



DECIPHERPCP

FP7 – 288028

Framework Programme (FP) 7

ICT -2011.5.3

Patient Guidance Service (PGS), safety and healthcare record information reuse
Combination of CP & CSA

Deliverable D5.1 EHR-PHR interfaces and PHR platforms state-of-the-art report



DECIPHER “ EHR-PHR interfaces and PHR platforms
state-of-the-art report” by DECIPHER Consortium is licensed
under a Creative commons Attributions Share Alike 4.0
International License
(<http://creativecommons.org/licenses/by-sa/4.0/>)

FP7 – 288028
Framework Programme (FP) 7
ICT -2011.5.3
Patient Guidance Service (PGS), safety and healthcare record information reuse
Combination of CP & CSA



DECIPHER PCP

Work Package:
WP5 – European PHR Platform Specification & Reference Implementation

Deliverable 5.1
EHR-PHR interfaces and PHR platforms
state-of-the-art report

Version: 1.0

Status: Final

Date of Issue: 31 October 2013

File name: DECIPHER D5 1 PHR Platforms State-Of-The-Art V1 0.docx

Public

Document Information

Full title	Distributed European Community Individual Patient Healthcare Electronic Record			
Project Number	FP7 – ICT - 288028	Acronym	DECIPHER	
Start date Project	February 1st, 2012 (actual: January 25th, 2013)	Duration	48 months	
Project Coordinator	AIAQS Agència de Qualitat i Avaluació Sanitàries de Catalunya (SPAIN)			
Project URL	http://www.decipherpcp.eu			
EU Project Officer	Jaakko Aarnio			
Document History				
Date of delivery	Contractual: 31/10/13	Actual: 31/10/13		
Nature	Report			
Dissemination Level	Public (PU)			
Responsible Author	Jaakko Lähteenmäki	e-mail: jaakko.lahteenmaki@vtt.fi		
	Partner: VTT	Phone: +358 405149869		
Date	Version	Author	Change	Status
31.10.2013	1.0	J.Lähteenmäki	Final editions. Version submitted to Commission.	

Authors	Name	Partner
Main author	Jaakko Lähteenmäki	VTT
Co-authors	Rossana Alessandrello	AIAQS
	Giorgio Cangoli	Ancitel
	Maria Cristina Corradini	Ancitel
	Marie Jeannine Decool	AIAQS
	Ignasi Garcia-Mila Vidal	TicSalut
	Hannu Kaijanranta	VTT
	Juha Leppänen	VTT
	Montserrat Moharra Frances	AIAQS
	Anjeza Saliaj	Ancitel
Marius Spinu	ESTAV Centro	

Public

Keywords	cross-border health, mobile health, personal health record, healthcare interoperability
Abstract (for dissemination)	The DECIPHER PCP project (Distributed European Community Individual Patient Healthcare Electronic Record) is challenging the industry to develop a mobile health application (DECIPHER App). Support for cross-border health is a specific design target for the application. The application shall provide an up-to-date view of a person's health data and a tool for self-management of health. Particular challenges follow from the need for the application to connect with country-specific data health-data repositories and the need for automatic language translation. The pre-commercial procurement (PCP) model is applied for the procurement of the DECIPHER App. The model involves parallel development of several ideas, from which one or a few will eventually be selected for commercial procurement. The procurement will be carried out jointly by three procurers: TicSalut (Catalonia), Estav Centro (Toscana) and Trustech (United Kingdom). This state-of-the-art study provides technical background information for the development and procurement of the DECIPHER App.

Distribution List		
Date	Issue	E- mail
30/10/2013	Report to DECIPHER Team	Alessandrello, Rossana <ralessandrello@gencat.cat>; mc.corradini@cleliasnc.eu 'Marius Spinu' <marius.spinu@estav-centro.toscana.it>; f.tistarelli@cleliasnc.eu; bertagnini@ancinnovazione.it; "Giorgio Cangioli" <giorgio.cangioli@gmail.com>; 'Giada Mennuti' <g.mennuti@confindustriatoscanaservizi.it>; "Deed Richard (RW3) Trustech" <richard.deed@trustech.nhs.uk>; Patrick Mathieu, Jean <jpmathieu@gencat.cat>; 'Ignasi Garcia-Mila Vidal' <igarciamila@ticsalut.cat>; Suzan Ikavalko <Suzan.Ikavalko@culminatum.fi>; Kauko Huhtinen <Kauko.Huhtinen@culminatum.fi>; Sampol Mayol, Caterina <csampol@gencat.cat>; Maspons Bosch, Ramon <ramon.maspons@gencat.cat>; Moharra Frances Montserrat <mmoharra@gencat.cat>
31/10/2013	Report to EC and Project Officer	jaakko.aarnio@ec.europa.eu

Table of Contents

1	EXECUTIVE SUMMARY	6
2	INTRODUCTION	8
3	CROSS-BORDER ASPECTS OF PERSONAL HEALTH RECORDS	9
3.1	Cross-border health in Europe	9
3.2	DECIPHER cross-border PHR architecture	10
3.3	PHR as a global consumer product	12
3.4	Legal Aspects	14
3.4.1	Procedural Legal Aspects	14
3.4.2	EU directives for personal data protection	14
3.4.3	Regulatory requirements for Medical Devices	15
3.4.4	Healthcare-related legislation	16
3.5	PHR as part of the healthcare process	17
3.5.1	Need for PHR data in healthcare process	17
3.5.2	User identity in PHR and EHR	18
3.6	Language translation	18
4	EXISTING PHR SERVICES	20
4.1	Stand-alone PHRs	21
4.2	Tethered PHRs	22
4.3	Interconnected PHRs and ecosystems	22
4.3.1	HealthVault	23
4.3.2	Monitoring device ecosystems	24
4.3.3	Taltioni PHR platform	25
4.3.4	Validic	26
4.3.5	Personal Health Channel (Catalonia)	26
4.4	Mobile health applications	27
4.4.1	Chronic disease management	27
4.4.2	Sports and wellness support	28
4.4.3	Management and access of personal health information	28
5	EU STRATEGIES AND RTD ACTIVITIES	28
5.1	EU strategies and policy	28
5.2	epSOS	30

5.3	Calliope	30
5.4	eHGI	30
5.5	LOD2	31
5.6	Semantic Health	32
5.7	SemanticHealthNet	32
5.8	MovingLife	32
5.9	Antilope	33
6	STANDARDS AND OPEN SPECIFICATIONS	33
6.1	eHealth standards institutions	33
6.1.1	CEN/TC 251 – Health Informatics	33
6.1.2	Continua Health Alliance	33
6.1.3	Health Level Seven (HL7)	34
6.1.4	Integrating the Healthcare Enterprise (IHE)	34
6.1.5	ISO/TC 215 – Electronic Health Records	35
6.2	Connectivity	35
6.3	Clinical coding systems	37
6.3.1	Overview	37
6.3.2	Semantic interoperability aspects of DECIPHER App	38
6.4	Authentication	39
6.4.1	Authentication methods	39
6.4.2	Authentication and identity aspects of PHRs	42
6.5	Patient summary	43
6.6	Security and privacy	46
6.7	Accessibility	47
7	ACCESS TO THE EHR SYSTEMS OF THE DECIPHER PARTNERS	47
8	CONCLUSIONS	49
9	DEFINITIONS	51
10	ABBREVIATIONS	52
11	APPENDIX 1: EXAMPLES OF MOBILE HEALTH APPLICATIONS	54

1 Executive summary

The DECIPHER PCP project (Distributed European Community Individual Patient Healthcare Electronic Record) is challenging the industry to develop a mobile health application (referred as DECIPHER App in this report). Support for cross-border health is a specific design target for the application. The application shall provide an up-to-date view of a person's health data and a tool for self-management of health. Particular challenges follow from the need for the application to connect with country-specific health record systems and the need for automatic language translation.

The pre-commercial procurement (PCP) model is applied for the procurement of the DECIPHER App. The model involves parallel development of several ideas, from which one or a few will eventually be selected for commercial procurement. The procurement will be carried out jointly by three procurers: TicSalut (Catalonia), Estav Centro (Toscana) and Trustech (United Kingdom).

This state-of-the-art study provides technical background information for the development and procurement of the DECIPHER App. The objective of the DECIPHER architecture is to enable a set of basic functionalities as outlined in Section 3.2. Most importantly, the DECIPHER App requires access to Electronic Health Record (EHR) data residing in national health-data repositories. There are many challenges – both technical and privacy-related - in accessing the EHR records of patients (citizens) by other applications. Therefore applications accessing EHR systems are typically tethered – e.g. solutions provided by the national authorities and bound to particular EHR systems.

In the DECIPHER App a realistic approach has been chosen: the application is not connecting EHR systems directly, but relies on Personal Health Records (PHR's), which are already existing or being developed in different countries. Where available, also Patient Access services included in the epSOS infrastructure may be used to access health records. PHR's are increasingly connected with EHR's and are therefore attractive channels for accessing personal health data. The DECIPHER App shall include the necessary functionalities in order to connect with these country-specific services and exchange information with them as required by the addressed use cases.

Several EU-level activities addressing cross-border health are on-going. The most important activity, from the architectural perspective is the epSOS project, which has been able to define and demonstrate a working infrastructure for cross-border health. The Patient Access Service is highly relevant from the DECIPHER perspective especially since it provides a mechanism for automatic language translation. The epSOS project is ending by the end of 2013 and it is currently being planned how the development and deployment of the infrastructure will continue. The DECIPHER project shall closely follow epSOS and other related EU-projects in order to be informed about the plans concerning epSOS and its successors. Complementary mechanisms for language translation should be considered in DECIPHER to cover situations where epSOS interfaces are not available.

