



RIDE

"A Roadmap for Interoperability of eHealth Systems in Support
of COM 356 with Special Emphasis on Semantic
Interoperability"

COORDINATION ACTION

PRIORITY 2.4.11 Integrated biomedical information for better health": eHealth

RIDE D4.4.1 – RIDE ROADMAP III

FINAL

Due Date: February 15, 2008 (Month 24 + 45 days of grace period)
Actual Submission Date: January 10, 2008
Project Start Date: January 01, 2006
Project End Date: December 31, 2007
Project Duration: 24 months
Leading Contractor Organization: METU-SRDC

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document History:

Version	Date	Changes	From	Review
v0.1	August 22, 2007	Initial version created	METU	METU
v0.2	August 29, 2007	Draft version of Section 3 added	METU	METU
v0.3	August 31, 2007	Section 3 completed	METU	METU
v0.4	September 10, 2007	Section 4 – Technical details added	METU	METU
v0.5	September 15, 2007	Introduction, roadmapping methodology	METU	METU
v0.6-1	September 26, 2007	Further editing	METU	All partners
v0.6-2	September 27, 2007	Minor changes, references	METU	All partners
v0.6-3	October 11, 2007	Comments from OFFIS	OFFIS	All partners
v0.6-4	November 15, 2007	Contribution from OLE on content level interoperability ('realist ontology' approach)	OLE	All partners
v0.7	November 23, 2007	Contribution from NTUA-ICCS on clinical pathways and workflows	ICCS	All partners
v0.8	November 30, 2007	Contribution from OFFIS on guidelines and decision support systems	OFFIS	All partners
v0.9	December 27, 2007	Consolidation of all contributions, comments and the section on "clinical statement interoperability"	METU	All partners
v1.0	January 3, 2008	Comments from the consortium	EuroRec	All partners
v1.1	January 8, 2008	Contribution from CNR on the strategies and patient summaries; other comments	CNR	All partners

RIDE Consortium Contacts:

N°	Organisation	Street name and number	Post Code	Town/ City	Country Code	Title	Family Name	First Name	Phone N°	Fax N°	E-Mail
1	METU-SRDC	Inonu Bulvari	06531	Ankara	Turkey	Prof. Dr.	Dogac	Asuman	+90-312-2105598	+90(312)2101004	asuman@srdc.metu.edu.tr
2	OFFIS	Escherweg 2	26121	Oldenburg	Germany	Dr.	Eichelberg	Marco	+49-441-9722-147	+49-441-9722-102	eichelberg@offis.de
3	IFOMIS	Campus Saarbrücken	66041	Saarbrücken	Germany	Prof.	Smith	Barry	+49(0)681/302-64777	+49(0)681/302-64772	phismith@buffalo.edu
4	EUROREC	co IDISS - Croix-Rouge Française route de Platon	42400	Saint Chamond	France	Prof.	DeMoor	Georges	+32-9-2403421	+32-9-2403439	georges.demoor@ugent.be
5	CNR	Piazzale Aldo Moro 7	00100	Roma	Italy	Prof.	Rossi Mori	Angelo	+39 06 86 090 250	+39 06 86 090 340	angelo@itbm.rm.cnr.it
6	NTUA, ICCS	42, Patision street	10682	Athens	Greece	Prof.	Mentzas	Gregoris	+302107723895	+302107723550	gmentzas@softlab.ntua.gr
7	NUIG, DERI	University Road	na	Galway	Ireland	Dr.	Vitvar	Tomas	+353 91 495270	+353 91 495270	tomas.vitvar@deri.org
8	IHE-D	Stresemannallee 19	60596	Frankfurt	Germany	Prof.	Wein	Berthold B.	+49-241-559 559 1	+49-241-559 558 2	wein@radiologie-aachen.de
9	OLE	Hazenakkerstraat 20a	B9520	Zonnegem (Sint-Lievens-Houtem)	Belgium	Dr.	Ceusters	Werner	+32 475 486 587	-	werner.ceusters@ecor.unisaarland.de

ACRONYMS	7
1 INTRODUCTION	8
1.1 RIDE ROADMAP METHODOLOGY	10
2 EXECUTIVE SUMMARY	12
3 REQUIREMENTS FOR ACHIEVING INTEROPERABILITY	14
3.1 THE STRATEGIES FOR THE DEPLOYMENT OF EHEALTH INTEROPERABILITY	14
3.1.1 Three Contexts: Local Integration, Operational Workflows, Shared Care.....	14
3.1.2 The Main Features of The Three Contexts.....	15
3.2 KEY ISSUES TO FACILITATE EHEALTH INTEROPERABILITY	16
3.3 ORGANIZATIONAL FRAMEWORK	17
3.3.1 Roles and Stakeholders	17
3.3.2 Governance Models	18
3.3.3 Financial Incentives and Mechanisms.....	18
3.4 POLITICAL AND LEGAL FRAMEWORK	19
3.4.1 How to improve Participation	19
3.4.1.1 Key points for Patient Participation.....	19
3.4.1.2 Key points for Healthcare Provider Participation	19
3.4.1.3 Key points for Insurer Participation.....	20
3.4.2 How to improve Competition.....	20
3.4.3 Leveraging Standards.....	20
3.4.3.1 Interoperability Dimensions for Standards	20
3.4.3.2 Collaboration in Standards Harmonization and Development.....	21
3.4.4 Privacy, Security and Legal Frameworks.....	21
3.4.4.1 Responsibilities at the National Level	22
3.4.4.2 Responsibilities at the Community Level.....	22
3.4.4.3 From Privacy Principles to Policies.....	23
3.5 ARCHITECTURAL INTEROPERABILITY	25
3.5.1 Principles.....	25
3.5.2 Strategy for Architectural Interoperability	30
3.5.3 Testing, Certification and Accreditation	32
3.6 MONITORING AND EVALUATION	32
4 TECHNICAL DETAILS	33
4.1 ARCHITECTURAL MODELS	33
4.1.1 Centralized Storage	34
4.1.2 Federated Architecture with Repositories	34
4.1.3 Federated Architecture with Locally-Held Data	34
4.1.4 Peer-to-Peer Networks	34
4.1.5 PHR Repositories	34
4.2 CONTENT INTEROPERABILITY	35
4.2.1 A Collection of Context-dependent Definitions of Patient Summaries.....	35
4.2.2 Clinical Statement Interoperability	35
4.2.3 ‘Realist Ontology’ Approach	39

4.2.4	Recommendations About Content Interoperability	42
4.3	CLINICAL PATHWAYS, GUIDELINES, DECISION SUPPORT SYSTEMS, WORKFLOWS.....	43
4.3.1	Clinical Pathways.....	43
4.3.1.1	Operational Issues on Shared Clinical Pathways	43
4.3.1.2	Trends and Motivations	43
4.3.1.3	Adaptive Clinical Pathways Approach	44
4.3.1.4	Adaptation utilizing semantic technologies	45
4.3.1.5	Example Scenario	45
4.3.2	Guidelines	46
4.3.3	Decision Support Systems.....	47
4.3.3.1	Technical Issues in the combination of Guidelines and DSS.....	47
4.3.4	Workflows.....	48
4.3.4.1	Interoperability between IT systems.....	48
4.3.4.2	Semantics required in workflow management.....	50
4.3.4.3	Example Scenario	50
4.3.5	Recommendations on clinical pathways, guidelines, DSS and workflows	50
4.4	SERVICES AND FEATURES.....	51
4.4.1	Identity Management Services	51
4.4.1.1	Patient Identification Services	51
4.4.1.2	Patient Identity Matching Services	52
4.4.1.3	User Identity Management Services	52
4.4.2	Data Services.....	53
4.4.2.1	Record Locator Services.....	53
4.4.2.2	Data Retrieval Services	54
4.4.2.3	Subscriber Services	55
4.4.2.4	Publisher Services	56
4.4.2.5	Data Routing Services	57
4.4.2.6	Transformation Services.....	58
4.4.2.7	Content Validation Services	58
4.4.2.8	Central EHR Storage Services.....	59
4.4.3	PHR Services	60
4.4.3.1	Patient Access to Clinical Information and Audit Logs.....	60
4.4.3.2	Maintaining PHR.....	61
4.4.3.3	Consent Management Services.....	62
4.4.4	Monitoring and Evaluation Services	63
4.4.4.1	Pseudonymization and Re-Identification Service	63
4.4.4.2	Providing Data for Secondary Use	64
4.4.4.3	Notification Services	65
4.4.5	Management Services	65
4.4.5.1	Registries for Participating Organizations	65
4.4.5.2	Registries for Healthcare Providers	66
4.4.6	Privacy/Security Features.....	67

RIDE D4.4.1 – RIDE ROADMAP III (Month 24)

4.4.6.1	Audit Logging	67
4.4.6.2	Person Authentication	67
4.4.6.3	System Authentication.....	67
4.4.6.4	Authorization.....	67
4.4.6.5	Data Integrity Checking.....	68
4.4.6.6	Error Handling.....	68
4.4.6.7	Secure Transport.....	68
4.4.6.8	Non-Repudiation	68
5	CONCLUSION.....	68
6	REFERENCES	70

ACRONYMS

CDA	Clinical Document Architecture
CEN	European Committee for Standardization
DSS	Decision Support System
EHN	European Health Network
EHR	Electronic Health Record
EHRcom	Electronic Healthcare Record Communications
GP	General Practitioner
HL7	Health Level Seven
ICT	Information and Communication Technology
IHE	Integrating the Healthcare Enterprise
NHN	National Health Network
PHR	Personal Health Record
RHN	Regional Health Network
SOA	Service Oriented Architecture
SWRL	Semantic Web Rule Language
WSDL	Web Services Description Language

1 INTRODUCTION

RIDE is a roadmap project for interoperability of eHealth systems leading to recommendations for actions and to preparatory actions at the European level. This roadmap aims to prepare the ground for future actions as envisioned in the action plan of the eHealth Communication COM 356 by coordinating various efforts on eHealth interoperability in member states and the associated states.

The main goal of the final RIDE Roadmap, RIDE Roadmap III, is to create a strategy complementing the principles developed in RIDE Roadmap I and the technical solutions proposed in RIDE Roadmap II. For this purpose, RIDE Roadmap III uses the knowledge and experience gained through the roadmapping process (the methodology and the roadmapping process are explained in Section 1.1 in detail). Furthermore, the common issues addressed in the Draft Recommendation of the Commission on eHealth Interoperability¹ and the RIDE Project are explicitly indicated by giving references to the Draft Recommendation on eHealth interoperability.

The Draft Recommendation of the Commission on eHealth Interoperability stresses the significance of eHealth Interoperability as follows¹:

*Although **interoperability is not a goal in itself**, since the Member States are now directing their health policies to subscribe to a paradigm of common visions, common values, and eventually common standards² with regard to health service provision throughout Europe, a definitive focus is now required on eHealth interoperability.*

RIDE Roadmap III first focuses on a high conceptual level and then concentrates on the necessary interoperability requirements in Section 3. eHealth Interoperability requirements are defined in four different categories:

1. Organizational Framework
2. Political and Legal Framework
3. Architectural Interoperability
4. Monitoring and Evaluation

Within these requirements, the possible solutions are discussed and the principles are presented for the stakeholders. These principles are then mapped to the technical interoperability framework providing the core set and the additional set of functionalities for eHealth interoperability capable of exchanging information at the European level. The technical details are presented in Section 4. This approach is also inline with the Draft Recommendation of the Commission on eHealth Interoperability:

The Commission also aims to start with a high conceptual level and shift towards technical details:

(...) the actual steps – which will be undertaken in tandem – will start at a high conceptual level, and will increasingly shift towards technical development and concrete solutions¹.

The technical details are presented with four major headings:

1. Architectural Models
2. Content Interoperability
3. Clinical Pathways, Guidelines, Decision Support Systems, Workflows
4. Services and Features

¹ Draft Recommendation of the Commission on eHealth Interoperability,
http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=369

² See for example the Health Council outcome of 30 November, 2006.

Architectural models introduce the possible types of healthcare networks such as centralized, decentralized or federated ones, and prepare the ground for involvement of all types of networks that exist in the Member States. Since establishment of a health information space at the European level is a matter of health data exchange, Content Interoperability section focuses on the data content standards. Clinical Pathways, Guidelines, Decision Support Systems, Workflows present the interoperability problems of supportive eHealth mechanisms. Finally, the Services and Features define the core set and additional set of functionalities that are recommended for EU eHealth Interoperability.

The Draft Recommendation of the Commission on eHealth Interoperability focuses on access of healthcare professionals to patient health information across Europe as its ultimate goal:

*Therefore, the ultimate goal of this Recommendation is to contribute to enabling the provision of a means of **authorised healthcare professionals to gain managed access to essential health information about patients, subject to the patients' consent, and with full regard for data privacy and security requirements**. Such information could include the appropriate parts of a patient's **electronic health record, patient summary, and emergency data** from any place in Europe: within countries, in cross-border regions, and between countries¹.*

The RIDE Roadmap shares the same major objective with the Commission's recommendation. The RIDE Roadmap also supports some secondary goals which are the by-product of eHealth interoperability such as providing data for secondary use.

The recommended functionalities for the health networks in regional, national and the European level are defined under six groups:

- Identity Management Services
- Data Services
- Personal Health Record (PHR) Services
- Monitoring and Evaluation Services
- Management Services
- Privacy/Security Features

For each of these groups:

- Use cases,
- Services involved,
- Illustrative scenarios and
- Required security/privacy features

are described within Member States and across Member States.

This roadmap pays specific attention to existing systems and services of the Member States; one principle of the roadmap is leveraging the previous collaborative work and investments of the participants. A Brief summary of the current situation in eHealth in each of the Member States are available at³.

³ <http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>

RIDE D2.1.1 - A Brief Survey of the eHealth Initiatives of Austria

RIDE D2.1.1 - Current European practices in providing interoperability in eHealth domain: KMEHR-BIS and BE-HEALTH - Belgium

RIDE D2.1.1 - Survey of Cyprus Health Care System

RIDE D2.1.1 - Survey of eHealth Practices - Czech Republic

RIDE D2.1.1 - Danish Healthcare System

RIDE D2.1.1 - Survey of NHS Connecting for Health - England

RIDE D2.1.1 - A Brief Survey of the Digital Health Record Project conducted by the Ministry of Social Affairs of Estonia

RIDE D2.1.1 - A Brief Survey of the Initiative by the German Federal Ministry of Health

RIDE D2.1.1 - Survey of eHealth Practices in Greece

The Draft Recommendation on eHealth Interoperability pays attention to existing systems and services of the Member States:

The guidelines to be developed should apply to all Member States which each have their very different health systems and services¹.

The RIDE Project produced a dedicated Legacy Integration/Modernization Strategy⁴ which concentrates on “reusing existing investments on the IT infrastructure in the Member States to achieve RIDE vision”. This strategy intends to present concrete and possible ways and practices of achieving a European eHealth Interoperability Framework with legacy eHealth applications but avoids recommending any particular technology direction. Furthermore, RIDE Deliverable D2.1.4 - European Good Practices describes the practices in Europe that are suitable for interoperability.⁵

1.1 RIDE Roadmap Methodology

Robert Galvin, former Motorola chairman and advocate of Science and Technology roadmaps, defines Roadmaps as follows [1]: “A ‘roadmap’ is an extended look at the future of a chosen field of inquiry composed from the collective knowledge and imagination of the brightest drivers of change in that field. Roadmaps communicate visions, attract resources from business and government, stimulate investigations, and monitor progress. **They become the inventory of possibilities for a particular field.**” A roadmap provides a consensus view or vision of the future Science and Technology (S&T) landscape available to decision makers. The implementability of a final Roadmap is as important as its strategic value [2].

Inline with these definitions, the RIDE Project followed a systematic roadmapping process which is visualized in Figure 1.

RIDE D2.1.1 - Current European practices in providing interoperability in eHealth domain - Hungary

RIDE D2.1.1 - Current Practices in Ireland

RIDE D2.1.1 - Current European practices in providing interoperability in eHealth domain - Latvia

RIDE D2.1.1 - Survey of HealthNet - Luxembourg

RIDE D2.1.1 - Survey of Malta Health Care System

RIDE D2.1.1 - CurrentPractices - The Netherlands

RIDE D2.1.1 - A Brief Survey of the Initiative by the Dutch National ICT Institute for Healthcare (NICTIZ)

RIDE D2.1.1 - Survey of Norway Healthcare Services

RIDE D2.1.1 - A Brief Survey of the use of ICT in the Health Sector in Poland

RIDE D2.1.1 - Current European practices in providing interoperability in eHealth domain - Portugal

RIDE D2.1.1 - Current European practices in providing interoperability in eHealth domain - Slovenia

RIDE D2.1.1 - Current European practices in providing interoperability in eHealth domain - Spain

RIDE D2.1.1 - CurrentPractices - Sweden

RIDE D2.1.1 - Survey of CARELink in Sweden

RIDE D2.1.1 - Survey of eHealth Practices - France

⁴ RIDE D4.4.5 - Integrating the Legacy eHealth Applications of the Member States into the RIDE Technical Framework, <http://www.srdc.metu.edu.tr/webpage/projects/ride/deliverables/D4.4.5-IntegratingTheLegacyEHealthApplications-v1.1.doc>

⁵ RIDE D2.1.4 - European Good Practices, <http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>

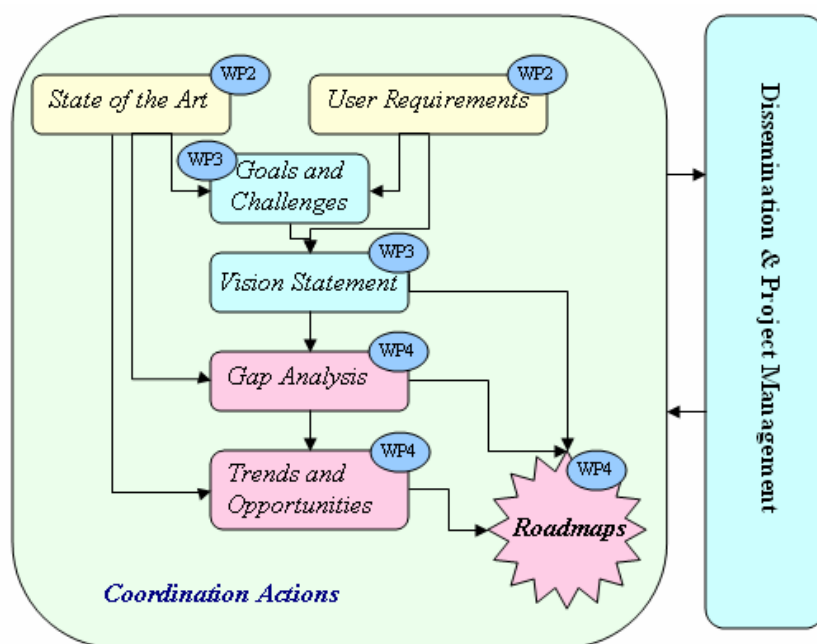


Figure 1 RIDE Roadmapping Process

First, surveys on the state-of-the-art were performed which covered standardization efforts for providing semantic interoperability in the health domain. In parallel to this, the current state of eHealth interoperability in the EU Member States as well as US and Canada were investigated. Then the interoperability requirements of applications in the eHealth domain were investigated to determine the goals and challenges, where the “State-of-the-Art” and the “Requirement Analysis” provided the necessary input. In order to visualize the goals and to see how the current requirements can be addressed in the future, a set of visionary scenarios were developed. Next, the gaps that exist between “as-is” situation and the desired future description identified in the RIDE vision statement (“to-be” situation) were identified. This was supported by a migration strategy for the legacy eHealth applications for assuring the participation of the Member States by recognizing their previous investments and preventing them from having to invest into a completely new technology. On the way to achieving the roadmap, the RIDE project also analyzed the trends and opportunities in the healthcare IT, and documented the limitations of current policies and strategies. Moreover, the RIDE Consortium presented proposals to eHealth standardization bodies.

Built upon all of this work, this iterative process involved development of three versions of the RIDE Roadmap.

The first version of the RIDE Roadmap (RIDE Roadmap I, Month 12) provided a top-down framework that describes the attitudes of ICT and Health World for connected health, an approach to come up with enactment factors from policy objectives, metrics to characterize the roadmapping activities, and a taxonomy which systematically expresses the content of a national or regional Roadmap towards eHealth in Europe. The taxonomy defines the following four main streams;

- Enabling activities on the infrastructure and to achieve basic interoperability (building the technical infrastructure, setting up proper regulatory framework, security and privacy, produce or adopt standards and reference materials to achieve semantic interoperability, setting up certification process on quality and safety of eHealth solutions)
- Vertical services to increase the efficiency of current care-related workflows
- A problem-oriented perspective, to enhance the quality and the appropriateness of care provision, plus
- The meta-level issues arising from the three main streams and supporting activities

The second version of the RIDE Roadmap (RIDE Roadmap II, Month 20) concentrated on “enabling activities on the infrastructure and to achieve basic interoperability” which is identified as first stream in the taxonomy given in the first version of the RIDE Roadmap. The goal of RIDE Roadmap II was to enumerate possible ways of rapid, accurate, and secure exchange of electronic healthcare records among authorized users which includes the patient himself. Within this version, the intention was to

provide the starting point of a technical framework necessary for creating a European Interoperability framework, however, avoiding the recommendation of a particular technology direction.

RIDE Roadmap II considered all prominent technologies and standards relevant for the Member States in achieving a European eHealth Interoperability Framework based on a Service Oriented Architecture (SOA), namely;

- IHE Integration Profiles,
- CEN/TC 251 EN 13606, and
- HL7 version 3 and the HL7 Clinical Document Architecture (CDA).

Moreover, it described how each of the necessary core Member State services (Locator Service, Patient Identification Service, Audit Services, Professional Identity Service, and Provider Identity Service) can be implemented by using the abovementioned alternative technologies. It even provided WSDL definitions of the services; for detailed technical information please refer to RIDE Roadmap II [7].

2 EXECUTIVE SUMMARY

RIDE Roadmap III is the final destination of the RIDE roadmapping process. Although RIDE Roadmap III is a self-contained document, it should be noted that it is a compilation of all the knowledge and experience gained while progressing with the RIDE roadmapping process that has been adopted by the project as a methodology. For this reason, references to the previous deliverables appear in the document. Furthermore, the common issues addressed in the Draft Recommendation of the Commission on eHealth Interoperability¹ and the RIDE Project are indicated explicitly.

Today, most of healthcare provision is local. The information exchange usually occurs in the citizen's own community. However, in order to enable a European-wide interoperable clinical data exchange, there is a need for a common underlying network providing the necessary core functionalities. Furthermore, the minimum security standards required to assure secure data exchange or patient identification mechanisms should be applied Europe-wide so that all participants interconnect with standard interfaces of the core functionalities.

For the purposes of the present deliverable, the issues on eHealth policies and the related strategies on interoperability are considered within three major contexts:

1. The long-established problem for the managers of healthcare facilities about the interoperability among the applications *within their facility* is coming across severe difficulties for the increasing scale of integration;
2. The current problem for national and regional authorities to support the transformation of operational paper-based workflows about services (e.g. booking, prescriptions, diagnostic services) at a regional scale, *across healthcare facilities*;
3. The innovation in the organizational models of the *shared care processes*, by facilitating “3C”: the Continuity of care, the Collaboration among healthcare operators and with the citizens, the Communication among them.

The interoperability issues in the three contexts involve very different challenges in the deployment of the “connected health”; the non-technological factors such as issues on regulations, economics, involvement of stakeholders, and role of public agencies to support the deployment and the research are equally relevant as well.

The issues on eHealth interoperability across heterogeneous Information Systems show an unprecedented challenge, and require new roles for the Authorities and a careful planning.

So far, healthcare informatics was mostly coping with circumscribed solutions within individual facilities. According to this approach, a technological novelty should be assessed when it is introduced by the market, to realise its optimal usage and its efficacy compared to other solutions. It should be maintained, updated and replaced when required. This is the case for most current ICT administrative solutions and successful novelties such as local EPR systems, authoritative knowledge on the web, e-booking, e-prescribing and patient summaries.

