vigilance authorities will solve the problem.

The two following schema summarizes the two cases.

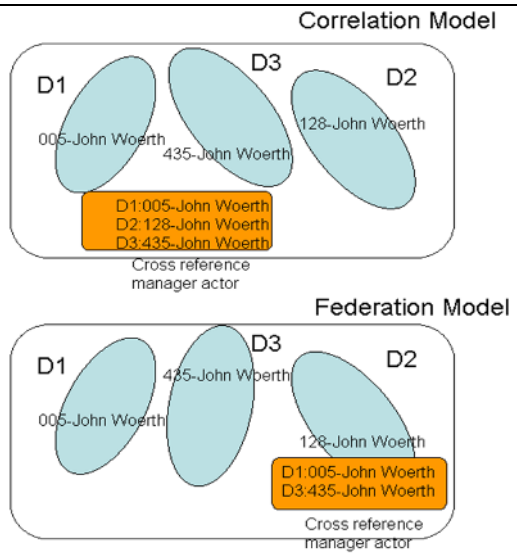
The cross referencing patient identifier actor links the three numbers at the same level, each number is known with the assigned authority of the domain. In the federation domain, the exchange will be carried out using the master patient identity. Each patient identity is also identified with the assigned authority of the domain.	

Figure 10 — Architecture model

5.2.2 Sharing medical information between healthcare providers

In his/her life, the patient will see several healthcare professionals, probably in more than one healthcare organization. He/she will be identified by each of the healthcare providers from their Patient identifier domain. In the case of the continuity of care, data needs to be shared between those healthcare providers using a cross referenced patient identity. The principal actions to obtain a cross-referenced patient identification between domains safely are as follows:

— identify the patient in each patient identifier domain with one and only one valid patient identity;

— establish and follow a cross reference domain policy with all domains which agree to share information;

— establish a cross reference link between patient identities of the involved domains in the patient cross reference manager actor.

It is obvious that the cross-reference domain policy will be adapted to the context: the cross reference domain policy describing how to manage the link between identities within hospitals (generally using a federation model) is very different of the policy for multi-national domains (correlation model).

In the case where the patient identifier domain does not yet belong to the patient cross referenced identifier domain, the management authority shall contact their counterpart in the other domain to establish an

agreement between them according to the cross reference patient identifier domain. For an isolated domain where the exchange is exceptional, a procedure shall be described to include this case.

All these actions are described in the next sections, dependent upon the cross referencing policy and model of implementation. The use of a federation identifier or the correlation identifiers will give different kinds of usage. The Cross reference patient identifier domain might be used in the following cases:

— within a healthcare organization when a patient identity Source is not used by all systems;

— between healthcare providers involved in a health network at the local, regional or national level;

— between countries in the case of the patient mobility.

5.3 Identity cross-reference management process

5.3.1 General

The process comprises the following actions:

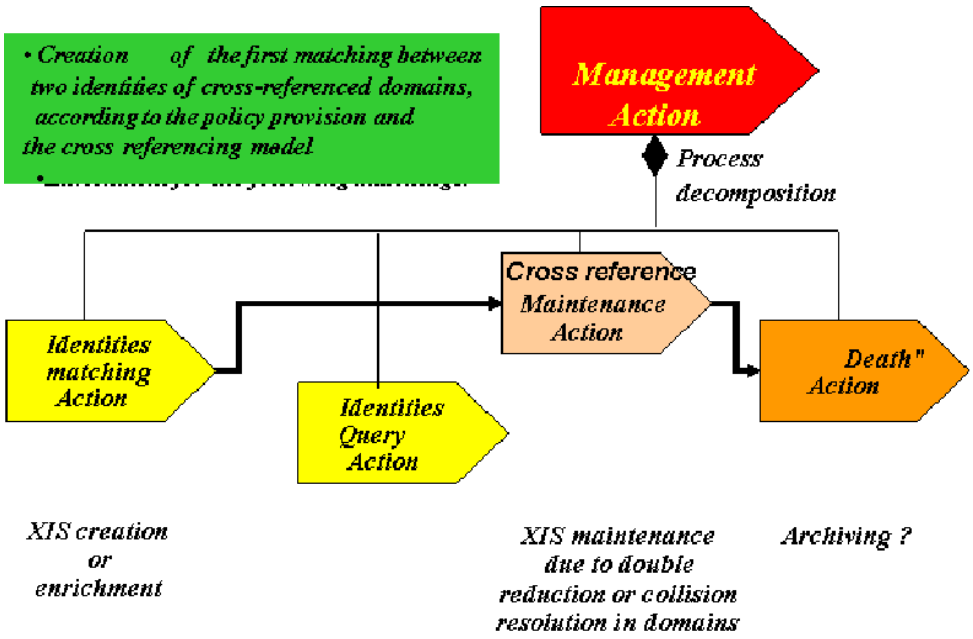


Figure 11 — Cross referencing patient identity management process

Four main actions are defined, dependent upon of the local cross reference policy:

— identities matching action: this action creates the first link between patient identifiers coming from two domains and adds the new patient identifiers when necessary;

— identities query actions: this action permits the query to the cross-reference patient identifier manager actor for retrieve one or more patient identifiers from one or more patient identifier domains when authorized;

— cross-reference maintenance action: during the lifecycle of the cross reference patient identifiers, some events will update the cross reference patient identifier link already existing corresponding to the update registered at the patient identifier domains as duplications, collisions, update of the traits; etc;

— action upon death: some cross reference patient link shall be removed upon death of the patient.

