A Technological Framework for EHR Interoperability: Experiences from Italy

Mario Ciampi[1](✉), Mario Sicuranza[1], Angelo Esposito[1,2], Roberto Guarasci[3,4], and Giuseppe De Pietro[1]

[1] Institute for High Performance Computing and Networking, National Research Council of Italy, Naples, Italy
{mario.ciampi,mario.sicuranza,angelo.esposito, giuseppe.depietro}@na.icar.cnr.it

[2] Department of Engineering, University of Naples Parthenope, Naples, Italy

[3] Institute for Informatics and Telematics, National Research Council of Italy, Rende, CS, Italy

[4] Department of Linguistics, University of Calabria, Rende, CS, Italy
roberto.guarasci@unical.it

Abstract. Electronic Health Records (EHRs) systems enable the construction of longitudinal collection of health information about individual patients, by integrating health data produced by the healthcare facilities. The advantags associated with the use of such systems are in terms of improvement of quality of care and cost reduction. An important barrier to the availability of exhaustive longitudinal collections of health data is represented by the lack of interoperability among EHR systems. In Italy, each region has been developing its own EHR systems according to the national guidelines and technical specifications compliant to the indications provided by a Italian Law issued in 2012 and updated in 2013. This paper describes the national technological framework designed from a National Technical Board for making interoperable the regional EHR systems each other, preserving the privacy of the patients. The framework, based on a System-of-Systems approach, enables healthcare professionals both to (i) consult health documents associated with a patient, even if they are produced in other regions, and (ii) register new health documents for patients assisted by other regions.

Keywords: Electronic health record · Interoperability · Framework · Italy

1 Introduction

The use of ICT in healthcare has resulted in a considerable development of health information systems (HISs) in order to both enhance the quality of care services, and simultaneously reduce costs [15,25]; the most important example of HIS is the Electronic Health Record (EHR), which allows a fast exchange of clinical data between different healthcare organizations. In the last decades, many

C. Röcker et al. (Eds.): ICT4AWE 2016, CCIS 736, pp. 80–99, 2017.
DOI: 10.1007/978-3-319-62704-5_6

countries in the world have made significant efforts to develop EHR systems [13]. The International Organization for Standardization (ISO) defines EHR as a repository of patient data in digital form, stored and exchanged securely, and accessible by multiple authorized users. It contains retrospective, concurrent and prospective information and its primary purpose is to support continuing, efficient and quality integrated health care.

Despite such efforts in the realization of EHRs, the systems developed, at different levels (for example regional and national), are very often not able to interoperate each other [24], due to a plethora of reasons. First, each country or regional domain is characterized by its own legal requirements, especially about privacy protection. Second, countries or regions have typically different needs, depending on their dimension, number of citizens, number of healthcare facilities, etc. Finally, the development of the systems have been started in different periods, adopting or applying diverse standards in different ways [20].

The lack of interoperability among these systems can result in decreased levels of quality of patient care and waste of financial resources. In fact, when a patient benefits from a health service outside her/his health care domain, the health professional that treats the patient is not able to access the patient health information, due to the impossibility of cooperation between the EHR system used by the health professional and the one related to the patient. Therefore, the health professional typically requires the patient to repeat a clinical exam already executed. With respect to interoperability, several levels of interoperability are defined in literature [22]: *technical interoperability*, for which the systems share the communication protocols making possible, e.g., the exchange of bytes between them; *syntactic interoperability*, which aims at making the systems capable of communicating and exchanging data through the sharing of data formats; *semantic interoperability*, whose purpose is to enable systems to exchange data and interpret the information exchanged in the same way; *organizations & services interoperability*, where business processes are shared between the systems.

The importance of making EHR systems able to interoperate each other has motivated by the increase of the phenomenon of the patient mobility for reasons of care. For example, we can consider Italy where 570k hospitalizations are made by patients in a region different from that they reside only in 2015 [1]. In Italy, the autonomy about healthcare delivered by the Italian Constitution to each region caused the spread of heterogeneous regional EHR systems. After some national initiatives aimed at proposing a first architectural model at national level, the emanation of Italian norms has allowed defining both (i) the national architectural model of reference, and (ii) the functional and privacy requirements to be respected by all the Italian regions.

This paper, extending the concepts illustrated in a previous work [18], describes the Italian architecture for EHR system interoperability, developed by a National Technical Board, coordinated by the Agency for Digital Italy (AgID) and the Ministry of Health, with the technical support of the National Research Council of Italy (CNR) and the participation of the Ministry of Economy and Finance and Italian regions.

This paper is organized as follows. Section 2 provides some background and related work on the main standards, projects on e-health data interoperability and the description of the Italian context. Section 3 describes the main features of the national infrastructure for EHR systems, highlighting the cross-border business processes. Section 4 provides some technical details about the architecture of EHR systems and security issues. Finally, Sect. 5 concludes the paper with some final remarks and indications for future works.

2 Background and Related Work

2.1 Health Informatics Interoperability Standards

In order to achieve interoperability, the use of standards is a mandatory requirement. This section briefly describes the main health informatics standards, such HL7 and CEN ISO EN13606, and several initiatives, such openEHR and IHE, that promote the use of standards for health information systems development and integration.

The CEN/ISO EN13606 is a European norm from the European Committee for Standardization (CEN) also approved as an international ISO standard. It is designed to achieve semantic interoperability in the electronic health record communication. The overall goal of the CEN ISO 13606 standard is to define a rigorous and stable information architecture for communicating part or all of an electronic health record among EHR systems, or between EHR systems and a centralized EHR data repository [2].