The *connected health* requires a different, complementary approach. It stems from new organisational models for an economically sustainable evolution of healthcare, such as chronic disease management, patient empowerment and clinical governance. The innovation of healthcare processes and governance will benefit from methodological and practical support in the management of the information content. Connected Health should be anticipated by a cultural and organisational change that requires Continuity, Collaboration and Communication among actors, facilitated by innovators working closely with healthcare professionals and managers.

Connected Health should support the synchronisation of activities across facilities – especially when clinical pathways involve primary care, hospitals and social care – according to a mutual recognition of responsibilities and a natural coherence of objectives and plans.

The initial idea of longitudinal EHR produced a bias towards the clinical issues and interoperability of systems, versus the organisational and managerial needs. These latter require new methods and tools to support the 3C's across facilities and to control the overall behaviour of the system – especially on long-term conditions with a relevant role of patients and informal carers.

Almost all member states either have developed or are developing their National Health Networks [5]. Sometimes these national networks are composed of smaller Regional or Organizational Health Networks. These networks should be linked by directories of identifying information pointing to the sources of records, which could be achieved by means of Record Locator Services (details are presented in Section 4). This way, the data will stay where they are created (privacy aspect) and the existing infrastructure of participants will be leveraged.

RIDE Roadmap III first focuses on a high conceptual level and then concentrates on the necessary interoperability requirements in Section 3. eHealth Interoperability requirements are defined in four different categories:

1. Organizational Framework
2. Political and Legal Framework
3. Architectural Interoperability
4. Monitoring and Evaluation

Among all the requirements for achieving interoperability of eHealth systems at the European level, architectural interoperability plays an important role since it provides the basis for the success of others. The aim is to promote the use of standards and the establishment of common communication platforms as indicated by the European Commission in the Draft Recommendation of the Commission on eHealth Interoperability.

In order to achieve the interoperability of eHealth systems at the European level, it is advised that the European Health Network is built on a set of architectural principles that could favour the integration of existing/evolving national health networks and new developments. In this regard, twenty principles focusing on the architectural interoperability are defined in the roadmap. Development of eHealth Network and its standards cannot ignore the previous efforts in the Member States, by standardization bodies, European Commission (the eHealth projects supported by the Commission) and the industry groups. There is no need to start from scratch.

It is advised that only the minimum number of protocols and functionalities essential to widespread exchange of health information are specified as part of the European Health Network (EHN). The EHN should provide for a real-time, secure and voluntary health information exchange for all parties, and should consist of a minimum set of standards and a minimum set of core services, such as the Patient Identification Service (the details of services are presented in Section 4). It is worthwhile to leave to the local (regional or national) systems those things best handled locally. The deployment of the EHN can start with core services and can accommodate a modular structure for the possible future services of clinical data exchange and use. This could be considered as a **“plug-in”** based infrastructure.

Moreover, the development of EHN should avoid the **“rip and replace”** strategy. It should recognize the previous investments of the member states which could be local, regional and national developments and/or eHealth strategies; i.e. the current state-of-the art in general. This is also critical for assuring the participation of the member states since it will prevent them from having to invest into a completely new technology. RIDE “Deliverable 4.4.5 - Integrating the Legacy eHealth Applications of the Member States into the RIDE Technical Framework” presents an integration and migration strategy so as to protect existing investments on IT frameworks in the European Union.

It is also advised that the EHN is based on open industry standards for messages and design so that all interested parties can participate on an even basis. All information flowing over the network must adhere to standard interfaces. A by-product of such effort might be the acceptance of common interfaces all over the EU.

Establishment of a Europe-wide health information exchange infrastructure is not a breathing time activity. An incremental process is essential for the deployment, where growing (in physical coverage) and evolving (increasing functionality) pilots are being developed. However, these pilots should not be implemented locally. Participation of at least two Member States in a pilot activity is essential. In each step, the implemented functionalities should be fully tested so that the rest is built upon strong pillars. The knowledge and experience gained by the participating organizations should be exploited to the service of newly participating organizations or member states.

Business level use cases are very useful tools to define the scope of an interoperability problem and to understand and to describe the functionalities and capabilities of a system on a more abstract level. The RIDE Project has taken this approach and in RIDE Deliverable D2.3.1 Requirements Analysis for the RIDE Roadmap⁶, all the use cases related with eHealth interoperability have been described.

3 REQUIREMENTS FOR ACHIEVING INTEROPERABILITY

3.1 The Strategies for The Deployment of eHealth Interoperability

First of all, the major features of the change management process, i.e. of the programs for the deployment of eHealth, must be understood.

The introduction of ICT in the healthcare sector started in the '70s as a spontaneous activity within each facility. Nowadays the authorities are intervening heavily to coordinate, regulate, finance pilot projects, and deploy large scale infrastructures.

Most of the EU Member States have a strategic Roadmap on the deployment of eHealth. Several Member States have a "Competence Centre", or an Agency, or a policy office at the Ministerial level.

The attention of the authorities to the deployment of eHealth is a reality all around the world, and there are many commonalities, independently of how the health services are organized, i.e. both in countries with a prevalent public ("universal") health system (e.g. in UK), and in countries with a prevalent private insurance-based system (e.g. in USA).

The major features of this phenomenon are described in the proceeding sections.

3.1.1 Three Contexts: Local Integration, Operational Workflows, Shared Care

For the purposes of the present deliverable, the issues on eHealth policies and the related strategies on interoperability are described within three major contexts:

1. The long-established problem for the managers of healthcare facilities about the interoperability among the applications *within their facility*⁷, that is being faced by standardization bodies since more than 15 years, and is coming across severe difficulties for the increasing scale of integration;
2. The current problem for national and regional authorities to support the transformation of operational paper-based workflows about services (e.g. booking, prescriptions, diagnostic services) at a regional scale, *across healthcare facilities*. This context involves the extension of the interoperability to large jurisdictions. This context is aiming at improving the efficiency of the healthcare system, and involves administrative activities and care activities with "subordinate responsibilities";
3. The innovation in the organizational models of the *shared care processes*, by facilitating "3C": the Continuity of care, the Collaboration among healthcare operators and with the citizens, the

⁶ RIDE Deliverable D2.3.1 Requirements Analysis for the RIDE Roadmap,
<http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>

⁷ Include also the typical workflows for administrative and surveillance purposes (e.g. for reimbursement, notification of infectious diseases).

Communication among them⁸. This context aims at supporting the clinical decisions of healthcare professionals and the behaviour of citizens about their life style and compliance to therapy (patient empowerment). It involves clinical activities with “parallel responsibilities”.

The interoperability issues in the three contexts involve very different challenges in the deployment of the “connected health”; equally relevant are the non-technological factors, i.e. issues on regulations, education, economics, involvement of stakeholders, and role of public agencies to support the deployment and the research.

3.1.2 The Main Features of The Three Contexts

The deployment strategies for each context involve different actors, different business models, and a different distribution of benefits. The size and the complexity of the intervention is also very different, as well as the cultural and organizational impact.

The task of the authorities is to produce a balanced eHealth policy and the related strategies to support in a coherent manner the three contexts.

The **first context**, made of independent micro-strategies within each facility (or a coherent set of facilities, e.g. belonging to the same care provision organization), requires the spontaneous adoption of implementation guides for the most relevant workflows, e.g. as the ones produced and tested by the IHE initiative.

The introduction of ICT was gradually managed so far within each facility, when the leadership, the users and the context was considered ready for each new step; the overall benefit was also local, with advantages and disadvantages at level of individuals within the scope of the facility.

The other contexts create nowadays a pressure to satisfy the ability to take part in more complex programs.

The **second context** involves specific operational tasks for *all* the facilities of certain categories in the jurisdiction, e.g. to send/receive prescriptions or laboratory test results.

The policies are inspired by the technological opportunities and have some impact on risk management. The increase of the efficiency and the timeliness of the workflows brings a clear benefit to each involved facility, and there is a perceived organizational benefit for the patient; a strong leadership and a simultaneous training of a large number of users are needed; specific ICT applications must be in place in all the facilities; an exchange infrastructure must be in place, with appropriate security measures.

After some pioneering activities in some member states (e.g. in Denmark, Belgium, Sweden), in most European Member States, the authorities are taking a proactive role on this context:

- to coordinate the efforts (e.g. by a Policy Team in the Ministry of Health, an Office for the National Coordinator, a Competence Centre, a governmental agency),
- to adopt suitable regulations and standards,
- to achieve the deployment of an infrastructural backbone (e.g. healthcare cards, security measures, registries of citizens, professionals and facilities), and the production of an infostructure (e.g. reference care pathways, task-specific clinical datasets and structured content of clinical documents, reference nomenclatures), and
- to promote a set of coherent pilot projects, the transfer of the know-how and research programs.

The **third context** requires a more deep involvement of the authorities, the healthcare professionals and the citizens in the design of the innovative organizational models and in the change management.

⁸ EHTEL and the CNR-ITB, with the support of the RIDE Project, organized an International Conference on “3C - Continuity, Collaboration, Communication: challenges for healthcare, opportunities for eHealth” (Rome, 24-25 May 2007), in collaboration with the Standing Committee of European Doctors (CPME), the Pharmaceutical Group of the European Union (PGEU), the European Hospital and Healthcare Federation (HOPE), the European Federation of Nurses Associations (EFN), and the European Union of Medical Specialists (UEMS).

It is a really innovative and unexplored field, and it shows several issues that require specific research activities.

The stress is in the management of the clinical Information and Communication assisted by Technology, that is represented here through the modified acronym IC(T). The eHealth policies are inspired by health priorities, e.g. prevention of the consequences of chronic diseases (disease management), prevention of cancer and coordination of elderly care.

The deployment of eHealth programmes involves simultaneously the professional skills of the users in the whole jurisdiction; in successful programs, there is a shift of workload from certain facilities to other ones (e.g. from hospital to territory) with evident clinical benefits for the patients; a very strong leadership and a simultaneous endorsement of a large number of professionals are needed; local Electronic Patient Record applications must be in place in all the facilities; an infrastructure for sharing clinical documents must be in place.

3.2 Key Issues to Facilitate eHealth Interoperability

Before analysing the strategies and policies needed to realize the vision of EU wide e-Health interoperability, the key facilitators for this mission should be identified. The following list identifies a series of key facilitators:

- A strong political will to achieve the vision and a central leadership by the European Commission to coordinate it
- Agree on the minimum requirements for the legal framework allowing for interoperability
- Agree on and create the basic privacy, security, authentication, and traceability framework allowing for interoperability
- Agree on the common principles concerning identification of patients, health professionals, and health institutions.
- Agree on standard interfaces for exchanging data as well as on reference clinical pathways, data sets and coding schemes (i.e. the Infostructure)
- Determine the how the proposed interoperability will be tested and certified
- Ensure the required funding for coordination and pilot applications
- Follow a “use case” based approach and agree on use cases to be developed

In addition to identifying the key facilitators, it is essential to recognize key barriers that must be overcome. Such barriers have already been identified in⁹ for USA. In the EU case, major barriers include the following:

- *Clinician Adoption:* In some Member States, clinicians and healthcare organizations currently rely on paper records to provide clinical care. The adoption of EHRs by clinicians in the EU is still not at the expected level. There seems to be a need for incentives to ensure clinician adoption of EHR systems.
- *Finance:* In order to assure a broad participation of diverse stakeholders into the process of providing e-Health interoperability and connectivity in Europe, there should be incentives for stakeholders to invest jointly for this purpose. There is a need for considerable investment required by providers, particularly physicians and hospitals, in order to transform the health care system from a paper-based system to a digital system. However, actual benefit from these investments is not shared in balance between the governments, insurers, and other stakeholders. Consequently, the EU needs an investment strategy that addresses this value imbalance and aligns the actual benefit and return on investment realization.
- *Consumer Demand:* European citizens do not sufficiently involve themselves in making decisions about their own health. As a result, there is little demand from the public for quality, performance and cost information. With the transition from paper-based to digital information,

⁹ Development and Adoption of A National Health Information Network, Response to ONCHIT's RFI

tools that enable citizens to make better and more cost-effective decisions about their own health care must be provided.

3.3 Organizational Framework

An organizational framework is necessary both on national and on European level, in order to construct a stable basis for EU-wide eHealth interoperability.

The Draft Recommendation of the Commission on eHealth Interoperability¹ also puts special emphasis on the organizational framework:

To agree on an organisational framework for interoperability that recognises the autonomy of each Member State in what concerns the development of the relevant eHealth infrastructure and services, but creates a common domain with the necessary interfaces to enable the national domains to interact.

Before describing the organizational framework, the kinds of entities and stakeholders that could compose the framework are described.

3.3.1 Roles and Stakeholders

In order to create and maintain EU wide eHealth interoperability, a wide range of constituents are required to contribute into the process. The following lists the primary stakeholder groups, both private and public and their importance in eHealth interoperability activities at the national and the European level:

- **Healthcare Consumers:** This is a key constituent group that should be convinced that a European and nationwide health network is a positive program to improve health care for all citizens. Therefore, a fundamental goal of the Member States should be to increase the involvement of citizens as informed consumers of health care services. It is a fact that participation will increase with improved access to their health care data. Furthermore, patients are playing a far greater role in the capture and verification of the data for which they are the ultimate source such as demographic data, family history, allergies, and the symptoms and other characteristics of their medical problems. Therefore, consumer participation is very important and it depends on patients trusting the system to not misuse their data and to provide access for the organizations involved in their care.
- **Healthcare Professionals:** A healthcare professional is a person who delivers health care professionally to any individual in need of health care services. Healthcare professionals will be the primary users of a National or European Health Network. The quality and efficiency of care delivery will be significantly enhanced by their ability to access complete and accurate patient information.
- **Healthcare Providers:** A healthcare provider is an organization such as a hospital, a primary care centre, a laboratory, etc., which delivers health care professionally to any individual in need of health care services. Healthcare providers are primary data sources for a National or European Health Network. Incentives may be needed to increase their involvement.
- **Insurers:** Insurers/payers are the constituents who benefit significantly from health connectivity networks. By providing citizens and providers with useable clinical information, health care quality will improve and health care costs may decrease. Because of the possible substantial cost savings that will occur through the intelligent use of health care information technology, the insurers need to contribute to the e-Health interoperability activities both in National and European level.
- **Governments:** In many Member States, the governments are also the major constituents for National Health Networks with their subgroups (public health service providers, agencies for quality of care analysis, public hospitals, university research) that have an interest in eHealth services.
- **European Commission:** The European Commission needs to play a leadership role in European-wide e-Health interoperability activities. The Commission is in the best position to

play a conciliatory and integrative role among industry, standard development organizations and governments.

- *Health IT Vendors:* The contributions of vendors of health care information technology applications and services to eHealth interoperability are very high since they invest in the development of business models and products that support improved data access. In order to assure vendor adoption, the industry should be involved in the process.

3.3.2 Governance Models

There are three governance models to control e-Health interoperability activities and particularly to achieve a National Health Network for a Member State. The following lists the roles and responsibilities of various stakeholders in each of the three models:

- *Government Leading:* In this approach, the government is the principal decision maker governing the National Healthcare Network in a centralized, top-down manner. Other stakeholders could play consultant or advisory roles. In this model, the government is responsible for all aspects of governing, financing, and setting standards and policies including developing, operating, and maintaining a National Healthcare Network to facilitate a nationwide consensus.
- *Federation of Regional or Local Communities:* Many member states like Italy, Austria, and Spain have regional governmental bodies which also govern the health in their region. Rather than using a centralized, top-down approach, such Member States may use a bottom-up governance approach through regional organizations. In this model, community-based health information exchange efforts are coupled with the overall National Healthcare Network governance process. There are several challenges for the regional governance model including high variability in infrastructure development and the (possibly inconsistent) use of standards.
- *Public-Private Collaborative Entities:* In this model, a new public-private collaborative entity, comprised of public and private stakeholders, including physicians and other providers, federal and state government, payers, industry vendors and associations, regional governance bodies, public health, and consumer privacy and patient advocate representatives, could be created to supervise, finance, develop, set policies and standards for, and deploy a National Healthcare Network.

3.3.3 Financial Incentives and Mechanisms

Sustainable evolution of healthcare is a major challenge for most Member States. The extreme fragmentation of care provision, the increase of elderly people, the diffusion of expensive medical devices require the introduction of new organisational models (e.g. chronic disease management, patient empowerment) and thus a strong involvement by the authorities to support the deployment of effective modernisation programs.

The organisational innovation is a must, and will imply a technological innovation through ICT. The basic interoperability infrastructure should be complemented by the set up of a suitable infrastructure. The investments needed for the change management in the healthcare provision will imply also a relatively modest investment in eHealth infrastructure.

In the meanwhile, governance bodies may also decide on funding mechanisms and financial incentives for e-Health interoperability which requires eHealth networks. These mechanisms may include grants, loans, refundable taxes for physicians to support electronic health data sharing, user fees, and reimbursement differentials¹⁰. Loan programs may be used as key business and governance mechanism to build a National Healthcare Network. Loans can be used by Regional Healthcare Organizations to build smaller networks (building blocks) for National Healthcare Network, by industry vendors to build products based on specified standards and to build test beds to test these products. Another funding mechanism can be user fees collected through for transactions, subscriptions or other methods. In this way, the user of the information will bear the financial burden of maintaining the

¹⁰ Summary of Nationwide Health Information Network (NHIN) Request for Information (RFI) Responses, U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology

National Healthcare Network. The following user fee methods can be used to fund National Healthcare Network operations and maintenance:

- Subscription fee paid by regional or local organizations for disease management or payment by research projects e.g. to obtain de-identified information for their research.
- User fee for individual providers based on subscription or transactions that retrieve information from other organizations.
- User fee for patients who are able to review, contribute to, and amend their records and see who has accessed their information by means of some utility (e.g. PHR).
- Subscription fee paid by insurers.

Certification fee paid by vendors for product certification for compliance to standards specified for eHealth interoperability.

Financial incentives are another critical component in the development of a sustainable business model for a National Healthcare Network. Since the health care market has not widely adopted interoperability to date, incentives are required not only to advance adoption, but also to set a foundation for health care payment based on quality of care. Amongst these incentives; pay for use and pay for performance programs are very important.

3.4 Political and Legal Framework

3.4.1 How to improve Participation

In order to realize the vision of e-Health interoperability and connectivity in the Member States and on the Europe-wide level, vendors must adapt their products, providers and payers must evolve their processes, and patients must increase their participation in parallel tracks.

3.4.1.1 Key points for Patient Participation

A fundamental strategy for the Member States and Europe should be to increase the involvement of citizens as informed consumers of health care services. The only way to improve patient participation is to improve access and control over their health care data. On the other hand, participation also depends on patients trusting that their data will not be misused and national or European e-Health connectivity networks make their data available only to authorized organizations or individual healthcare professionals involved in their care. Patients should also recognize that the data they control is important for their individual care, for public health agencies, and for the research on new treatments. In conclusion, in order to attract patient participation, there is a need for Member States to improve their regulatory frameworks by mapping the privacy policies to the technology which will provide highly secure access and control to assure citizens that their data will not be misused. Furthermore, governments should realize strategies and policies to increase the availability of easy to use applications that can be used by patients to view their data.

Finally, in order to increase the informed participation of the patients and to address their concerns in a face-to-face manner, it is recommended that education and training are organized in public environments, including on the Internet.

3.4.1.2 Key points for Healthcare Provider Participation

The value of eHealth interoperability to governments and stakeholders depends on the participation of providers to achieve a critical mass. One of the fundamental challenges facing healthcare provider organizations to participate in regional, national or European-wide e-Health networks is a lack of computerized storage of the patient records they maintain. Other organizations have computerized the management of some patient data; however, data is used for internal business needs rather than in support for a longitudinal record. The few organizations with full EHR systems seldom have the capacity to support external access to their data. This type of organizations will participate more effectively if they share a common interface standard.

3.4.1.3 Key points for Insurer Participation

The development of secure healthcare networks could also help insurers to collaborate more effectively with providers to improve efficiency and establish care standards. Member States can attract insurer participation by providing incentives for performance improvement. For instance, this can include incentives for the delivery of disease management services to better care for the chronically ill. They should also heavily address reimbursement issues while designing their national healthcare network.

3.4.2 How to improve Competition

Providing EHR interoperability will encourage private sector competition. Currently, vendor products manage patient information within the boundaries of an enterprise. The exchange of EHR data across Member States, whether it is the emergency data set or the patient summary data, will require exposing this data through standard interfaces so that they can be shared. This will generate a significant demand for adapters to wrap existing legacy applications to expose EHR data as services according to clearly defined interface standards.

Having such common interface specifications (a more unified eHealth market) will guarantee safe investment through economies of scale and hence will attract more vendor participation including SMEs which can specialize in developing wrappers for certain applications conforming to the standard interfaces. It will also mean safer investment for governments; through the standard interfaces defined they not only can share across Member States but also nationally if they wish. Through standard interfaces, interoperability will be maintained while permitting vendor differentiation.

3.4.3 Leveraging Standards

The adoption of interface standards by industry regarding the exchange of patient health information is a key factor driving eHealth interoperability in Europe. Up until now, many vendors have provided closed, proprietary systems which cause industry fragmentation and complicate the interoperability problem. Although some gaps remain, most standards required to achieve European-wide e-Health interoperability already exist. In this section, we discuss how to achieve interoperability through the use of standards and the roles of Governments and Standard Development Organizations in the long road for a widespread adoption of standards.

3.4.3.1 Interoperability Dimensions for Standards

Some of the main concepts for e-Health interoperability are: medical terminologies, message and content standards, communication protocols together with their security and privacy requirements as classified in¹⁰. In the light of these concepts, standards for e-Health interoperability can be classified into four major groups:

- *Terminology/Coding Standards:* Terminology/Coding standards are used to describe medical concepts using controlled terminology and coding schemes. These standards are essential for data interoperability. These sets of standards would be the bridge between custom implementations of other standards, where translations to or from the master set would facilitate health information exchange among health applications.
- *Message and EHR Standards:* To be able to exchange information among heterogeneous healthcare information systems, messaging interfaces (also called interface engines) are used. Typically, a messaging interface gathers data from the back-end application systems, encodes the data into a message, and transmits the data over a network to another application. On the receiver side, the received messages are decoded, processed and the data which have been received are fed into the receiver's back-end systems to be stored and processed. When proprietary formats are used in messaging, the number of the interfaces to be developed increases drastically. Therefore, standard interfaces are used. Currently, the Health Level 7 (HL7) Version 2 Messaging Standard is the most widely implemented message interface standard in the healthcare domain. However, being HL7 Version 2 compliant does not imply direct interoperability between healthcare systems. This stems from the fact that Version 2 messages have no explicit information model, but rather vague definitions for many data fields and contain many optional fields. This optionality provides great flexibility, but

necessitates detailed bilateral agreements among the healthcare systems to achieve a kind of interoperability. To remedy this problem, HL7 Version 3 is being developed, which is based on an object-oriented data model, called the Reference Information Model (RIM).

Currently, EHR information is stored in all kinds of proprietary formats in a multitude of medical information systems available on the market. A number of interface standardization efforts are progressing to provide the interoperability of electronic healthcare records such as CEN/TC 251 EN 13606 EHRcom, openEHR and HL7 Clinical Document Architecture (CDA).

- *Privacy and Security Standards:* These standards define how to enable secure transactions, provide data protection and protect privacy.
- *Network Communication Standards:* Once data is represented in a standard format for semantic and syntactic interoperability, these types of standards are also necessary to provide a way for data to be transmitted between the various endpoints. Web services and service-oriented architectures (SOA) are current industry trends in this field.