5.3.2 Cross reference Patient identifier Domain policy

The Formal Policy shall be agreed by consensus with all Patient identifier domain authorities. Such a Formal Policy should define rules, procedures, actors authorized to manage the process. The Formal Policy comprises the following sections:

— Policy Scope and Objectives;

— the patient identifier domains which are involved in the cross reference identifier domain (including all healthcare providers);

— the implementation model (federation or correlation);

— the Information architecture and technical aspects (format of the identifiers and demographic data, messages, standard, archiving, systems, etc);

— the process and the actions to proceed at the creation and maintenance of identities in the cross-reference patient identifier management actor;

— the profiles and the roles of the actors involved and their roles: for example four categories of actors are selected: patient, administrative staff, practitioners, nurses, cross reference identity administrators;

— cross-reference identification authorities: the authorities are the management authority and the patient cross-reference vigilance authority; the first authority has the responsibility to define the patient identity policy and the management and the second will check the quality of the patient identity profiles stored in the cross reference patient identifier domain;

— communication architecture;

— security of the cross reference patient identity management: privacy, availability, integrity, audit trail;

— quality indicators: number of failures to link two identities, number of notifications coming from patient identifier domains, number of users of the service per category of actors;

— respect of patient rights.

5.3.3 Identities matching action

To establish identities matching actions requires a strong prerequisite, which is that the matching shall be done only with **valid identities** in each patient identifier domain. Then it should be forbidden to create matching if the identities are in temporary or inactivate status.

Before any matching, the patient shall give his/her consent and shall know how the cross reference patient identifier domain will be managed. All the procedures are defined in the Cross reference patient identifier domain policy and in the patient charter (see Annex A).

Generally some pertinent traits are stored in the cross reference patient identifier domain; however these should be the strict minimum for best management, but sufficient to promote the matching. These traits should be defined in the policy.

All the patient identifier domains should be registered and their addresses known and a contract established between them. At the first identities matching action, the cross reference manager actor will establish a link between two or more validated patient identities when an order is made by an actor. In the case of the federation model where one patient identifier domain is considered as a source, the patient identifier is mandatory for the first link. In the case of correlation, all the patient identifiers are at the same level. To be available, the created link shall be confirmed by the user and validated.

5.3.4 Identities Query action

The query occurs when a healthcare provider from one patient domain wants to access to some medical data of a patient which are stored in another domain. To obtain the information, a query to the cross reference manager actor is needed to obtain the identifier from the other domain.

The data needed to solve the query are the identifier of the first domain (if correlation model) or the source identifier (if federation domain), the domains for which the return identifiers are intended.

The user shall verify that the return identifiers correspond to the patient by querying patient identifier domains for pertinent traits and checking.

In the case where the list is empty, the return code will advise the user that:

— there is no matching identities corresponding to the identifier;

— other matching identities exist.

In the case where no selected domains were expressed, all the list of existing identifiers and domains is returned.

All the returned matching identities returned are validated.

5.3.5 Maintenance action

5.3.5.1 General

As seen in the chapter on the patient identifier domain, the patient identity can change during the life of the patient (merge identity, removal identity, update demographic data, etc). Errors can also be introduced by the cross reference manager actor (link between two identities are not available, patient decides not to authorize the link, etc).

To maintain good quality of the cross reference matching identities, the management of these errors is required. The actions are:

— notification of updates and events;

— updating the link between identities;

— logical removal of the link between identities;

— checking with the cross reference manager actor.

5.3.5.2 Notification of updates and events

The notification will list each patient identifier domain involved in the link with the selected patient identity. Three kinds of notification shall be available:

— notification at the creation of the link between at least two patient identities;

— notification of an update of the demographic data or the state of the patient identity coming from one patient identifier domain: the cross reference patient identifier manager actor shall be listed first;

— notification after an update of the link between identities.

The rules of the notification shall be described in detail in the cross reference domain charter. Generally the domains (including patient identification domains and cross reference domains) registered in the cross

reference domain shall always be notified when an event occurs. At the reception of the notification, every domain has the responsibility to check the impact of the change in their system.

5.3.5.3 Update the link between two or more identities

The update shall be done by the authorized actors (administrators) defined in the policy. The update could be the modification of the link between two or more identities. For example, a merging action occurs in a patient identifier domain A. at the cross reference domain level, all the links with the different identifiers of the patient identity shall be checked and new link should be established. The old link will be depreciated and in a period of time will be updated. All the updates should be audited and all the patient identifier domains should be notified of the update. The same action shall be done when a removal action occurs in one patient identifier domain. However, such action is risky and could modify heavily the relationships between patient identities. The decision of this update shall be taken with the cross reference domain authority and will involve all actors and healthcare providers with interest in the link. The policy should detail precisely the procedure for such an event.

EXAMPLE Two patient identities Mr John Woerth and Mr John Woerthe, both that the Hospital of Amsterdam merged: Mr John Woerth becomes the active patient identity and Mr John Woerthe the inactive because of duplication.

However, Mr John Woerth is linked with the patient identity Mr John Woerth in hospital at Oxford and Mr John Woerthe is also linked with Mr John Woerth in hospital of Dover. When the two identities are merged, then a new link between Mr John Woerth (in hospital of Amsterdam) and Mr John Woerth in hospital of Dover is also created.

The cross-reference domain authority should accept these updates. All the linkage concerning Mr John Woerthe are depreciated by updating the period of time attached at these links (end of period = date of the update event). There is no difference in the action taken in the two models.

In the case of collision, the cross reference authority will select each patient identity of each domain already linked for each new patient identity of the domain. The update shall be under the control of the authority.

5.3.5.4 Logical removal of the link between identities

The consequences of this action are the same than the previous action. No physical removal action is authorized. All logical removals are audited and the organizational procedure should be the same as for the previous action.