Health Level Seven International (HL7) [3] is a non-profit organization involved in the development of international health informatics interoperability standards. The goal of these standards is supporting the exchange, integration, sharing and retrieval of electronic health information. HL7 messaging standards define the language and data structure required for information integration among HISs. Version 2 of the standard (HL7 v2) is currently implemented in numerous health organizations, whereas Version 3 (HL7 v3) is based on an object-oriented model called *Reference Information Model* (RIM). Clinical Document Architecture (CDA) is a standard derived from the RIM with the aim of specifying clinical documents structure and semantics. Currently, HL7 is involved in the definition of a new health interoperability standard, named Fast Healthcare Interoperability Resources (FHIR), which combines the best features of the previous versions [4].

openEHR [5] is an international not-for-profit foundation, which issued a detailed and tested specification for an interoperable HIS platform. Such a vision of openEHR had a significant influence on the development of the healthcare industry standards, such as HL7 and CEN EN1360610, with recommendations for an interoperable interconnection of HISs. OpenEHR consists of a generic information reference model, application-specific archetypes [14] and context-specific templates.

Integrate the Healthcare Enterprise (IHE) is an international initiative founded by Radiological Society of North America (RSNA) and Healthcare Information and Management Systems Society (HIMSS) with the goal of supporting the integration of HISs through existing standards. IHE promotes the coordinated use of established standards such as HL7 to address specific clinical needs in support of optimal patient care. IHE constantly defines Integration Profiles within Technical Frameworks, to provide definitions on the implementation of health standards in order to meet clinical needs and solve problems related to specific use cases: a known example of a Technical Framework is the *IHE IT Infrastructure Technical Framework*. In this context, the integration profile more relevant in the IT Infrastructure domain is Cross-Enterprise Document Sharing (XDS), which has the scope of facilitating the sharing of patient electronic health records across health enterprises [6]. IHE XDS aims at facilitating the sharing of clinical documents within an affinity domain (a group of healthcare facilities that intend to work together) by storing documents in an ebXML registry/repository architecture.

2.2 Health Interoperability Projects

This subsection describes the most relevant international interoperability projects on the development of EHR systems.

Canada Health Infoway is an independent, federally-funded, not-for-profit organization with the responsibility of accelerating the adoption of digital health solutions across Canada. Along with the Canadian provinces and territories, Infoway provided a national framework called EHR blackprint, with the aim of guiding the development of the systems in each different province. The key elements of the framework, built following a Service-Oriented Architecture (SOA) based on the HL7 Version 3 standard, are: gateways, data repositories, registry services, infostructure, access mechanisms [7].

U.S. Healtheway (now Sequoia) is a non-profit, public-private partnership that operationally supports the eHealth Exchange project. With production starting in 2007, eHealth Exchange has become a rapidly growing community of public and private organizations, with the aim of facilitating the exchange of health information in a trusted, secure, and scalable manner. The exchange is realized through Web Services conforming to specifications based on IHE integration profiles. Finally, in order to support the health information exchange at local and national level, an open-source software named CONNECT has been developed [8].

epSOS project was an European project aimed at promoting the interoperability among the EHR systems of EU Member States. The scope of the epSOS project, which involved 25 different European countries, was to realize a large-scale pilot testing the cross-border sharing of two kinds of health documents: patient summary and electronic prescription. To achieve such an objective, a service infrastructure was designed, built, and evaluated. The national EHR systems communicate each other by means of gateways, named National Contact Points (NCPs), by exchanging: (i) messages based on IHE specifications, and (ii) clinical documents in the HL7 CDA format [9]. Starting from the results achieved in the epSOS project, the projects *Simple European Networked Electronic Services (e-SENS)* and *Expanding Health Data Interoperability Services (EXPAND)* have been activated. The e-SENS project covers different aspects of ICT applied to cross-border processes in domains such as e-Health, e-Justice, e-Procurement and business setup; it goes towards the idea of the European Digital Market. The EXPAND project is characterized by a network of 16 EU Member States with the aim of moving towards an environment of sustainable cross-border European services, through the Connecting Europe Facility (CEF) at European level and the development of national infrastructures and services.

2.3 Italian Context

This subsection describes the Italian context about eHealth. The Italian Government, since 2003, has identified a number of general objectives for the national health service in the light of changes in the social panorama and the national policy, with the basic requirement to guarantee citizens health protection, social security, and equity, quality and transparency in the care. These national plans have enabled various regional systems to develop independently infrastructure and services for e-health. In fact, in Italy there are different regions (provinces and autonomous), each of which with its health autonomy.

The Italian regions, driven by different needs, have developed services for e-health independently. In this way, highly heterogeneous and hardly interoperable systems have been obtained. The "e-Government Plan 2012" made by the Italian Ministry for Public Administration and Innovation has defined a set of digital innovation projects to modernize and make more efficient and transparent public administration, in order to promote the simplification and digitization of primary health care services.

A reference model was developed in the "Electronic Health Records guidelines" approved by a National Technical Board. The guidelines produced are compliant to the national normative and to the European strategic approach, according to which the role of the citizen-patient has a central value [21]. In Italy, a first prototypal architectural model for the realization of an interoperability secure EHR infrastructure, named InFSE [19], was defined and developed within three conjunct projects between the Department of Technological Innovation of the Presidency of the Council of Ministers and CNR.

The infrastructure, in absence of a norm, was designed with the aim of enabling interoperability among regional EHR systems. The components of the infrastructure were implemented and used in experimentations that have had the scope of enable the interchange of clinical documents by means of the interoperability of some regional EHR systems. The software components of the InFSE infrastructure were also used within the national IPSE project linked to epSOS, in which 10 Italian regions were involved. The aim of the project was to make regional EHR systems able to interoperate each other for the interchange of patient summaries.

The Laws 179/2012 and 98/2013, and the subsequent decree DPCM 178/2015 (Decree 178, 2015), have provided the Italian legal system of a definition of EHR, meant as the set of digital health and social-health data and documents generated from present and past clinical events, about the patient. According to the norms, EHR can be used for three finalities: (a) prevention, diagnosis, treatment and rehabilitation; (b) study and scientific research in the medical, biomedical and epidemiological field; (c) health planning, verification of the quality of care and evaluation of health care. The decree DPCM of 29 September 2015 n. 178 defines the rules by which the Italian regions have to set up their EHR systems.