3.4.3.2 Collaboration in Standards Harmonization and Development

A number of standards are needed to provide interoperability of messages, EHRs, network communication and privacy and security. Having more than one standard for the same purpose, however, does *not* help with interoperability. In this respect, the good news is a new joint initiative among the three important Standard Development Organizations in the eHealth area, CEN/TC 251, ISO/TC 215, and HL7, for coordination and collaboration of health informatics standard development. “The purpose of *Joint Initiative on SDO Global Health Informatics Standardization* is to enable common, timely health informatics standard by addressing and resolving issues of gaps, overlaps, and counterproductive standardization efforts through”:

- “A mutually agreed upon and used decision process for international standardization needs”
- “Coordinated standards, strategies and plans, with the future goal of making all standards available through ISO”
- “An integrated work program”
- “Focused, specific resolution of overlapping and counteracting standards within the participating SDOs existing work programs”

3.4.4 Privacy, Security and Legal Frameworks

Privacy and security should be viewed as fundamental business and technical requirements of any Healthcare Network in developing the architecture, data access and control policies, business rules and governance models, and not viewed as constraints or trade-off elements. Major privacy considerations for eHealth interoperability whether it is regional, national, or European-wide include the following:

- *Patient Identification:* Patient Identification is the leading privacy concern for which two alternative solutions exist. One of them is using national patient identifiers, but the risk of accidental and intentional privacy and security breaches is heightened with the existence of a national patient identifier. Furthermore, from a technical perspective, a national patient identifier is not necessary, as there are combinations of matching (“record linkage”) algorithms, neural networks, and/or heuristic methods that can accurately identify patients without a national identifier. On the other hand, there are also concerns about using algorithmic patient identifiers instead of a national patient identifier since the management of false positive identifications (i.e., where the wrong patient record is provided) and false negatives (i.e., where the patient’s record exists, but is not found) could be extensive and difficult to manage.
- *Record Ownership:* Although the EU directive on data protection states that patients should own their health record, it should be determined who maintains it, what constitutes it, and which medical providers or payers should have access to the record in whole or in part.
- *Patient Consents:* When sharing private data about a patient, it is important that the patient should be able to determine the access rights and privacy requirements for the shared data. However, there are some technical and regulatory difficulties in integrating patient consent into

privacy infrastructure, propagating the consents across the network and managing them, obtaining consents for new data, representing consents and mapping them into machine readable policies.

- *Role-based Access:* Role-based access mechanisms would allow patients to grant permission to classes of providers at a given institution to view certain portions of their records while screening information from other users.
- *User authentication:* User authentication is *the* key issue that should be handled before any privacy measure. Various forms of authentication may be required before a user could view, change, or add data to specific patient records.
- *Lack of User Knowledge:* Users (healthcare providers and patients themselves) should be educated about the sensitivity of information, and the exact effect and meaning of privacy rules.
- *De-identified data:* De-identified data are very useful for public health and clinical research. Therefore, the mechanisms to de-identify and re-identify data should be developed.

Privacy safeguards for an interoperable European Healthcare Network must be analyzed and implemented at three different levels: European, National, and Community. While a set of minimum privacy standards will have to be established at the European level to satisfy basic requirements, additional privacy protections, particularly in the area of patient consent, will have to be developed nationally or regionally to assure compliance with the diverse Member State confidentiality laws.

3.4.4.1 Responsibilities at the National Level

The following actions are proposed at the national level in relation to privacy and security:

- Develop policies that ensure patient access to their health information and to review an audit trail of who accessed their records.
- Establish policies enabling a hierarchical authorization structure to meet different requirements. In this structure, the first thing to be done could be determining the categories of information for which different authorizations may be permitted (e.g., sensitive health information, mental health information, psychological health information; infectious diseases; medications; emergency medicine information; continuity of care information, etc). In the second tier, users could be categorized for which different levels of access may be authorized. The combination of user privileges and data restrictions would then determine access.
- Determine mechanisms and standards how patients can be fully informed about providers' use of data before their information is exchanged through the network.
- Establish policies mandating that the written notice given to patients contain certain disclosures about how information is used and exchanged through the National or European Healthcare Network.
- Establish policies and mechanisms that enable patients to decline to have their information exchanged through regional, national or European level.
- Ensure that there exists a National level directory of all providers in the Nation. Each provider should have a unique identifier in this directory.
- Develop federated identity management architecture for the network.

3.4.4.2 Responsibilities at the Community Level

The third level of privacy management for the European Healthcare Network will be local. At this level, regional healthcare networks (a number of connected healthcare institutes) in the Member States will play a critical role. These relatively small connected networks can serve as the "trusted entity" that establishes confidence among data users, consumers and the general public in the privacy and security of the information exchanged through the National Healthcare Networks. Furthermore, Regional Healthcare Networks can receive the responsibility of managing and enforcing the national level privacy activities and policies in their own region.

Moreover, under the Community Level, the following roles of stakeholders can be analyzed.

- Physicians and other health care providers could educate and inform patients of authorization rights and responsibilities at the point of care.
- Public health entities could contribute to the policy development process regarding different privacy scenarios in public health.
- Vendors of EHR and PHR systems could provide the functionalities that enable patients' electronic access, allow for interoperability between EHR and PHR systems, and enable Role Base Access Control over different types of medical data.
- Standards development organizations could develop the necessary patient oriented vocabularies for data and role categories and standards for PHR systems.

3.4.4.3 From Privacy Principles to Policies

The Organization for Economic Co-operation and Development (OECD) has determined eight privacy principles in its privacy guidelines [4]. The European Union has adopted many of these principles and in particular, they were codified in the European Union's Directive on Protection of Personal Data, implemented in 1995. In this section, we briefly describe these principles and how necessary policies can be deducted from these principles and then how these policies can be mapped to the use of technology. With this methodology, these principles could be used as main points for legal directives and regulatory frameworks.

The followings are the eight principles that the OECD defined in its privacy guidelines:

a) Collection Limitation: *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

The main point for this principle is that the patient should be able to restrict the collection of his/her medical data according to the purpose of collection. Therefore, there is a need for a policy which defines possible collection purposes. The policy should be easily understood by patients since patients may give reference to these collection purposes in their consents.

b) Data quality principle: *Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.*

The quality of health care depends on the existence of accurate health information. Consequently, the following policies or procedures should be developed in order to cover this principle:

- Policies to ensure accuracy, consistency, and completeness of data.
- Policies that enable patients to check their information and request corrections for any error
- Policies that enable patients to control data use and to correct any misuse of data
- Policies that define liabilities of health care providers, organizations, system owners in the case of any unexpected behaviour (e.g. loss of data, incomplete data, security breaches, etc) or health information made unavailable by the patient.

For this principle, backup systems and integrity checking systems can be used to ensure quality, accuracy and availability. There is also need for services to enable patients to access and review his/her records.

c) Purpose specification: *The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

This principle which can also be called "minimization" states that data use must be limited to the amount necessary to accomplish specified purposes. Data can be collected for one legitimate reason and then reused for different or unauthorized purposes. Minimization will reduce this type of privacy violations. The following policies should be developed in order to cover this principle:

- Policies which define acceptable uses of systems.
- Policies that states data collected for one purpose shall not be used for another.

Audit systems can detect unauthorized uses of data so can partially ensure 'purpose specification' principle. Standards for expressing purpose of uses are also needed to provide interoperability.

d) Use limitation principle: *Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 928 except: (a) with the consent of the data subject; or (b) by the authority of law.*

The 'Use Limitation' principle complements the 'Purpose Specification' principle by stating that the use of health information should be limited to those purposes specified by the data recipient. The following policies and procedures should be developed in order to cover this principle:

- Policies defining separate use agreements for different categories of users (e.g., disclosure to health care providers for purposes of treatment, disclosure to health plans for payment).
- Policies specifying the special type of data which are not allowed to be shared because of special sensitivity (e.g., alcohol/drug abuse history, psychiatric treatment).
- Policies defining the authorization and patient consent procedures.

On the technology side, mechanisms that will ensure security to prevent unintended disclosures, mechanisms that can filter responses to queries, and auditing systems are required.

e) Security safeguards principle: *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.*

In order to prevent data loss, corruption and modification, security safeguards are required for each system. Networked environments will be particularly susceptible without adequate security controls. Various technical security precautions such as identity management tools, auditing, authenticating, and other security tools can strengthen information privacy. Security policies are required for each type of system which defines the responsibilities of users and appropriate measures to maintain the security.

f) Openness principle: *There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.*

One of the key issues in privacy is the openness about developments, policies, and technology with respect to the treatment of personal health data. Patients should be able to understand what information exists about them, how that information is used, and their rights and control over that information. This will increase confidence in individuals with regard to data privacy and increase participation in health data networks. In order to provide openness, each system should provide adequate proper notice of privacy practices.

g) Individual participation principle: *Individuals should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; (b) to have communicated to them, data relating to them 1) within a reasonable time; 2) at a charge, if any, that is not excessive; 3) in a reasonable manner; and 4) in a form that is readily intelligible; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to them and, if the challenge is successful, to have the data erased; rectified, completed, or amended.*

European directives also state that every individual should have the right to request and receive information regarding who has that individual's health data and what specific data the party has, to know any reason for a denial of such request, and to challenge or amend any personal information. Individuals have a vital interest in their own personal health information so such rights increase their participation which will then promote data quality, privacy, and confidence in privacy practices. The following policies and procedures should be developed in order to cover this principle:

- Procedures defining the way of patient access to information when information is maintained by provider or third party vendor (e.g. PHR systems).
- Policies which define patient's responsibilities for consent prior to sharing data.
- Policies defining meaningful and privacy rules and clauses that provide granular and role based access control

h) Accountability principle: *A data controller should be accountable for complying with measures which give effect to the principles stated above.*

Monitoring the user actions in the system and holding the logs for accountability will have a great effect on privacy. Accountability tools can help to identify and address privacy violations and security breaches by holding accountable those who violate privacy requirements.

3.5 Architectural Interoperability

Among all the requirements for achieving interoperability of eHealth systems at the European level, architectural interoperability plays an important role since it provides the basis for the success of others. The aim is to promote the use of standards and architectures, and the establishment of common communication platforms as dictated by the European Commission in the Draft Recommendation of the Commission on eHealth Interoperability.

3.5.1 Principles

In order to achieve the interoperability of eHealth systems at the European level, it is advised that the European Health Network is built on a set of architectural principles that could favour the integration of existing/evolving national health networks and new developments. In this regard, twenty principles concentrating on the architectural interoperability are defined after exhaustive survey of the ongoing efforts:

a) Leverage previous collaborative work and investments of participants: Development of a European eHealth Network and its standards cannot ignore the previous efforts in the Member States, by standardization bodies, European Commission (the eHealth projects supported by the Commission) and the industry groups. There is no need to start from scratch.

Moreover, it is advised that the development of EHN avoids a “**rip and replace**” strategy. It should recognize the previous investments of the member states which could be local, regional and national developments and/or eHealth strategies; i.e. current state-of-the art in general. This is also critical for assuring the participation of the member states since it will prevent them from investing into a completely new technology.

Thus, the requirements of economic sustainability and practicality demand a clear migration path for all participants in the health information architecture. Any proposed migration path must take into account the current structure of the healthcare systems in member states, and with minimum replacement where necessary. The RIDE Project has made considerable progress related with these issues. “Deliverable 2.1.4 – European Good Practices” presents the state-of-the-art roadmaps, infrastructures, applications of member states and gives clue about their future perspectives. “Deliverable 4.4.5 - Integrating the Legacy eHealth Applications of the Member States into the RIDE Technical Framework” presents an integration and migration strategy so as to protect existing investments on IT frameworks in the European Union and adapt them to the envisioned “RIDE network”.

This approach is inline with the Draft Recommendation of the Commission on eHealth Interoperability, actions for architectural and technical interoperability:

Member States. *Undertake a comprehensive survey of existing technical infrastructures that support health systems and services throughout the European Union. Identify the providers (including the companies involved) of these eHealth systems and services solutions.¹*

Currently, vendor products manage patient information within the boundaries of an enterprise. The exchange of EHR data across Member States, whether it is the emergency data set or the patient summary data, requires exposing this data through standard interfaces so that they can be shared. This will generate a significant demand for adapters to wrap existing legacy applications to expose EHR data as services according to clearly defined interface standards.

Having such common interface specifications (a more unified eHealth market) will guarantee safe investment through economies of scale and hence will attract more vendor participation including SMEs which can specialize in developing wrappers for certain applications conforming to the standard interfaces. It will also mean safer investment for governments; through the standard interfaces defined

they not only can share across Member States but also nationally if they wish. Through standard interfaces, interoperability could be maintained while permitting vendor differentiation.

b) Top-down and bottom-up design: It is advised that the design and implementation strategy of the RIDE Roadmap, thus European Health Network, includes both “**top-down**” and “**bottom-up**” elements. There is a need for both local (member state and lower levels) and European-wide initiatives.

In fact, most of the healthcare is local; i.e. the information exchange usually occurs in the citizen's own community. However, in order to enable European-wide interoperable clinical data exchange, there is a need for a common underlying network providing the necessary core functionalities. This represents the top-down aspect of the EHN. Specifically, the minimum security standards required to assure secure data exchange or patient identification mechanisms could be Europe-wide so that all participants interconnect with standard generic interfaces of the core functionalities. By basing the network on standards and by complying with the “leveraging previous applications principle”, the system can work with a variety of hardware and software thus saving participating institutions from being forced to adopt a non-standard solution.

c) Build a network of networks: The European Health Network could be in the form of a network of networks, without any centralization of health records and without European-wide unique identifiers. Almost all member states have developed or are developing their National Health Networks [5] and sometimes, these national networks are composed of smaller Regional or Organizational Health Networks. These networks should be linked by directories of identifying information pointing to the sources of records, which could be achieved by means of Record Locator Services (more information is available in Section 4). This way, the data will stay where they are created (privacy aspect) and the existing infrastructure of participants will be leveraged.

d) Utilize a “thin” architecture: It is better if only the minimum number of protocols and functionalities essential to widespread exchange of health information are specified as part of the European Health Network. EHN should provide a real-time, secure and voluntary health information exchange for all parties, and should consist of a minimum set of standards and a minimum set of core services, such as the Patient Identification Service (the details of services are presented in Section 4). It is worthwhile to leave to the local (regional or national) systems those things best handled locally.

This approach can also be seen in the Draft Recommendation of the Commission on eHealth Interoperability, the objectives:

The understanding is that the necessary actions will be built on the minimum infrastructure and minimum steps required.¹

e) Architecture for the future: The deployment of the EHN can start with core services and can accommodate a modular structure for the possible future services of clinical data exchange and use. This could be considered as a “**plug-in**” based infrastructure.

f) Be open and standards based, built on a ready set of data standards: It is advised that the EHN is based on open industry standards for messages and design so that all interested parties can participate on an even basis. All information flowing over the network must adhere to standard formats. For this purpose, it is considered that agreement of Member States on a minimum set of standards for data and messaging would be very useful. Rapid development could be achieved if focus is on implementing the “**ready set**” of data standards that are mature and proven.

The Commission's approach is also inline with this principal's content, in the Draft Recommendation of the Commission on eHealth Interoperability, actions for architectural and technical interoperability:

Member States: Agree on the application of a minimum number of standards appropriate to eHealth systems and services.¹

There are several dimensions of interoperability in different levels and in order to address these successfully, it would be better if standards are grouped according to their usage:

- *Coding/terminology standards:* The nomenclature that is used to describe medical concepts (diagnoses, processes, medications, etc.) by coding schemes. These standards address common vocabularies and data interoperability.
- *Clinical data standards:* Descriptions of how to represent clinical data items (health records, emergency data sets, etc.) within well-structured definitions. The data representation standards address common vocabularies and data interoperability.
- *Messaging/interaction standards:* The underlying protocols for inter-application communication within the network and the definition of the content of the transferred messages.
- *Security standards:* Security protocols and definitions that allow for the representation of data in protected structures.

It is necessary to address these standards for achieving interoperability in healthcare. RIDE Roadmap II¹¹ enumerates possible ways of achieving eHealth interoperability based on all prominent standard alternatives.

g) Vendor and technology neutrality: The participants of any network (European Health Network, Member States' National Health Networks, Regional or Organizational Networks) must not be bound to any single vendor, a set of vendors or types of technology. Rather, the participants should be independent to make their own selections with regard to their specific business and IT relationships, as long as they adhere to the standards agreed at the European level.

h) Decentralization: The European healthcare system is fragmented by its nature. Many types of healthcare institutions exist, from big hospital systems to individual practices. Therefore, the design of EHN should be able to accommodate *voluntary, partial and incremental participation*.

Considering the legal and market realities of healthcare, clinical data should stay where they are. Decentralization leaves clinical data in the control of healthcare providers with a direct relationship with the patient, greatly reduces the risk of misuse by ensuring that there is no single "bucket" holding identifiable clinical data, and leaves judgments about who should and should not see patient data in the hands of the patient and the physicians and institutions that are directly involved with his/her care.

One critical detail regarding decentralization, even though the infrastructure is decentralized it may still support and facilitate aggregation of data for public health monitoring, quality management and other secondary uses.

i) Location and retrieval of health data: It is necessary that the EHN and its sub-networks enable a correct locating of a health record. Patient identification is important in this respect and it is detailed in the other principals. Furthermore, location of a health record does not mean much if an authorized body could not successfully retrieve it. Therefore, the networks should also enable a seamless transfer of requested data, independent of the underlying physical interface. For this purpose, standards-based messaging capabilities can be adopted by the networks as core services.

j) Central storage of sufficient data to identify patients and locate records: A minimum set of metadata (e.g. Record Locator Service index entries) may be required at a European level for operation of essential EHN functions. Of course, as it is discussed in the previous principal, there is no requirement for central storage of clinical data.

k) Patient identification without a European-wide unique ID: Patient identification is very critical since it is the first step towards locating a clinical record. It is required that patient identification is implemented as one of the core services of the EHN and that it works in interaction with the Record Locator Service. However, implementation of a European-wide unique identifier for all European citizens is not advised. Implementation of a European-wide unique ID has some critical disadvantages. First of all, the political culture of some member states is not amenable to even national identifiers due to privacy concerns. Secondly, a European-wide ID could not be implemented in a short period, it would require many years.

Instead, patient identification could be realized by demographics data. The Record Locator Services can implement "matching algorithms" for this purpose. Unfortunately, there is not any standard matching algorithm. The EHN may decide the minimum criteria in this respect, i.e. a minimum

¹¹ RIDE D.4.4.1 – RIDE ROADMAP II, <http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>

matching probability for false positive of 1 in 100.000. It is worthwhile to mention that null values are always less dangerous than false positives. The details of the Person Identification Service and Record Locator Service can be found in the technical details section.

The identifier mechanisms are also mentioned in the Draft Recommendation of the Commission on eHealth Interoperability, objectives:

This approach (interoperability) will be founded on a number of distinct challenges e.g., resolution of appropriate and secure identifiers for patients, health professionals, and institutions.¹

l) *Healthcare provider identification:* Similar to patient identification, it is required that the network enables mechanisms to identify and locate healthcare providers, which can be large institutions or small primary healthcare organizations. Again, it is not meaningful to implement European-wide unique identifiers for the healthcare providers. Within a network (regional, national or European), its Record Locator Service should be capable of identifying the healthcare provider and locating the records. Some member states have national unique identifiers for the healthcare providers and some members do not. However, as long as identification is resolved seamlessly within a national or regional network, the data exchange in the European level could not be interrupted. Healthcare provider identification is mentioned in the Draft Recommendation of the Commission on eHealth Interoperability, as well.

m) *Modular Service Oriented Architecture:* It is necessary that the EHN architecture is open, scalable and modular so that its components can be periodically refreshed as technology evolves. A modular design could lower the barrier to entry for new participants and allow for an easier, necessary integration of legacy health information technology investments. Service Oriented Architecture (SOA) is able to provide these necessary priorities.

The second version of the RIDE Roadmap II¹¹ considers all prominent technologies and standards relevant for the Member States in achieving a European eHealth Interoperability Framework based on a Service Oriented Architecture (SOA), namely IHE Integration Profiles, CEN/TC251 EN 13606, and HL7 version 3 and the HL7 Clinical Document Architecture (CDA). It describes how each of the necessary Member State services (Locator Service, Patient Identification Service, Audit Services, Professional Identity Service, and Provider Identity Service) can be implemented by using alternative technologies. The details of the services, such as the WSDLs definitions are given in RIDE Roadmap II¹¹.

Furthermore, the RIDE consortium has also produced a deliverable addressing legacy healthcare applications, namely “D4.4.5 - Integrating the Legacy eHealth Applications of the Member States into the RIDE Technical Framework”, which presents an integration and migration strategy so as to protect existing investments on IT frameworks in the European Union. Further information on SOA-based legacy integration strategy is available in RIDE Deliverable D4.4.5.⁴

n) *Security and auditability:* Although paper-based methods are old record keeping technology, to be honest, by nature they are quite efficiently secure since most of the time they have only one copy and they are usually stored behind the locked doors. On the other hand, the apparently limitless ability to search and analyze huge amounts of digital clinical data poses security and privacy challenges that the electronic health networks must satisfactorily address.

The architecture must provide both patients and providers with a high degree of trust that their healthcare information is protected from unauthorized access, and will not be used for purposes outside of their knowledge and consent. For this purpose, apart from the secure messaging and data encryption methods which are addressed in Section 4, enhanced and trustworthy auditing mechanisms must be developed that will keep track of each action. In this way, any actor in the network could not deny responsibility of any action he/she/it took.

o) *Coordinated PHRs and EHRs:* Efforts to increase connectivity in healthcare serve for a major objective: “active involvement of citizens in managing their health care and gaining the benefits of having their health information in a format easily accessible to them”. Citizens do not desire the health information for themselves only, they also want to be assured that professionals who provide services to them can get the information they need in a timely, accurate, and usable way.

Although many of them are not capable of communicating with each other, today many healthcare professionals enjoy the comfort of managing their patients' records through Electronic Health Record (EHR) systems. Personal Health Record (PHR) systems, through which individuals can access, manage and share their health information in a secure and confidential environment, are gaining popularity. The efforts through establishment of European health information space would support PHR and moreover, the PHR would be in coordination with EHR. Interoperable PHR and EHR is truly a necessity and should be a principle of design from the beginning. Otherwise, there will definitely appear many duplicates of a citizen's health record, which will not be easily managed. For this purpose, related clinical data standards that are capable of handling EHR, PHR and emergency data set in a coordinated way could be selected, if available.

p) Privacy and consent based permissions management: The European Health Network and its sub-networks must provide the security and privacy controls needed to assure citizens that their data will not be misused. From the legislative point of view, there are a number of laws protecting the privacy of sensitive health data. These are mentioned in the "Political and Legal Framework" section and in the architectural structure; these laws should definitely be addressed by the components to be developed.

An individual is the true owner of his/her health data; therefore it is actually normal that access to health information of an individual is subject to consent of that individual. The above mentioned PHR mechanisms can be enriched with consent-based authorization functionalities, so that citizens have a saying in the management of their own health. Moreover, citizens may be able to keep track of who has accessed or modified their health data. Permissions management could be so skilful that a citizen can grant/limit access to a specific section of or even to an individual item within his/her PHR for a healthcare professional from a specific proficiency.

The following paragraph taken from the Draft Recommendation of the Commission on eHealth Interoperability also unfolds the critical significance of patient consent:

*Therefore, the ultimate goal of this Recommendation is to contribute to enabling the provision of a means of **authorised healthcare professionals to gain managed access to essential health information about patients, subject to the patients' consent, and with full regard for data privacy and security requirements.***¹

q) Pseudonymization and re-identification of protected health information: Sometimes, for research or monitoring purposes for instance, patient-identifying information must be hidden before it is shared among parties of the European Health Network. In these cases, the core services of the network or EHRs or PHRs should be able to pseudonymize the private health data before sharing it for secondary usage. Moreover, there may be cases that require the re-identification of the pseudonymized data. Again the network or EHRs or PHRs should be capable of re-identifying the pseudonymized data for authorized parties.

Such an example case may be constructed as follows: avian-flu cases are being monitored at the European level by the help of the EHN. Instantly, when an incident occurs, an alert is sent to the correspondent public health administrator (i.e., Ministry of Health) of the patient. Then, obtaining the administrative rights and the mandate to follow up emergent communicable diseases, the correspondent public health administrator requests the re-identification of the pseudonymized data. The party that pseudonymized the data verifies the authorization of public health administrator and sends the original data to it. The public health administrator takes the necessary action.

r) Flexibility: Any hardware or software could be used for health information exchange as long as it conforms to a set of essential requirements defined explicitly by the European Health Network. The network must be able to scale and evolve over time. It should easily catch up with future technologies to arrive¹².

s) Accuracy: Accuracy in identifying both a patient and his/her records with no tolerance for error is an essential element of health information exchange. There could also be feedback mechanisms to help healthcare organizations to fix their faulty data when errors are discovered¹³.