5.3.5.5 Checking the cross reference manager actor

At chosen intervals (to be determined by the cross reference domain authority), the links between patient identities already existing should be checked and verified for contribution to the quality of the patient domain. Tools shall be available to the authority to facilitate the work. Procedures for resolving problems shall be described in the policy charter.

6 Recommendations

6.1 General

In this clause some recommendations are presented. They do not claim to be exhaustive but they give some guidelines coming from best practice. The recommendations are classified by actors: Healthcare provider, authority, suppliers and insurances for three types or organization: within healthcare professional, between healthcare professionals and between countries.

6.2 Use Case 1: Within a healthcare organization

6.2.1 Healthcare providers — Organizational requirements

Individual healthcare providers should define a patient policy and set up the management authority and the patient vigilance authority. The management authority has the responsibility to define the patient policy and the patient vigilance has the responsibility to ensure the quality and the security of the patient identification within the healthcare organization. If a cross reference domain is created within an healthcare organization, the patient policy should take into account the constraints generated by the cross reference process. In the first instance this should be defined by the Chief Executive, Chief Information Officer, representatives of practitioners, nurses and others categories of professionals involved in the care. The second instance is composed by at least one administrative and one member of the medical staff to reflect the everyday identification process.

The healthcare organization shall take into account the rights of the patient by publishing in the Patient Charter all the information needed by the patient.

The healthcare organization shall plan education to explain to the users the identification process used and the update when occurs. Then all the users concerns by the patient identification are known and a role attached for security reasons.

The healthcare organization shall:

— define a Patient identifier Domain policy;

— create management and vigilance authorities;

— define the Patient Charter (if this charter is not defined at a higher level);

— plan education for the users.

6.2.2 Software suppliers

Several Health Information System architectures are available today corresponding to the implementation model:

1) one patient identity source which is the referencing patient identities: all systems will use and exchange with it;

2) patient index in each system and reconciliation process for patient identification between systems;

3) patient index in each system managed by a cross referencing manager actor.

We strongly recommend within a healthcare organization to implement a patient identity source to be sure that in all wards, the professionals uses the same patient identifier. The reason is that all objects (label accompanying all specimen), information, medical records will be stick with the same patient identifier. The patient identity will be available in all systems within the healthcare organization.

NOTE In some case, some patients are directly identified in the department (case of laboratory or radiology departments). We also recommend to register this patient at the patient identity source to be sure of the quality of the identification and to ensure a good healthcare coordination between healthcare providers for these patients.

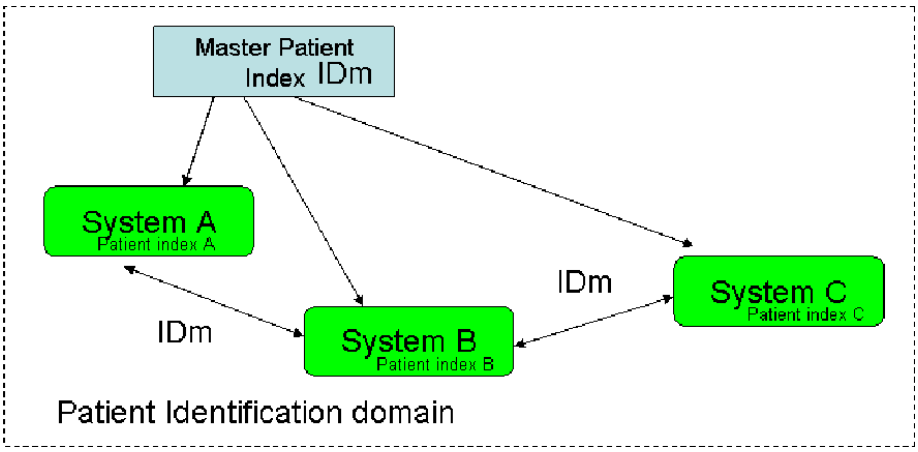


Figure 12 — Distribution of patient identity source in the hospital systems

Each healthcare provider should promote mapping across systems to establish which systems have the responsibility to register patient identification.

The Patient identity source shall implement methods for reducing errors. The process of validation of patient identities should be determined to promote the responsibilities within healthcare organizations. This would allow periodic checking by the patient identification vigilance authority for the number of non-validated patient identities and thus the quality of the process. The status of patient identities should be exchanged by using messages which contains absolutely a field containing this data (see for example HL7 V2 or V3 messages).

We recommend the implementation of the status described in section XX for any system managing patient identification.

To follow the quality of the patient identification, the patient cell of identito-attentiveness shall define indicators which will be implemented in the systems and workflow for solving problems when they occur. For example, when an error is observed by any user, it could be registered and sent to the patient vigilance authority which has the responsibility of solving the problem by advertising the user responsible of the error for correction or to prevent any medical mistake by sending a message to the users.

6.2.3 Insurance providers

In most of cases, the insurance providers use their own insurance identification which is sometimes used by the healthcare providers to identify the patient. Several cases are found over Europe:

— patient has a card and uses it directly for care: no difference between insurance number and health number;

— patient has an insurance card: this card is used for billing.

The card will permit the registration of the traits of the patient when the data have sufficient quality (the healthcare providers trust the third party (the insurance organization) or when there is no ambiguity between the patient and the card that the patient will present.

We recommend to healthcare providers to verify the quality of the patient information before any registration of the data.

6.3 Use Case 2: Healthcare coordination

6.3.1 General

Two main cases are described in this section:

— The first subsection provides recommendations to the healthcare providers for a best management of patient identity process.

— The second subsection provides recommendations for software suppliers.