The regulatory framework has permitted to a National Technical Board to define a set of reference guidelines for the implementation of the EHR systems [17]. Then, a set of technical specifications, which establish the main requirements to be met by the regions, have been defined to guarantee interoperability at different levels:

– *technical interoperability* is assured by sharing communication protocols among services interfaces;
– *syntactic interoperability* is reached by the use of common data formats;
– *semantic interoperability* is guaranteed by adopting both same data formats and coding systems;
– *organizations & services interoperability* is enabled by the sharing of common cross-border processes.

3 National Framework for EHR Systems

3.1 Overall Architectural Model

The national framework of EHR in Italy is a system of systems composed by all the regional interoperabile EHR systems able to share health documents by providing and using a set of health services. Each regional EHR system is been developing (or will be developed) in accordance with the requirements specified by the norm, guidelines and specifications. The defined framework allows the preservation of the various regional EHR systems autonomy, and enables interoperability between them. The architecture of each system is characterized by: (i) a central registry for the management of metadata associated to the health documents related to patients for the localization and management of these ones, and (ii) health repositories containing clinical documents. Each patient has a single reference region, called Healthcare Assistance Region (RDA). The Healthcare Assistance Region has to manage all the documents related to its patients, not only those produced in its healthcare facilities, but also the documents created in another region. In the case a patient is cured in a region different from RDA after having required a health care service, the clinical document produced is archived in a repository of this region, which is in charge of providing metadata about the document to the Healthcare Assistance Region. For this reason, the regional systems expose a set of services, including: search for documents, retrieve documents, communicate metadata to RDA.

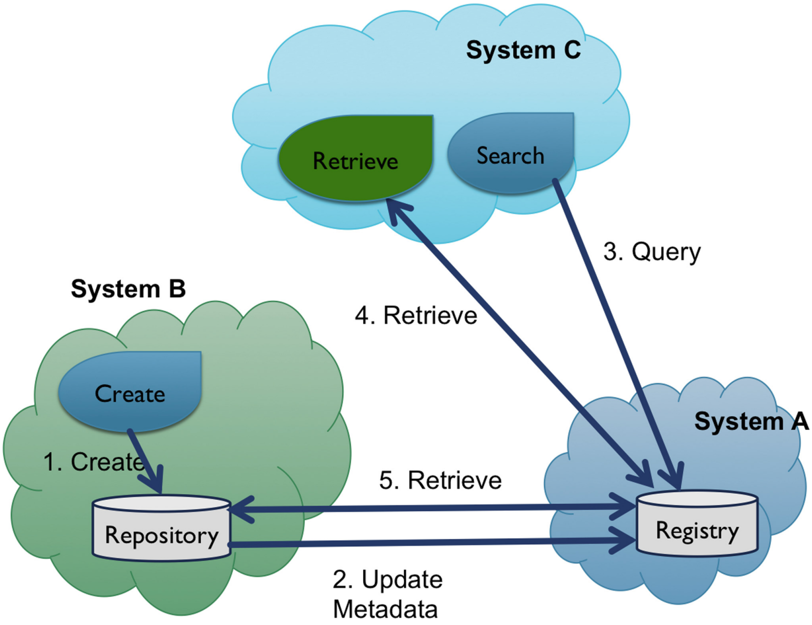

Fig. 1. Interactions among the regional EHR systems.

Figure 1 shows the interactions between three possible regional EHR systems:

- creation of a clinical document (operations 1. Create and 2. Update Metadata);
- search for and retrieve a clinical document (operations 3. Query and 4. Retrieve).

The interaction for the creation of a clinical document expects that a patient (with RDA = System A) points to system B for a clinical event. In this way, the system B generates a document, which is inserted in a repository. Then the system B sends the metadata of the document to system A. The search and retrieve interactions require that the system C searches for the document (created before). The patient's RDA system is represented by the system A, so the search operation is carried out from the system A, after that system C requests to retrieve the document to the system A, which finally requests it to the system B and manages the request acting as a proxy. It is clear that these iterations require the knowledge of a range of information, including for example the patient's RDA. Below in paragraph Sect. 3.3 the processes related to these interactions are detailed.

3.2 Requirements of EHRs

Several organizational and architectural constraints are taken into account in the definition of the architecture for the interoperability framework for EHR systems. The main constraints are the following:

- **Patient Consent:** every patient can take advantage of the functionalities offered by the EHR system of the health care provider region of the patient. To this aim, she/he has to express two types of consent: (i) Uploading consent, which is a consent enabling the population of the EHR with her/his clinical documents by the health facilities; (ii) Consultation consent, which is a consent enabling the consultation of the EHR by health professionals. Specifically, the patient is allowed choosing the professional roles permitted to access her/his EHR by defining specific privacy policies.
- **Index Metadata Model:** the Healthcare Assistance Region of the patient has the responsibility of maintaining index metadata related to all the documents related to its patients, even if such documents are produced and maintained by health facilities sited outside the region.
- **Proxy-based Interoperability Model:** the system of the health care provider region has to operate as a mediator with the other regional systems in all the cross-border processes in which its patients are involved.
- **First Implementation of EHRs:** even if EHRs can contain a multitude of topologies of information, the first mandatory kinds of clinical documents to be accessible via EHR are patient summary and laboratory report. Then, in the first phase, only details about the finality of care of the patient are defined.

3.3 Cross-Border Processes

This subsection describes the set of cross-border processes that have been defined in order to enable the application communication among regional EHR systems.

The interoperability requirement among EHR systems requests a shared architecture topology at national level, for which each regional EHR system must provide a set of interoperability services.

All the regional nodes cooperate according to a joint architectural model based on a federated approach, by exposing and invoking the services of the other nodes. These services are needed for sharing all EHR information at national level. Each regional node has to offer a series of services designed to ensure interoperability with other regional nodes, which themselves make use of these services. In the context of interregional interactions, such nodes can be grouped in three classes:

- **Provider Node:** is the node that offers an interoperability services.
- **Consumer Node:** is the node that benefits from an interoperability service.
- **Proxy Node:** is a node that provides support services.

The interactions among different types of nodes are shown in Fig. 2.