¹² The Connecting for Health Common Framework: Overview and Principles

¹³ The Connecting for Health Common Framework: Overview and Principles

t) Incremental deployment: Establishment of a Europe wide health information exchange infrastructure is not a breathing time activity. An incremental process is essential for the deployment, where growing (in physical coverage) and evolving (increasing functionality) pilots are being developed. However, these pilots should not be implemented locally. Participation of at least two Member States in a pilot activity is essential. In each step, the implemented functionalities should be fully tested so that the rest is built upon strong pillars. The knowledge and experience gained by the participating organizations should be exploited to the service of newly participating organizations or member states. This way, they could easily overcome the previously faced challenges.

Finally, it is necessary that the incremental process is not limited with small scale pilots, rather supported with large scale pilots encapsulating various flavour of possible participants in the network. There are significant efforts in this respect supported by the European Commission. In the 2007 Call of ICT PSP¹⁴, under “Theme 3: ICT for sustainable and interoperable health services”, there are two major objectives the Commission is waiting for collaborative proposals [8]:

- Objective 3.1: EU wide implementation of eHealth services to support continuity of care: patient’s summary and ePrescription (Pilot Type A)
- Objective 3.2: Experience sharing and consensus building in eHealth (Thematic Network)

Pilot Type A projects are building on Member States or associated countries initiatives and will help to ensure EU-wide interoperability of ICT-based solutions/services that are being launched or are already in operation in the Member States or associated countries. The consortium must include at least 6 relevant national administrations. The reason is clear; the final outcome of a Pilot Type A project will be a set of common specifications (acceptable by all Member States and associated countries) and building blocks. It is expected that these kinds of supportive actions by the European Commission will act as a catalyst in establishing a well-connected European Health Network.

3.5.2 Strategy for Architectural Interoperability

After determining the architectural principles for e-Health connectivity networks, we would like to discuss the strategy and main steps to achieve interoperability in e-Health domain. There are three levels to define interoperability as follows:

- **Business Level:** In this level, main health objectives and policies such as ‘patient empowerment’, ‘exchange of medical data’ or ‘e-Prescription’ are analyzed to produce business use cases. Business use cases can be identified in many ways, however, the main point is to select a small number of use cases to start with to ensure achievability. For instance, if we consider the ‘exchange of medical data’ objective and analyze it at the European Level, ‘Exchange of Basic Emergency Dataset cross Member States’ would be the use case that we should start with. While working on business use cases, the first step is determining the business process to illustrate the need for specific types of information exchanges or scenarios. For example, ‘Update of Emergency Dataset’ and ‘Clinician queries and retrieves Emergency Dataset’ may be two business processes in this use case. The business process will help to determine the concepts, capabilities, functionalities and expectations from systems involved in the process. Each business process should be illustrated with a scenario to make the process more understandable and clear. After determining the business process and illustrating it with a scenario, we can easily identify the use case stakeholders and main issues that should be resolved to implement the use case. For instance, issues considered for the ‘Exchange of Basic Emergency Dataset cross Member States’ use case may be as follows:
 - Lack of interoperability among data standards (terminologies, structure, templates) used in different Member States for the Emergency Dataset.
 - Matching patients across Member States.
 - Identifying and authenticating clinicians across Member States.
 - Maintaining audit records for interactions.

¹⁴ http://ec.europa.eu/information_society/activities/ict_psp/calls/call_proposals_07/index_en.htm

Consequently, business level use cases are very useful tools to set the scope of an interoperability problem and to understand and describe the functionalities and capabilities of systems in more abstract level.

The RIDE Project has taken this approach and in RIDE Deliverable D2.3.1 Requirements Analysis for the RIDE Roadmap¹⁵, all the use cases related with eHealth interoperability have been described. A very detailed analysis of the use cases from the implementation point of view is presented in RIDE Deliverable D.3.1.1 – Goals and Challenges I¹⁶.

- **Service Level:** On this level, the specified functionalities, capabilities or issues from the business level are detailed and expressed as services. Services can be perceived as building blocks of the connectivity networks where each building block defines a functionality or capability on an abstract level. For instance, if we continue with our example, the following list of services/functionalities can be identified:
 - *Locator service/functionality:* If the emergency data sets or patient summaries are going to be shared across Member States, in order to retrieve the data, it has to be located first. So there is a need for a locator service. In order to "find a specific patient's data with demographic information", the Locator Service needs to index all submitted medical summaries with the patient's demographic information and possibly with other metadata attributes. Metadata format and terminologies used in the metadata need to be uniform EU-wide.
 - *Patient matching service/functionality:* The Locator Service needs to use a matching service that runs an algorithm determining which records are probable matches. There is no standard matching algorithm that can be adopted EU wide, because the work on matching is highly sensitive to local characteristics of the data set being queried.
 - *Healthcare Professional Authentication service/functionality:* When a physician is using the locator service to access a patient's records, he should be able to authenticate himself. For this to be realized the Member States must provide healthcare professional authentication services together with the locator services. Even in the case of emergency data, the accessor must be authenticated. Otherwise reports in the media about misuse of the system may cause the whole system to collapse.
 - *Security service/functionality:* Another functionality needed is secure messaging and data encryption methods.
 - *Auditing service/functionality:* The final functionality needed is auditing mechanisms to keep track of each action on the data accessed. In this way, no one can deny the responsibility of any action taken on the data.

Different use cases may share the same services as it can be seen from the example (e.g. security service, auditing service, etc). Therefore, these services can be perceived as abstract building blocks for the construction of bigger architectures and business process.

All the service level implementation details of these services are presented in RIDE Deliverable RIDE D.4.4.1 – RIDE ROADMAP II¹⁷.

- **Integration Profile Level:** Integration Profiles are guidelines for implementers that identify relevant standards and define how to apply them to satisfy the requirements of a use case. Integration profiles may also be perceived as common technical interoperability building blocks which maximize reuse of specification and implementation methods, while allowing for evolutionary growth within a domain. They constrain standards where necessary and show how to use them in specific use cases. Therefore, the integration profile level is the final step after Business and Service levels in which the actors, transactions, data requirements are

¹⁵ RIDE Deliverable D2.3.1 Requirements Analysis for the RIDE Roadmap, <http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>

¹⁶ RIDE D.3.1.1 – Goals and Challenges I, <http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>

¹⁷ RIDE D.4.4.1 – RIDE ROADMAP II, <http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>

bound together. Integration profiles do not specify the internal execution of systems but specify the interface between systems both in communication and on data level. In this way, they provide for an interoperability based on standards, possibly more than one, where each standard is used for a different part of the use case. Integration profiles also ease the certification process by enabling the vendors to provide conformance claims based on integration profiles and actors in these profiles. Currently, profiling seems to be the most trendy and useful tool to provide interoperability. It is also very popular in the e-Health domain. For instance, the industry consortium Integrating Healthcare Enterprise¹⁸ publishes integration profiles for several interoperability problems.

3.5.3 Testing, Certification and Accreditation

Testing is very important to guarantee interoperability and certification. Certification of the interfaces and applications that will be part of the network is a significant necessity because of two main benefits it provides:

1. Ensuring the compliance with the standards and implementation guides; thus enabling the interoperability of the newly participating bodies inter network.
2. Reducing the costs of building health information networks, by building upon the successfully certified systems that have been developed as a result of huge investments and efforts; thus avoiding the replication of efforts for each application, service or network.

A certification methodology for the participants can be developed in parallel with the preparation of a detailed technical specification of the European Health Network. It would be better if vendors and solution providers are provided with a “Reference Implementation”, which is fully compliant with the detailed technical specification. The certification and accreditation process should require the full but minimum set of criteria necessary for interoperability. It should encourage new participants and innovative developments.

The Draft Recommendation of the Commission on eHealth Interoperability also focuses on certification and accreditation of eHealth interoperability initiatives:

At the level of certification and accreditation of eHealth interoperability in Europe, it is considered that there is either a need for a single certification process that is valid throughout the European Union or a means of mutual recognition of each Member State's certification mechanisms.¹

When it is considered for the European Health Network, all participating organizations (that is the National Health Networks) are subject to the same set of conditions; so certification steps are identical. However, as building a “network of networks” is a recursive process and certification of the systems involved within an NHN is also necessary, national and regional certification processes should respect the different business and technical requirements of the participants. These systems may be subject to distinct certification requirements.

Finally, the certification and accreditation process could also ensure the quality requirements of the systems connected to national/European-wide health network, such as uptime, response-time, maintenance, up-to-datedness of information that are explicitly stated in the Draft Recommendation of the Commission on eHealth Interoperability.

3.6 Monitoring and Evaluation

The final requirements for the establishment of a well-connected European health information space are monitoring and evaluation. The European Health Network is not just about a patient's health record exchange; although this is the major objective, when eHealth interoperability objective is achieved, it would not be meaningful not to exploit it to its full potential for gaining collaborative benefits.

Once the data exchange capability has been realized and the flow of data into public health organizations is possible, these authorized public organizations could be enhanced with ICT-based

¹⁸ <http://www.ihe.net/>

statistical monitoring and public alert notification tools. These tools can improve general notifications of possible outbreaks as well as identification of specific patients who may need to be treated and tracked. Bio-surveillance is one popular evolving trend that could be achieved by performing data mining on the clinical data gathered from the dispersed repositories in the health network. It is desired that public health outbreak alerts are generated and announced automatically by the monitoring services of the health networks instantly. A more general use case could be the collection of statistical data from the participating healthcare organizations by the appropriate authorities and decision-makers. Without ICT support, this process requires tremendous effort and adds extra work to administrative staff.

The Draft Recommendation of the Commission on eHealth Interoperability also states the significance of monitoring capabilities:

*Finally, health and healthcare are not only important for each individual but also in **providing important indicators of the state of a society or community**. Statistics about health are an important part of a health information system. The **ability to share relevant information at a pan-European level to the appropriate authorities and decision-makers** would be a helpful outcome that can emerge from the introduction and expansion of eHealth interoperability.¹*

In order to realize these objectives, as it is explained in detail in the architectural interoperability section, even though the infrastructure is decentralized, it is essential that the infrastructure still supports and facilitates aggregation of data for public health monitoring, quality management and other similar functions. Moreover, sometimes patient-identifying information must be hidden before data is collected. Therefore, the core services of the network or EHRs or PHRs should be able to pseudonymize the private health data before sharing it for secondary usage and should also be capable of re-identifying the pseudonymized data for authorized parties when necessary.

The continuous evaluation of the participating systems and the underlying infrastructure is another major activity that needs to be addressed. The high quality and accuracy of the systems should be assured. With the introduction of certification and accreditation, it is almost guaranteed that the systems are qualified enough to participate to the general network. However, certification is a one-shot process, it is realized at the beginning and it is highly probable that long term behaviour of the systems cannot be monitored precisely during the certification experiments.

For the continuity of high quality service, a continuous evaluation of the systems and their management may take place. In this respect, the minimal qualitative criteria can be defined and the progress of the systems and services can be measured according to these criteria. As it is the case for certification, again, evaluation processes should guard the different business and technical requirements of the participating applications.

Evaluation is mentioned in the Draft Recommendation of the Commission on eHealth Interoperability too:

Member States and the European Commission. *Both parties should define the quantitative and qualitative criteria, and milestones, to measure the progress of the interoperability of eHealth (in particular for electronic health records) and the benefits achieved by the systems and services developed by the Large Scale Pilots. Continuous evaluation of both systems and their management should be integrated in any proposed scheme.¹*

The activities mentioned in this section may seem as secondary objectives in contrast to achieving interoperable data exchange in the Europe level. However, their benefits are not negligible so that they need to be addressed starting from the design phase.

4 TECHNICAL DETAILS

4.1 Architectural Models

European eHealth interoperability requires a Healthcare IT connectivity network that will connect the existing networks. Note that in the EU there are both regional networks such as the one in the Lombardia region in Italy and national networks such the one in Denmark. In this section we briefly

describe the architectural models for any type of Healthcare Connectivity Network and provide some suggestions on what level (European, National, or Regional) these architectural models can be more useful and effective. Similar architectural models have been proposed in¹⁰.

4.1.1 Centralized Storage

In this architecture all data that is desired to be shared are maintained into a centralized repository. Therefore, services or functionalities over data like security, privacy, authentication, and system management are also centralized. Entities in the network submit data to, and request data from, the central site. The major advantages of this architecture are providing a single source for all patient data, a single set of interface standards, security policies, etc. which simplifies the technical and operational requirements for the system. However, large volumes of data will cause network bottlenecks and it would be very hard to develop, manage or operate this architecture if the number of endpoint systems connected to the centralized storage is high. Consequently, using this architecture in European or even in National Level is not rational. This type of networks should be used in regional level especially to connect a number of healthcare organizations which has no storage capabilities in underserved regions.

4.1.2 Federated Architecture with Repositories

This architecture provides a one level federation for centralized repositories. At the national level, this model would empower regional organizations to develop networks and manage the privacy, security, and authentication issues for their region. Local providers would send their data to the regional network repository. At the national level, record locator pointers would be maintained so that patient records could be located across regions. Although the model provides some level of hierarchy, for regions with many healthcare organizations, centralized repositories would become easily overloaded.

4.1.3 Federated Architecture with Locally-Held Data

This architecture provides a full federation between healthcare providers who would store the data on their local systems. Over this level, there are regional broker systems maintaining the pointers to records stored at the local provider level. The architecture can be made more hierarchical by putting broker systems over broker systems. Therefore, the model is the most suitable one for both European and National level. For example, when an authorized user needs a patient information, he/she can contact the regional registry, which would identify known locations where the patient had records stored (e.g., hospital, clinic). If the patient consent allows, the regional registry can also query the National Registry and find the records about the patient in other regions. In the same manner, the National Registry can query the European Health Record Registry and find the records located in other European countries. After locating the records, there are two alternative approaches to retrieve the record. One of them is to contact the provider that stores the record directly in a peer-to-peer manner. The second alternative is to allow the registries to broker the access and exchange of information instead of allowing that final step to happen in a peer-to-peer fashion.

4.1.4 Peer-to-Peer Networks

In this model, the necessary standards are defined so that providers and other data holders can communicate directly with each other, without requiring any intermediation from a hub. Endpoint systems should be able to accept requests for data, authenticate the requestor, identify the patient, and package the requested data securely for transmission. Although this model provides strong access control for patients and providers, since there would be no central or regional repositories of patient identifiers and pointers in this model, there would be network bottlenecks if the number of peers in the network increases. Therefore, this model is only suitable for small regional networks.

4.1.5 PHR Repositories

This model is not an individual model but an auxiliary one that can be used together with the others. Patient health information repositories would be controlled and owned by the consumer and could be managed by a third party (e.g. public portals, PHR systems, e-Cards).

4.2 Content Interoperability

4.2.1 A Collection of Context-dependent Definitions of Patient Summaries

A first approach to achieve content interoperability is through the definition of the criteria to build Patient Summaries, for the sharing of relevant patient information.

Following the approach of HL7 CDA, three levels of granularity may be considered in the definition of the structure of a clinical document:

1. CDA LEVEL 1 - the basic HL7 standard (release 2) offers the primitives to represent in a structured way the header of a clinical document and its body. No clinical constraints are provided about the content of the body. The standard provides the mark-up to identify the document sections, but not their admitted values.
2. CDA LEVEL 2 – the implementation guide known as CCD (clinical care document) provides the names and codes of the sections, and the format for a structured representation of the clinical statements within each section. No constraint is given about *which* clinical data should be present in the document. This level is suitable for a generic patient summary, where the author decides which data are actually relevant for a given patient in a given context, to be included in the summary.
3. CDA LEVEL 3 – a specific “clinical dataset” is provided by a suitable physicians organisation, to specify the (minimal) set of data to be shared in a predefined clinical situation, e.g. to share patient data between a GP and a specialist about asthma or diabetes according to a predefined clinical pathway. The name of the data element should be coded through a recognised coding scheme (e.g. LOINC). This level is suitable for “Problem-specific Patient Summaries”.

In addition to the definition of a clinical dataset, an effective interoperability is achieved in a local (or regional, national or European) community by defining the admitted values for each data element. For each qualitative data element, an explicit agreement should specify the subset of a recognised coding scheme (e.g. SNOMED) that is admitted in that context. For each quantitative data element, the scale and the range should be declared.

4.2.2 Clinical Statement Interoperability

Within the scope of the RIDE Project, the work entitled “Achieving Clinical Statement Interoperability using R-MIM and Archetype-based Semantic Transformations”¹⁹ which addresses the interoperability of Electronic Health Records structure and content has been realized and accepted for publication in IEEE Transactions on Information Technology in Biomedicine. In this section, this work will be summarized.

Generally, an EHR includes clinical statements such as observations, laboratory tests, diagnostic imaging reports, treatments, therapies, drugs administered, and allergies. Formally, a clinical statement is an expression of a discrete item of clinically related information that is recorded because of its relevance to the care of a patient²⁰.

At the moment, EHR information is stored in all kinds of proprietary formats through a multitude of medical information systems available on the market. Typical formats include relational database tables, structured document-based storage in various file types and unstructured document storage such as digitized hardcopies maintained in a classical document management system. Furthermore, the data may either be structured or unstructured, and may or may not conform to an open standard. These result in severe interoperability problems.

¹⁹ Kilic O., Dogac A., Achieving Clinical Statement Interoperability using R-MIM and Archetype-based Semantic Transformations, IEEE Transactions on Information Technology in Biomedicine, to appear, <http://www.srdc.metu.edu.tr/webpage/publications/2007/KilicDogac.pdf>

²⁰ HL7 Version 3 Standard: Clinical Statement Pattern, Release 1, <http://www.hl7.org/v3ballot/html/domains/uvcs/uvcs.htm>

To address the EHR interoperability problem, there are several standards currently under development which aim to provide standard interfaces to existing proprietary systems. The standardization efforts include the Health Level Seven (HL7) Clinical Document Architecture (CDA), the European Committee for Standardization (CEN) EN 13606-1 (referred to as EHRcom) and the openEHR. Such standards define the structure and the markup of the clinical content to make EHR exchange interoperable and they have been studied in detail in “RIDE D2.2.1 - Standardization efforts for providing semantic interoperability in eHealth domain”²¹ and in “A Survey and Analysis of Electronic Healthcare Record Standards”²².

However, having more than one standard introduces the interoperability problem among institutes using different standards. In order to address this need, in this work, the interoperability of EHR standards which are derived from the HL7 Reference Information Model (RIM)²³ is addressed. Then, it is possible to map HL7 CDA and CEN EN 13606-1 EHRcom clinical statement instances to each other by using archetypes and semantic tools and techniques.

A reference information model, like the HL7 RIM, defines a generic structure to express the concepts in a domain. This generic reference information model is then refined to subdomains and later to specific domain concepts. For example, HL7 RIM is used to derive the Domain Message Information Model (D-MIM) through a refinement process where only the required classes, attributes, relationships for building the messages for a particular domain are included. The next step is to build the Refined Message Information Model (R-MIM) by including the necessary classes, attributes and associations used in a set of messages for a particular subdomain. Finally, the Hierarchical Message Descriptions are built from the R-MIMs and made available in the form of message schemas, such as XML Schema Definitions (XSD).

With this methodology, for instance, HL7 RIM can be specialized into “Clinical Document Architecture” for expressing clinical documents; “Clinical Genomics” for expressing clinical and personalized genomics data and “Claims and Reimbursement” for handling claims and reimbursements. Defining a generic RIM and specializing it to subdomains makes it possible for the RIM to stay static and stable, and the concepts derived in R-MIMs can be traced back to the RIM.

The approach taken in CEN recognizes the importance of EHR interoperability. The possibility to represent the constructs of the CEN Reference Model as classes and attributes of the HL7 RIM is ensured²⁴. For this purpose, CEN has produced a D-MIM correspondence of its reference model by deriving it from the HL7 RIM. The EHRcom R-MIM can be generated in a similar way as described in HL7 Development Framework (HDF)²⁵. As an example, in Figure 2, a part of the HL7 RIM and the corresponding R-MIMs of EHRcom and CDA is given.

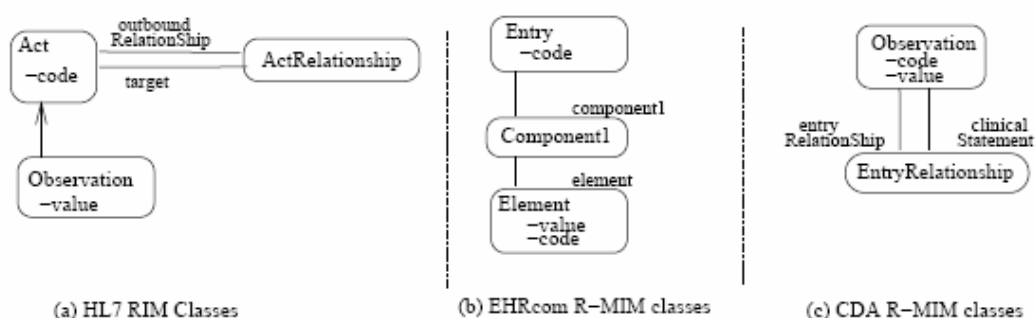


Figure 2 A part of the HL7 RIM and the corresponding R-MIMs of EHRcom and CDA

²¹ RIDE D2.2.1 - Standardization efforts for providing semantic interoperability in eHealth domain, <http://www.srdc.metu.edu.tr/webpage/projects/ride/deliverables/RIDE-D2.2.1-standards-09.doc>

²² Eichelberg M., Aden T., Riesmeier J., Dogac A., Laleci G., A Survey and Analysis of Electronic Healthcare Record Standards, ACM Computing Surveys, Vol. 37, No:4, December 2005. (Ranks the 1st in "Top 10 Most Popular Magazine And Computing Surveys Articles Downloaded In May 2006")

²³ HL7 Reference Information Model. <http://www.hl7.org/v3ballot/html/infrastructure/rim/rim.htm>

²⁴ CEN/TC 251, EN 13606-1, Health Informatics - Electronic Health Record Communication - Part 1: Reference Model, http://www.centc251.org/WGI/N-documents/WG1_N06-15_EN13606-1_FV.pdf

²⁵ HL7 Development Framework (HDF), <http://www.hl7.org/v3ballot/html/help/hdf/hdf.htm>

As a result, it is possible to transform the clinical statement instances between EHR standards by using semantic mechanisms based on the R-MIM derivations and archetypes. In order to express more specialized semantics, there is a need to use “archetypes”. An archetype is a reusable, formal expression of a distinct, domain-level concept such as “blood pressure”, “physical examination”, or “laboratory result” expressed in the form of constraints on data whose instances conform to some reference information model²⁶. In other words, an archetype specializes an information model concept. For example, when the archetype reference model is chosen to be HL7 CDA R-MIM, archetypes can be specified by placing constraints on the attributes of the HL7 CDA R-MIM “Observation” class, to define concepts like “Heart Rate” or “Penicillin Allergy”.

The R-MIM based mapping and transformation of two EHR instances that conform to different standards are accomplished in two phases as shown in Figure 3:

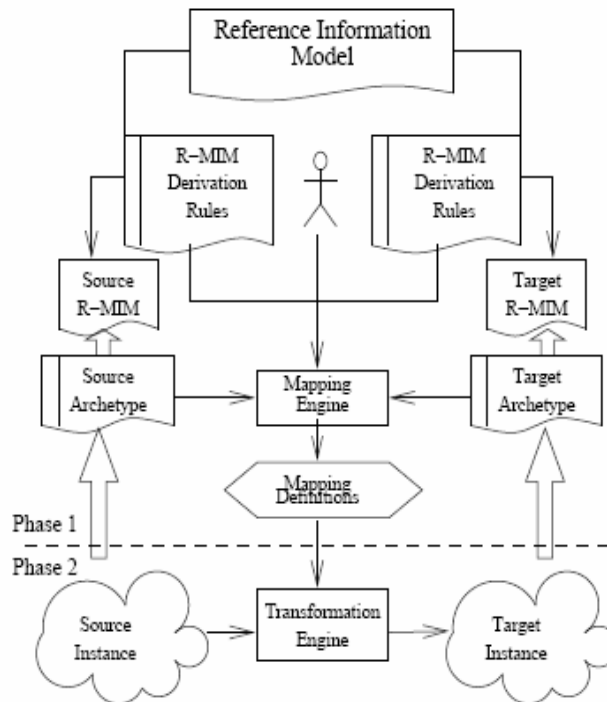


Figure 3 An Overview of the System Architecture

- In the first phase, the “Mapping Definitions” are produced between two archetypes which are based on different R-MIMs but express the same clinical concept. The classes of the source and the target archetypes are compared in order to discover the origins of the classes in the RIM to find out matching properties. Since this process involves reasoning, the OWL representations of the RIM, the R-MIMs (the source and the target) and the archetypes (the source and the target) are used. The mapping definitions produced in this phase are stored to be used later.
- In the second phase, the “Mapping Definitions” are used to transform one EHR instance to another. Since the source EHR instance is in XML format, first it is converted into an OWL instance. This process is called “Normalization”. Given the archetype of the source EHR instance, the “Normalizer” tool implemented creates its instance in OWL. Then the “Transformation Engine” developed uses the “Mapping Definitions” to create the target EHR instance in OWL. The next step is denormalizing the target EHR instance in OWL to XML format.