Mobile health applications are largely available for various areas ranging from personal wellness management to chronic disease management. Applications are most typically not connected to EHR systems, although also tethered mobile applications exist. Many apps support several

languages, but none of the found applications were known to support language translation mechanisms based on clinical codes. This functionality, to be included in DECIPHER App will evidently exceed the state-of-the art of current apps.

Existing PHR-platforms are increasingly available. Microsoft's HealthVault is most important of the commercial global platforms. It provides a technologically viable solution for connecting PHR's with clinical EHR data. So far, however, there is little evidence of existing operational usage of HealthVault for EHR-PHR integration. Anyway, since there are on-going HealthVault-based pilots in UK, it seems to be currently the most likely mechanism for accessing personal health data in UK. In Catalonia and Tuscany, there are regional services, which provide Patient Access to medical records. These services will be used by the DECIPHER PCP project.

Connectivity of health information between service components (PHR systems, EHR systems and related service components) is highly important. There are several existing standards addressing this area. Concerning Europe, most important are HL7 standards and IHE profiles. Concerning PHR interfaces, it seems to be most important that health information content follows HL7's Continuity of Care Document standard, since this is most widely applied in PHR systems and also eSOS compatible.

Usage of clinical code systems is important in order to enable semantic interoperability and automatic language translation of coded terms. This is another feature of DECIPHER App which is expected to exceed the state-of-the-art of current apps. The usage of clinical codes seems not to be common in current mobile applications based on the available information. Concerning EHR systems in Europe especially ICD-10, ICPC2 and ATC are widely used and should be supported. Additionally LOINC, which provides the main structure of the CCD file should be supported. The usage of SNOMED CT is considered by some European countries and may need to be supported at a later stage.

Authentication is an important functionality, which affects both security and user experience. Certificate-based mobile authentication (certificate on SIM card) are emerging in some countries, but are not yet widely available. While this is the case, it is likely that password based authentication is currently the best choice for mobile apps. Latest phone models are offering advanced technologies, such as fingerprint authentication, which can improve user experience while maintaining a high level of security.

2 Introduction

The DECIPHER PCP project (Distributed European Community Individual Patient Healthcare Electronic Record) is challenging the industry to develop a mobile application (referred as DECIPHER App in this report), which provides an up-to-date view of a person's health data and a tool for self-management of health. "Mobile application" in this context refers to software applications or browser-based applications designed to be used in smartphones, tablet computers or other mobile devices. Support for cross-border health is a specific design target for the application. The DECIPHER App will be purchased in the project through a pre-commercial procurement process. The specific use cases and functionalities to be supported by the DECIPHER App are defined in Deliverable 2.1 (Needs Assessment Report). The scope of this state-of-the-art study is to provide a review of technologies relevant for the specification and design of the DECIPHER App. The review also covers legal and other non-technical issues, which have impact to the technological and architectural choices to be made.

Despite of the prevailing globalization trends, health delivery systems and health records are still severely limited by national borders. The DECIPHER PCP project will take the challenge of leading the development of an innovative mobile application connecting with health records of different countries. As the healthcare infrastructures of different countries are variable, a flexible solution compatible with multiple standards and open interfaces is required. Moreover, legislation and rules concerning security and privacy are country-dependent and shall be carefully taken into account. DECIPHER will closely follow and interact with the on-going epSOS¹ project, which is developing and piloting an infrastructure for secure transfer of patient summaries between healthcare providers in different countries. The DECIPHER App will exploit the epSOS infrastructure when and where it is available. The application will be designed in the way which allows it also to be used independently of epSOS. The approach of the DECIPHER PCP project is based on the usage of Personal Health Records (PHR)² referring to health and wellness information stored in services under control of the individual.

A new approach is being applied also in the development and deployment of the DECIPHER App. The pre-commercial procurement (PCP) model involves parallel development of several ideas, from which one or a few will eventually be selected for commercial procurement. The PCP model is particularly targeted for radical innovations arising from the interactive and iterative design process. The DECIPHER PCP project covers three iterative development and testing phases, after which the participating procurers will be responsible for the commercial procurement actions.

This state-of-the-art study provides technical background information for the development and procurement of the DECIPHER App. In Section 3 we first provide a summary of the most important cross-border aspects, including the targeted architecture and legal aspects. Section 4 presents a

¹ www.epsos.eu

² Kaelber DC, Jha AK, Johnston D, Middleton B, Bates DW. A research agenda for personal health records (PHRs). *J Am Med Inform Assoc.* 2008;15(6):729–736.

review on existing PHR services including platforms and ecosystems as well as individual mobile health applications and services. In Section 5 we present a summary of related EU initiatives and RTD activities. Most relevant standards and open specifications concerning the DECIPHER App are covered by Section 6. The status concerning access to health records in each of the DECIPHER procurer-countries is summarized in Section 7. The conclusions of the study are presented in Section 8. .

The topics listed above are wide and it is not possible to provide an exhaustive review of all of them. Instead, the study has been focused to aspects, which are relevant concerning the overall architecture defined in Section 3.2 and the use cases defined in DECIPHER deliverable 2.1.

3 Cross-border aspects of Personal Health Records

3.1 Cross-border health in Europe

In the context of applications and services, the term “cross-border” is used in multiple ways. For example, “cross-border mobile payment” refers to a mobile application for carrying out payments by citizens of different countries to pay for goods and services in another country.

Cross-border health, in general, refers to the possibility of the citizen to use healthcare services abroad. The recent EU Directive¹ (2011/24/EU) addresses patients’ rights for cross-border healthcare. The directive provides clarity about the rights of patients who seek healthcare in another member state and supplements the rights that patients already have at EU level. According to the directive, a European citizen visiting another country should receive the same public healthcare services at the same cost as the local citizens insured in the country. In order to support the fulfilment of this right, the European Health Insurance Card (EHIC)² has been launched. It is issued in each European country by the national health insurance provider.

Closely related to the Directive (2011/24/EU) is the need for pan-European or global electronic identity. This problem is widely recognized. At European level the eHGI initiative has submitted Conclusions on “eID EU Governance for eHealth Services”³. Important work towards European level electronic identity is also being carried out in the STORK 2.0 project⁴.

In parallel with the legislative development, there is a need for standard-based information systems for cross-border transmission of health record data needed in care delivery. The epSOS project has defined and developed an infrastructure for the exchange of Electronic Health Record (EHR) data. The infrastructure is designed for secure exchange of the Patient Summary⁵, which

¹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF>

² <http://ec.europa.eu/social/main.jsp?catId=559>

³ http://www.ehgi.eu/Lists/Posts/Attachments/8/Conclusions_eID%20EU%20Governance_Copenhagen%202012%20-%20Approved.pdf

⁴ <https://www.eid-stork2.eu/>

⁵ http://www.epsos.eu/uploads/tx_epsosfileshare/D3.2.2_Final_definition_functional_service_requirements_-_Patient_Summary.pdf

provides the treating doctor with general information (e.g. name and gender) and the most important medical data about the patient (e.g. risks, allergies and surgeries).

Building on and complementing the epSOS infrastructure, the DECIPHER PCP project provides a cross-border health solution based on the utilization of Personal Health Records (PHR). PHR is a health record under direct control of the individual citizen. It includes both clinical and non-clinical data, which may have been transferred from information systems, such as EHR systems, or which may have been manually entered by the person, or which may have been directly transferred from health monitoring devices. While PHR's are directly controlled by the person, it is technically and legally more easily applied to cross-border use than the EHR. It is up to the individual PHR owner to decide about sharing the PHR contents with innovative applications, which may also support cross-border use. Moreover, the PHR may contain important pieces for non-clinical information, which does not exist in the EHR.

3.2 DECIPHER cross-border PHR architecture

The DECIPHER Needs Assessment report (D2.1) outlines a set of use cases to be supported by the DECIPHER App. The report also outlines the following functionalities needed to serve the use cases:

- F1 – secure access to the PHR from mobile devices
- F2 – possibility to edit/save PHR data
- F3 – possibility to generate epSOS compatible reports
- F4 – possibility to display / print reports
- F5 – translate capabilities (by using epSOS PAC or other available service)

The overall reference architecture for DECIPHER has been defined in the way that these functionalities can be fulfilled. The purpose of the overall reference architecture, depicted in Figure 1, is to provide a framework for the review of technologies in this State-of-the-Art study. The reference architecture does not include country-specific infrastructural services, such as authentication and authorization solutions. For the procurement, the DECIPHER project will need identify the interfaces indicated in Figure 1 in sufficient detail corresponding to the actually available services (e.g. PHR systems and translation services) in each country. It is important to note, that these services differ from country to country so that the DECIPHER App needs to incorporate support for different interfaces. A detailed architecture will be defined and included in the Call For Tender of the DECIPHER App.

As shown in Figure 1, the citizen has EHRs in his Country of Affiliation. The DECIPHER App connects with the PHR system and/or the epSOS Patient Access Service enabling access to the EHR records. The DECIPHER App provides functionalities for managing the personal health information contents. The functionalities include options to show data to the healthcare professional (HCP), print data on paper and transfer structured data via storage media, such as a USB memory. DECIPHER App may also send information through secure email or store it in cloud services. It is up to the citizen to decide about using these functionalities and about disclosure of personal health information to the HCP. In a typical case the mobile application consists of a client part

(mobile application or browser) and the server part. Also the application architecture, where the mobile application is directly connected with the PHR system is possible.