Every regional EHR systems have to implement cross-border processes (and the related services) according to a Service Oriented Architecture (SOA) paradigm. Such processes have to satisfy a set of national business processes, according to which each region may assume a different role (Fig. 3):

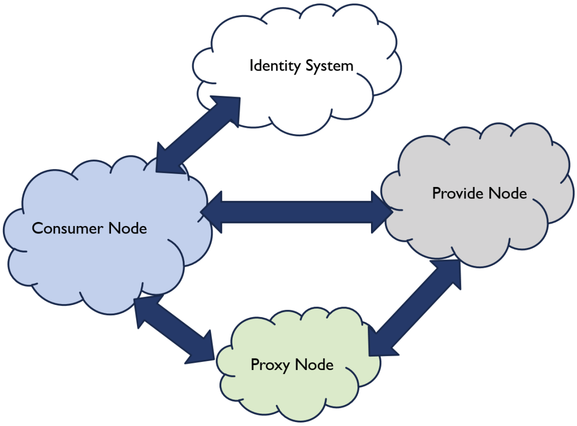

Fig. 2. Interactions among nodes.

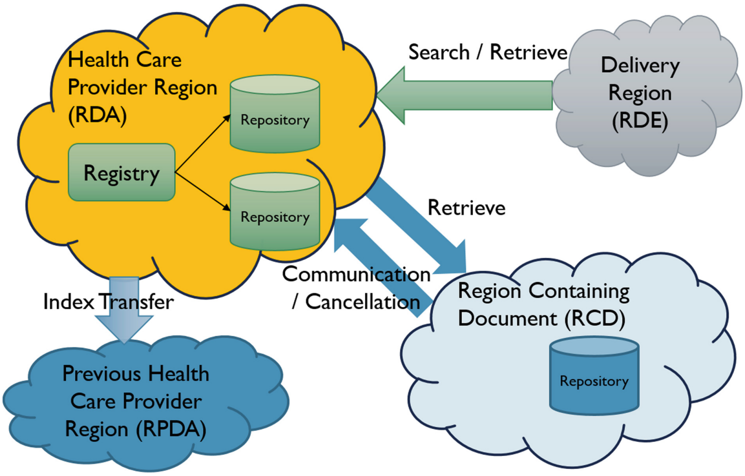
Health Care Provider Region (RDA)
Registry
Repository
Repository
Search / Retrieve
Delivery Region (RDE)
Retrieve
Communication / Cancellation
Index Transfer
Previous Health Care Provider Region (RPDA)
Region Containing Document (RCD)
Repository

Fig. 3. Roles in the cross-border processes.

- **RDA** (Healthcare Assistance Region)**:** is the region that manages (through metadata) clinical documents and security policies related to a patient which the region has in charge. The document management is performed by memorizing specific metadata associated to documents, allowing thus the localization and management of the clinical resources;
- **RCD** (Region Containing a Document)**:** is the region in which a specific document has been created and maintained; the document is stored in a repository of the region, but the metadata are managed by RDA (RCD can coincide also with RDA);

- **RDE** (Region of Service Delivery)**:** is the region that provides an health service to a patient, so RDE is able to search for a document and/or to create a document;
- **RPDA** (Previous Healthcare Assistance Region)**:** is the region that previously has taken in charge a patient, managing his/her clinical documents. The patient may choose to change his/her Healthcare Assistance Region**:** in this case all the metadata and policies will have to be transferred from RPDA to the new RDA.

The possible cross-border processes are described below:

- *Searching for documents*: RDE requires RDA to consult the EHR of the patient. RDA returns the list of documents for which the user has access rights. Figure 4a shows the request of this service.
- *Retrieving a document*: RDE, after obtaining the list of documents, requires RDA retrieving a document. RDA returns the document if the user has access rights. Eventually, RDA forwards the request to RCD if the document is available outside. Figure 4b shows the request of this service.
- *Creating or updating a document*: RDE transmits to RDA the list of metadata of a document created/updated for a patient of this one (the document is stored in RDE, which therefore serves as RCD). RDA stores the metadata in its system.
- *Invalidating a document*: RCD requires RDA to perform a logical deletion of metadata related to a document, due to the invalidation of this one.
- *Transferring of index*: a new RDA requires RPDA to transfer the index of the EHR (list of all metadata and privacy policies) associated with the patient. RPDA returns the index, which is registered in the new RDA, and then disable it. After the transfer, the invalidation process on the transfered documents has to be performed.
- *Patient identification*: RDE requires the Identity System, which is a central system at the national level, the identification of a patient, in order to obtain the patient's personal data (such as name, surname, etc.) and a patient identification assertion. Figure 4a shows the request of this service.

Figure 4 shows the relationship between regional systems through the processes. In order to achieve semantic interoperability, several standards in different domains exists, e.g. CIDOC-CRM [10] in the cultural domain. Due to its specificity, to assure semantic interoperability for the e-health domain, suitable standards have been individuated: HL7 CDA Rel. 2 specifies the structure and semantics of clinical documents, whereas clinical content is represented by using a set of classification and coding systems, like the international standards International Classification of Diseases, Ninth Revision, Clinical Modification (ICD9-CM), Logical Observation Identifiers Names and Codes (LOINC) and Anatomical Therapeutic Chemical (ATC) or the national standard Marketing Authorization (AIC).

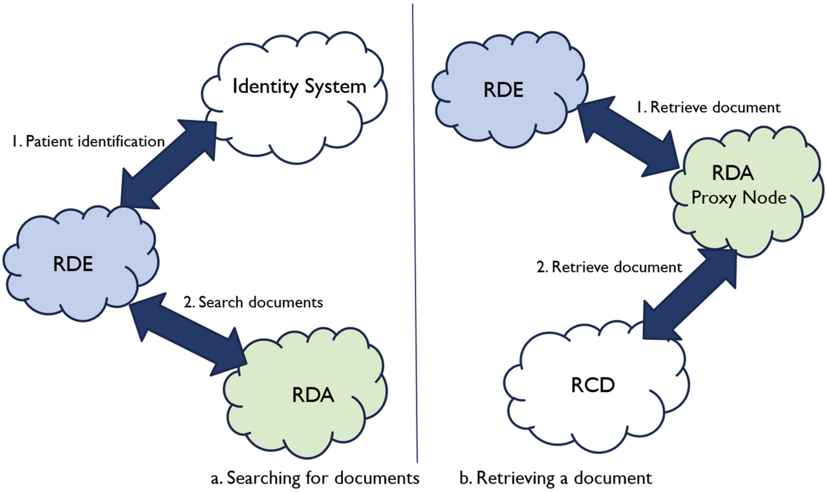

Fig. 4. Roles in the cross-border processes.