Deriving Archetype Property Mappings Based On R-MIM Derivations

In order to transform the source clinical statement instances to target EHR instances, it is first necessary to map the archetype of the source instances to the archetype of target instances. When

²⁶ T. Beale, S. Heard. Archetype definitions and principles (Revision 0.6), http://svn.openehr.org/specification/TRUNK/publishing/architecture/am/archetype_principles.pdf

two archetypes are declared to be expressing the same clinical concept, it is necessary to compare classes of the source and target archetype in order to discover the origins of the classes in the RIM to find their matching properties. The archetype property mapping algorithm is responsible of this mapping process.

For example, considering two archetypes given in Figure 4 (a) and (b) which define the same clinical concept, namely “Body Temperature”, but constraining the EHRcom R-MIM and the HL7 CDA R-MIM respectively. When two archetypes are declared to express the same clinical concept, the algorithm starts by comparing the classes of the source and target archetypes to discover the origins of the properties in the classes in the RIM. First, the algorithm finds that the “EHRcom-BT” is a specialization of the “Entry” class of the EHRcom R-MIM and the “Entry” is a specialization of the “Act” class of the HL7 RIM. Therefore the “code” property whose domain is the “Act” class of the HL7 RIM is inherited by the “EHRcom-BT” class through specialization. Similarly, the “CDA-BT” class is found to be a specialization of the “Act” class of the HL7 RIM. For the same reason, the “code” property is inherited by the “CDA-BT” class. Since there is no restriction that limits the maximum cardinality of the “code” property to “0” in any of these classes and their super classes, the “code” attribute of the EHRcom-BT is discovered to match the “code” attribute of the “CDA-BT” by the Mapping Engine. The code attribute of “Element-BT” is also discovered to match the “code” attribute of the “CDABT”. If the domain expert decides that one of the mappings is not suitable, the generation of the mapping can be prevented by marking the source property to be discarded.

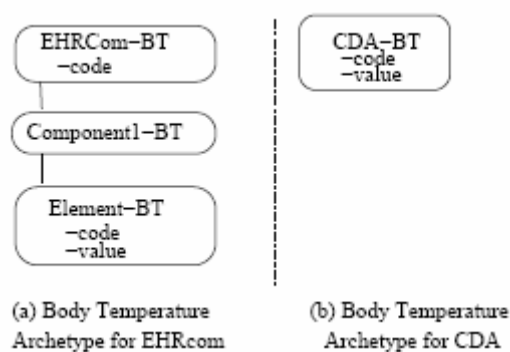


Figure 4 “Body Temperature” Archetypes based on EHRcom and HL7 CDA

In fact, during the property mapping process, a property is identified through a path involving all the relations from root class to the property. For example, the “value” attribute of the class “Element-BT” is denoted through the path “EHRcom-BT/component1/element/value”. The property mappings are defined by matching the paths. For example, the “EHRcom-BT/component1/element/value” path matches the “CDA-BT/value” path since both “CDA-BT” and “EHRcom-BT” are eventually derived from the “Observation” class of the HL7 RIM.

Transforming EHR Instances Using Archetypes

The inputs of the EHR instance transformation process are the source clinical statement instance in XML format and the “Mapping Definitions”. A clinical statement instance has a hierarchical structure. Therefore the transformation starts from root object in the source instance hierarchy then the process recursively continues with the child objects in this hierarchy.

Since the clinical statement instance is in XML format, it is first converted to OWL. In order to perform this conversion, it is necessary to find the archetype to which the source instance conforms to. The OWL representation of a source instance is constructed from its archetype. The next step is finding the “Mapping Definitions” from the source archetype to the target archetype. The discovery is based on the semantics of the mapping definitions such as the archetypes involved, and the authorship.

When such a mapping is found, the “Transformation Engine” starts creating the target EHR instance in OWL using the property mappings available in the “Mapping Definitions”. After processing the property mappings, default values are assigned to the properties of the target instance. The final step is to transform the target OWL instance to XML format.

It should be noted that in some cases the cardinality of the property pairs do not match. To handle such cases, the attribute transformation algorithm also checks the cardinality of the relations taking part in the path of the target property. The algorithm compares the cardinality of the source property with the cardinality of the properties in the target path from the leaf node to the root class.

After the creation of the target instance, default values specified in the archetype mapping definition are assigned to the attributes in the target instance.

4.2.3 ‘Realist Ontology’ Approach

Principle: use of formal methods

For some years now it has been commonly accepted that both the development and use of clinical terminology should be supported by formal methods. This is a thesis that we strongly support. But we wish no less strongly to insist that formal methods alone are not enough. (Thus the use of a Description Logic-based system appears, for example, not to have provided any guarantee for the absence of errors in SNOMED-CT [²⁷].)

Our principal thesis, here, however, is that a role can and must be played by *realist ontology* in making better biomedical terminologies. Realist ontology can not merely help in detecting errors and in ensuring intuitive principles for the creation and maintenance of systems of a sort that can help to prevent errors in the future. More importantly still, however, it can also help in ensuring that terminologies are compatible with each other. Note that we say ‘*realist ontology*’, in order to distinguish ontology in our understanding from the various related things [²⁸] which go by this mean in contexts such as formal knowledge representation. It is a realist conception of ontology which underlies statements such as:

The UMLS is an extensive source of biomedical concepts. It also provides a large number of inter-concept relationships and qualifies for a source of semantic spaces in the biomedical domain. However, the organization of knowledge in the UMLS is not principled nor consistent enough for it to qualify as an ontology of the biomedical domain [²⁹]

In the tradition of analytical philosophy, ontology is understood not as a software implementation or as a controlled vocabulary, but rather as ‘*the science of what is, of the kinds and structures of objects, properties, events, processes and relations in every area of reality*’ [³⁰]. Ontology as it concerns us here is a theory of those higher-level categories which structure the biomedical domain, the representation of which needs to be both unified and fully coherent – and as closely allied as possible to the representations used by clinicians in formulating patient data – if terminologies and coding systems are to have the requisite degree and type of interoperability. Ontology in this realist sense is already being used as a method to find inconsistencies in terminologies and clinical knowledge

²⁷ See for instance:

Ceusters W, Smith B. Ontology and Medical Terminology: why Descriptions Logics are not enough. Proceedings of the conference Towards an Electronic Patient Record (TEPR 2003), San Antonio, 10-14 May 2003 (electronic publication).

Ceusters W, Smith B, Kumar A, Dhaen C. Mistakes in Medical Ontologies: Where Do They Come From and How Can They Be Detected? in Pisanelli DM (ed) "Ontologies in Medicine. Proceedings of the Workshop on Medical Ontologies, Rome October 2003" IOS Press, Studies in Health Technology and Informatics, vol 102, 2004.

Ceusters W, Smith B, Kumar A, Dhaen C. Ontology-Based Error Detection in SNOMED-CT® Proc. Medinfo 2004.

Bodenreider O, Smith B, Kumar A, Burgun A. Investigating subsumption in DL-based terminologies: A case study in SNOMED CT. In: Hahn U, Schulz S, Cornet R, editors. Proceedings of the First International Workshop on Formal Biomedical Knowledge Representation (KR-MED 2004); 2004. p. 12-20.

²⁸ N. Guarino, P. Giaretta, "Ontologies and Knowledge Bases: Towards a Terminological Clarification". In Towards Very Large Knowledge Bases: Knowledge Building and Knowledge Sharing, N. Mars (ed.), pp 25-32. IOS Press, Amsterdam, 1995.

²⁹ Bodenreider O. Medical Ontology Research: A Report to the Board of Scientific Counselors of the Lister Hill National Center for Biomedical Communications. May 17, 2001 (<http://etbsun2.nlm.nih.gov:8000/pubs/pdf/2001-MOR-BoSC.pdf>)

³⁰ B. Smith. [Ontology](#), in L. Floridi (ed.), *Blackwell Guide to the Philosophy of Computing and Information*, Oxford: Blackwell, 2003, 155–166

representations [³¹] such as the Gene Ontology [³²] or the UMLS Semantic Network [³³]. The method has also proved useful in drawing attention to certain problematic features of the HL7 RIM [³⁴, ³⁵, ³⁶].

Mappings between systems

Biomedical terminologies can only be compared amongst each other, or used without loss of information within an Electronic Healthcare Record (EHR) system, if they share a common framework of top-level ontological categories. Often one talks in this connection merely of a shared or common *semantics*, meaning thereby the sort of regimentation that can be ensured through the use of enabling technologies such as RDF(S) [³⁷] and OWL [³⁸] that currently enjoy a wide interest through their association with the Semantic Web project, not to forget systems such as Protégé that are able to cope with them in a user-friendly way [³⁹]. On closer inspection, however, one discovers that the 'semantics' which comes with languages like RDF(S) and OWL is restricted to that sort of specification of meaning that can be effected using the formal technique of mathematical *model theory*, which is to say that meanings are specified by associating with the terms and sentences of a language certain abstract set-theoretic structures, taking Alfred Tarski's 'semantic' definition of truth for artificial languages as paradigm [⁴⁰]. Model theory assumes that the language refers to a 'world', and describes the minimal conditions that a world must satisfy in order for a 'meaning' (or 'interpretation' in the model-theoretic sense) to be assignable to every expression in the language. The idea is to provide an abstract mathematical account of the properties that any such interpretation must have in such a way as to make as few assumptions as possible about its actual nature or intrinsic structure, thereby retaining as much generality as possible. The chief utility of a formal semantic theory is thus not to provide any deep analysis of the nature of the things described by the language. Rather, the power of formal semantics resides at the logical level, above all in providing a technical way to determine when inferences are valid, i.e. when they preserve truth [⁴¹].

Model theory is thus metaphysically and ontologically almost completely neutral. Merely to formulate statements in a language such as OWL is far from building an ontology in the sense of ontology that is employed by analytical philosophers, and neither would translating a terminology into OWL turn it into an ontology. Such translation would indeed allow consistent reasoning about the 'world' – but only in the model-theoretic sense of 'world' that signifies not the flesh-and-blood reality with which biomedicine is concerned, but rather merely some highly simplified set-theoretic surrogate. The task of ensuring that the latter somehow corresponds in broad terms to the real world of what happens and is the case is, in the semantics literature, almost never addressed. In our view, however, this task – and indeed the whole detour via semantic models – is in fact superfluous: the job of ontology is not the construction of simplified models; rather, **an ontology should directly correspond to reality itself** in

³¹ Smith B, Ceusters W. Towards Industrial-Strength Philosophy; How Analytical Ontology Can Help Medical Informatics. *Interdisciplinary Science Reviews*, 2003, vol 28, no 2, 106-111.

³² Barry Smith, Jacob Köhler, Anand Kumar: On the Application of Formal Principles to Life Science Data: a Case Study in the Gene Ontology. In: Erhard Rahm (Ed.): *Data Integration in the Life Sciences*, First International Workshop, DILS 2004, Leipzig, Germany, March 25-26, 2004, Proceedings. *Lecture Notes in Computer Science* 2994, Springer 2004, 79-94.

³³ Schulze-Kremer S, Smith B, Kumar A. Revising the UMLS Semantic Network Medinfo 2004. *Proc. Medinfo* 2004.

³⁴ Lowell V: Actions in Health Care Organizations: An Ontological Analysis in: *Proceedings of MedInfo 2004*, San Francisco.

³⁵ Lowell V, Smith B: Speech Acts and Medical Records: The Ontological Nexus. in: *EuroMISE 2004*, Prague.

³⁶ Smith B, Ceusters W. HL7 RIM: An Incoherent Standard, *Stud Health Technol Inform.* 2006;124:133-138. (Presented at MIE2006)

³⁷ RDF Semantics. W3C Recommendation 10 February 2004 (<http://www.w3.org/TR/rdf-mt/>)

³⁸ OWL Web Ontology Language Semantics and Abstract Syntax. W3C Recommendation 10 February 2004 (<http://www.w3.org/TR/owl-semantics/>)

³⁹ Protégé OWL plug-in (<http://protege.stanford.edu/plugins/owl/>)

⁴⁰ Model Theory. *Stanford Encyclopedia of Philosophy* (<http://plato.stanford.edu/entries/model-theory/>)

⁴¹ Guha RV, Hayes P. LBase: Semantics for Languages of the Semantic Web. NOT-A-Note 02 Aug 2002 (<http://www.coginst.uwf.edu/~phayes/LBase-from-W3C.html>)

a manner that maximizes descriptive adequacy within the constraints of formal rigour and computational usefulness.

Applying realist ontology to terminologies and EHR architectures means in the first place applying it to those entities in reality to which these artifacts of the human intellect refer, such as concrete patients, diseases and therapies. We do this to serve at least one important goal, namely making terminologies coherent, both internally as well as in their relation to the EHRs in or for which they are used.

It is essential to this endeavour that we give terminologies and EHRs themselves their appropriate place in reality and that we understand their nature and purposes in terms of a coherent ontological theory. Although terminologies can themselves be viewed as (simple) models of a certain portion of reality, they are in fact as real as the words we speak or write and as the patterns in our brains. We should thus use the realist ontology framework to analyze how terminologies and electronic healthcare records fit into a realist ontology, and thus also how they relate to the patients, physicians, diseases, etc. towards which they are directed.

Already a very superficial analysis of a coding system such as the International Classification of Diseases [⁴²] reveals that this system is not in fact a classification of *diseases* as entities in reality. Rather it is a classification of *statements about disease phenomena which a physician might attribute to a patient*. As an example, the ICD-10 class *B83.9: Helminthiasis, unspecified* does not refer (for example) to a disease caused by a worm belonging to the species *unspecified* which would be some sub-species of *Acanthocephalia* or *Metastrongylia*. Rather, it refers to a statement (perhaps appearing in some patient record) made by a physician who for whatever reason did not specify the actual type of *Helminth* the patient was suffering from. Neither OWL nor reasoners using models expressed in OWL would complain about making the class *B83.9: Helminthiasis, unspecified* a subclass of *B83: Other helminthiasis*; from the point of view of a coherent ontology, however, such a view is nonsense: it rests precisely on a confusion between ontology and epistemology [⁴³].

A similar confusion can be found in EHR architectures, model specifications, message specifications or data types for EHR systems. References to a patient's gender/sex are a typical example. Some specifications refer to it as “administrative sex” (leaving it to the reader of the specification to determine what this might actually mean). The possible specifications of *administrative sex* are then *female*, *male*, *unknown*, or *changed*. *Unknown*, here, does not refer to a new and special type of gender (reflecting some novel scientific discovery); rather it refers to the fact that the actual gender is not documented in the record.

An interpretation along these lines does not work in every case, however. Consider those specifications which refer explicitly to “clinical observations”, as is the case for Corbamed-COAS (“Clinical Observations Access Server”), which consists of:

any information that has been captured about a single patient's medical/physical state and relevant context information. This [information] may be derived by instruments such as in the case of images, vital signs, and lab results or it may be derived by a health professional via direct examination of the patient and transcribed [sic]. This term applies to information that has been captured whether or not it has been reviewed by an appropriate authority to confirm its applicability to the patient record. [⁴⁴]

When in an EHR system that claims to follow the COAS specifications, the specification “*unknown*” would be registered for gender, then that specification has to be interpreted that an observation has been made with respect to the patient's gender, and that as a result of that, an unknown kind of gender has been observed. Of course, that is not supposed to be the idea.

⁴² World Health Organisation. ICD-10 - The International Statistical Classification of Diseases and Related Health Problems, tenth revision (<http://www.who.int/whosis/icd10/>).

⁴³ Bodenreider O, Smith B, Burgun A. The Ontology-Epistemology Divide: Case Study in Medical Terminology. Submitted to the Third International Conference on Formal Ontology (FOIS) 2004.

⁴⁴ 3M, Care Data Systems, Inc., CareFlow/Net, Inc., HBO & Company, Philips Medical Systems, Protocol Systems, Inc. CORBAMED-COAS: clinical observations access server specification. Version 1, April 2001. (<http://www.medcom.dk/picnic/deliverables/01-04-06%20coas%20specs.pdf>)

4.2.4 Recommendations About Content Interoperability

European and international efforts towards standardization of biomedical terminology and electronic healthcare records were focused over the last 15 years primarily on syntax. Semantic standardization was restricted to terminological issues around the semantic triangle paradigm [⁴⁵] on the one hand and to issues pertaining to knowledge representation (and resting primarily on the application of set-theoretic model theory) on the other hand.

Moves in these directions are indeed required, and the results obtained thus far are of value both for the advance of science and for the concrete use of healthcare telematic applications. We can safely say that the syntactical issues are now resolved and also that the problems relating to biomedical terminology (polysemy, synonymy, cross-mapping of terminologies ...) are well understood – at least in the community of specialized researchers.

In the short term, a significant progress in content interoperability can be made by the adoption (possibly at European level) of international terminologies and coding schemes, as well as of two kinds of standardised structures for clinical documents to be shared:

- A generic structure for clinical documents, as for example in CDA-CCD, providing the list of the potential sections of clinical documents and the standard structure for the clinical statements within each section, suitable for the representation of generic Patient Summaries;
- A collection of clinical datasets, to be used to share context-specific Patient Summaries, devoted to the sharing of data among professionals in relations to particular clinical pathways.

This task should be performed by professional organisations, with the support of Member States.

Furthermore, regarding the interoperability of EHR structure and content, an approach is presented that describes how the clinical statements of two different EHR standards derived from the same RIM can be mapped to each other by using archetypes, R-MIM derivations and semantic tools. The approach is demonstrated with EHRcom and HL7 CDA instances; which proves that it is applicable in achieving clinical statement interoperability.

Although the approach seems to be dependent of HL7 RIM, in fact it is possible to achieve the same results with other reference information models. The main point is that, interoperability of various EHR standards is quite easily achievable if these EHR standards could be derived from a single, small but complete reference information model.

Finally, it is time to solve the problems of semantics by using the theories and tools that have been developed so far, and that have been tested under laboratory conditions [³¹]. This means using the right sort of ontology, i.e. an ontology that is able explicitly and unambiguously to relate coding systems, biomedical terminologies and electronic health care records (including their architecture) to the real world.

To do this properly will require a huge effort, since the relevant existing standards need to be reviewed by experts who are familiar with the appropriate sort of ontological thinking (and this will require some effort in training and education). Even before that stage is reached, however, there is the problem of making all constituent parties – including patients (or at least the organizations that stand up for them), healthcare providers, system developers and decision makers – aware of how deep-seated the existing problems are. Having been overwhelmed by the exaggerated claims on behalf of XML and similar silver bullets of recent years, that would solve everything, they must be informed about the fact that XML alone isn't a silver bullet. And for sure, we must also be careful in not giving realist ontology a similar silver bullet status.

In Europe, the CEC's seventh Framework Program might provide good opportunities, and undoubtedly, similar initiatives can be found in the US, in Australia and in the Far East. Collaboration at an international level is in any case required if we want systems developed in different places to be of any value for those that did not contribute to their development.

The message of realist ontology is that, while there are various different views of the world, this world itself is one and unique. It is our belief that it is only through that world that the various different views can be compared and made compatible. To allow clinical data registered in electronic patient records

⁴⁵ Ogden, C.K., & Richards, I.A. (1927). *Meaning of meaning*. New York: Harcourt, Brace & Company.

by means of coding (and/or classification) systems to be used for further automated processing, it should be crystal clear whether entities in the coding system refer to diseases or rather to statements made about diseases, or to procedures and observations, rather than statements about procedures or observations. As such, coding systems used in or for electronic healthcare records should be given a precise and formal semantics that is coherent with the semantics of the record as well as with the real world parts that are described by them.

4.3 Clinical Pathways, Guidelines, Decision Support Systems, Workflows

4.3.1 Clinical Pathways

Clinical pathways can be utilized for the implementation of medical guidelines in a specific healthcare environment and they can decrease undesired variability of medical practice [9]. In contradiction with the medical guidelines, clinical pathways enclose multidisciplinary valuable resources like personnel, education level, medical equipment availability and other operational and administrative information. Medical guidelines require the consensus between medical experts. On the other hand, clinical pathways require a consensus between multidisciplinary personnel taking actions during the treatment execution. Clinical pathways constitute treatment process patterns which aim to increase both the healthcare process quality and the utilization of resources. Consequently, a clinical pathway may deviate from a clinical guideline due to administrative reasons, and a treatment scheme may deviate from the clinical pathway due to patient's symptoms during its execution.

In order to support the execution of treatment schemes based on clinical pathways and to relief the medical personnel, IT software solutions are required which will handle the healthcare business processes in an efficient manner [10]. Such systems would be responsible for the observation of the execution and the current status of the applied clinical pathways, offer the characteristic of automatic recognition of exceptional events and provide decision support services in order to handle the exceptions in an efficient and effective way. Moreover, the specific software systems should be capable of dynamically adapting the treatment process so as to control the appropriate modifications. The IT systems supporting Clinical Pathways execution and management could be installed both on intra- and inter-organizational level, since they are capable of monitoring the overall treatment scheme of patient as they are being executed.

4.3.1.1 Operational Issues on Shared Clinical Pathways

According to the RIDE Deliverable D4.3.1 on Policies and Strategies, three kinds of artefacts may assist the healthcare professionals and the patients in the deployment of shared clinical pathways and thus should be routinely processed by the eHealth infrastructure:

1. A representation of the reference clinical pathway and of the actual care plan currently followed by the patient;
2. The notification about the life cycle of a care mandate. A care mandate can be partial or comprehensive, temporary or permanent. The information system of a healthcare professional should be able to issue a notification to the cooperation infrastructure about each change in the life cycle of a care mandate (request, acceptance, suspension, completion, abort, etc). The notification should include the motivation and the objectives of the mandate. In this way each actor participant in the care of a patient can be aware of the other actors having a responsibility on the patient;
3. The notification about the healthcare-related events in which the patient is involved, especially if they influence the tasks to be performed by the different actors, as for example the contacts with the facilities and the evolution of the health problems.

These artefacts are the substrate to allow the actors to “feel as a system”, i.e. to let the healthcare system behave as a system with respect to the patient.

4.3.1.2 Trends and Motivations

The trends in healthcare business processes and their establishment and utilization in the healthcare routine are up to now quite mature. Nevertheless, there are several open issues / challenges that further motivate the research and implementation of IT solutions that support the execution of self-adaptive Clinical Pathways [11]:

- **Clinical Pathways Adaptability:** The traditional clinical pathways are normally static and lack dynamicity. Moreover, they are standard procedures applicable to a patient taxonomy not addressing the case of each individual patient. Moreover, they do not always take under consideration the most current medical, operational, and financial knowledge [12]. Nevertheless, there is a significant percentage of patients that encounter serious and significant variations from the established Clinical Pathways during their treatment scheme execution. In those cases, the adaptability of Clinical Pathways is of major importance since each patient needs to be treated as a special and unique case.
- **Maintenance:** The implementation of Clinical Pathways is based on medical guidelines and additional types of knowledge. The maintenance of the healthcare business process suffers from the continuous update, since both the medical guidelines and the circumstances inside a healthcare organization change constantly. The continuous and easy maintenance of the established Clinical Pathways is required since their structure needs to be able to change constantly as the medical and administrative circumstances are changing inside a healthcare organization.
- **Medical Guidelines Formalization:** The formalization of medical guidelines is being performed in a specific and per case manner. Their formalization is required since their parameters will be able to be processed by an IT infrastructure that supports their execution. Several attempts have been made towards the direction of Medical Guidelines formalization, but a unified approach is required so as to allow the medical personnel to model the medical guidelines in a way that they will be machine-readable, interpretable and editable.
- **Clinical Pathways Modelling:** The modelling of Clinical Pathways lacks a formal structure. Different approaches exist in the area of modelling. Their interoperation could be of major importance since the Clinical Pathway exchange between healthcare organizations could facilitate the execution of the treatment schemes utilized. The establishment of a common representation standard would enable the sharing of CPs, the shared execution of discrete parts of a CP from different healthcare organizations and moreover the execution of a CP across member states. A common modelling methodology will lead to the creation of IT systems that will be able to import and execute designed Clinical Pathways.
- **Real-time information capturing:** Information capturing consists one of the major factors for success of the treatment scheme executed for each patient. The lack of real-time information fed to the clinical pathway creates a major need, since the information collected could lead to major reconfigurations of the executed Clinical Pathway. The interoperability between such systems could further enhance the execution of CPs. The IT infrastructure for CP execution should be able to receive data in a standardized format so as to integrate them and utilize them as parameters during the decision making concerning the execution of the next steps of the CPs.
- **Real-time knowledge recycling:** The knowledge recycling during the execution of a Clinical Pathway constitutes one of the major challenges for the area. The knowledge feedback would be valuable since the knowledge update is able to redefine the Clinical Pathway and the model of the exception rules. The semantic enablement of such an IT infrastructure would optimize the decision making through the utilization of the appropriate ontologies. The ontologies will be continuously updated and maintained through the execution of semantic web rules.