6.3.2 Between healthcare providers

When healthcare providers decide to work together and to share medical information, it is necessary to establish a general framework for the sharing information by defining the parameters, the scope, the responsibilities and the period of time for such sharing. A contract or an agreement depending of the context (between two healthcare providers or within region) should then be signed by each healthcare provider to ensure cooperation. The patient identification or the cross reference policies of each healthcare provider should reflect this collaboration.

Healthcare providers deciding to work together should compare their identification processes to determine the compatibility between them and to determine the shared identification process. They also have to determine which kinds of patients are concerned by the exchange of information.

Those healthcare providers should define the cross reference patient identification policy which ensures the coherence of the shared identities and the identification rules and procedures to apply. They also ensure the quality of the patient identification.

Those healthcare providers should also set up the cross reference management authority composed by representatives of each healthcare provider and a cross reference patient vigilance authority.

They should take into account the rights of the patient by publishing and publicising in reception areas information needed by the patient (dependent upon the regulations).

The healthcare providers should plan education programmes to explain to the users the cross reference identification process used and the updating process when it occurs. Then all the users concerned by the cross reference patient identification should be known and the role reflected in contracts of employment.

The participating healthcare providers should:

— define a Cross Reference Patient identifier Domain policy;

— create management and vigilance authorities;

— define or update the Patient Charter in each healthcare organization (if this charter is not defined at a higher level);

— plan education for the users.

Healthcare providers should undertake mapping the systems affected by the cross reference patient identification and security aspects shall be highlighted.

The cross reference charter should detail:

— the implementation model (federation or correlation);

— the security and privacy aspects;

— which systems are authorized to exchange and their roles;

— which common applications are in charge of professional directory, nomenclatures;

— the standards used for exchanging patient identification;

— the format of the patient identity used for the exchange.

The following schema summarizes different approaches of cross reference implementation models (not exhaustive):

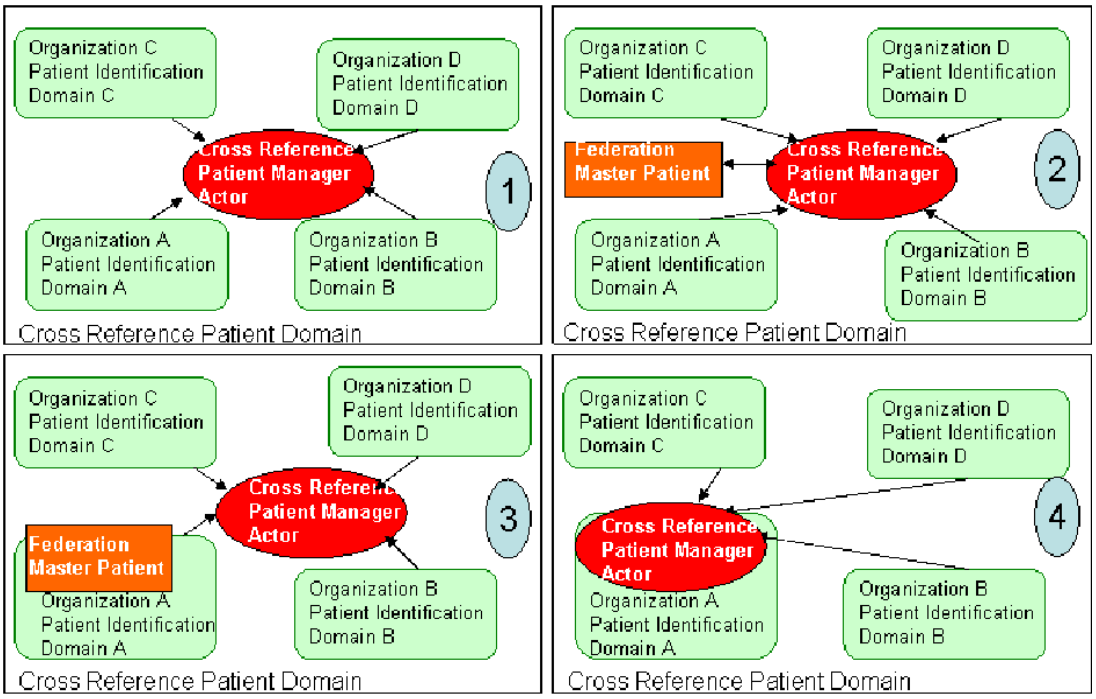


Figure 13 — Some examples of architecture within cross referencing domain

❶ Correlation Model: The cross reference patient manager actor is managed by a supra organization (example at the regional level).

❷ Federation Model the cross reference manager actor is grouped with a Patient Identity Source and hosted at the regional level. The information exchanged between Healthcare use only the federation patient identity.

EXAMPLE 1 In a country as Italy, the patient identity source is supported by the insurance card which is delivered at the regional level.

❸ Federation Model: the Patient Identity Source is hosted by one of the healthcare providers. No example known at this stage.

❹ Correlation Model with the cross reference manager actor hosted by one of the healthcare provider.

EXAMPLE 2 Hospital shares information with GPs in the same town. The Cross Reference Patient Manager actor is supported by the hospital.

No Implementation of the case 3 is known. Generally the cases 1 and 2 are most often used.

6.3.3 Software suppliers

The software suppliers involved in cross referencing domains will have to apply the cross reference charter for the part which addresses healthcare systems.

They have to:

— understand the architecture model;

— apply the patient identity and cross reference patient identity functions;

— apply the standards and formats chosen by the healthcare cross reference domain;

— apply the security policy defined for the cross reference domain;

— produce their conformance of the requirements (the certification should be explored).

The supplier shall specify in detail the workflow that he will implement in the system. In the Federation model, there are several ways to feed the Cross reference Patient identity Manager:

1) the Patient identity Source is already fed by validated identities and the link is done one by one with validated patient identity coming from the organization within domain;

2) the Patient identity Source is fed at the same time than the link is done.