PHR systems may be publicly or privately provided services used in a particular country or globally. The epSOS Patient Access Service refers to a national mechanism enabling patient's access to the EHR and usage of epSOS semantic services for optional language translation¹. The PHR interface in Figure 1 shall support the exchange of Patient Summary content and other PHR information as relevant in the DECIPHER use cases. It is important to note that the PHR and PAC interfaces shown in Figure 1 are conceptual interfaces referring to a variety solutions available in different countries. Also the file interface is conceptual and refers to different physical interfaces. In the absence of epSOS /PAC, the DECIPHER App may also connect epSOS semantic services directly, if that option is available.

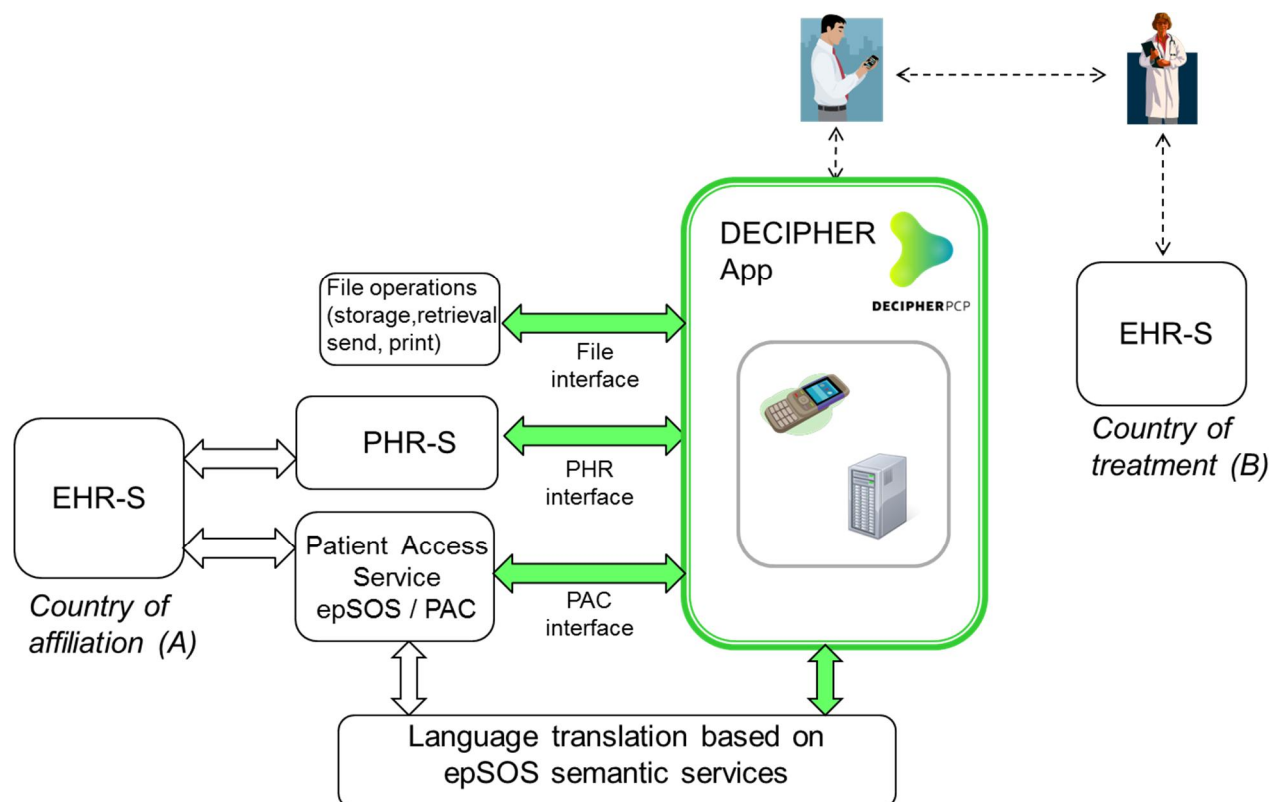


Figure 1. Overall DECIPHER cross-border PHR architecture.

Various types of PHR systems exist. Examples from the DECIPHER PCP project member countries are the Personal Health Channel (PHC) of Catalonia, the Patient's Access to the FSET (EHR) of Tuscany and the Taltioni PHR platform of Finland. In UK, the national Summary Care Record is currently available only for healthcare professionals, but local pilots using PHR's are ongoing².

¹

http://www.epsos.eu/uploads/tx_epsosfileshare/D1.4.3_EED_Services_including_specifications_for_all_services_01.pdf

² <http://www.uhs.nhs.uk/AboutTheTrust/Myhealthrecord/Myhealthrecord.aspx>

Also various types of commercial PHR services – not bound to a specific country and platforms – are available and can potentially be connected with the DECIPHER App. Different existing PHR solutions will be discussed in Section 4.

The availability of clinical data via the PHR depends on respective technical solutions in each country. Some PHR solutions (e.g. Sweden's "Health Account" in development¹) use Microsoft's HealthVault platform, which has an open Web Service interface. Also the solutions of Catalonia and Finland have open interfaces allowing their integration with the DECIPHER App. The status concerning PHR and Patient Access solutions in the DECIPHER PCP procurer countries is described in Section 7.

From the technical point of view the purpose of this state-of-the-art study is to review standards, specifications, technologies, platforms and products as relevant concerning the overall architecture of Figure 1. Important issues to be covered are:

- Existing PHR-platforms. These may be used as the PHR System of Figure 1 (Section 4.3).
- Existing mHealth applications. These cover similar functions as DECIPHER App and should be taken into account in the application design (Section 4.4).
- EU-level activities. Several activities are addressing cross-border health issues and shall be taken into account in selecting standards and technologies for the DECIPHER App (Section 5).
- Connectivity. Standards and open specifications applicable for exchanging health information (6.2).
- International coding systems and health information structures. These are essential in order to achieve semantic interoperability (Sections 6.3 and 6.5).
- Authentication methods. Secure, but user friendly authentication solutions should be identified for the the DECIPHER App (6.4).
- epSOS infrastructure. epSOS services are highly relevant concerning DECIPHER App and it is important to understand how they can be utilized in DECIPHER (Section Error! Reference source not found.).
- Access to EHR data. Solutions to access and retrieve data from the national EHR systems are essential for the DECIPHER App (Section 7).

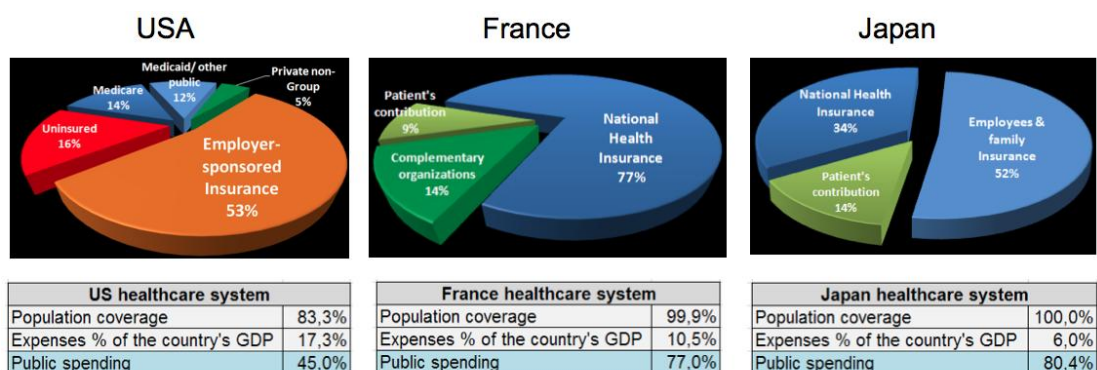
3.3 PHR as a global consumer product

Commercial PHR products emerged first in the USA and later on in the rest of the world. According to recent study by the GSMA Association and PWC² the worldwide mobile health revenue is expected to reach about US\$ 23 billion across all stakeholders – mobile operators, device vendors, healthcare providers and content/application players - by 2017. The study forecasts that monitoring services account for the largest market share - US\$ 15 billion by 2017.

¹ <http://www.dagensmedicin.se/nyheter/capgemini-fixar-halsokontots-it-plattform/>

² <http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsmapwctouchinglivesthroughmobilehealthreport.pdf>

PHR usage around the world seems to be related to the type of healthcare financing model. The Med-e-Tel study from 2012 (Figure 2) shows clear differences between the American, European and Japanese financing models.



- **USA: more than 100 PHRs** . Elsewhere: EHR pushed by gvts & few significant PHRs ...
- (30% free; 70% paid)
- 7% patients & PHRs online, 3.2% users

Figure 2. Healthcare financing models and PHR adoption (source: Med-e-Tel / 2012).

This analysis reflects the fact that the PHR market started in the United States and a favourable ecosystem has now been founded there. However, a worldwide expansion, seems conceivable.

The United States Government encourages the adoption of PHR as a structural element of health care¹ and promotes the choice from a wide range of systems both free and paid². One example of a successful and widely used service is Kaiser Permanente’s PHR which has around 4 million users.

The commercially available PHRs are already many in a booming market which increasingly requires professionalism and advanced services. General purpose products seem not to be economically sustainable in spite of a large number of users. For example, Google has already moved away from the PHR market by terminating its Google Health service.

The available PHR solutions are technologically heterogeneous and there is a lack of standardization in the PHR area, especially related to connectivity between EHR and PHR systems. For example, international coding systems covering all PHR data is needed for semantic interoperability. Currently, coding systems cover clinical data well, but do not cover data related to proactive health maintenance.