4.3.1.3 Adaptive Clinical Pathways Approach

The solution concerning the abovementioned challenges / issues regarding Clinical Pathways is the design and development of IT infrastructures which enables the adaptation of clinical pathways in order to serve the personalization of the treatment plans for each patient. The following technological axes present some of the required characteristics to be implemented so as to serve the real-time adaptability of Clinical Pathways:

- **Real-time adaptation of clinical pathways:** The specific technical need could be accomplished through the utilization of continuous reasoning over the “current” knowledge stored in the domain ontology, so as to adapt each step of the clinical pathway under execution. The pathway in this

case, is not totally predefined. A skeleton is utilized and once the execution begins, there is a constant reasoning at the end of each “milestone” of the CP so as to decide on the next actions concerning the treatment procedure.

- **Semantic Web Rule Language (SWRL) Rule Base:** Additionally, such an IT solution should enclose a rule-set created by utilizing SWRL [13] language in order to integrate the rule-base with the ontology. The rule-base would be able to create new facts and update the ontology accordingly, thus creating new knowledge as each pathway evolves. This feedback would constantly update the knowledge stored in the ontology and lead to better results concerning the adaptation of the pathway.
- **Establishment of a meta-model for each clinical pathway:** Furthermore, the definition of a meta-model for each clinical pathway to be executed would enable the definition of clinical pathways templates. The meta-model encloses atomic and complex sub-pathways which are fed to the process execution engine. The integration of discrete parts and connections could result to the establishment of the meta-model of the pathway to be executed. Consequently, a repository of atomic and complex parts of clinical pathways could be established and maintained so as to allow the dynamic composition of the skeleton of the appropriate CP for each patient.

4.3.1.4 Adaptation utilizing semantic technologies

The proposed Clinical Pathway adaptation methodology is based on a meta-model clinical pathway establishment. Each clinical pathway to be executed will comprise a meta-model of a set of atomic and complex sub-processes. The atomic processes are executable parts of the healthcare business process forwarded to the execution engine. The complex processes will be sub-workflows which contain atomic processes and a set of decisions. The atomic and the complex processes will be interconnected in the meta-model level. Their connections are based on SWRL rules. Once an atomic or complex process is executed, the rule-base will be triggered. The knowledge existing inside the ontology, the current clinical status of the patient and the rule-set will be interoperating in order to select the next executable part of the clinical pathway. Thus, the adaptation will occur during each step of the pathway execution. During each cycle of execution, the triggering of the rule-base may result to new knowledge creation that will be utilized in next steps during the execution. This fact ensures the constant update of medical, organizational and operational knowledge stored inside the ontology and consequently to the rule-base. The specific adaptation approach will lead to efficient, effective and self-adaptive clinical pathways.

4.3.1.5 Example Scenario

According to a real-life scenario, a patient confronts a health problem and decides to visit a healthcare organization for treatment. Once the admission is performed, an initial set of medical examinations is decided to be performed. The result set of the initial examinations provides valuable information for the clinical status of the patient which leads to the decision concerning the selection of the appropriate clinical pathway to be executed. The execution of the treatment scheme produces exceptions which are handled on real-time basis by the implemented software prototype.

More specifically, once the patient is admitted to the healthcare organization, its IT infrastructure should become aware of the data accompanying the specific patient. So, an initial data entry for the medical record dataset is performed. This procedure is performed either manually or automatically if the patient's medical record is received from another healthcare organization.

Once the clinical status of the patient is set, the CP execution infrastructure proposes an initial set of examinations to be performed. Afterwards, the result set of the tests is inserted into the medical record of the patient. The system proposes an appropriate clinical pathway according to the diagnosis. So, the execution of the treatment scheme begins, under the constant inspection of CP execution environment. Once an exception occurs, the IT system receives the exception information, executes the required rule-set and proposes the next “step” of the treatment scheme. The “step” derives from the following two categories:

- **Atomic process:** a single step procedure, executable by the process execution engine.
- **Complex process:** a multiple step procedure. It is a set of atomic processes without decision making. A complex process may contain parallel execution paths leading to a unified result.

The above-mentioned procedure is repeated during the execution of the treatment scheme of the patient. This way, the personalization of treatment for each patient is highly ensured, increasing the possibilities for the most suitable treatment.

4.3.2 Guidelines

The lifetime cycle of guidelines can be separated in the preparation and the distribution of them:

- **Guideline preparation**

- The first task of reviewing all “relevant” information on a specific topic is difficult. Information systems like abstract surveys and direct connections to major scientific schools are of utmost importance. The main challenge is first to get a complete survey about existing information, the next is to distinguish between different types of quality and correctly appoint the right class to the information reviewed. Two developments in medical information structure are moving in the right direction: 1. The MEDLINE Service of the National Institutes of Health (NIH) is becoming broader, more journals are now listed than ever before. 2. The publishers offer from time to time more journals in digital format, presenting scientific articles more or less free for download and usage.
- Comparison of the articles, understanding the different aspects of information offered therein, judging the competence and relevance to the guideline that has to be developed is the main task after retrieving those information. This could be supported by a kind of “good practice in scientific research” catalogue that must be free enough to enable independent thoughts, but close enough to prevent systematic or biased scientific errors.
- The fine-tuning of the new-found publications with the already existing guidelines in the referenced topic has to be carried out manually. This is a time consuming task of high responsibility. It cannot be supported by automated information processing, but can be leveraged by authoring systems.
- Publishing for comments and balloting will be an easier task. However, it seems more urgent to get the right people involved, having experience with the topic, being familiar with comment systems, coming to the right points of determining meaningful and obsolete rules compared to clinical practice. Here yellow pages, administered lists of contacts and centrally surveyed addresses are involved.
- The period of internal consensus finding will be a task that can be supported by editor systems and selection algorithms. Mainly it will be performed during face-to-face conferences and workshops.
- All together, these tasks are supportable by electronic means. However, the judgement and selection of information has to be performed by humans.

- **Guideline deployment**

- The first task is the publishing. The Clinical Guidelines have to be made knowledgeable by medical professionals. Information services, society internal infostructures, and congress information have to be used. These services can be supported by digital means. They should also be available in departmental and healthcare information systems for automatically presenting to the medical professionals during login.
- The guidelines have to be available on request. This requires a specific interface between the requesting user and the guidelines repository. It will depend on the user how the interface will act. A human user might contact through full text search, a machine user will ask for specific diseases and symptoms or dedicated clinical pathways. For those requests a vocabulary has to be built in. Semantic understanding has to be implemented into the answering system. If a complete ontology is offered to the administration system of the guidelines' repository an easy selection according to relations between different items can be supported.
- The requesting system – if the user is a computer program – has to follow specific rules. It has to deduct from data entries the relevant diagnoses or symptoms to transfer the correct request to the request interface. Another approach will be from a workflow point of view to request the optimal medical pathway for a specific set of constellations in the Electronic Health Record of the patient.

4.3.3 Decision Support Systems

A dedicated single task system normally has a single, specified input channel and will produce a specific output, tailored to the systems intention. Examples could be “detection of calcifications” in mammograms, “presentation of therapeutic strategies in case of sudden drop in heart rate” for cardiological patients. Examples for these systems are image-based computer assisted diagnosis systems for mammography or chest computed tomography. Another system would be a CT guided therapy planning system for liver transplantation / resection. Globally EHR-based systems have to offer a generic input interface for the connection to EHRs. This requires a common language for the detection of desired input items, logistics to follow widely accepted rules and a common understandable output. Information is drawn from the electronically available patient information as well as a rule database and will be used to steer directly workflow features or help the attending physician.

Technical Details are presented in the following:

- **Input:** Even, if the system is a single, stand-alone system, the input should consider the standards, given in the specified field of work. If more than one standard will be available, feasible standards should be supported to have a maximum of interoperability. If available – a metastandard should be used, that might guarantee interoperability even with future developments and will provide interconnectivity to other systems defining well the open and optional parts in a given standard (compare Integrating the Healthcare Enterprise technical frameworks).
- **Output:** The output has to be easy to understand, unambiguous and precise. It should consider imponderabilities and weight the differential response, displaying certainty factors for a specific response depending on the input available. A clear indication has to be given on which data the decision was based on. The result should be given in a community-wide accepted format that could be recycled by other systems to ease the use of information.
- **Ontology:** To develop systems that might work in different technical environments, an image of the real world should be available to those programs. Therefore a dedicated and detailed ontology should be available for the understanding of internal dependencies and hierarchical features.
- **Semantics:** Typically the biggest challenge is to understand the medical and technical terms in a precise and distinct way. Definition tables have to be available for further clarification and clearing of different aspects of a piece of information.
- **Development cycle hysteresis:** Knowledge is dedicated to develop and change. There have to be adaptation procedures in case of changes in the knowledge / reference database. If the decision has direct impact on the input factors, hysteresis adaptations should be available to prevent oscillation of the system.
- **Relevance and up-to-dateness of model information:** To understand and evaluate the results of a decision support system, the relevance and up-to-dateness of the calculated data should be indicated. On the other hand easy methods should be provided to update the reference model of a decision support system.
- **Availability of data:** Decision support can only be as valid as the input data and reference model data are available. Specific legislation (data protection law) in some member states might require encryption and therefore hiding of information. It has to be known, which possibly necessary data was not available for conclusion and what has to be entered in order to provide a meaningful output and result.

4.3.3.1 Technical Issues in the combination of Guidelines and DSS

- To simplify and co-ordinate medical actions, it is necessary to grant resources for the survey of the scientific development. Experts have to read and condense information. A specific cycle of renovation of publicly available information has to be introduced to guarantee the up-to-date and correct information of the services and Medical Guidelines.
- A deep understanding and culture of using medical guidelines has to be taught for medical professionals.
- A reliable technical infrastructure for distribution and requesting guidelines has to be set into action.

- Generally data quality management is an important issue in this respect. For instance, how accurate and reliable is the knowledge data source? Is it complete? There is a need for guidelines on the definition and distribution of such knowledge data sources. Some knowledge bases may be incomplete at the present time; interacting databases (like order-by-indication or order-by-drug-class) may be inconsistent from each other due to a lack of standards for names and classification.
- Some error checking features may not be broadly feasible due to the lack of availability of supporting patient data. For example for laboratory data, this is needed for drug monitoring and dosing guidance. Another example of patient data that may not be available to drive clinical decision support is a list of active problems and/or diagnoses using a coded vocabulary. It is required that a decision support system is able to get access to the relevant data like lab results, EHR etc.
- The medical parameters travelling between the different medical systems must be intelligent enough to assist the decision support system for monitoring the healthcare process and real-time delivery of alerts and recommendations. For example, in emergency situations when data is transferred from different monitoring devices, the system must act as an intelligent system to take appropriate decisions and inform the physician when data threshold reaches an alarm limit.
- An initial set of guidelines should be assigned to each patient, but at a certain moment, a decision support system could be deviated to a different guideline by a new clinical situation; for example, a patient with chronic heart failure could have a myocardial infarction during monitoring and, therefore, should be re-assigned to specific guidelines for this case. Widely accepted rules for assigning and switching guidelines must be defined. Due to medical, ethical and practical requirements, the e-Health system needs definitions of the minimal speed for the guidelines execution in order to reach a decision (recommendation/alert). This aspect could generate changes in the guidelines model tool if the times of execution are medically considered to be dangerously long for the patient's safety.

4.3.4 Workflows

E-health interoperability targets to a shared policy and a business process framework that will support appropriate business collaboration models between healthcare provision organizations and provides a sustainable environment in which interoperable solutions can be created, deployed, and managed. In order to maintain a shared environment, coordinated business interactions require a common understanding of business function even though alternative delivery mechanisms and channels may be employed. In the context of the RIDE Project, a patient visits various departments or organizations so as to receive the appropriate treatment scheme. The role of **healthcare workflow-management by use of IT** is to adjust and homogenize the contributions of those departments in terms of timing, quality and functionality.

In the light of the above-mentioned statements, RIDE roadmap proposes that one of the concerns of e-health experts should be to increase the automation and try to simplify the management of critical, and complex healthcare business processes that span multiple systems, and multiple healthcare organizations. Business Process management and system interoperability will enable the collaboration between various trading partners; healthcare providers, intermediaries, third-party administrators (TPAs), Pharmacy Benefit Management (PBMs), financial services, care management partners, etc.

4.3.4.1 Interoperability between IT systems

The cross-enterprise applications need to support any type of document regardless of content and format. Therefore, a document-content neutral Integration Profile could provide a standards-based specification for managing the sharing of documents that healthcare entities have decided to explicitly share, such as documents containing simple text, formatted text, images or structured and vocabulary coded clinical information. The IHE (Integrating the Healthcare Enterprise) initiative has been widely adopted for radiology, PACS, but still needs to be fully adopted by RIS, dedicated screening and reporting systems, etc, in order for these systems to eventually interoperate seamlessly.

For a successful support of cross-organisational business processes, interoperability has to be captured beyond current protocol based approaches developed in the Web Services stack. All collaboration between organisations is performed following a higher level business goal. For the understanding of interoperability it is important that managers and process owners are able to capture

this goal by modelling interaction from a high level business point of view [15]. Collaboration Business Processes (CBPs) have to be modelled capturing the overall business context of a collaboration and have to be linked up with private processes and resources without exposing private information. The methodology that is proposed in this roadmap aims at providing a suitable solution in this context. Methodology consists of three aspects [14]:

- A. Structuring complex cross-organisational business processes by applying swimlanes.
- B. Introducing views as a layer of abstraction above private processes called views. The approach allows for high level modelling of CBPs, enabling a scalable exposition of internal processes. Furthermore it provides a mechanism to flexibly link up internal processes with varying partner processes.
- C. Introducing Business Process Definition Metamodel (BPDM) as a modelling methodology based on UML supporting the view concept.

In the context of cross-organisational process models, the activities of each partner have to be clearly distinguished and single responsibilities as well as interfaces have to be defined. This requires a suitable graphical representation for CBPs that allows for modelling the process as one coherent end-to-end process, but still clearly shows which partner performs which action. Each swimlane contains activities performed by one participant of the process or additional information about the process. This concept is only about structuring the layout of models and does not offer a methodology to model processes. In addition it is methodology independent. It can be used in conjunction with different methods and applied in different tools.

For a successful integration, business partners have to model their interaction from a high level business point of view, independent of an underlying implementation. On the other hand they have to link their existing internal processes and resources to the agreed interaction model and offer process-oriented interfaces to the outside world. An important requirement in this context is to enable organisations to conceal its private processes to preserve autonomy and privacy. White-box exposition of internal knowledge, such as internal process steps, data, and resources cannot be expected.

However, successful implementation of cross-organisational business processes requires information sharing and exposing parts of the internal processes. The level of exposure can vary, and contracts with partners as well as trust building may lead to revealing more internal information as the business relationship develops. A particular interaction may require involved partners to adapt for the purpose of the communication. This adaptation can not necessarily be reflected in the partners' private (internal) business processes without inflicting their ability to interact with other partners in a different context. The decision about how much knowledge will be shared and which insight into the internal process is given, is clearly business-driven and made by process owners or managers. Managers and process owners decide about the context of the interaction with their business partner and define the first high level view of the CBP. This requires modelling techniques that support modelling of partner interaction from a business viewpoint and that allow for model-based information hiding and exposing, without involving coding. It is the intent that a process modeller can leave a private process unchanged and relate it to a process-based interface which can be adapted to interact in a specific collaboration.

The main idea of view-based modelling of CBPs is to introduce process views as an additional layer above the private processes of an organisation [16]. Process views provide a process-oriented interface between business partners. Private processes are only known to their owning organisation and not exposed to the outside world. Process views are an abstraction of the private processes, containing information that needs to be published for the purpose of a specific interaction. From a structural perspective, private processes consist of (private) tasks and (private) dependencies, whilst process views consist of view tasks (synonym: virtual tasks) and view dependencies (synonym: virtual dependencies). Several tasks of a private process can be combined to one view task. [17],[18]

Based on one private process, different views can be generated and thus they can reflect the specific requirements of multiple interactions. CBPs are then constructed by interweaving process views of different organisations [19]. By means of distribution and outsourcing, a CBP indirectly connects private business processes in a cross-enterprise business scenario. The inter-enterprise coordination thus builds on a distributed business process model where partners manage their own part of the overall business process. A CBP specifies tasks that each of the parties is required to perform as agreed in their contract. This is considered a promising concept to selectively hide details of private processes, whilst providing a process-oriented interface to facilitate the state-oriented communication

between trading partners. Furthermore, views allow for offering different perspectives on the same internal process when interacting in a different context.

4.3.4.2 Semantics required in workflow management

Semantics is a promising area that is expected to reconcile different business entities in several ways. First, and maybe the most important reconciliation aspect will be the data reconciliation. The application of this approach will make it possible to share information with the only constraint of having the same meaning rather than the same structure and data types. The semantics could be utilized in all the layers of a business process architecture. Firstly, they could be utilized so as to further enhance the data that are exchanged among heterogeneous information systems. Healthcare domain contains the most diverse information systems. So, data semantic enhancement could be of major importance for the successful interoperability between legacy healthcare information systems.

Additionally, semantics could be utilized for the enhancement of services. Each offered service by a healthcare organization could be semantically enhanced so as to be easily characterized and interpretable by an IT system. Finally, semantic enhancement is required between workflows. The metadata could be utilized for the characterization of workflows in order to be searchable, and machine interpretable.

4.3.4.3 Example Scenario

Mary Brown having health problems decides to visit a private diagnostic centre to have some laboratory tests. She visits the diagnostic centre and has a blood test. The diagnostic centre has a repository containing the Electronic Health Records and the Health History of its patients. Once the blood test is performed, a Clinical Decision Support System provides additional support to the Medical Doctor to diagnose the health problem of Mrs. Brown.

After the laboratory test results are gathered, it is decided that Mrs. Brown should be treated in a hospital. Her electronic health record, accompanied with the last results of the blood test, is forwarded to the appropriate hospital. Once Mrs. Brown arrives to the hospital, her personal health data are already stored in the repository of the hospital. Her admission is performed by the Hospital Information System, which is responsible for the whole treatment procedure.

Moreover, her health data are being used by the Clinical Pathway module of the hospital. The Clinical Pathway selector is responsible for the selection of the appropriate pathway of treatment according to her lab tests and results. The Clinical Pathway execution is performed and the Monitor module is being used in order to ensure the improvement of Mrs. Brown's health status and alert the Medical Doctors once any of the defined thresholds are passed.

During the treatment procedure, Mrs. Brown needs to take a Computer Tomography. Since the hospital she is admitted to does not have the appropriate equipment, she is moved to another hospital so as to have the examination. Once the CT is performed, the medical images are transferred to the hospital she is admitted electronically and securely, in order to be utilized by her medical doctors. In order to achieve that, cross-enterprise workflow management is established between the hospitals concerning the transfer of medical data.

Finally, once the treatment finishes and Mrs. Brown's health status improves she is able to leave the hospital. Once she is out, she begins the procedure of her reimbursement of the hospitalization costs. She visits her insurance company and presents the invoices of the hospital she has been admitted. The software modules of the insurance company check her eligibility, perform the reimbursement estimation and finally generate the reimbursement report. Mrs. Brown is reimbursed and healthy again.

4.3.5 Recommendations on clinical pathways, guidelines, DSS and workflows

The Member states should implement a central repository for the infrastructure, including clinical guidelines and clinical pathways, with a representation of the responsibilities of the actors and of the care mandates potentially involved. They should install a mechanism which keeps the infrastructure up to date – in a transparent and traceable way and make it human and machine searchable.

They should provide a mechanism to design the structure of clinical documents to be shared among healthcare professionals, according to the shared clinical pathways and guidelines, as well as to register the subsets of the coding schemes suitable for these clinical documents.

Possibly a list of the names of clinical documents and their sections required for the management of relevant clinical pathways should be adopted at National or European level, as well as the related coding schemes for events and kinds of contacts.

There is a need for an institution which defines and controls the interfaces to DSS, the needed input data, the expected output and the up-to-datedness.

4.4 Services and Features

4.4.1 Identity Management Services

4.4.1.1 Patient Identification Services

Patients may have records identifying them in more than one system in a National Healthcare Network or even in different National Healthcare Networks. In order to share patients' clinical data, the National and European Healthcare Networks must have a mechanism for identifying patients. These types of services resolve the identity of patients either from given partial demographic information or from given identifiers in different scopes (national unique patient identifiers, regional or local identifiers with matching mechanisms).

a) Within a Member State:

Member States can choose one of the two alternatives for patient identification according to their regulations about person identification. If it is possible to use unique identifiers, this is the simplest and the most effective way to implement patient identification services. The second alternative requires a more complex system. Each system in the National Healthcare Network may register the patients to regional or national master patient index registries with their own identifiers. The master patient index registries provide matching mechanisms between identifiers so that the patient identification is achieved. Another alternative can be using partial demographic information and matching algorithms for any kind of identification.

b) Across Member States:

Using partial demographic information and matching algorithms based on this information seems to be only possible way for patient identification across Member States since some Member States are not able to provide national identifiers because of their regulations. However, if a cross-border query is being made to just the home country of a patient where unique IDs are operational, then identification via the ID of patient is applicable as well. In order to provide more accuracy, a manual review can be required for matching patients across Member States.

Illustrative Scenario:

Dr. Martinez works for a clinic that has an EHR system connected to the National Healthcare Network of Spain. The National Healthcare Network of Spain is comprised of regional networks, each of which has a master patient index registry. Dr. Martinez has a new patient, Mr Bauer. Mr Bauer is registered in the EHR for Dr. Martinez's practice. The EHR system sends a new registration message to the regional network the system is located in, and the information is integrated into the master patient index registry. On Mr Bauer's next visit, he informs Dr. Martinez that he has records at a hospital in Germany and a clinic in Malaga which is connected to another regional network in Spain. Dr. Martinez makes an inquiry through the National Healthcare Network to obtain a copy of these records. As a first step in locating these records, the regional network (the one Dr. Martinez is connected to) reviews its master patient index registry to identify those that might be a match for Mr Bauer. No matching is found in current regional network. Then the National Healthcare Network is searched for possible matching, and one match is found in the master patient index registry of the regional network of Malaga. Dr. Martinez also wants to find the records in Germany. The Spanish National Healthcare Network updates the query so that master patient indexes given in the query is converted to partial demographic information specified for European Patient Identification Service. The service finds two possible matches that have identical information but different addresses. Both matches are displayed to Dr. Martinez who confirms the correct address with Mr Bauer.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging

- Authentication of the user and the system
- Secure transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.1.2 Patient Identity Matching Services

As mentioned in 4.4.1.1, in order to share patient data within and among National Healthcare Networks it is necessary to have mechanisms to match patient identities in the absence of a single national identifier. Even when an identifier may exist, there is a need for identifying common patients because existing systems may not have adapted to the identifiers, or identifiers are not fully synchronized.