These two ways can be split in more precise use cases.

The Software suppliers shall claim of the Cross Reference Patient identifier Domain policy before any implementation. They should describe precisely the use cases that they are able to implement.

The question of certification is today an open issue as well as for the patient or healthcare providers and the software suppliers. The problem of the responsibility is an acute problem: if the quality of the patient identity is not good, the risk of chosen the bad patient is important.

6.4 Use case 3: Cross-border, the Europe case

6.4.1 General

Because of the increased patient mobility in Europe, the sharing of medical records across national boundaries is required more and more. Each country has their own regulations and different modalities to conciliate patient identification at a national or regional level, with insurances (private or public), healthcare providers, or national identities.

For example, in the Netherlands, a national patient identifier is implemented but in Italy, regional identifiers are used for healthcare and insurances. In France, a national insurance identifier exists and will be completed by a national patient identifier for care.

Use case: a German patient, on vacation in Italy has a heart attack. He/she is routed to the emergency department and the medical practitioner wants to consult the patient summary and the medication list. To access to the medical information, the practitioner needs at first to have the authorization of the patient (following the patient right) and the system will have patient identifier of the patient domain and the address of the medical record of the patient.

6.4.2 Organizational requirements

As in previous case, all recommendations described are valuable. Because of the variability of the model implemented in each country and within individual countries, it is recommended that at the European level, each country/region will define which patient identifier system it decides to use.

At the European level, every country has the responsibility to conciliate identities within its own health governance and regulation. Then it is assumed that every country/region is a patient identifier domain at the European level and the country/region has the responsibility to maintain the quality of the patient identifier domain.

(See B.4, the Netc@rd project and B.5, the FIDIS project, as examples).

The definition of the Cross reference patient policy shall be developed at the European Level with all countries involved. The qualified European organization which will ensure the role of the management authority shall be identified. The cross reference patient vigilance authority should be ensured at each country level.

6.4.3 Information system

Each country/region should support a patient identity Source and a cross reference manager.

The Cross reference manager actor should be able to link the different patient identity attributes at the appropriate level, depending of the territorial organization, but should also be able to link the national/regional patient identity with the patient identities attributed in other countries (for mobile patients). Processes to obtain this registration across boundaries and use cases should be described in detail in the Cross reference policy charter.

Requests to the patient cross reference manager actor with the patient identifier and the assigning authority are required to established relationships with the national registry of the Electronic Health Record, if it exists. Otherwise the response should be given to the assigning authority, stating its location and prospective local patient identifier.

In the following simplified diagram, an example of the access of the patient summary is described:

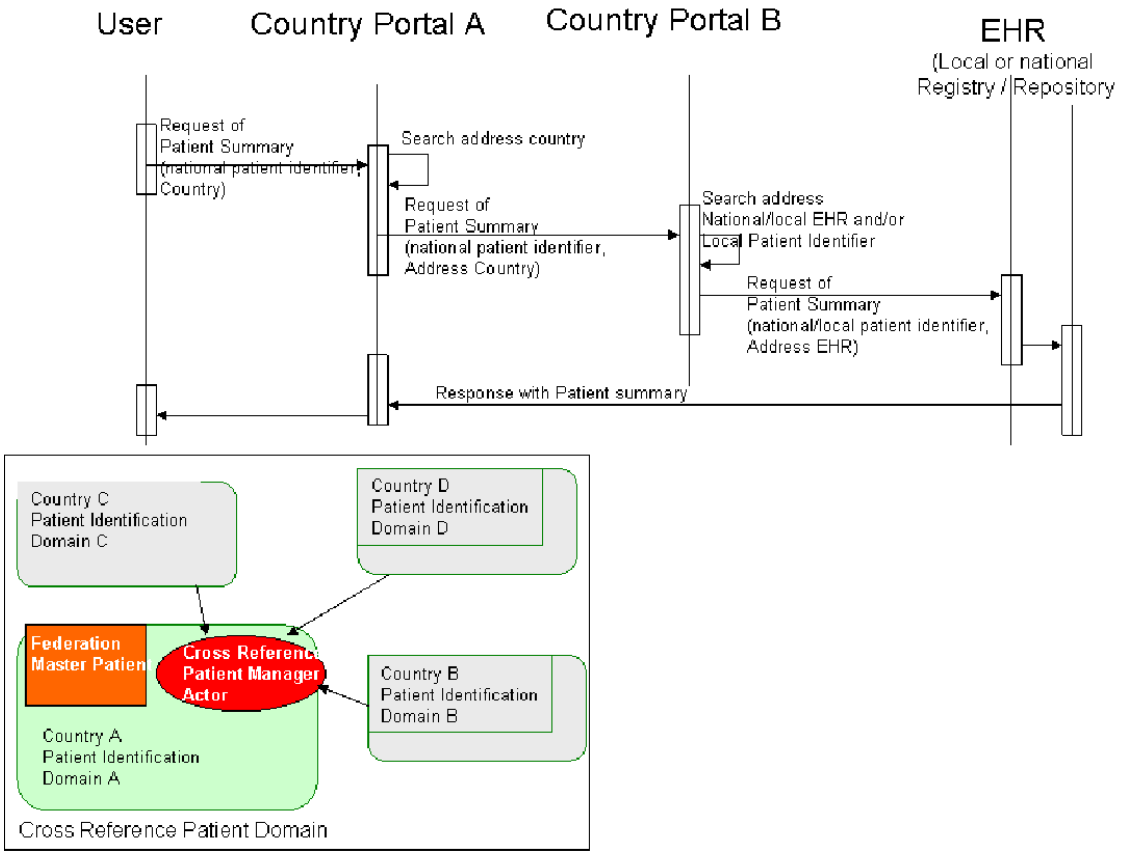


Figure 14 — Sequence diagram for a request to identity between country

In Country 1, a user asks for a summary of the medical record for a patient from another country. He gives the detail of the system and the national patient identifier for the country concerned.