It is expected that multi-channel access to PHR will become the trend facilitating market consolidation and products of immediate daily use. This is mainly thanks to the access via mobile devices. This direction is followed by some applications recently introduced in the portfolio of the major players in the smart phone market.

¹ <http://www.medicare.gov/manage-your-health/personal-health-records/personal-health-records.html>

² <http://www.myphr.com/resources/choose.aspx>

3.4 Legal Aspects

The DECIPHER PCP project has two types of objectives that can be classified as (i) procedural and (ii) technical. Both objectives will face several legal aspects. Even if each DECIPHER PCP project partner has high level internal competencies on legal issues, such skills are basically limited at national level. Therefore, the consortium has decided to use European level legal support to be sure that all aspects will be correctly managed.

3.4.1 Procedural Legal Aspects

The European public bodies have to respect complex legislation for procurement. The legislation aims to guarantee:

- Good economic conditions
- Optimal operational path
- Impartiality for the supplier selection
- Fair competitiveness among competitors

Such rules are clearly defined by national laws and are also documented into European level guidelines. The European Directive 2004/18/EC addresses the coordination of procedures for the award of public works, supply and service contracts. The directive enlarges the application area at European level and highlights this by presenting three main principles:

- Community-wide advertising of contracts so that firms in all Member States have an opportunity of bidding for them
- The banning of technical specifications liable to discriminate against potential foreign bidders
- Application of objective criteria in tendering and award procedures

Those principles are required even in pre-commercial procurement, according to Commission's PCP Communication (COM(2007)799 & SEC(2007)1668)¹ – "Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe".

3.4.2 EU directives for personal data protection

The current data protection legislation in Europe is mainly based on the EU Data Protection Directive (95/46/EC)². The directive defines the basic principles to be followed by the register controllers responsible for maintaining repositories containing confidential personal data. It provides guidelines for the overall approach, e.g. by defining that "the controller must implement appropriate technical and organizational measures to protect personal data". The directive also defines the necessary conditions for transferring data to another country. The main requirement is that the recipient country ("third country") "ensures an adequate level of protection" of the personal data. This is typically interpreted (e.g. by the national legislation in Finland) at least to include all countries of the European Union. In general, the Data Protection Directive emphasizes

¹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:067E:0010:0015:EN:PDF>

² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF>

the power of the individual to decide about disclosure of the data. In case the data subject has “given his consent unambiguously to the proposed transfer” the transfer can be made to any third country.

Currently, EU activities are on-going towards General Data Protection Regulation (GDPR)¹. The new regulation will clarify the existing directive in several points. In particular, it will include more specific definitions related to data access by the data subject himself. For example, the personal data register controller is proposed to be obligated to release to the data subject his own data in a structured form which allows the data to be further used². This requirement is aligned with the citizen’s demands. Also the recent report of the eHealth Task Force “Redesigning health in Europe for 2020”³, highlights the needs to “liberate data”. Concerning, the objectives of DECIPHER, such legislation is welcome and will help in opening the access to clinical data in the EHR systems.

3.4.3 Regulatory requirements for Medical Devices

The Medical Devices Directive covers the regulatory requirements of the European Union for Medical Devices⁴. The original Medical Device Directive (MDD) (93/42/EEC⁵) has been later modified by directive (2007/47/EC⁶), which, for example, clarifies the coverage of software by the MDD. Concerning mHealth applications, two MDD classes are relevant⁷. “Class 1” refers to “medical devices” with low risk. In this case, a self-evaluation by the manufacturer according to the MDD requirements is sufficient. “Class 2a” refers to “low-medium risk medical devices”, in which case the evaluation has to be carried out by a specific external organization (“notified body”).

Products addressing the U.S. markets are subject to the regulations of the U.S. Food and Drug Administration (FDA)⁸. This FDA regulation shall be taken into account in addition to the European Commission Medical Directive. The FDA regulation was updated on September 25th 2013 to include mobile applications. According to the new released FDA guide:

“Many mobile apps are not to be considered medical devices and FDA does not regulate them. Some mobile apps may meet the definition of a medical device but because they pose a lower risk to the public, FDA intends to exercise enforcement discretion over these devices.(...) The FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient’s safety if the mobile app were to not function as intended. This subset of mobile apps the FDA refers to as mobile medical apps.”

¹ http://en.wikipedia.org/wiki/General_Data_Protection_Regulation

² http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

³ <http://www.president.ee/images/stories/pdf/ehf-report2012.pdf>

⁴ <http://ec.europa.eu/health/medical-devices/documents/guidelines/>

⁵ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0042:en:NOT>

⁶ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:EN:PDF>

⁷ <http://www.601help.com/Regulatory/mdd.html>

⁸ <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/default.htm>

Concerning both FDA regulation and MDD, it is important to review the intended use of the applications. “Intended use” means the medical purpose assigned to a product by its manufacturer through the label and promotional material.

In the case of DECIPHER App intended use could be described as below:

- Support the process of patient management (scheduling patient appointments, billing purposes)
- Systems intended to store, archive and transfer patient data
- Help patients (i.e. users) self-manage their disease or conditions without providing specific treatment or treatment suggestions
- Provide patients with simple tools to organize and track their health information
- Provide easy access to information related to patients’ health conditions or treatments
- Help patients document, show, or communicate potential medical conditions to health care providers
- Enable patients or providers to interact with Personal Health Record (PHR) or Electronic Health Record (EHR) systems.

Concerning the usage scenarios listed above FDA intends to exercise “enforcement discretion”, meaning that FDA does not intend to enforce requirements under the FD&C Act (Federal Food, Drug, and Cosmetic Act)¹.

Concerning MDD a specific guidance document² released by the EC, provides support for assessing if a particular software is covered by the MDD or not. According to the guidance document, storage, archival, communication, lossless compression and simple search are examples of functionalities which are not covered by the MDD. Instead, for example, software which includes diagnostic functionalities or provides automatic decision support in the context of healthcare is considered to be a “medical device”. Such decision support functionalities may be included in the DECIPHER App, in which case it would be considered as a medical device by the MDD.

Also, it is worth to highlight that if the DECIPHER App includes translation/transcoding services to make the patient data available, readable and understandable by all the professionals in all EC languages, the DECIPHER App will most probably qualify as medical device. In such case, specific quality assurance criteria will be added either to DECIPHER PCP tender specifications or to the subsequent public procurement of innovation initiative (in compliancy with ISO 13485).

3.4.4 Healthcare-related legislation

Legislation related to healthcare services is mostly national – the exception being directive 2011/24/EU concerning patients’ rights for cross-border healthcare. A considerable part of the national legislation is related to defining how individually identifiable health information shall be treated during the healthcare process, how it should be archived and how it can be transferred between organizations. Concerning the DECIPHER PCP project, the most relevant issue is how

¹ <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf>

² http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf

clinical information can be transferred from the health organizations' EHR systems into person centric PHR systems. Typically, legislation does not prevent transfers of clinical information as long as an informed consent given by the patient exists¹. This enables interfaces between EHR and PHR systems, which are important for ensuring access to personal health data for the DECIPHER App. After data has been moved to the PHR or the DECIPHER App, it is not anymore under responsibility of the healthcare service provider. Consequently, the specific healthcare-related legislation should not anymore be applied. For example, in case the patient displays or discloses PHR data to care personnel, the accuracy of the data should be evaluated by the care givers in the same way as a paper document or oral information received from the patient.

3.5 PHR as part of the healthcare process

3.5.1 Need for PHR data in healthcare process

Despite the differences among countries, in overall, EHR systems are quite well established. There is also an increasing number of activities for ensuring national availability of EHR data for healthcare providers. The main role of the PHR is to serve as an information repository for the individual person. There are still several situations, in which the health professional would need to access the PHR contents. For example, the following data groups may be valuable during a patient encounter or in order to follow-up the patient's status remotely:

- measurements (e.g. blood pressure) carried out at home
- self-assessment results
- lifestyle data (nutrition and physical exercise)
- clinical information (when not available in the EHR system - e.g. abroad)

From the health professional's viewpoint the usage of PHR data differs from the usage of EHR. Inaccurate data may occur in the PHR and the health professional shall evaluate the usefulness and reliability of the data before using it as a basis of care decisions. When data from the PHR is utilized in the care process e.g. as a basis of prescription, appropriate documentation should be made e.g. by copying a PHR extract to the EHR with annotations by the healthcare professional.

Application "prescription" is a new concept related to exploiting health and wellness applications in clinical care. Especially mobile apps are expected to be useful e.g. by enabling health monitoring at home and by motivating patients for healthier life styles. Application prescription is a "strong recommendation" for a patient to start using a particular application, with anticipated positive health outcome. The application prescription could also be connected with a subvention mechanism enabling the cost of the application to be paid by the healthcare payor (e.g. health plan).

Happtique² is offering an mHealth platform, which enables health service providers distribute mobile apps for their patients and staff. The service provider, e.g. a hospital, can establish a market place which contains a collection of "white-listed" applications for various purposes and

¹ <http://www.finlex.fi/fi/laki/alkup/1992/19920785#Pid1897893>

² <http://www.happtique.com/mhealth-platform/>

target users. The company also offers a Prescribing Tool which enables healthcare professionals to securely prescribe apps and other content for their patients.