There is no standard matching algorithm that can be adopted Europe-wide since such algorithms are highly sensitive to local characteristics of the data set being queried. For instance, an algorithm may provide better matches for Anglo-Saxon names than French names. Therefore, it is advisable not to specify algorithms for regional networks so that they can use or tune any algorithm for their local characteristics. The algorithms should give probabilities for matches and the minimum level should be calculated which decreases the number of false positives into very low values. Matches approaching but not reaching that level should not be returned to avoid incidental disclosures. Further, the non matching data elements should not be presented to avoid fishing.

4.4.1.3 User Identity Management Services

Management of user credentials including identifiers, demographics, and functional and structural roles is crucial for data privacy. Briefly, Identity Management facilitates a standardized means for organizations to share identity information and entitlements in a trusted fashion between organizations and exchange tokens that refer to specific users, their attributes, privileges in a secure and trusted manner. As a result, organizations have more complete information about the identity of the user so that they can use them in access management and providing accurate audit records.

Federated Identity Management is the most effective way to manage user identities in healthcare networks. Two main actors in Federated Identity Management are Identity Provider and Service Provider. The identity provider is responsible for the identity management of the user, including enrolment, provisioning, password management, and general account management. The service providers leverage their trust relationships to accept and trust information provided by an identity provider on behalf of a user, without the direct involvement of the user. This enables businesses to offload identity and access management costs to business partners within the federation.

Member States can construct an identity provider hierarchy where clinical organizations stand at the leaf level and regional or local identity providers stand on the upper levels. Together with a federated architecture, Member States can use centralized identity providers which provide some basic identity information like unique national professional identifiers, role certificates (e.g. license for doctors, etc). Identity Management across Member States requires national root identity providers for each Member State.

Illustrative Scenario:

Dr. Pierre is a general practitioner in France and his office system is connected to the Regional Healthcare Network of Rhone-Alpes. The Regional Healthcare Network uses Health Professional e-Identity card (such as the Sesame Vitale Card) to identify and authenticate the users. Ms. Amelia visits Dr. Pierre complaining of chest pain. She informs Dr. Pierre that she had been previously treated in the Brussels Medical Center for chest pain. Dr. Pierre determines that specific findings and historical EKG data from Ms. Amelia's prior encounters would be important in evaluating her condition. Therefore, he decides to query and retrieve the records from Brussels Medical Center over the European Healthcare Network. Dr. Pierre inserts his professional e-Identity card into the card reader connected to his computer and his clinical information system uses the credentials in the card to authenticate him to the Regional Healthcare Network of Rhone-Alpes. The Regional Healthcare Network hub, while routing the query to National Hub, constructs an assertion for Dr. Pierre including the credentials in the card and adding a profession certificate which indicates that Dr. Pierre is a legal doctor in Rhone-Alpes. The National Healthcare Network Middleware of France constructs a new assertion by mapping the identity information in the received assertion to the format specified for

European Healthcare Network and sends the assertion to National Healthcare Network of Belgium together with the query.

4.4.2 Data Services

4.4.2.1 Record Locator Services

The Record Locator Service locates health records within an RHN, NHN or within the EHN for a patient who has been successfully identified by the Patient Identification Service. The operation of the Record Locator Service depends on the Patient Identification Service. The Record Locator Service stores the location of health records residing in repositories and provides authorized users with information on where these health records are located. The user may be able to instruct the Record Locator Service to seek for health records within just a certain RHN or NHN instead of the complete EHN. Moreover, the user can make a record request to a specific NHN. As a result, the authorized user retrieves a list of locations that have records for the identified patient available, within an RHN, NHN and possibly from several NHNs; which is the EHN.

a) Within a Member State:

If a member state has a decentralized health network that is composed of RHNs, then each RHN will have its own Record Locator Service. Within an RHN, after the identification of the patient, an authorized user requests patient record locations through the EHR/PHR system. While doing so, the user is able to force the request to be processed only within the RHN or NHN.

In case of a location request within the RHN, the Record Locator Service returns the list of locations that have records for the identified patient available.

In case of a location request within the NHN, if the NHN is composed of RHNs, then the regional Record Locator Service of the patient communicates with Record Locator Services of other RHNs. According to the responses, the regional Record Locator Service compiles all the locations matching the user's request and the user retrieves those as a list. Otherwise, if the NHN is centralized, the national Record Locator Service directly returns the list of locations.

b) Across Member States:

If the user requests his/her location request to be processed Europe-wide, then this request is forwarded to the NHN through the EHR/PHR system. This is a direct forward in the case of a centralized NHN, whereas the request is forwarded by the Record Locator Service of an RHN in the case of a federated NHN.

The Record Locator Service of NHN distributes the request to Record Locator Services of other NHNs and asks for their health records for the identified patient. These NHNs complete their internal location processes as described for "Within a Member State" above. The Record Locator Services of other NHNs return a list of any record locations for the specified patient.

Finally, the national Record Locator Service compiles all the responses and provides the list of patient record locations to EHR/PHR system either through an RHN or directly.

Illustrative Scenario:

Mr. Mendez is admitted to a hospital for coronary artery bypass grafting surgery in his home town located in Spain. The National Health Network of Spain is comprised of regional networks. At the time of admission, the hospital EHR notifies its Regional Health Network that Mr. Mendez has a record in the hospital's system. After recovery, Mr. Mendez is discharged from the hospital. Then, Mr. Mendez proceeds with his routine visits with his General Practitioner, Dr. Martinez. In Mr. Mendez's first visit after the surgery, Dr. Martinez wants to see the health records of his patient related with the surgery. Dr. Martinez uses his EHR system to request Mr. Mendez's records from the hospital. Being in the same region, the Record Locator Service of the RHN searches its registry and returns the information that a record is available for Mr. Mendez at the hospital where he had surgery. Dr. Martinez requests the records about the surgery. Mr. Mendez says that he missed the last GP visit before the surgery because he visited his daughter in Malaga. Dr. Martinez wants to make sure that he has all the records about Mr. Mendez and makes an inquiry on the national level through its regional Record Locator Service. The regional Record Locator Service communicates with the national Record Locator Service of Spain for this purpose. However, no record is found in the Spanish NHN. Mr. Mendez mentions that the previous year, during a trip to Italy, he was treated for tachycardia in a hospital

where he had been taken by the tour organizers. This time, Dr. Martinez makes an inquiry to the EHN through the Spanish NHN to locate the records for Mr. Mendez in Italy. The Record Locator Service of Italy communicates with its regional Record Locator Services and sends a response to Spanish NHN indicating that there are records for Mr. Mendez at the hospital where he was treated the previous year. Dr. Martinez requests to retrieve Mr. Mendez's records from the Italian NHN.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Authorization of the user
- Identification of the patient
- Secure transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.2.2 Data Retrieval Services

The NHN (or RHN where applicable) enables patients/citizens to access their own records, and enables healthcare providers/healthcare professionals to view or access patient records within or across NHNs (that is, within the EHN). There are many policy problems that should be considered in this respect; such as the patient's consent to limit retrieval of data by some providers. The Data Retrieval Service should respect to all policy implementations.

When a patient or a professional requests health records, the location of the relevant records are determined by the NHN, those records are filtered according to the policy and patient permissions and the eligible ones are sent to the requestors. Data Retrieval Service should support retrieving a complete record or individual parts of it.

a) Within a Member State:

After successfully locating the records, a patient or provider requests data from a specific location through his/her PHR/EHR, namely PHR/EHR 1. This request is processed by the associated NHN. The NHN requests the data from PHR/EHR 2, which is the original source of the data. PHR/EHR 2 returns the data to the NHN and the NHN forwards the requested data to PHR/EHR 1.

b) Across Member States:

After successfully locating the records, a patient or provider requests data from a specific location through his/her PHR/EHR, namely PHR/EHR 1. This request is processed by the associated NHN, namely NHN 1. NHN 1 realized that request is made to a specific location outside NHN 1. NHN 1 requests the data from NHN 2, where the organization with the record participates. NHN 2 requests the data from PHR/EHR 2, which is the original source of the data. PHR/EHR 2 returns the data to NHN 2 and NHN 2 forwards the data to NHN 1. Finally, NHN 1 forwards the requested data to PHR/EHR 1.

Illustrative Scenario:

Mr. Mendez informs his GP, Dr. Martinez about his recent visit to a cardiologist about the coronary artery bypass grafting surgery he had before. Through his EHR, Dr. Martinez requests his RHN to retrieve these records. Both Dr. Martinez's EHR system and the cardiologist's EHR system participate to the same RHN. The RHN requests the records from the cardiologist and sends them to Dr. Martinez's EHR. Mr. Mendez also mentions the tachycardia treatment he had in Italy the previous year. Dr. Martinez makes a request to his RHN for these records. The RHN forwards this request to Spanish NHN. The Spanish NHN requests the records from the Italian NHN. The Italian NHN requests the records from the organization where the records are stored (here, if Italian NHN is composed of RHNs, then one more recursive step would be necessary). The Italian NHN receives the records and forwards them to the Spanish NHN. Spanish NHN forwards them to RHN where Dr. Martinez's EHR participate. Finally, the RHN returns the records to Dr. Martinez's EHR system.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Identification of the patient
- Provider Identity Service
- Access Management Services
- Error Handlers
- Secure Transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.2.3 Subscriber Services

The Subscriber Services identify subscribers who request notification of new information published to the EHN, and permit those subscribing entities to gather data through the Publisher Services. Patients can determine through their PHR systems that specific providers, their PHR and their relatives receive copies of all or parts of updates to their medical information. They can update their preferences whenever they want. An authorized physician may also subscribe himself/herself or his/her colleague. The NHN should store the list of subscribers for each patient through its Subscriber Services. The Publisher Services work in collaboration with the Subscriber Services in order to distribute the data to the patient's PHR and the specified providers based on patient preferences.

a) Within a Member State:

The patient manages the subscriber list and their privileges through his/her PHR. The necessary modifications are handled via the PHR interface. The patient indicates the PHR and specific providers that should receive copies of all or selected updates to their medical information. For the subscription process, the providers should be identified. The Subscriber Service collaborates with Provider Registry through the Provider Identity Service.

The updates are stored by the Subscriber Service of the NHN (or, needless to say, RHN if the NHN is a network of networks). The Subscriber Service also confirms the updates back to the patient through the PHR.

b) Across Member States:

The only difference with the "Within a Member State" case is that the patient opts to subscribe for providers from other NHNs this time. The Provider Identity Service of patient's NHN communicates with Provider Identity Services of target providers' NHN. When the providers are successfully identified in this way, the updates are again stored by the local NHN's Subscriber Service. The Subscriber Service confirms the updates back to the patient through the PHR.

Illustrative Scenario:

Mr. Murdock tracks the management of his own healthcare through a PHR application. Apart from his General Practitioner, two specialists are involved in his healthcare on a regular basis. After his regular visits with these physicians, they either prescribe new medications or tell him to continue with the existing ones. In order to ensure that each provider has access to his complete medication profile, Mr. Murdock uses his PHR to subscribe his GP, physicians and his daughter for any updates that can occur in his medication list. Moreover, Mr. Murdock also wants to ensure that his GP has a complete picture of his health status. Therefore, he subscribes his GP to receive any changes in his healthcare, such as copies of lab results ordered by any provider. These patient consent preferences are updated over the PHR that Mr. Murdock uses and confirmed by the NHN that Mr. Murdock participates. The subscribers' list and their preferences are stored by the Subscriber Service of the NHN.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Person Authentication
- System Authentication
- Provider Identity Service
- Access Management Services
- Secure Transport
- Non-Repudiation with Digital Signatures

4.4.2.4 Publisher Services

The Publisher Service is complementary to the Subscriber Service. When data is received by the NHN (could be sent by a laboratory, provider, clinical system, etc.), the Publisher Service of the NHN reviews the header of the data and, comparing with the patient's subscription preferences gathered via the Subscriber Service, sends the data to the patient's PHR and to the patient specified providers. The recipients could be within the same NHN (RHN) or in other NHNs.

The joint work of Subscriber Services and Publisher Services enables the patient and the providers an efficient and seamless way to gather health data. A publish-subscribe mechanism is much more effective than traditional poll-based services.

a) Within a Member State:

A clinical information system routes a message, such as lab result, through its associated NHN for delivery to the recipients. The Publisher Service of the NHN reviews the header of the data in order to identify the patient associated with the message. Then the Publisher Service reviews the patient's subscription preferences gathered via the Subscriber Service. The subscribers are identified and all of them reside with the NHN. The data is routed to the subscribed PHR of the patient and/or EHR of the providers.

b) Across Member States:

A clinical information system routes a message, such as lab result, through its associated NHN for delivery to the recipients. The Publisher Service of the NHN reviews the content of the data in order to identify the patient associated with the message. Then, the Publisher Service reviews the patient's subscription preferences gathered via the Subscriber Service. The subscribers are identified and one of the recipients resides in another NHN. The first NHN routes the data to the Publisher Service of the second NHN. Finally, the Publisher Service of the second NHN sends the data to the EHR/PHR indicated by the first NHN.

Illustrative Scenario:

Continuing with the scenario of the previous service, namely the Subscriber Service, Mr. Murdock makes one of his regular visits to his physician. The physician prescribes new medications for Mr. Murdock. This medication order is routed through the NHN. The Publisher Service of the NHN collaborates with the Subscriber Service and determines that the order for Mr. Murdock should be distributed to his GP, the two physicians and his daughter. The NHN routes copies of the medication to the providers designated by Mr. Murdock. At a later time, a copy of lab result for Mr. Murdock is also routed to his GP through the NHN, in the same way.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- System Authentication
- Provider Identity Service
- Access Management Services
- Secure Transport
- Data integrity checking

- Non-Repudiation with Digital Signatures

4.4.2.5 Data Routing Services

Sometimes the health record of a patient may need to be forwarded to multiple entities and during this process an NHN may need to determine the identity of the receiving organization and person. For instance, apart from the responsible physician, a lab result may need to be routed to another physician as a copy. The NHN (or RHN if applicable) will have to determine how to route the message, from the demographics information of the physician, the organization of the physician and the system in that organization as the target destination. The routing may appear within an NHN or across NHNs.

One critical point is that during the routing process the NHN has to conform to the access control permissions defined by the patient. It is also possible that the Data Routing Service of the NHN could not identify the recipient uniquely. This situation can be overcome by requesting the acknowledgement of the requestor. Then, after the recipient is resolved clearly, the data which could be medication records, lab results, patient summary records, etc. is routed to the recipient.

a) Within a Member State:

A clinical information system routes a message, such as lab result, through its associated NHN for delivery to the recipients. The Data Routing Service of the NHN reviews the content of the message in order to identify the recipients and their systems where the message should be sent. The NHN checks its Provider Registry through the Provider Identity Service and locates the records of the recipients within itself. Conforming to the patient's access control permissions, the Data Routing Service of the NHN routes the message to the identified recipients.

b) Across Member States:

Similar with the "Within a Member State" case, but this time the NHN could not successfully locate one or more of the recipients in its provider registry and determines that a designated recipient or system is associated with another NHN. The first NHN requests the second NHN to determine if the recipient matches a subject in its registry. After receiving the subject match event, first NHN forwards the message to second NHN for routing to the recipients. Finally, the second NHN routes the data to the EHR/PHR system of the recipient.

Illustrative Scenario:

Mrs. Larter makes a visit to his physician, Dr. Lee for a discomfort. For better diagnosis, Dr. Lee orders a laboratory test for her and together with the order, he also requests that a copy of the lab test results be sent to his colleague, Dr. Bennet, since he will be on holiday by the time the lab results are returned. Mrs. Larter goes to the lab and completes the tests. The lab results are electronically sent through the NHN that the laboratory participates to. In this case, both physicians and the laboratory participate to the same NHN. The result message indicates that both Dr. Lee and Dr. Bennet should receive copies of the test results. The NHN checks its Provider Registry through the Provider Identity Service and successfully locates records of both physicians. (At this point, if the NHN were not able to locate Dr. Bennet within itself, then it would have to make a query to the NHN associated with the healthcare provider where Dr. Bennet practices.) Since Dr. Lee is the one who ordered the lab test, there is no problem with the patient permissions. The lab results are sent to the EHR system Dr. Lee uses. However, the NHN has to check the access control permission of Mrs. Larter for Dr. Bennet. Luckily, before ordering the lab test, Dr. Lee informed Mrs. Larter about the situation and she gave Dr. Bennet the necessary permission. As a result, the NHN sends the lab results to the EHR system Dr. Bennet uses, too.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Authorization of the user
- Provider Identity Service
- Access Management Services

- Secure transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.2.6 Transformation Services

The RHNs, NHNs and the EHN will allow all healthcare providers and consumers to both share and access health records. However, the data is kept in many different formats in many different edge systems and it is not possible and not desirable to modify the schema and content of those records. In order to realize data exchange among different healthcare providers, the health networks provide a set of transformation services that will normalize the data format and make all of the standardized data elements into a semantically neutral form, as dictated by the legal entity which is responsible of the standardization activities within a health network. The transformation services also cover transformation of coding term standards used in clinical documents. Needless to say, translation of proprietary formatted data into standardized data elements is the responsibility of the participating healthcare provider. Support of the healthcare networks in this respect will enable European-wide interpretation of the health records by providing adapters for the varying number of well-accepted standards.

a) Within a Member State:

During a health record exchange, after receiving the request, the data source system PHR/EHR 1 sends the record to its associated NHN (or RHN if applicable). The legacy PHR/EHR 1 system uses a different health record standard than the one dictated by the NHN. The transformation services of the NHN convert the data to its native format. The receiver system, PHR/EHR 2 has a different format for health records, too. When sending the record to PHR/EHR 2, the transformation services automatically make the necessary converting. The data is successfully accessed by PHR/EHR 2.

b) Across Member States:

During a health record exchange, after receiving the request, the data source system PHR/EHR 1 sends the record to its associated NHN, NHN 1. The legacy PHR/EHR 1 system uses a different health record standard than the one dictated by NHN 1. The transformation services of NHN 1 convert the data to its native format. NHN 1 forwards the data to the EHN for delivery by NHN 2, the health network of the receiver system, PHR/EHR 2. The data is converted to the format accepted in the EHN level. NHN 2 gets the data. The receiver system, PHR/EHR 2 has a different format for health records, too. When sending the record to PHR/EHR 2, the transformation services automatically make the necessary converting. The data is successfully accessed by PHR/EHR 2.

Illustrative Scenario:

Mr. Mendez informs his GP, Dr. Martinez about his recent visit to a cardiologist about the coronary artery bypass grafting surgery he had before. Dr. Martinez's EHR system uses CEN - EHRcom (EN 13606) as the EHR content standard whereas the cardiologist's EHR system uses HL7 CDA. Both systems participate in the same NHN and the NHN has accepted EHRcom as its native format. Through his EHR, Dr. Martinez requests his NHN to retrieve Mr. Mendez's records from the cardiologist's EHR. The NHN requests the records from the cardiologist. Cardiologist's EHR system sends the records. The data is converted to NHN's native format EHRcom from HL7 CDA. Since Dr. Martinez's EHR also accepts EHRcom, the data is sent to Dr. Martinez directly.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Error Handlers
- Data integrity checking

4.4.2.7 Content Validation Services

The RHNs, NHNs and the EHN should be able to determine that an inspected message adheres to the transformation standards endorsed by the health network, if any; that is the message is properly formatted and contains valid and necessary data. If the message does not conform to the standards,

the Content Validation Service of the network reports the problem back to the sender of the data and interrupts the transfer of the message. Moreover, if there is a requestor of the data in the environment, it is also acknowledged with another error report.

a) Within a Member State:

The sender system, EHR/PHR 1 sends the message to its associated NHN. NHN's Content Validation Service inspects the message. If the message is valid, it is sent to receiver, EHR/PHR 2. Otherwise, the delivery of the message is interrupted, an error report is generated and sent to EHR/PHR 1.

b) Across Member States:

The sender system, EHR/PHR 1 sends the message to its associated NHN, NHN 1. NHN 1's Content Validation Service inspects the message. If the message is valid, it is passed to NHN 2, the health network of the receiver system. Otherwise, the delivery of the message is interrupted, an error report is generated and sent to EHR/PHR 1.

Illustrative Scenario:

Mr. Mendez informs his GP, Dr. Martinez about his recent visit to a cardiologist about the coronary artery bypass grafting surgery he had before. Dr. Martinez's EHR system participates in Andalusia RHN and the cardiologist's EHR system in Catalonia RHN. Through his EHR, Dr. Martinez requests Andalusia RHN to retrieve Mr. Mendez's records from the cardiologist's EHR. The Catalonia RHN requests the records from the cardiologist. Cardiologist's EHR system sends the records. The message is inspected by the Catalonia RHN and it is decided that the content of the message does not conform to standards. Catalonia RHN interrupts the delivery of the message. An error report is sent to cardiologist's EHR and another error report is sent to Dr. Martinez's EHR via Andalusia RHN as an acknowledgement. The error report is examined on the cardiologist's EHR side and necessary actions, such as notifying the product vendor of the defect, are taken.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Error Handlers
- Data integrity checking

4.4.2.8 Central EHR Storage Services

This service is necessary for the health networks that choose to implement centralized storage solutions. As it is explained in Section 4.1.1, in this architecture all data that is desired to be shared are maintained in a centralized repository. Entities in the network submit data to, and request data from, the central site and these functionalities are managed by the Central EHR Storage Services of the health network. Using this architecture at the European or even at the national level is not effective for storing complete EHRs of patients. This type of networks could be used at regional level especially to connect a number of healthcare organizations which has no storage capabilities in underserved regions.

a) Within a Member State:

The healthcare provider participating in an RHN uses its EHR interface to access and manage health records of its patients; there is no local storage capability. Through the interface, the physician updates a record and saves the action. The central repository updates the data and notifies the central registry.

In case of locating a record, the central registry is searched through the EHR interface of the healthcare organization. A list is returned in the same way and the physician accesses to the record he decides to retrieve.

b) Across Member States:

If a member state is using a centralized storage architecture, then the other member states which are exchanging health records will not discover the difference. All of the services that have been described so far behave in the same way and no interruption occurs. Within the internal course of the network,

the records are queried directly from the central registry; the retrieval and update of the records are realized directly on the central repository.

Illustrative Scenario:

Living in a rural area, Ms. Harper makes a regular visit to her GP, Dr. Davis working in the only primary care provider of the area. This rural area is participating in an RHN which implements centralized storage capabilities for its members. Through the EHR interface provided by the RHN (could be a web page or a desktop application) Dr. Davis requests the records of his patient Ms. Harper. Access to data is managed directly by the central EHR Service and the record is presented to Dr. Davis. After the usual check-ups, Dr. Davis prescribes a new medication list to Ms. Harper. This is updated in the central repository of the RHN and the repository notifies the central registry. Confirmation of update is received by Dr. Davis.

At a later time, an authorized physician participating in another RHN requests the records of Ms. Harper. The data is retrieved from the central repository of the RHN, not from the primary care provider.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Identification of the patient
- Provider Identity Service
- Access Management Services
- Error Handlers
- Secure Transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.3 PHR Services

4.4.3.1 Patient Access to Clinical Information and Audit Logs

Patient's access to their health information enhances the patient's ability to make well informed decisions about their healthcare and healthy lifestyles. Therefore, there is a need for Member States to allow the patients to access clinical information and audit logs of their data that were stored or processed through the National Healthcare Network. Secure PHR Systems can be the key enabler for patients to gather and share information with adequate safeguards. The following lists several business and technology models which provide PHR capabilities to the consumer:

- Web portals provided by commercial vendors, insurers, providers, or regional health organizations;
- Desk-top solutions with or without networking capabilities
- Centralized PHR solutions on a national level.

Realizing the patient access to clinical and audit information mentioned above is dependent on overcoming a number of issues and obstacles in today's environment. The major issue is authentication of patient into the healthcare network. Authentication can be solved by Federated Identity Management where the PHR system plays the Identity Provider role and authenticates the patient on behalf of the network.

PHR systems can be connected to the network either on national or regional level. As a node in the network, PHR systems enable the patients to query and retrieve any record about them in regional, national or European networks.