4 Technical Details

4.1 Architecture Components of EHR Systems

All the regional EHR systems are based on the registry/repository paradigm. The clinical documents produced by the health facilities are stored in repositories and indexed in a regional registry (managed by RDA) by means of appropriate metadata. The metadata, as mentioned above, are appropriate information associated with the document that allow the management of the documents, including the ability to locate them. For each clinical document is necessary to manage a set of metadata. The mandatory metadata are: document type, document state, document identifier, creation date, author identifier, patient identifier, repository reference. The interoperability of the regional EHR systems is based on a nationwide federated model, based on a System-of-Systems approach, where each regional system is realized by taking into account local needs. In order to make the regional systems able to interoperate each other, each EHR system exposes a set of cross-border services, which preliminarly verify the possession of the rights by the user and provide all the functionalities needed to manage, search, and consult metadata and documents. The architecture of the distributed system at national level is shown in Fig. 5.

The security model adopted is based on a Circle of Trust among the regions. Each region is responsible for the claims made in the process of request of the cross-border services provided by the other regions. In addition, all the communications among the regional systems are exchanged through the Public Connectivity System (SPC), the Italian technological infrastructure for exchanging information assets and data between Public Administrations. Specifically, every

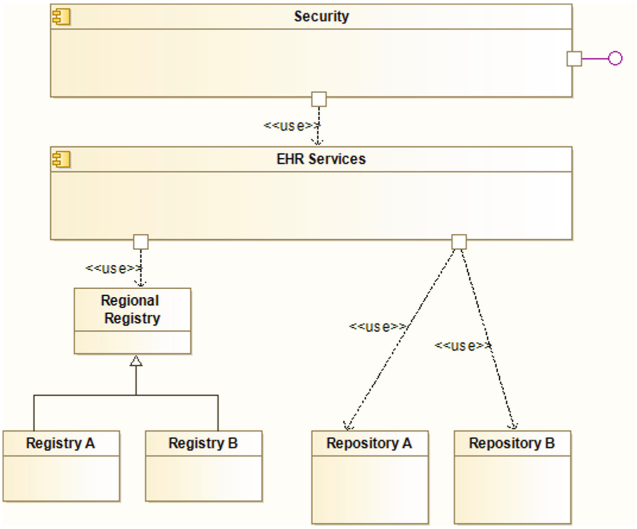

Fig. 5. Architecture of a regional EHR system.

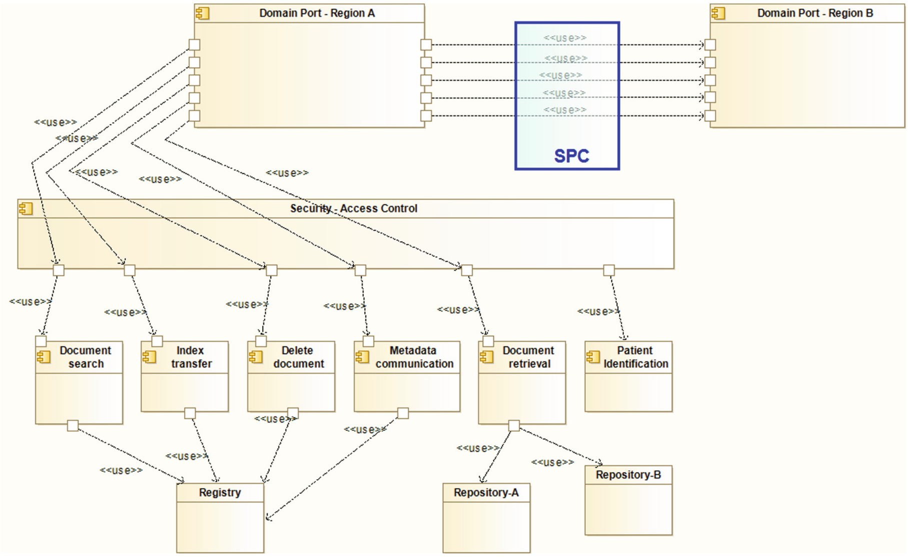

Fig. 6. Interactions among EHR systems through the SPC infrastructure.

cross-border service is linked to the SPC infrastructure by means of specific software components called Domain Ports, as shown in Fig. 6.

4.2 Cross-Border Services

The cross-border services to be implemented according to the business processes described above have to be able to exchange messages compliant to IHE XDS.b transactions [6], opportunely localized at Italian level. IHE XDS profile [11] provides specifications for managing the exchange of documents that care delivery organizations have decided to share. The IHE transactions are shown in Fig. 7. A brief description of the structure defined for the communication with the services is provided below:

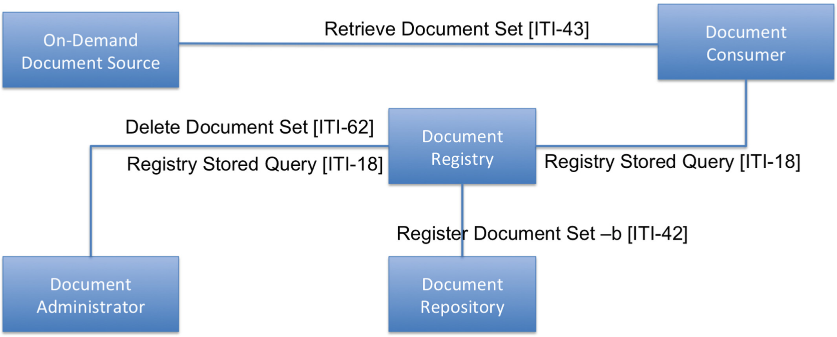
On-Demand Document Source
Retrieve Document Set [ITI-43]
Document Consumer
Delete Document Set [ITI-62]
Registry Stored Query [ITI-18]
Document Registry
Registry Stored Query [ITI-18]
Register Document Set –b [ITI-42]
Document Administrator
Document Repository

Fig. 7. Actors and roles of the IHE XDS profile.