3.5.2 User identity in PHR and EHR

In the EHR systems the patients are identified by their real name and person id. This identity is based on the national person identification systems, such as the social security number. In the global interconnected PHR solutions (such as the HealthVault), the users are identified by “online identity” (such as Microsoft Account or OpenID¹). Depending on the user’s choice, the online identity can be either anonymous or non-anonymous. However, even in the latter case a global PHR service provider does not have a practical way to verify the real identity of the user. Consequently, it is challenging to exchange information between a global PHR service and a national health service provider. Tethered PHR solutions (Section 4.2) avoid this problem as they allow the PHR to be based on a strong national authentication method and real person identity.

3.6 Language translation

Localization and internationalization refer to adapting computer software to different languages, regional differences and technical requirements of a target market. This kind of adaptation is an important part of application development targeting at global products. Concerning cross-border health applications there is a specific challenge related to the language translation of the health information content. Personal health information - either manually inserted by the individual or entered by the healthcare professionals – may be stored in different languages depending on the native language of the individual and the country where he is being treated. Translation of personal health information may be necessary if the individual is being treated abroad and the healthcare professional does not understand the language used in the patient’s health records.

In order to provide understandability of documents across languages and healthcare systems epSOS provides semantic services that allow to translate essential medical and administrative information within epSOS-compliant documents into the language of the data-consumer. This translation is performed according to the semantic framework represented in the following figure.

¹ <http://openid.net/>

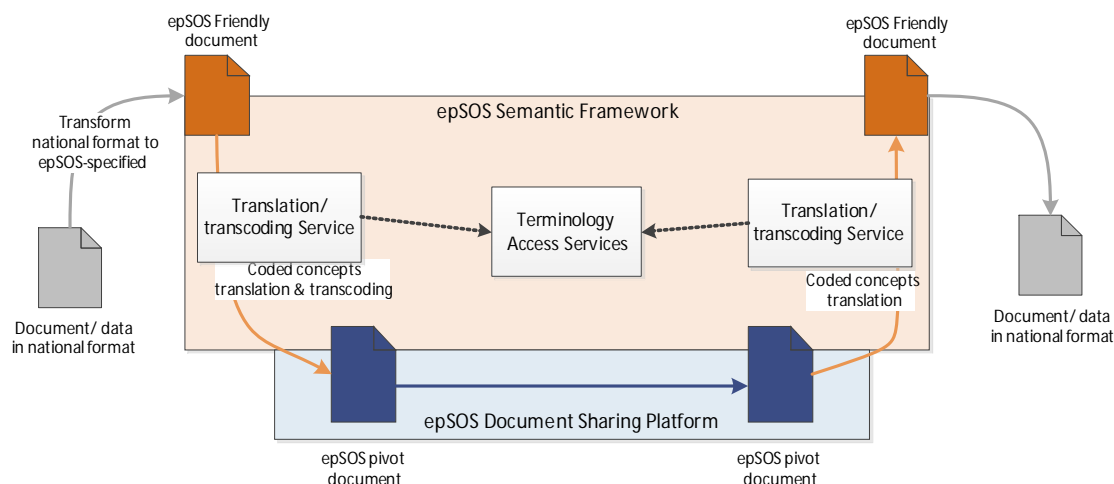


Figure 3. The epSOS Semantic Framework ¹.

A local document is transformed into a common syntactical structure based on the HL7 CDA standard; then transcoded (if needed) and translated into a common document (called epSOS pivot document) for being finally translated into the target country language (usually the country of treatment).

These activities are performed through the epSOS Semantic Services that can be divided into two main categories:

- The transformation services performing translation and transcoding
- The Terminology Access Services (TAS) providing functionalities for access to terminology repository or repositories.

Those services rely on:

1. The Master Value Sets Catalogue (MVC): a collection of Value Sets that includes terms used within certain parts of the epSOS pivot documents (e.g. parts describing the patient demographics or the clinical problems) based on standardized code systems such as ICD-10, SNOMED CT, ATC, EDQM and UCUM.
2. The Master Translation/Transcoding Catalogue (MTC) The epSOS Master Value Sets Catalogue contains, in addition to the original terms, their translation in different languages corresponding to the respective countries and the possible mappings (cross-referencing, transcoding) with other code systems that are used at the national level. The translation and the transcoding are under national responsibility.

The epSOS project will officially end on December 2013, with a six month extension for the piloting phase. After this date other European projects like the Trillium Bridge² (EU-US exchange of Patient

² <http://www.epractice.eu/files/Trillium%20Bridge%20-%20Catherine%20Cronaki.pdf>

Summaries) or e-Sens¹ are supposed to keep on using the epSOS semantic services, involving countries that are currently piloting in epSOS. Moreover - as project outcome - a set of Open Source Components have been developed by epSOS² and made available for usage, for allowing each country to build its own National Contact Point/semantic services.

However, the following elements need to be taken in account:

- Semantic sustainability issues have identified by the epSOS project itself (see the epSOS deliverable 2.2), including the well-defined scopes in which the epSOS translation services can be applied; issues that will be subject of other EU initiatives like the EXPAND project.
- Not all the countries involved in the DECIPHER PCP project are piloting in epSOS.

Considering that, in case the required translation services could not be covered by the epSOS services as they are applicable, alternative solutions will be evaluated.

In the case where epSOS semantic services are not available, DECIPHER language translation of coded terminology could also be carried out based on the availability of terminologies in different languages. Such functionalities are already built in the SNOMED CT³ and the same approach could be used with other code systems for which different language versions exist.

Another problem is free text, which is not translated even in the epSOS system. An interesting approach could be usage of automatic translation services^{4,5}. In such approach, it would be important to notify the risk of errors in the text and the original text should also be available for checking.

4 Existing PHR services

PHRs can be categorized depending on their connection with EHRs and other applications⁶ (Figure 4). Examples of each group are presented in the following sections.

¹ <http://www.esens.eu/home.html>

² This open source project is called OpenNCP and all the information about this project (including sources) are available under the <https://openncp.atlassian.net> platform.

³ <http://www.who.int/classifications/terminology/spackman.pdf>

⁴ <https://developers.google.com/translate/>

⁵ <https://datamarket.azure.com/dataset/1899a118-d202-492c-aa16-ba21c33c06cb>

⁶ <http://www.albertahealthservices.ca/org/ahs-org-ehr.pdf>

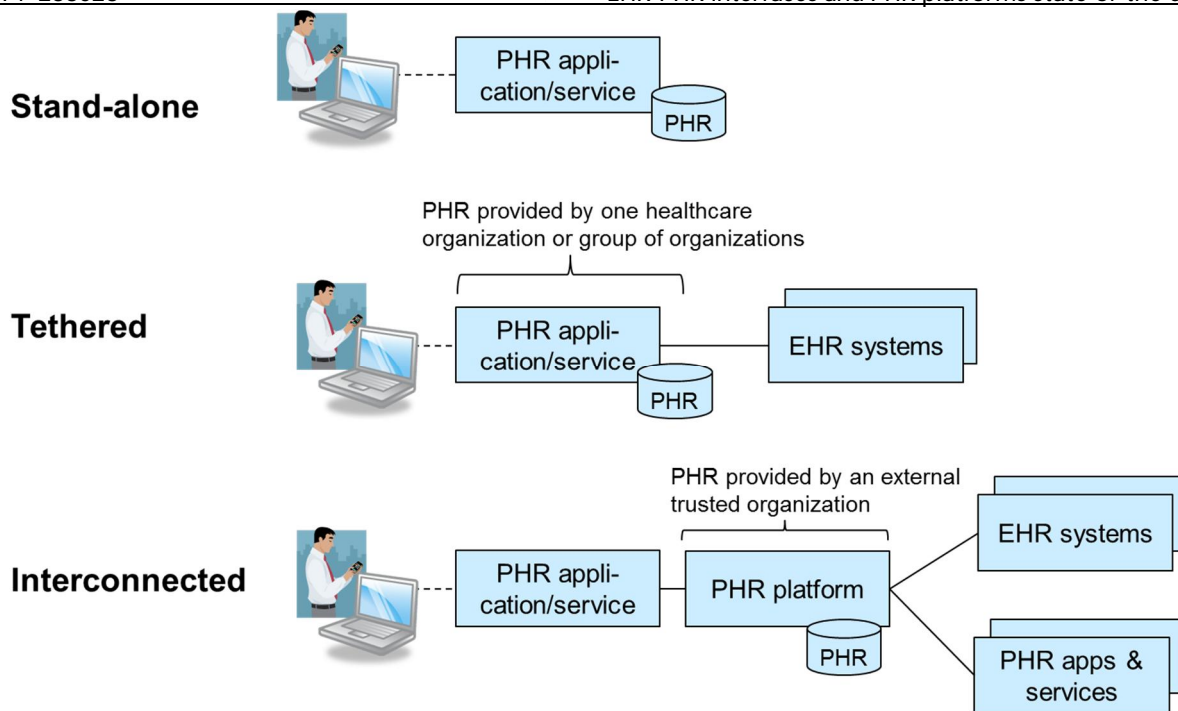


Figure 4. Categorization of PHRs.

4.1 Stand-alone PHRs

Stand-alone PHRs can be relatively simple, since the data is stored and maintained within one system. Stand-alone PHR applications may be connected with measurement devices, but sharing of measurement data e.g. with EHR systems is not possible. The disadvantage is the need for manual entry of clinical data. Therefore stand-alone PHR systems do have only limited value from the healthcare process perspective. Such systems can still be beneficial as they are easy to use and can support the patient in the organization of personal health data. Some examples of a stand-alone PHRs are listed below:

- World Medical Card¹ is originally based on a smart card where the doctors fill in patients' medical information. Currently also web-based storage is supported.
- WebMD² is primarily a service for accessing information health and diseases. The service also includes a PHR for storing and organizing personal health data.
- Vivaport³ is a multilingual, web-based PHR portal developed in the framework of the EU's ICT for Health flagship project.