The system sends the message to the national portal 1 of the receiving country which is coupled with national patient identity source and the cross reference manager actor if needed and the locator for each country participating to the cooperation.

The receiving country portal 1 sends to the portal 2 (the home country of the patient) the request for a summary of the medical record together with the patient identifier. The portal 2 checks the existence of the patient identifier and searches for the location of the national registry of EHRs (or the local patient EHRs).

At The portal 2 level, the cross reference manager actor translates eventually the national patient identifier to the local patient identifier. The portal 2 then sends the request to the registry which asks the repository. The repository sends to portal 2 (or directly to the portal 1 in the receiving country) which send the response to the user.

All these actions should take place within a secure environment, which is not described in this example.

This example shows a distributed environment where each country has his own responsibility of the quality of their patient identifier domain. In the case of error occurs, its responsibility is compromised. This situation represents best practice and offers guidance whether to accept cooperation or to remove it.

Exchanging medical records data between states requires the patient identifier from the assigning authority of the country receiving the request.

Annex A
(informative)

Policy charter of the patient identifier domain

A.1 Policy Charter of the Patient Identifier Domain

The policy charter covers at least the following items:

a) Charter Objectives:

1) to ensure that a person is represented by only one patient identity in the system;

2) to give the right to access to the pertinent data to the right healthcare provider in accordance with the confidentiality policy;

3) to minimize the risk of not obtaining the medical information;

4) to ensure secure communication with other patient identifier domains;

5) to archive long term medical information in good conditions;

6) to contribute to improved quality of medical activity statistics;

7) to improve the interoperability between systems within or between healthcare providers;

b) Glossary: *description of all terms used in the document*;

c) Application Domain: the policy charter is applicable to one or more organizations for a type of population, a set of actors, in a location;

EXAMPLES:

1) Hospital St Michel at Rennes which has three buildings located on three different sites (all administrative information of the building);

2) The actors are medical secretaries, doctors, administrative staff, nurses and all others medical staff, IT Engineers and staff;

3) List of medical services: cardiology service, laboratory, radiology, etc.;

4) IT system: description of the systems or applications which use the patient identity (EHRs, RIS, LIS, ADT, billing application, etc).

d) Authorities:

1) the management authority: the management authority is chaired by the director of the hospital and is composed by the chief of cardiology service, the radiologist secretary, the IT project leader of the ADT application;

2) period of meeting: once per month at the beginning and one a year after validation of the charter;

3) mission: defines the charter policy, defines the resources, updates the charter, represents the organization in a cross referencing patient identifier domain when exists, determines indicators, controls the quality of the patient identifier domain;

4) the Patient identifier vigilance authority: is chaired by the chief of admittance service and is composed by the secretary of the admittance service, the manager of this authority and the nurse of the cardiology service;

5) period of meeting (solving problem): twice a month;

6) mission: check the list of duplicates, collisions, solve the problems, hotline for users, educates users;

e) Rules:

1) What is the identifier? description of the identifier (8 characters, beginning with?), what identifier to use when the system is broke down;

2) Traits of patient: description, format, typo rules;

3) Rules for archiving patient identities;

4) Rules for deletion;

5) Others rules;

f) Procedures: *list of the procedures already available or to be defined*;

EXAMPLES Creation, update, detection of duplicates, detection of collisions, procedure for when system is not available, procedures for anonymity of VIP's or staff.

g) Information System: describing in detail all applications or systems concerned, architecture of the system, the messaging systems and the standards used, servers, archiving, database, network;

h) Security aspects:

1) Table of the access rights: description of the roles and access rights of the healthcare professionals to the patient identifier services;

2) Authentication: description of the modality to authenticate the users for each application;

3) Availability of the system;

4) Data protection;

i) Quality indicators: *describe the indicators used to improve the quality*;

EXAMPLE Rate of duplicates per month, rate of collision per year, rate of updates per month.

j) Respect of the patient rights: *description of the patient charter (guidance Point 10 of the European Standards on Confidentiality and Privacy in healthcare can help)*;

Healthcare providers shall ensure that patients and/or their legal representative are informed in a manner appropriate for the patient's communication needs of:

1) what kinds of information are being recorded and retained;

2) the purposes for which the information is being recorded and retained;

3) what protection is in place to ensure non-disclosure of their information;

4) what kind of information sharing will usually occur;

5) the choices on information sharing available to them;

6) how their information may be used and disclosed;

7) about their right to access and where necessary to correct the information held about them within healthcare records;

8) The information required to be provided to them by national law implementing Directive 95/46/EC; and

9) country specific legal provisions or principles governing disclosure.

Annex B
(informative)

Norms, standards and other references

B.1 General

The list of norms and standards are not exhaustive but are those well-known at this time or are implemented by software. We have selected ISO/TS 22220:2011 and IHE profiles. HL7 V2 or V3 are not described because their implementation is directly described in IHE profiles.

B.2 ISO/TS 22220:2011, Identification of subject of Healthcare

This ISO Technical Specification was prepared by ISO/TC 215. It is based on the principles that it is difficult to have a reliable identification of individuals. The difficulties often met are:

— the variability of the quality of the identification;

— the capacity of the patient to provide the right information;

— the variability of the matching identities method;

— the respect of the wishes of the patient.