Illustrative Scenario:

Mr. Smith provided permission for his medical data to be shared via the European Healthcare Network. Now, he would like to know which data have been accessed or disclosed in the network. Mr. Smith uses a commercial PHR system which he has published as his legal PHR to National Healthcare Network of UK. The PHR system gives USB identity cards to its customers for authentication and provides a desk-top solution with networking capabilities. Mr. Smith logs in to his PHR by using his identity card and asks to view the access and disclosures of his data that occurred within the European Healthcare Network. Because Mr. Smith lives in Netherlands in the summer, his data are processed through two different National Healthcare Networks. Smith's PHR system sends a request for access and disclosure records to the National Healthcare Network of UK since it is linked to it. The National Healthcare Network queries its own records and other National Healthcare Networks to find access and disclosure records for Mr. Smith. The National Healthcare Network of Netherlands returns the access and disclosure records, where the records are forwarded to Mr. Smith's PHR. The PHR provides Mr. Smith with a display of his access and disclosure records for review.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Authorization
- Secure transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.3.2 Maintaining PHR

Patients may also want to have the ability to make their information available to their healthcare providers in ways which respect privacy and confidentiality. This data exchange requires that National Healthcare Network systems provide services that identify where the consumer's PHR data are stored and appropriately share the location with the healthcare providers. PHRs can include a variety of clinical and administrative information. Some of these include:

- Demographics/Registration Information
- Insurance Information
- Emergency Contact Information
- Medications and Allergies
- Laboratory Results
- Health Problems (using patients wording)
- Health Conditions (medical sensor/device readings, etc.)
- Diagnosis Codes
- Patient Consent

Member States may specify a core PHR dataset and enforce PHR systems to maintain the specified data. The starting point can be Registration Information. Medications, allergies and health problems should be also included in PHR.

Maintaining a PHR up-to-date is the major problem that should be overcome to assure accurate information any time. Publish/Subscribe services play a major role in this process. PHR systems can subscribe to the Record Locator Service that it is linked to. Then, when new information which is related with PHR (medication, allergy, etc) is registered to Record Locator Service, subscribed PHR system can be notified. However, intelligent filtering services are needed for Record Locator Service to match the subscription with the metadata of new information.

Illustrative Scenario:

Angelina is a 58-year-old citizen who has created a Personal Health Record using a portal that is provided by the Regional Healthcare Network of Lombardy in Italy. The PHR system stores the medication history and current medications which healthcare providers are able to access. The PHR system subscribes to Record Locator Service of Lombardy for records which include new medications on Angelina. Angelina has been treated for her cardiological problems and discharged two days ago with Discharge Summary report. As usual, the report is registered to Record Locator Service. It includes a 'Medications' section annotated with a terminology code. The subscription mechanism executes the filtering on metadata and finds out that the record includes a 'Medications' section. Therefore, it notifies the PHR system. PHR system retrieves the record, extracts the section and updates its internal database with the information. Now, Angelina experiences a heart attack and she is in an ambulance on the way to a hospital. The emergency personnel in the ambulance want to view current medications of Angelina. He connects to the PHR system of Lombardy by using his mobile device and accesses to current medications.

4.4.3.3 Consent Management Services

When sharing private data about a citizen, it is important that the citizen should be able to determine the access rights and privacy requirements for the shared data. Citizens may choose to limit the providers that may view the records within their PHR or EHR data that is shared among providers over the regional, national or European healthcare networks. The research problems in this respect include the following:

- How to integrate patient consent into a privacy infrastructure? How to map the rules in the patient consent into access control policies?
- How to propagate the obtained patient consents across distributed networks and how to manage the updates?
- How to apply existing rules to new data or how to enable citizens to dynamically define new rules for the new data?
- How to represent citizen consents? Is a high level specialized language or model needed? How to use the existing security, privacy and access control languages within this model?
- How to overcome citizen's lack of knowledge about the sensitivity of information, and the exact effect and meaning of privacy rules?

a) *Within a Member State:*

Although fine-grained access control is vital for privacy, not all users have enough knowledge for making access control choices at granular level for their own private data. Furthermore, some users may show little interest in such an access control. Being aware of these diverse requirements, it is advised that Member States implement layered, configurable, and easy-to-use consent management infrastructure.

The first layer can be determining an opt-in or opt-out model for a regional or national health network. The opt-out model can be suitable for a regional network, which means patients' information can be shared in the network unless the patient gives consent to forbid sharing. On the other hand, an opt-in model should be used for large National Healthcare Networks consisting of several regional networks since few patients have health related relationships in different regions. An opt-in model means that the patient would have to actively consent to having his or her information available via the network.

The second layer can be the management of consents which determines access control rules for a list of roles (e.g. general practitioner, researcher, etc) and confidentiality levels (general clinical information, sensitive clinical information, administrative information, etc) for information. The roles and confidentiality levels should be specified for National Healthcare Network as standards and patients should be able to give a consent that matches roles with confidentiality levels to restrict the access to their clinical information. In this layer, annotation of medical records with confidentiality levels can be done by the authors of records (e.g. doctors, etc) according to policies or guidelines specified for the National Healthcare Network.

After setting basic high-level consents for patients, management of consents for fine-grained and more specific information may be implemented. In this layer, PHR systems can be used to manage the patient consents. Since PHR systems are the interaction point with the patients, for any record or data that patient can view by using his/her PHR system, patients can define detailed and fine grained

consents. PHR systems can store these consents and serve them to other providers for access control processes.

b) Across Member States:

An opt-in model should be selected for European Healthcare Networks. In order to overcome interoperability problems about the role, confidentiality level and other related vocabularies between Member States, mapping services are required.

Illustrative Scenario:

Ali uses a PHR system which is connected to National Healthcare Network of Turkey. The PHR system also stores Ali's consent about sharing his PHR data. He accesses his PHR and requests to update his permissions. He has changed primary care providers and wants to remove his old provider and to add his new primary care physician. Ali adds the new primary care physician (functional role assignment) and grants this provider access to all of his records. A week earlier, Ali had a visit with an urologist. The PHR system notifies Ali that the report written by the urologist and lab results are ready. He reviews the report and lab results and realizes that he has contacted syphilis. He thinks that he should put restrictions for the report and the lab results. He annotates these records as sexual health data, and states that his sexual health data can only be accessed by his urologist. After a while he goes to his monthly appointment with his primary care provider, Dr. Can. Dr. Can queries the National Healthcare Network of Turkey to retrieve all reports about Ali created during the previous month. All medical records except the urologist's report and lab results are shown to Dr. Can.

4.4.4 Monitoring and Evaluation Services

4.4.4.1 Pseudonymization and Re-Identification Service

Sometimes, for research or monitoring purposes for instance, patient-identifying information must be hidden before data is shared among parties of the EHN. In these cases, the NHN or EHRs or PHRs is able to pseudonymize the private health data before sharing it for secondary usage. Moreover, there may be counter cases that require the re-identification of the pseudonymized data, e.g., when public health officials must contact a patient regarding a communicable disease. Again the NHN or EHRs or PHRs is capable of re-identifying the pseudonymized data for authorized parties. For this, the NHN reviews the request or re-identification and decides whether the requestor is authorized to receive the re-identified data. In the positive case, if the data is pseudonymized by NHN, then re-identification is done by NHN and the data is sent to requestor. If an EHR or PHR pseudonymized the data, NHN forwards the request to source system. The source system re-identifies the data and returns it to NHN. NHN forwards the re-identified data to the authorized requestor. In the negative case, no data is returned to the requestor, but an access right error.

a) Within a Member State:

An authorized secondary user requests that its associated NHN provides re-identification of a specific pseudonymized data. The NHN validates the authorization of the requestor, re-identifies the data and sends to the requestor.

If an EHR/PHR application pseudonymized the data, then the NHN forwards the request to EHR/PHR. The source system re-identifies the data and returns it to the NHN, which forwards it to the original requestor.

b) Across Member States:

An authorized secondary user requests that its associated NHN, namely NHN 1, provides re-identification of a specific pseudonymized data. NHN 1 validates the authorization of the requestor. NHN 1 forwards the request to NHN 2, which is the health network of the original source. NHN 2 re-identifies the data and forwards it to NHN 1. NHN 1 sends the de-identified data to the requestor.

If an EHR/PHR application pseudonymized the data, then NHN 2 forwards the request to the EHR/PHR. The source system re-identifies the data and returns it to NHN 2. NHN 2 forwards it to NHN 1. NHN 1 sends the de-identified data to the requestor.

Illustrative Scenario:

Avian-flu cases are being monitored on a European level by the help of the EHN. Instantly, when an incident occurs, an alert is sent to the correspondent public health administrator (i.e., Ministry of

Health) of the patient. Then, obtaining the administrative rights and the mandate to follow up emergent communicable diseases, the correspondent public health administrator requests the re-identification of the pseudonymized data. The request is forwarded to the original source that pseudonymized the data. The source verifies the authorization of public health administrator and returns the de-identified data. The public health administrator takes the necessary action.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Authorization of the user
- Error Handlers
- Secure Transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.4.2 Providing Data for Secondary Use

This service provides capabilities for the “Monitoring and Evaluation” requirement explained in Section 3.6. Upon the request by authorized parties, the health networks (RHNs, NHNs or the EHN) will support these secondary users by gathering data from source systems by invoking the necessary queries. The responsible network uses secondary users’ parameters to construct a query for the source system, i.e. EHRs and PHRs. The query requests the data that meets secondary users’ criteria. The source systems return the data to the responsible network, who forwards them to the authorized requestor. The Pseudonymization and Re-Identification Service that is explained in Section 4.4.4.1 is heavily used by this service.

It is desired that public health outbreak alerts are generated and announced automatically by the monitoring services of the health networks instantly. Bio-surveillance is again achievable by these services. A more general use case is collection of statistical data from the participating healthcare organizations by the appropriate authorities and decision-makers.

a) Within a Member State:

The NHN (or RHN if applicable) receives the request from the secondary user. The NHN verifies the authorization of the requestor, constructs the query based on requestor’s parameters and sends it to the PHR/EHR to obtain data meeting the selection criteria. The PHR/EHR examines its data, determines the ones meeting the criteria of secondary users and returns them to the NHN. The NHN provides the results to the secondary user.

b) Across Member States:

NHN 1 (or RHN if applicable) receives the request from the secondary user. NHN 1 verifies the authorization of the requestor. NHN 1 constructs the query based on requestor’s parameters and forwards it to NHN 2. NHN 2 sends a query to PHR/EHR 2 to obtain data meeting the selection criteria. PHR/EHR 2 examines its data, determines the ones meeting the criteria of secondary users and returns them to NHN 2. NHN 2 forwards the data to NHN 1. NHN 1 provides the results to the secondary user.

Illustrative Scenario:

Dr. Mylan, a researcher at a public health research institute, is monitoring the diabetes activities in her own country. She requests pseudonymized data on lab results for patients with diabetes who are older than 65, together with her authorization information. Her associated NHN examines the request and after deciding that Dr. Mylan and her institute are qualified for this type of request, it constructs the related query and distributes it to its participating source systems, namely EHRs and PHRs. The source systems return the data conforming to the criteria as a list of pseudonymized results. The NHN gathers the data from the source systems and makes a compilation. For those that are not pseudonymized, the NHN performs the pseudonymization. The compilation is then sent to the Dr. Mylan, for helping her in her research with diabetes monitoring in elderly.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Authorization of the user
- Pseudonymization and Re-Identification
- Error Handlers
- Secure Transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.4.3 Notification Services

The work by researchers, analysts and public responsible bodies may give birth to public or personal alerts that should be emergently distributed to source systems and people. For this reason, the RHNs, NHNs and the EHN have notification services that will ease the distribution of alerts and messages to target bodies. The alert may be a public health outbreak alert that interests everyone or a specific event for an individual. The service supports these kinds of individual or general delivery.

a) Within a Member State:

The researcher sends the alert to his/her associated NHN (or RHN if applicable) for delivery. NHN resolves the recipients; if it is an alert for a specific recipient, then the alert is forwarded just to that receiver. Else, the alert is forwarded to all EHR/PHR systems involved.

b) Across Member States:

The researcher sends the alert to his/her associated NHN (or RHN if applicable), NHN 1 for delivery. NHN 1 resolves the recipients and forwards the alert to NHN 2 for delivery. NHN 2 resolves the recipients; if it is an alert for a specific recipient, then the alert is forwarded just to that receiver. Otherwise, the alert is forwarded to all EHR/PHR systems involved.

Illustrative Scenario:

In parallel with the “Pseudonymization and Re-Identification” service scenario, notified by the case of avian flu, the public health officer notifies all doctors and hospitals of a certain district about the avian flu case and tells them to specifically look for patients with symptoms related to this disease and take the necessary precautions in handling these patients. The EHR systems of the doctors receive the message via Notification Service and display it to the interest of doctors.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user
- Authorization of the user
- Secure Transport
- Non-Repudiation with Digital Signatures

4.4.5 Management Services

4.4.5.1 Registries for Participating Organizations

There is a need for National Healthcare Networks to maintain information on each organization, network and system that participates in its information exchange. The Participating Organization Registry should assign a unique identifier for each system or organization that agrees to participate. The records in the registry may include: privacy policies of organization, entity demographics,

contacts, messages supported, capabilities and services. The identifier assigned to each organization/system can be used in each transaction in the network for system authentication as a complementary identifier. This identifier should not replace a national or regional identifier, if any. Participating systems can also search the registry to view the policies, services and capabilities of other systems that they want to interact with.

Illustrative Scenario:

The Vienna General Hospital has established an agreement with the Austrian state to participate in the National Healthcare Network. The Vienna General Hospital provides its registration data. After submitting the information, the registration data is reviewed and the registration is approved. The registry assigns a unique identifier to the hospital, and Vienna Hospital is informed that their system should use this identifier for interactions with the National Healthcare Network as specified in the network policies.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Authorization
- Secure transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.5.2 Registries for Healthcare Providers

Similarly, Healthcare Provider Registry can be implemented to store and provide healthcare professional's information. Stored information may be the unique identifiers given to each health professional in that region, demographics information, role information, certificates, etc. This information can be used in authorization procedures for the information exchange in the networks. It might also have the functionality as Yellow Pages for more detailed information (e.g. address).

Illustrative Scenario:

Dr. Damek is a family practitioner in Czech Republic and has already been registered to the Healthcare Provider Registry. Dr. Damek moved in a new office last week. Therefore, he wants to update his address and telephone information in the registry. He connects to the registry portal and provides the new information. Eliska wants to visit Dr. Damek because of her acne problem. She goes to the office but she realizes that Dr. Damek has moved away. She decides to use the Yellow Page service provided by her PHR portal which uses the Healthcare Provider Registry as information source. Consequently, Eliska retrieves the new address of Dr. Damek and visits the new office.

Required Security/Privacy Features:

The necessary security and privacy features can be listed as follows:

- Audit Logging
- Authentication of the user and the system
- Authorization
- Secure transport
- Data integrity checking
- Non-Repudiation with Digital Signatures

4.4.6 Privacy/Security Features

In this section security and privacy features that are common transactions between any system that sends or receives information to or through the Regional, National or European healthcare networks are described.

4.4.6.1 Audit Logging

In addition to preventive security, procedures need to be in place for the detection of security breaches and other misuse of data. Audit Logging is a widely recognised reactive security methodology that is used to retain the details of interactions in healthcare connectivity networks. Audit records may facilitate the detection of unauthorized actions, non-compliant behaviours and informing the patient about the medical or administrative actions related with his/her medical records.

While preventative security requires a high degree of standardization, so that everyone can, for example, use the same encryption scheme, reactive security requires less standardization. The main point is the ability to detect the events which should be logged according to policies. Therefore, the events that require audit logging for systems (e.g. EHR, PHR) interacting with National Healthcare Network and the middleware systems of National Healthcare Networks (e.g. record locator service) should be specified. Furthermore, the architecture of audit record repositories should also be determined such as centralized or distributed. If regional healthcare networks exist in a Member State, using regional audit record repositories where all edge systems connected to the regional network stores their audit records will be very useful. In this way, patient access to these audit records will be very easy. Otherwise, each health system can use its own repository and there is a need for federation to provide the patient a single view of audit records.

4.4.6.2 Person Authentication

All participating systems have to authenticate the user that is the direct user of a system before permitting access to Regional, National or European Healthcare Network functions. Furthermore, these systems should construct a federation, each of them acts as identity provider of its users and vouch for users to federation partners.

Authentication level is vital in the federation. A list of authentication methodologies, code lists for authentication levels and assignment of methodologies to strengths are necessary for National Healthcare Networks. Member States may also determine the acceptable authentication strengths that the participating systems are required to apply for its users who want to use National Healthcare Network. Similarly, acceptable authentication strengths may be specified for interactions on a European level. Certification of participating systems in this respect is very important to check the compliance of systems to authentication requirements.

4.4.6.3 System Authentication

For each transaction among systems in the National Healthcare Network, there should be a means for verifying that the systems that send and receive information are the systems they claim to be. In other words, a trust relationship should be established before any interaction between any systems. These trust relationships are proven at run time based on cryptographic techniques, including shared key encryption, public-key encryption, and digital signatures. Provisioning and sharing of these cryptographic entities can be provided by using the nation wide Participation Organization Registries.

4.4.6.4 Authorization

Authorization is the granting of rights, which includes the granting of access, based on permissions. Authorization cannot be reliably performed unless authentication has been performed on the user. An information sharing act in a Healthcare Network can be regulated by different policies based on patient consents, policies of participating organization and the laws or regulations of the specific jurisdictions in which the participants operate. Ensuring compliance with all these specified policies on information flow requires the following common capabilities in all the involved components:

- Participating organizations should take responsibility for accurately confirming the identity of all persons who use systems that can send and receive information through the EU Healthcare Network.

- Participating organizations should authenticate each user that can send or receive information through the EU Healthcare Network with a level of certainty at least as strong as that is specified for the network.
- Participating organizations should use specified User IDs (e.g. EU healthcare provider id) for its users which will be unique in the EU Healthcare Network.
- Standards that enable information flows through the healthcare networks should support the transmission of the user ID for all transactions performed on behalf of a user. They should also support the transmission of participating organization ID for all transactions.
- Standards should also support transmitting a description of the roles of users along with their unique identities.

4.4.6.5 Data Integrity Checking

Healthcare Networks should have the capability to prevent unauthorized alterations of messages sent to and through the network, and all alterations shall be logged. The receiver side shall be able to verify that the message has not been altered.

4.4.6.6 Error Handling

For each transaction or service among the systems participating the EU Healthcare Network, the possible event of errors should be specified. Furthermore, in the event of errors robust and informative information should be presented to systems or users.

4.4.6.7 Secure Transport

Transmissions between systems should be delivered confidentially and reliably. Encryption and secure channel standards should be specified in EU level.

4.4.6.8 Non-Repudiation

The standards used for exchanging messages shall ensure that the sender of such a message cannot reasonably deny that it was the source of the message. Similarly it should also include a means to ensure that once a participating system has received a message it cannot reasonably deny that it has received the message. Digital signatures and auditing systems are the main tools to ensure non-repudiation.

5 CONCLUSION

This document presents the final output of the RIDE Project, namely RIDE Roadmap III that is a distilled compilation of all the knowledge and experience gained while progressing with the RIDE roadmapping process.

RIDE Roadmap III first focuses on a high conceptual level and then concentrates on the necessary interoperability requirements:

1. Organizational Framework
2. Political and Legal Framework
3. Architectural Interoperability
4. Monitoring and Evaluation

For each of these requirements, the possible solutions are discussed and the principles are presented for the stakeholders. These principles are then mapped to the technical interoperability framework providing the core set and the additional set of functionalities for eHealth interoperability capable of exchanging information at the European level.

Within the technical details, available architectural models for the European Healthcare Network such as centralized, decentralized or federated ones; solutions and approaches for content level interoperability involving EHR interoperability and terminology interoperability; interoperability of

supportive systems such as decision support systems and clinical guidelines and finally the necessary and additional services/features of healthcare networks for eHealth interoperability are presented.

The most important recommendations of this roadmap can be summarized as follows:

- *Connected Health* should be anticipated by a cultural and organisational change that requires Continuity, Collaboration and Communication among actors, facilitated by innovators working closely with healthcare professionals and managers.
- It is advised that the European Health Network is built on a set of architectural principles that could favour the integration of existing/evolving national health networks and new developments.
- The previous investments of the member states that could be local, regional and national developments and/or eHealth strategies should be recognized. This is critical for assuring participation.
- It is advised that only the minimum number of protocols and functionalities essential to widespread exchange of health information are specified as part of the European Health Network (EHN).
- The deployment of the EHN can start with core services and can accommodate a modular structure for the possible future services of clinical data exchange and use. This could be considered as a “**plug-in**” based infrastructure.
- It is advised that the EHN is based on open industry standards for messages.
- An incremental process is essential for the deployment, where growing (in physical coverage) and evolving (increasing functionality) pilots are being developed.
- Interoperability of various EHR standards is better achievable if these EHR standards could be derived from a single, small but complete reference information model.
- European and international efforts towards standardization of biomedical terminology and electronic healthcare records should focus on an ontology that is able explicitly and unambiguously to relate coding systems, biomedical terminologies and electronic health care records (including their architecture) to the real world.

RIDE Project partners believe that RIDE Roadmap III will be of help to decision makers of Member States in the area of eHealth interoperability.

6 REFERENCES

- [1] R. Galvin, "Science roadmaps," Science, vol. 280, p. 803, May 8, 1998.
- [2] "Science and Technology Roadmaps", Ronald N. Kostoff and Robert R. Scahller, IEEE Transactions On Engineering Management, Vol. 48, No. 2, May 2001
- [3] Dossier Médical Personnel, <http://www.d-m-p.org/docs/EnglishVersionDMP.pdf>
- [4] OECD Privacy Guidelines, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
- [5] RIDE D2.1.4 - European Good Practices, http://www.srdc.metu.edu.tr/webpage/projects/ride/deliverables/RIDE_D2.1.4_EuropeanGoodPractices_v1.1.doc
- [6] New to SOA and Web services, <http://www.ibm.com/developerworks/webservices/newto/index.html>
- [7] RIDE D4.4.1 - RIDE Roadmap II, http://www.srdc.metu.edu.tr/webpage/projects/ride/deliverables/D%204%204%201RIDE-RoadmapII_v1.2interim.doc
- [8] ICT PSP Call 2007 Work Programme, http://ec.europa.eu/information_society/activities/ict_psp/library/ref_docs/docs/cip_ictsp wp.pdf
- [9] Campbell, H., Hotchkiss, R., Bradshaw, N., Porteous, M., 1998. Integrated care pathways. BMJ 316, 133-137.
- [10] Greiner, Ul., Ramsch, J., Heller, B., Löffler, M., Müller, R., Rahm, Er., 2004. Adaptive Guideline-based Treatment Workflows with AdaptFlow. Proceedings of the Symposium on Computerized Guidelines and Protocols, CGP 2004, Prague, IOS Press, 113-117.
- [11] Song, X., Hwong, B., Matos, G., Rudorfer, Ar., Nelson, C., Han, M., Girenkov, An., 2006. Understanding Requirements for Computer-Aided Healthcare Workflows: Experiences and Challenges. ICSE '06, May 20-28, Shanghai, China.
- [12] Colaert, D., 2007. Bringing the pieces together. Towards semantic interoperability in e-Health Workshop, RIDE Project, Brussels.
- [13] SWRL, <http://www.w3.org/Submission/SWRL/>
- [14] ATHENA project, Deliverable D.A2.1, "Cross-Organisational Business Process requirements and the State of the Art in Research, Technology and Standards"
- [15] "ATHENA European Integrated Project", 23.09.2005, www.athena-ip.org.
- [16] Liu, D.-R.; Shen, M., "Modeling workflows with a process-view approach", Proceedings of Seventh International Conference on Database Systems for Advanced Applications, Hong Kong, 2001, pp. 260 – 267.
- [17] Schulz, K.; Orłowska, M.E., "Architectural Issues for Cross-Organisational B2B Interactions", Proceedings International Conference on of Distributed Computing Systems Workshop, 2001, P. 79 – 87.
- [18] K.Schulz, Modelling and Architecting of Cross-Organisational Workflows, The School of Information Technology and Electrical Engineering, The University Of Queensland, Australia.
- [19] Chiu, D. K. W.; Karlapalem, K.; Li, Q.; Kafeza, E., "Workflow view based e-contracts in a cross-organizational E-services environment. Distributed and Parallel Databases", Volume 12, Issue 2-3, Dordrecht, 2002, pp. 193-216.