¹ <http://www.wmc-card.com/>

² <http://www.webmd.com/>

³ <https://vivaport.eu/>

4.2 Tethered PHRs

Tethered PHRs are closely connected with one or several EHR systems owned by one or several health service providers. In this case, the PHR is typically provided by a health service provider or jointly by a group of service providers. For the health service providers, this approach is natural: the PHR stays in their direct control and the PHR service can be optimized to support the care process. For example, online services such as appointment booking and questionnaires can be easily provided in the same service context. The disadvantage of tethered PHRs is that they are bound to certain health service providers, and are available to the individual only as long as he continues to be the customer of the provider. In addition to health service providers, also some insurance companies are offering tethered PHR services.

Tethered PHR systems are offered by many health service providers in many countries. Concerning legacy EHR systems, the implementation of required interfaces can be laborious, but many new EHR systems are shipped with some online and PHR functionalities included. For example, the Epic EHR system comes with an integrated PHR solution MyChart¹, which allows the patients to access their medical records. The challenge of many tethered PHR systems is that they are usually not designed for interacting with other PHR's and PHR services.

4.3 Interconnected PHRs and ecosystems

Interconnected PHRs are truly patient centric. They are typically offered by some other organization than a health service provider. The individual may use the same PHR continuously and connect it with health service providers as needed. Furthermore, interconnected PHRs may be connected with a number of other PHR applications and services, thereby enabling new innovative services which combine health data from different sources. This way, ecosystems of interoperable services are expected to emerge.

Business ecosystem² is a community consisting of interacting organizations and individuals. The community provides goods and services of value to customers, who are themselves members of the ecosystem. Ecosystems typically evolve around one or more leader organizations. Good examples are ecosystems lead by large ICT product vendors, such as Apple, Google, Microsoft, Nokia and Samsung.

In healthcare, ecosystems are formed e.g. around Electronic Health Record systems which are marketed by large international software houses, such as Epic and Cerner. Software providers and medical device manufacturers are in partnership with the EHR system vendors in order to link specific components to the integrated EHR solution.

Concerning the needs of the DECIPHER PCP project, most relevant are ecosystems which are formed around interconnected Personal Health Records. Such ecosystems are targeted to creating value by supporting individuals in health management. Currently, the most important global ecosystem is Microsoft's HealthVault. There are also ecosystems such as Fitbit and Withings (see

¹ <http://www.epic.com/software-phr.php>

² http://en.wikipedia.org/wiki/Business_ecosystem

Section 4.3.2), which are specifically targeted to support health monitoring. Validic is a platform connecting information from devices and other systems of wider scope than only health monitoring. Interconnected PHR ecosystems targeted for the needs of specific countries have been recently opened. These include the Finnish Taltioni and the Catalan Personal Health Channel (PHC). One interconnected PHR service was provided by Google. The Google Health service, however, was terminated in the end of 2012.

4.3.1 HealthVault

The HealthVault¹ platform provides a secure infrastructure for storing and accessing personal health data and a mechanism for other companies to build health and wellness applications exchanging data with the platform (Figure 5). HealthVault helps people collect, store, and share health information with family members and participating healthcare providers. HealthVault connects with a variety of third-party applications and devices to help people manage their fitness, diet, and health data. The HealthVault developer pages² provide detailed instructions and tools (SDK's) for building HealthVault compatible applications and connecting them with the HealthVault platform.

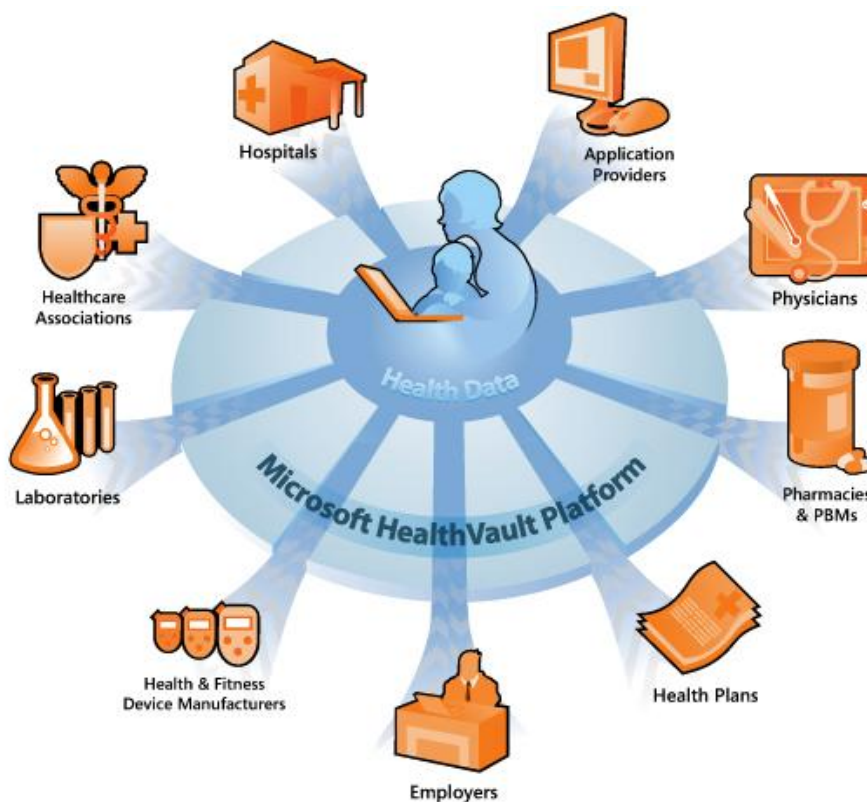


Figure 5. Microsoft HealthVault ecosystem.

¹ <http://healthvault.com>

² <http://msdn.microsoft.com/en-US/healthvault>

The HealthVault platform is available as a free and open service for individuals. Currently, there are two instances of the service: one in United States and another in United Kingdom. The user accounts are automatically allocated to either of the instances. The service user interface is available as mobile and web versions and in seventeen languages. Currently, the platform supports authentication based on Microsoft account, Facebook or OpenID.

As discussed in Section 3.5.2, the problem with the authentication methods referred above is that they are based on person's online identity and do not enable verification of the real identity of the person. In order to connect with EHR's, national authentication methods should be enabled. One customized PHR solution, based on HealthVault is currently being set-up in Sweden¹. This service ("Hälsokonto") will be provided nationally under control of the Ministry of Health and Social Affairs.

In Canada another HealthVault instance has been set up by the teleoperator Telus. The Telus Health Space service enables health providers to connect with the platform and provide health data to their customers' accounts.

4.3.2 Monitoring device ecosystems

The business model of monitoring device ecosystems is based on the customer buying a monitor device such as a blood pressure meter or scale. The customer is allowed to create a free account for handling and storing the monitoring data read from the device, on the service provider's server. The idea of the ecosystem includes an open interface through which other services than the original one may read or write the customer's monitoring or profile data. Such ecosystems have been provided by Fitbit², Withings³ and Zeo⁴, though the last one has been shut down in spring 2013. Fitbit products can monitor activity, sleep and weight. Withings products can monitor blood pressure, activity and weight.

The customer connects to the monitoring device by installable PC or mobile application, which conveys the data to the customer's account at the server. At the server, the user can view the monitoring data on a web dashboard solution. In addition to the original service provider there are several other listed service applications capable of accessing the same data. The API for accessing the data is open for new applications. The application developers will need to register their application in order to get the required application-id's. In order to get access to a specific customer's data the customer is directed through an authorization process, where s/he can accept or reject the new application's access rights. After success the application will have the appropriate user-id's. Authorization is typically based on the OAuth specification⁵. The application can then access the data by using the application-id's and user-id's. Data will be transferred in structured format, as XML or JSON. The monitoring services provide also the option for the other applications to get alarmed every time the customer updates the data on the server.

¹ <http://itivarden.idg.se/2.2898/1.506678/halsokontots-it-plattform-upphandlad> (in Swedish)

² <http://www.fitbit.com/>

³ <http://www.withings.com/>

⁴ <http://www.myzeo.com/>

⁵ <http://oauth.net/documentation/spec/>

4.3.3 Taltioni PHR platform

The Taltioni PHR platform¹ opened in the beginning of 2013 in Finland (Figure 6) and is available for free to all Finnish citizens. The service provider is a co-operative of 56 organizations representing private companies (software houses, integrators, wellness service providers, teleoperators and private health service providers) and public organizations (hospital districts, municipalities, research institutes and universities). The platform is categorized as an interconnected PHR service. It has been implemented by Medixine - a Finnish wellness company. The service is operated by Fujitsu under contract with the Taltioni co-operative.

Taltioni exposes an open interface based on Web Services standards enabling other services to connect and exchange information with the platform. Currently, six services have been connected to the Taltioni. The overall concept and technical interface is similar to HealthVault. The significant difference is that strong authentication methods are used. The Taltioni platform enables authentication by bank passwords (Tupas) or mobile certificates – both widely used mechanisms in secure online services in Finland. These methods are able to verify the Finnish person ID which means that exchange of information between Taltioni and EHR systems will be possible. In the case of one healthcare service provider (Terveystalo) lifestyle information from Taltioni is read to the provider's tethered PHR. Information flow – including clinical data - from the tethered PHR to Taltioni has been planned, but not yet implemented.