This document will provide guideline for improving the positive identification of subject of care within an healthcare organization or between healthcare providers. The technical specification provides a generic set of identifying information which is application independent.

The set of demographic data is split in two groups:

— the first group describes identifiers and names and quality.

— the second group contains others information as date of birth, address, death date, sex, mother's name, electronic communication and biometric data.

Each data are presented in a form and one or more standards are referenced. HL7v2.4 is often referenced for the data structure (not the last version HL7v2.5 and now HL7v2.6.)

The interest of this technical specification is to standardize the usual demographic data and proposes guidelines to use it.

B.3 IHE and profiles supporting Patient identification

B.3.1 General

IHE (Integrating the Healthcare Enterprise) is an initiative by healthcare providers and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinate use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better are easier to implement, and enable care providers to use information more effectively.

B.3.2 IHE-PAM-Patient administration management

IHE (Integrating the Healthcare Enterprise) has an objective to ensure that all required information for medical decision is correct and available to healthcare providers. IHE is both a process and a forum to encourage integration efforts. It defines a technical framework for the implementation of established message standards.

This profile establishes the continuity and integrity of patient data and coordinates the exchange of patient registration and update information among systems that need to be able to provide information regarding a patient's encounter status and location.

The PAM profile supports two patient encounter management scenarios: either one single central patient registration system serving the entire institution, or multiple patient registration systems collaborating as peers serving different clinical settings in an institution. (from IHE-PAM).

This profile defined two transactions based on message exchange to support patient identity and encounter information as well as movements within an acute care encounter. These transactions are named *ITI-030 Patient identity feed* and *ITI-031 Patient Encounter Management.* The standard used for the two transactions is HL7v2.5.

The transaction *ITI-030 Patient identity feed* supports the following events:

— create new patient;

— update patient information;

— change patient identifier list;

— link patient information (optional);

— unlink patient information (optional).

The transaction *ITI-031 Patient Encounter Management* supports the following events:

— admit inpatient;

— register outpatient;

— discharge patient;

— update patient information;

— merge patient identifier list

and options concerning inpatient/outpatient encounter management (pre-admit patient, change patient class to outpatient, transfer patient), pending event management (pending transfer, pending discharge), advanced encounter management(change attending doctor, leave of absence, return from leave of absence, move account information), temporary transfers tracking (patient departing-tracking, patient arriving-tracking), historic movement management.

This profile is very complete to manage exchanges for patient identity, encounter and movement within a healthcare organization.

B.3.3 IHE-PDQ-Patient Demographic Query

This profile provides for applications to query a central patient information server for a list of patients based on user-defined search criteria and retrieve a patient's demographic (and optionally visit or visit related) information directly into the application. Two transactions are available: *ITI-21 Patient demographics query*

and *ITI-22 Patient demographics and visit query.* This profile may play an integral workflow role in conjunction with other IHE profiles. It is for example possible to use this profile in a multi-domain environment.

This profile is based on HL7v2.5.

B.3.4 IHE-PIX-Patient Identification Cross Referencing

This profile supports the cross-referencing of patient identifiers from multiple patient identifier domains via the following interaction:

— the transmission of patient identity information from an identity source to the patient identifier 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 interest of this profile is that it supports all models of implementation, federation or correlation models by coupling a patient identity source with the patient cross reference manager actor. This profile is completely compatible with the description of cross reference patient identifier domain explained in the section X.

Three transactions are available: *ITI-8 Patient identity feed*, *ITI-9 PIX Query* and *ITI-10 PIX update Notification.*

This profile is based on HL7v2.5 for ITI-9 and ITI-10 but HL7V2.3.1 for ITI-8. The transaction ITI-9 is based on two segments *PID-3 Patient identifier List* and *PID-5 Patient Name*. The response does not contain any name when the answers are expected.

The transaction ITI-10 involves the Patient Identifier Cross reference manager actor providing notification of updates to the consumer.

B.4 Netc@ard for eHIC: Electronification of Healthcare Insurance Card

eHIC is a digital process of establishing a trustworthy of health Insurance data set at the health care service provider. It can also be used for associated inter-state back office, e-billing and reconciliation. The Netc@ard project (http://www.netcards-project.com) seeks to test and verify the concepts to allow coexistence of different platform and progressive migration of different countries toward IT supported arrangements, while maximizing the involvement of the national system already in place. The countries involved in this project are Austria, Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Slovak Republic and Slovenia.

The introduction of new specific Health chip Card Insurance card is not necessary while the eHIC trustworthy data set can be obtained either by scanning eye-readable eHIC or by reading national/regional smart card then by checking on line.

The following schema based on an example, summarizes the architecture (from Gie Vitale):

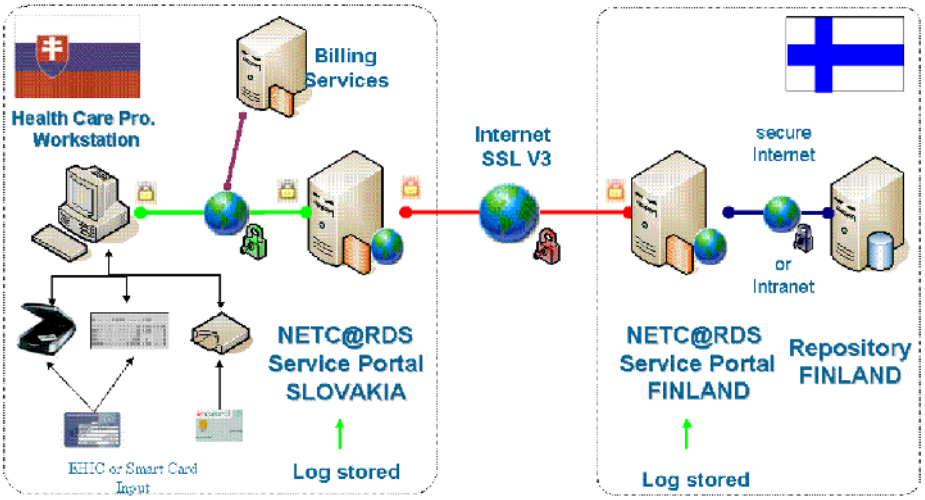


Figure B.1 — Architecture of Exchange of Insurance information between countries

Four use cases are identified:

— *CASE 1* is a full off-line scenario case. The NETC@RDS data set is captured from smart card memory by off-line software application for further processing. Scenario Case 1 could improve existing relatively poor off-line eye-readable security by requiring the ensured to key in a user PIN-code.