1. *Patient Identification*: allows authorized user to perform request of patient's identification and obtain the patient's identification assertion from the Identity System (that is an Attribute Authority in the federation). The communication protocol is compliant to the standard SAML 2.0 Protocol "AttributeQuery" [16].
2. *Document Search*: allows authorized users retrieving the index metadata related to documents satisfying specified search criteria (for example patient id, date, document type and status). The communication protocol of this service is compliant to the IHE ITI-18 transaction (Registry Stored Query), which consists in sending a query from the actor "XDS Document Consumer" (in this context represented by RDE) to the actor "XDS Document Registry" (in this context represented by RDA).
3. *Document Retrieval*: allows authorized users retrieving a specified document. The communication protocol of this service is compliant to the IHE ITI-43 transaction (Retrieve Document Set), which enables the request for document retrieval from the actor "XDS Document Consumer" (in this context RDE) to the actor "XDS Document Repository" (in this context, RDA).
4. *Metadata Communication*: allows authorized users sending index metadata to the health care assistance region of the patient to which a created/updated document refers to. The communication protocol of this service is compliant to the IHE ITI-42 transaction (Register Document Set-b), which enables

the submission of metadata from the actor “XDS Integrated Document Source/Repository” (in this context RDE = RCD) to the actor “XDS Document Registry” (in this context RDA).

5. *Index Transfer*: allows transferring the index of the EHR related to a patient from a regional system to another, after the change of the health care assistence region by the patient. The communication protocol of this service is compliant to the IHE ITI-18 transaction (Registry Stored Query), which enables the actor “XDS Document Consumer” (in this context the new RDA region) to send a request to retrieve all the EHR index of a given patient to the actor “XDS Document Registry” (in this context RPDA).
6. *Delete Document*: allows authorized users the cancellation of the metadata associated with a given document. The communication protocol of this service is compliant to the ITI-62 transaction (Delete Document Set), which enables the actor “XDS Document Administrator” (in this context, in the case of invalidation of a document correponds to RCD, or, in the case of EHR index transfer to RDA) to forward the document reference to be deleted to the actor “XDS Document Registry” (in this context, in case of invalidation of a document corresponds to RDA, or, in the case of EHR index transfer to RPDA), which provides the logic deletion of the requested document.

4.3 Security Issues

The main security issues treated concern user identification and access control, in that aspects like integrity, confidentiality and auditing are assured by the use of the SPC infrastructure as a secure channel of communication among the Italian Public Administrations. With specific regard to user identification and access control, the claims to be transmitted by every region in the SOAP messages exchanged among the cross-border services are attested by digitally signed SAML 2.0 assertions.

Each regional system must provide, as described above, a set of services to allow other systems communicating each other. For this reason, the definition of a shared security model has been a necessary step. The main security requirements that must be satisfied at the regional level are:

- Consent management;
- Visibility policies and obscuration;
- Access control;
- Patient identification.

The security model adopted in the Italian context allows the protection of the services offered by the regional EHR systems and the documents they maintain, by meeting the security requirements established by the national norms. Thus, it enables to respect the patient’s will expressed in terms of privacy. In fact the patient can provide or not the consents to the use of his/her EHR and he/she is able to specify who can access or not on his/her documents.

Consent Management. In Italy, the patient has to provide two different types of consents for making his/her EHR accessible, which are the "uploading" and "consultation" consents. If the patient provides the uploading consent, he/she allows healthcare professionals feeding the EHR with the clinical documents produced by them. Instead, with the consultation consent, he/she enables health professionals to access his/her clinical documents. The model provides the management of consents through meta-information stored in the patient's RDA. The meta-information about the consents are used both when creating a new document (in this case the uploading consent is verified) and when research documents (in this case the consultation consent is verified).

Patient Identification. A healthcare professional who intends to access a EHR has preliminarly to identify the patient of interest, because he/she has to be sure that the clinical information that she/he is going to receive in response is related to the patient for who she/he is carrying out a health service. This phase allows identifying the patient starting from his/her identification (the Italian fiscal code) or other personal information, such as name, surname and date of birth. This solution requires the presence of a national centralized Master Patient Index (MPI), and an appropriate service, named Identity Service. This service, received the request for identification, constructs an identity assertion, containing the information related to: current fiscal code, along with a set of possible previous fiscal codes, surname (at born), name, gender, date of birth, city of birth, province of birth, address of residence, Healthcare Assistance Region, etc. The identification assertion is included in the request messages for the provider system.

Access Control. The patient, according to the indications of the Italian Data Protection Authority, has to be able to indicate the set of healthcare professional roles that can have access to each clinical document of her/his EHR (visibility policies). The patient has also to be able to obscure (making inaccessible) her/his documents to specific healthcare professional roles (obscuration). The security model allows defining visibility policies and obscuration by managing appropriate meta-information associated with clinical documents, which precisely indicate the roles on the system that can access and the ones that cannot access for all the clinical documents. The meta-information is stored in the regional node of patient's RDA and used at the time of the request of the search for documents service. This meta-information is entered after the creation of the document, even if can be successively modified. With regards to the visibility policies and obscuration, appropriate security mechanisms based on access control techniches is used (more details are in [26]). The standard adopted for authentication and authorization data exchange is the Security Assertion Markup Language (SAML) [23]. SAML enables the exchange of assertions among different domains (different regional EHR systems), thus achieving the Single-Sign-On (SSO) among different EHR regional systems. This solution involves the use of SAML 2.0 and three different assertions: *identification assertion*, *attribute assertion*, and *RDA identity assertion*. The attribute and RDA identity assertions are built by the regional system of the healthcare professional (that is RDE). The access control approach consists in two different phases: the first phase is represented by the authentication of health professionals and patients, whereas the second one consists in the verification of the authorization for accessing clinical documents. Each system has its regional Attribute Authority (AA), which is a certification authority known at regional level. After the identification, the AA is in charge of constructing the attribute assertion. The identification assertion is built by the national centralized Identity System. All the assertions have to be digitally signed using the certificates and private keys issued by the central shared Certification Authority (CA), as better described below. During the authentication phase, the regional system has to: i) verify the user identities and the correct authentication of a healthcare professional, ii) generate the appropriate SAML assertion, which has to be sent to the provider system (another regional EHR system). The provider system must first verify the validity of the received SAML assertions (for example, the digital signatures) and then may authorize or not the healthcare professional to access its services.