The open Taltioni interface includes a mechanism based on the OAuth2 specification, which enables the connecting service to be authorized access personal health data resources in Taltioni based on strong authentication. This mechanism enables applications to be authorised during the first session after which the resources can be accessed based on a stored security token without the need for renewing the authentication.

¹ <http://taltioni.fi>



Figure 6. Taltioni – Finnish PHR ecosystem.

4.3.4 Validic

Validic ¹ (USA) is a PHR platform providing a “one-to-many” connection to a variety of mobile apps and monitoring devices. The platform provides an open API which e.g. health portals can use for integrating data from different applications and devices use by the portal customers. Validic is carrying out the task of integrations on behalf of the portal providers, which may be an attractive model appreciated by the providers.

4.3.5 Personal Health Channel (Catalonia)

The Personal Health Channel (PHC) is a PHR service being developed since 2010. PHC enables the access to personal health information transferred from the regional EHR system, which contains clinical reports from different healthcare providers. It also includes information on diagnostics, vaccines and drugs prescribed, allowing to print the ePrescription drug plan. Some healthcare providers and medical device vendors have started to provide specific services through the PHC like counselling, appointment booking and chronic disease management support. PHC is a public service offered by the Department of Health of Catalonia. It can be categorized as an interconnected PHR, since it enables users to share their PHR data with external services included

¹ <https://validic.com/>

in the “market place” of the service. Authentication to the PHC is based on a software digital certificate or Digital ID in a smartcard. Currently, all the population in Catalonia has access to the PHC. About 30.000 users access it frequently.

4.4 Mobile health applications

Hundreds of applications have already been developed to address specific health needs. Mobile health apps can help to monitor health conditions, track medication schedules, locate a hospital or doctor, stick to a healthier lifestyle, and get access to various types of health information¹.

There are several options for categorizing mobile health apps. GSMA identifies categories in two application areas²:

- Solutions across the patient pathway (wellness, prevention, diagnosis, treatment, monitoring)
- Healthcare systems strengthening (emergency response, healthcare practitioner support, healthcare surveillance, administration)

For the purposes of this study, mHealth applications have been grouped as:

- Chronic disease management
- Sports and wellness support
- Management and access of personal health data

Mobile applications intended for direct use of health professionals are largely available³, but these are not in the scope of the study.

Annex 1 provides a listing of mobile health application examples.

4.4.1 Chronic disease management

A large variety of applications is available for supporting chronic disease management. In most cases these can be classified as stand-alone PHRs. In many cases, measurement devices can be connected wirelessly with Bluetooth. It is common, that manual entry of data is always possible, which enables the use of the application also in the absence of a Bluetooth compatible meter. Typically supported monitoring parameters are: blood pressure, blood glucose, weight, SpO₂ (oxygen saturation), peak expiratory flow and body temperature. Wireless connectivity is supported especially by several blood pressure meter models. Also Bluetooth-enabled blood glucose meters are available (e.g. GlucoTel), but they are less common.

¹ http://www.myphr.com/Resources/mobile_PHRs.aspx

² <http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsmawctouchinglivessthroughmobilehealthreport.pdf>

³ <http://www.blackpear.com/applications/myhealthfile/>

4.4.2 Sports and wellness support

Sports and wellness support is addressed by a large number of applications. The applications typically enable tracking of food intake, weight, daily activities, steps and heart rate. Sport-oriented applications allow the storage of location data e.g. for registering running routes. Steps can be retrieved directly from phone movements and GPS navigation is available in almost all modern phones. Several heart rate monitoring devices support transmission of data to mobile phones over Bluetooth. A typical approach to collect weight data is to use service platforms like Withings or Fitbit, so that direct connection between the phone and the weight scale is not needed. Withings and Fitbit devices are connected by WLAN to cloud services, where the data is accessible for the mobile application.

Many mobile wellness applications support connectivity with Facebook, Twitter and other social media services in order to meet the need for the users to connect with their peer groups and share data.

4.4.3 Management and access of personal health information

Mobile applications for management and access of personal health information are especially relevant for the DECIPHER PCP project. This group of applications greatly benefit from connectivity with health records. Many of the applications listed in Annex 1 are connected to HealthVault, which enables them to share data with other apps. However, the connection with HealthVault does not mean that the applications would have access to clinical (EHR) data. EHR data may be stored in HealthVault in some limited pilots, but not yet in large scale and in all countries. Therefore, in many cases it is still up to the user to enter personal health data to the applications manually. MyChart is a tethered mobile application connected with the Epic EHR system. So this app enables EHR connectivity to the – mostly US-based - users which have their medical records in the Epic system.

5 EU strategies and RTD activities

5.1 EU strategies and policy

EU has set the following goals concerning eHealth¹:

- to improve citizens' health by making life-saving information available – between countries when necessary – using eHealth tools
- to increase healthcare quality and access by making eHealth part of health policy and coordinating EU countries' political, financial and technical strategies
- to make eHealth tools more effective, user-friendly and widely accepted by involving professionals and patients in strategy, design and implementation.

Recent actions and recommendations targeting at these goals have been listed below.

¹ http://ec.europa.eu/health/ehealth/policy/index_en.htm

Defining and promoting open standards is a controversial issue even within the European Commission, with different Directorates. On May 19, 2010, the European Commission launched the Digital Agenda for Europe which is the EU's strategy to help digital technologies, to deliver sustainable economic growth. Especially, the Digital Agenda comprises 101 actions in 7 pillars. Pillar II: Interoperability and standards includes a set of actions for proposing legislation on ICT interoperability, promoting standard-setting rules, providing guidance on ICT standardisation and public procurement, adopting a European interoperability strategy and identifying means of requesting significant market players to licence information about products or services.

EU has also initiated the creation of the European eHealth Interoperability Framework (EIF)¹. The Framework has recognized the important contributions e.g. by epSOS for healthcare interoperability. The purpose of the framework is to lift the project-specific contributions to the EU policy level in order to utilise it for large scale deployment of eHealth Services under the Connecting Europe Facility.

The European Commission's eHealth Action Plan 2012-2020² provides a roadmap to empower patients and healthcare workers, to link up devices and technologies, and to invest in research towards the personalised medicine of the future.

Communication (COM(2008)689) from the Commission on "telemedicine for the benefit of patients, healthcare systems and society" to the European Parliament highlights the benefits and potential and encourages member states to deploy telemedicine systems in various areas of healthcare³.

The EU's recommendation on cross-border interoperability of electronic health record systems (C(2008) 3282)⁴ provides guidelines for interoperable electronic health record systems, allowing for cross-border exchange of patient data within the Community so far as necessary for a legitimate medical or healthcare purpose.

Commission health strategy for years 2008-2013 (COM(2007) 630 final)⁵ provides a framework and objectives to the European work on core health issues, on integrating health in all policies and on addressing global health threats. The strategy includes "Dynamic Health Systems and New Technologies" as one of its three themes.

The standardization mandate "403" of the 2009 ICT Standardisation Work Programme⁶ (01 May 2007) to the European Standardization bodies (CEN, CENELEC and ETSI) aims at agreeing on or recommending standards relevant to eHealth.

¹ http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/en_GB/-/EUR/ViewPublication-Start?PublicationKey=KK0113147

² <http://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century>

³ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0689:FIN:EN:PDF>

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008H0594:EN:NOT>

⁵ http://ec.europa.eu/health/ph_overview/Documents/strategy_wp_en.pdf

⁶ <http://ec.europa.eu/enterprise/sectors/ict/standards/work-programme/>

5.2 epSOS

The European Patient Smart Open Services (epSOS)¹ project (2008-2013) is a cross-border e-health system whereby patient records, prescriptions and insurance information could be accessed electronically regardless of where the patient was being treated in Europe. Europeans traveling as tourists, working in another country, or visiting another country as an exchange student would benefit from this interoperability and electronic health data access. Industry leaders from healthcare and information technology are involved. The initiative is adopting a general policy to employ already developed international standards whenever possible, including standards from HL7, WHO, ISO, and others.

Successful pilots demonstrating the capabilities of the epSOS infrastructure have been carried out in the project. The exact approach for establishing a permanent infrastructure for eHealth cross-border services is under development. The DECIPHER PCP shall closely follow this development and utilize the infrastructure as relevant. In particular, the translation services will be highly useful for the DECIPHER App.

5.3 Calliope

CALLIOPE² stands for “CALL for InterOPERability” with the focus on eHealth. CALLIOPE is a network of collaborating organisations mandated with the planning and implementation of eHealth. CALLIOPE has been initiated by 28 founding members comprising 17 organisations representing national governments, eHealth centres and 11 EU-level stakeholder organisations of health professionals, patients, health insurers and industry. CALLIOPE has now produced final results, in terms of a collaboration platform successfully applied and ready to migrate and be further developed in other initiatives. The relevance of CALLIOPE to the DECIPHER PCP project is with the Networking and Co-ordination activities - including build-up of stakeholder co-operation - and it can also support EU level co-operation of public entities. One of its main achievements has been the establishment of a trusted, efficient platform for collaboration of organisations representing different interests around a shared goal. The project has not produced standards (but a very useful standardization report) nor applications or services, but a Roadmap for eHealth Interoperability. This Roadmap, of course, can also be a factual basis for making decisions in the DECIPHER PCP Project.

5.4 eHGI

The eHealth Governance Initiative (eHGI)³ is working to establish a governance structure for eHealth within Europe in order to ensure continuity of healthcare both at home and across borders. It is achieving this through the development of strategies, priorities, recommendations and guidelines designed to deliver eHealth in Europe in a co-ordinated way.