— *CASE 2* combines both smart cards and IT network applications. The NETC@RDS data set is thus downloadable from server when required. In scenario Case 2 the smart card application applies first for secure network connection to the relevant Health Insurance Provider server for online authentication. Ensured data set would be downloaded after successful completion of smart card authentication. However, the data set could be stored in the card as well for back-up solution in case server would be out of order or remote connections are down. This would be the preferred scenario.

— *CASE 3*. This is the full online scenario. The NETC@RDS data set is downloaded from remote server when manually typing-in ensured ID data and password at hospital. Data privacy could possibly be enhanced by use of health professional authentication certificates.

— *CASE 4* is a full off-line scenario case that will apply when none of the other scenario cases could be available. In Case 4, ensured information will be captured either from eye-readable European Health Insurance plastic cards that are foreseen after June 1st, 2004 or from certificates provisionally replacing the visual European Health Insurance Card6. Typing-in data from E-111/E-111+ paper forms as intermediate or temporary solutions for electronic data set completion will be / is also considered at early stage of the EHIC deployment. It shall be noted that any ensured citizen from any E.U Member-States could receive the service provided with Case 4 in the NETC@RDS pilot hospitals –i.e. not only ensured from the Regions in Member-States participating to the project.

In this architecture, the repository assumes the role of the national/ regional Patient Identity Source corresponding of a Patient identity domain.

The data set includes the information of:

— identification of the healthcare provider;

— identification of the Insurance Patient Identity (name, Insurance Number, period of validity);

— admission information;

— other insurance information.

B.5 FIDIS Future of Identity in the Information Society

The FIDIS (http://www.fidis.net/) is a network of excellence funded by the EU, 6th Framework Program. It address he requirements for the future management of identity in the European Information Society and contributing to the technologies and infrastructures needed.

One activity through the seven activities of the FIDIS is focused on the Identity. Four WP were defined and some of them are today finalized:

— Inventory of Topics and Clusters: focused on the definition of the concepts in this area;

— Set of use cases and scenarios;

— Models: describes processes and representation of the identification data and the different domains using these data identification;

— Identity in a Networked World - Use Cases and Scenarios.

Bibliography

[1] EN 13606-4, *Health informatics — Electronic health record communication — Part 4: Security*

[2] EN 14484, *Health informatics — International transfer of personal health data covered by the EU data protection directive — High level security policy*

[3] EN 14485, *Health informatics — Guidance for handling personal health data in international applications in the context of the EU data protection directive*

[4] EN ISO 12967-1, *Health informatics — Service architecture — Part 1: Enterprise viewpoint (ISO 12967-1)*

[5] EN ISO 13606-1, *Health informatics — Electronic health record communication — Part 1: Reference model (ISO 13606-1)*

[6] EN ISO 27789, *Health informatics — Audit trails for electronic health records (ISO 27789)*

[7] ISO 13606-3, *Health informatics — Electronic health record communication — Part 3: Reference archetypes and term lists*

[8] ISO/TS 22600-1, *Health informatics — Privilege management and access control — Part 1: Overview and policy management*

[9] ISO/TS 22600-2, *Health informatics — Privilege management and access control — Part 2: Formal models*

[10] ISO/TS 22600-3, *Health informatics — Privilege management and access control — Part 3: Implementations*

[11] HL7 v3, RIM Reference Information Model of HL7version 3 standard

[12] HL7 v2.5.1, HL7 Messaging standard version 2.5.1

[13] Service Functional Model Specification - Entity Identification Service (EIS), HSSP (joint endeavour between HL7 and OMG)

[14] *Person Identification Service (PIDS), (a.k.a. Patient Identification Service)*, Final Submission - Revision 7, OMG CORBAmed DTF, 98-01-09

[15] *General and detailed specifications for patient's identification*, 2001-2002, GIP GMSIH (France): *Principles of Patient Identification*

[16] *General and detailed specifications for patient's identification*, 2001-2002, GIP GMSIH (France): *Guideline for elaboration of the Patient Identification policy*

[17] *General and detailed specifications for patient's identification*, 2001-2002, GIP GMSIH (France): *Guideline for elaboration of the Cross Reference patient identification policy*

[18] *General and detailed specifications for patient's identification*, 2001-2002, GIP GMSIH (France): *Patient identification services*

[19] *General and detailed specifications for patient's identification*, 2001-2002, GIP GMSIH (France): *Cross Reference Patient identification services*

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

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

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

[23] *Foundations for the future, Priorities for health informatics standardisation in Australia*, 2005–2008, Information and Communications Technology Standards Committee (ICTSC) 2004 (ISBN 0 642 82642 0)

[24] *IHE IT Infrastructure Technical Framework*, Volume 1, (ITI TF-1) Integration Profiles

[25] *IHE IT Infrastructure Technical Framework*, Volume 2, (ITI TF-2a,b) Transactions

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™