Secure Message Exchange. During the exchange of clinical messages among regional EHR system, it is necessary satisfy the following requirements: *message confidentiality*, *message integrity*, *non-repudiation* of forwarded messages, *access control* of actors and services. The Web Services Security (WS-Security) [12] standard specifications are adopted and the communication can be protected by using Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS), on the top of the Transport Layer Security (TLS) standard. The exchanged SOAP messages have to contain the SAML assertions defined above, which are evaluated before being passed to the web service in charge. A portfolio of security assertions must be contained in all the transmitted messages. This portfolio contains the identity of the user who wants to access the EHR services, the user attributes (i.e. the user's role), information such as the purpose of use, the context in which the user is operating (e.g. ordinary or emergency), etc. The identity management is performed through a Circle of Trust of all the regional systems, which permits mutual trust relationships between the domains. In this way, the identity of the actors involved in the supra-regional transactions is ensured by a central trusted authority, which issues digital certificates to the regional domains. The message integrity is guaranteed by the use of the digital signature, which, along with the encryption, assures the non-repudiation of the forwarded messages. It is worth noting that some of these requirements are satisfied by the underlying SPC technological infrastructure. A more detailed description of the different kind of SAML assertions is reported below:

- *Identification Assertion*: certifies the identification data of a patient and her/his Healthcare Assistance Region; the assertion is issued by the national Identity System.
- *Attribute Assertion*: certifies the data relating to the user making the request, the operating environment and the type of activities to perform; the assertion is issued by the region that intends to use a cross-border service offered by another region.

- *RDA Identity Assertion*: certifies the identity of the Healthcare Assistance Region of the patient (RDA). This assertion, issued by RDA, is used in case of a request sent by RDE for retrieving a document available in RCD, through RDA, which acts as a proxy. RCD uses this assertion to verify if the request is really sent by RDA.

4.4 Central Services

In order to support the cooperation among the EHR systems, a national technical platform providing a set of central services has been realized. The services implemented have been identified analyzing the needs indicated by the regions in their project plans for the realization of their EHR systems.

The purposes of these services vary from managing service endpoints, to enabling the homogeneous presentation of the clinical documents represented according to the XML-based HL7 CDA format by means of national style sheets, to handling the terminologies. Besides, in order to support the correct development of the cross-border services by the regions, a test environment realizing the business processes described above has been implemented.

Such a test environment is able to simulate the behavior of a typical regional EHR system and allows regional domains verifying the correctness of the request

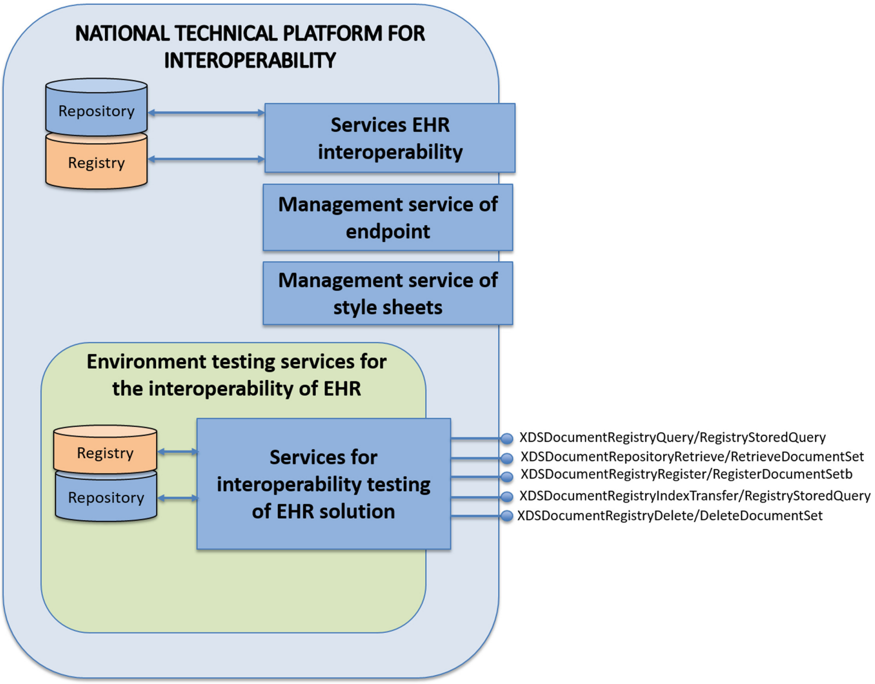
NATIONAL TECHNICAL PLATFORM FOR INTEROPERABILITY
Repository
Registry
Services EHR interoperability
Management service of endpoint
Management service of style sheets
Environment testing services for the interoperability of EHR
Registry
Repository
Services for interoperability testing of EHR solution
XDSDocumentRegistryQuery/RegistryStoredQuery
XDSDocumentRepositoryRetrieve/RetrieveDocumentSet
XDSDocumentRegistryRegister/RegisterDocumentSetb
XDSDocumentRegistryIndexTransfer/RegistryStoredQuery
XDSDocumentRegistryDelete/DeleteDocumentSet

Fig. 8. National platform for EHR interoperability.

messages for the invocation of the cross-border services. The set of interoperability services have been developed and made available in the national platform, as shown in Fig. 8. The developed platform provides in particular a test environment that allow the simulation of the interoperability services in accordance with the defined specifications: in this way the regions can simulate and test the request messages and identify the correct responses of the interoperability services. In order to enable this phase of testing, a Circle of Trust based on a single Certification Authority, which provides and maintains digital certificates used for digital signatures of the security assertions, has been set up.

5 Conclusions

In this paper, the Italian technological framework for EHR interoperability defined from a National Technical Board was presented. The architectural model of the framework was formalized in order to make interoperable the EHR systems developed by the Italian regions each other, preserving the privacy of the patients. The framework meets the organizational, functional and technical requirements provided by the Italian norms on EHR. In this scenario, patients clinical documents are accessible to all the authorized health professionals regardless of the region where the patient benefits from medical care. In order to ensure the privacy, the patient has to provide two different types of consents for making his EHR accessible, which are the "uploading" and "consultation" consents. In addition, the patient is able to define specific visibility policies, allowing or denying the access to her/his clinical documents on the basis on health professional roles. The availability of the documents is guaranteed by cross-border services based on the IHE XDS profile, which every regional EHR system has to make available, according to national common cross-border business processes. The security model of the national framework is based on the adoption of specific security standards, such as WS-Security and SAML assertions, which contain information about patient, health professional, context of use. SAML assertions are transmitted by every region in the SOAP messages exchanged among the cross-border services, in order to enable the verification of the access rights to EHR resources. Therefore, some central services have made available, including in particular a test environment that allow the simulation of the interoperability services in accordance with the national technical specifications. In this way, the regions can simulate and test the request messages and identify the correct responses of the interoperability services. As future work, it is planned to specify further technical details about some relevant aspects, like homogeneous use of digital signatures, style sheets, user access, coding systems and consent obtainment. These technical details will be addressed within interregional working groups.

Acknowledgements. The work presented in this paper has been partially supported by two joint projects between the Agency for Digital Italy and the National Research Council of Italy: Interventions to support the realization of the Electronic Health Record, prot. CNR 25751/2014, and Realization of services of the national interoperability infrastructure for the Electronic Health Record, det. AgID 61/2015.

References

1. (2016). http://www.istat.it/it/files/2015/09/Dimensioni-salute.pdf
2. (2016). http://www.en13606.org/
3. (2016). http://www.hl7.org/
4. (2016). http://hl7.org/fhir/summary.html
5. (2016). http://openehr.org/
6. (2016). http://www.ihe.net/
7. (2016). https://www.infoway-inforoute.ca/en/
8. (2016). http://sequoiaproject.org/ehealth-exchange/
9. (2016). http://www.epsos.eu/
10. (2016). http://www.cidoc-crm.org/official_release_cidoc.html
11. (2016). http://wiki.ihe.net/index.php/Cross-Enterprise_Document_Sharing
12. (2016). https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
13. Aminpour, F., Sadoughi, F., Ahamdi, M.: Utilization of open source electronic health record around the world: a systematic review. Off. J. Isfahan Univ. Med. Sci. **19**(1), 57–64 (2014)
14. Beale, T.: Archetypes: constraint-based domain models for future-proof information systems. In: OOPSLA 2002 Workshop on Behavioural Semantics, vol. 105 (2002)
15. Black, A.D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., McKinstry, B., Procter, R., Majeed, A., Sheikh, A.: The impact of ehealth on the quality and safety of health care: a systematic overview. PLOS Med. **8**(1), 1–16 (2011)
16. Cantor, S., Kemp, I.J., Philpott, N.R., Maler, E.: Assertions and protocols for the oasis security assertion markup language v2.0. OASIS Standard (2005), March 2005 http://wiki.ihe.net/index.php/Cross-Enterprise_Document_Sharing
17. Chiaravalloti, M., Ciampi, M., Pasceri, E., Sicuranza, M., De Pietro, G., Guarasci, R.: A model for realizing interoperable EHR systems in Italy. In: International HL7 Interoperability Conference Proceedings, pp. 13–22. HL7 Conference 2015 (2015). http://ihic2015.hl7cr.eu/Proceedings-web.pdf
18. Ciampi, M., Esposito, A., Guarasci, R., De Pietro, G.: Towards interoperability of EHR systems: the case of Italy. In: Proceedings of the International Conference on Information and Communication Technologies for Ageing Well and e-Health, vol. 1, pp. 133–138. ICT4AWE (2016)
19. Ciampi, M., Pietro, G., Esposito, C., Sicuranza, M., Mori, P., Gebrehiwot, A., Donzelli, P.: On securing communications among federated health information systems. In: Ortmeier, F., Daniel, P. (eds.) SAFECOMP 2012. LNCS, vol. 7613, pp. 235–246. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33675-1_21
20. Dogac, A., Laleci, G.B., Aden, T., Eichelberg, M.: Enhancing IHE XDS for federated clinical affinity domain support. IEEE Trans. Inf. Technol. Biomed. **11**(2), 213–221 (2007)

21. Commission of the European Communities, E.C: Together for health: a strategic approach for the EU 2008–2013 (2007). http://ec.europa.eu/health/ph_overview/Documents/strategy_wp_en.pdf
22. Kalra, D., Blobel, B.: Semantic interoperability of EHR systems. Stud. Health Technol. Inf. **127**, 231 (2007)
23. Lawrence, K., Sun, R.M., Nadalin, A., VeriSign, P.H.B.: Web services security: saml token profile 1.1. Terminology 5(3Usage), p. 7 (2002). https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf
24. Ludwick, D.A., Doucette, J.: Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. Int. J. Med. Inf. **78**(1), 22–31 (2009)
25. Shekelle, P., Morton, S.C., Keeler, E.B.: Costs and benefits of health information technology (2006)
26. Sicuranza, M., Esposito, A.: An access control model for easy management of patient privacy in EHR systems. In: 2013 8th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 463–470. IEEE (2013)