¹ www.epsos.eu/

² <http://www.calliope-network.eu/>

³ <http://www.ehgi.eu/>

The Initiative seeks a strong coordinated political leadership and the integration of eHealth into national health policies through its links to the eHealth Network^{1,2} (established by the Article 14 of the EU cross-border directive). The network brings together national authorities responsible for eHealth on a voluntary basis to work on common orientations in the area and to promote an interoperable and sustainable eHealth implementation across Europe.

Priority Areas of the eHealth Network are:

- eID EU Governance for eHealth Services
- Semantic and Technical Interoperability
- Data Protection
- Patient Summary and Other Priorities

All these priority areas are highly relevant concerning the DECIPHER App and are addressed by this State-of-the-Art report. The outcomes of the eHGI initiative shall be closely followed in the DECIPHER PCP project.

5.5 LOD2

LOD2³ is a large-scale integrating project co-funded by the European Commission within the FP7 Information and Communication Technologies Work Programme. Commencing in September 2010, this project comprises leading Linked Open Data technology researchers, companies, and service providers (15 partners) from across 11 European countries (and one associated partner from Korea). The project aims at large-scale utilization of structured information enabled by the semantic web technologies, such as the Resource Description Framework (RDF). In particular the project aims at:

- Enterprise-ready tools and methodologies for exposing and managing very large amounts of structured information on the Data Web.
- A testbed and bootstrap network of high-quality multi-domain, multi-lingual ontologies from sources such as Wikipedia and OpenStreetMap.
- Algorithms based on machine learning for automatically interlinking and fusing data from the Web.
- Standards and methods for reliably tracking provenance, ensuring privacy and data security as well as for assessing the quality of information.
- Adaptive tools for searching, browsing, and authoring of Linked Data.

The DECIPHER PCP project is aiming at an application where personal health information will be handled in a structured and semantically interoperable form. The tools provided by LOD2 have a high potential in enriching personal health information through usage of external resources in the open internet.

¹ http://ec.europa.eu/health/ehealth/policy/network/index_en.htm

² http://ec.europa.eu/health/ehealth/docs/decision_ehealth_network_en.pdf

³ <http://lod2.eu/Welcome.html>

5.6 Semantic Health

The Semantic Health project¹ (2006-2008) developed European and global roadmap for research in health-ICT, focusing on semantic interoperability issues of e-Health systems and infrastructures². The roadmap provides considerations and recommended actions in order to improve semantic interoperability of clinical data. It covers especially the needs concerning Electronic Health Record systems and usage of terminologies and ontologies. The roadmap addresses, for example coding systems and proposes actions for harmonizing and cross-mapping of the various systems used in Europe. Also the evaluation of possible adoption of SNOMED CT in Europe is proposed. The roadmap provides important background information for the DECIPHER PCP project, for which harmonized code systems and EHR interoperability are of high importance.

5.7 SemanticHealthNet

Building on the Semantic Health and Calliope projects, the SemanticHealthNet³ project (2011-2014) will develop a scalable and sustainable pan-European organisational and governance process for the semantic interoperability of clinical and biomedical knowledge, to help ensure that EHR systems are optimised for patient care, public health and clinical research across healthcare systems and institutions.

Through a clinically-driven workplan, exemplified in cardiovascular medicine, SemanticHealthNet will capture the needs for evidence-based, patient-centred integrated care and for public health, encapsulating existing European consensus in the management of chronic heart failure and cardiovascular prevention. These exemplars will be cross-referenced with other domains and stakeholder perspectives. The project will generalise and formalise the methods and best practices in how to combine and adapt informatics resources to support semantic interoperability, and how these can be developed and supported at scale.

5.8 MovingLife

The MovingLife project (finalized in April 2013) has delivered roadmaps for technological research, implementation practice and policy support with the aim of accelerating the establishment, acceptance and wide use of mobile eHealth solutions that will support lifestyle changes among citizens and improve disease management globally.

The roadmaps addressed a broad group of fundamental issues such as: technology options for applications and services; options for new and improved medical guidelines; user empowerment, acceptance, ethics and privacy; socio-economic environments and policy and regulatory frameworks. In particular the deliverable D2.1 (State of Play in Mobile Healthcare) provides valuable input for the DECIPHER PCP project.

¹ <http://www.semantichealth.org>

² http://www.gencat.cat/salut/ticsalut/flashticsalut/pdf/145_2_semantic_interoperability.pdf

³ <http://www.semantichealthnet.eu/index.cfm/news/>

5.9 Antilope

Antilope EU-project¹ of the Competitiveness and Innovation Programme (CIP) builds on Calliope and epSOS projects and is participated by HL7, IHE and Continua. The project is working on defining use cases for several eHealth scenarios, and defining the standardised documents that are applicable and should be used in order to achieve interoperability.

6 Standards and open specifications

6.1 eHealth standards institutions

This section provides an introduction to the primary standards bodies and related industry organizations carrying out specific work related to eHealth standards. This is not an exhaustive list of standards organizations but is meant to cover the most important ones concerning the EU European standardization perspective and the DECIPHER project scope. A comprehensive eHealth standardization status analysis has been provided by the Calliope project².

6.1.1 CEN/TC 251 – Health Informatics

CEN/TC 251 is the health informatics technical committee of Comité Européen de Normalisation, the European Committee for Standardization (CEN). CEN primarily publishes standards that address application and content layer issues in e-health such as CEN/TS 15699:2009 “Health informatics – clinical knowledge resources – Metadata” and CEN/TS 15212:2006 “Health informatics – Vocabulary – Maintenance procedure for a web-based terms and concepts database”. Most of the committee’s standards address aspects of information representation, message standards, electronic health records, and some areas of communication specifications between medical devices. Part of the committee’s charge is to address the European Commission’s health interoperability mandate – Mandate 403.

6.1.2 Continua Health Alliance³

Continua Health Alliance is a non-profit, open industry organization of healthcare and technology companies joining together in collaboration to improve the quality of personal healthcare. With more than 200 member companies around the world, Continua is dedicated to establishing a system of interoperable personal connected health solutions with the knowledge that extending those solutions into the home fosters independence, empowers individuals and provides the opportunity for truly personalized health and wellness management. Interoperability of personal health and fitness devices is a primary focus of this organization. Some of the technology and healthcare companies included among founding members of this group include Cisco Systems, GE Healthcare, IBM, Intel, Kaiser Permanente, Motorola, and others. One of the objectives of this

¹ <http://www.antilope-project.eu>

² <http://www.calliope->

network.eu/Portals/11/assets/documents/CALLIOPE_D4_3_Standardisation_Status_ReportN.pdf

³ www.continuaalliance.org

organization is to develop “design guidelines that will enable vendors to build interoperability sensors, home networks, telehealth platforms, and health and wellness services”.

Continua Health Alliance does not consider itself a standards body but rather an alliance that works to identify gaps in interoperability that prevent interconnection among diverse health products and devices. This organization focuses on three areas of e-health. The first area encompasses technologies geared toward health and wellness, particularly for managing weight and preventing the diseases associated with obesity. Interoperability in this area focuses on weight scales, Internet fitness coaching, pedometers, fitness equipment, and related wellness systems. The second area focuses on chronic disease management and particularly health monitoring and diagnostic systems. The third focus area addresses the aging world population and devices geared toward assisted living for the elderly.

6.1.3 Health Level Seven (HL7)¹

Health Level Seven International (HL7) is a not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. These standards define how information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between systems. HL7 standards support clinical practice and the management, delivery, and evaluation of health services, and are recognized as the most commonly used in the world. HL7's 2300+ members – including technology companies (e.g. IBM, Microsoft, Oracle), health providers (Quest Diagnostics, Kaiser Permanente), pharmaceutical companies (e.g. Eli Lilly, Novartis, GlaxoSmithKline,...) and government agencies (e.g. FDA, NHS, Infoway, ..). It includes approximately 500 corporate members who represent more than 90% of the information systems vendors serving healthcare.

The scope of HL7's standards activities is large. Like many other standards organizations, HL7 is organized into Work Groups chaired by two or more co-chairs and responsible for defining some area of HL7 standards. Some of HL7's many Work Groups include: Electronic Health Record Work Group; Clinical Decision Support Work Group; Security Work Group; Patient Care Work Group; Structured Documents Work Group; Pharmacy Work Group; Regulated Clinical Research Information Management; Clinical Interoperability Council; Public Health and Emergency Response Work Group, Mobile Health and more. HL7's stated vision is “to create the best and most widely used standards in healthcare”.

6.1.4 Integrating the Healthcare Enterprise (IHE)

IHE² is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems

¹ www.hl7.org/

² <http://www.ihe.net/>

developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively.

The group gathers case requirements, identifies available standards, and develops technical guidelines that manufacturers can implement. IHE also stages "connectathons" and "interoperability showcases" in which vendors assemble to demonstrate the interoperability of their products. IHE develops and publishes integration profiles, each describing a clinical information need or workflow scenario. The integration profiles provide recommendations of how to use established standards in the particular case represented by the profile. Information systems conforming with the a particular integration profile address the need/scenario in a mutually compatible way.

6.1.5 ISO/TC 215 – Electronic Health Records

The International Organization for Standardization (ISO) establishes e-health standards through its Technical Committee 215, "Health Informatics". TC 215 has a wide scope in the field of Health Information and Communications Technology. The objective of the committee is to promote interoperability between independent systems, to enable compatibility and consistency for health information and data and to reduce duplication of effort and redundancies. ISO's 93 standards in "Health Informatics" address healthcare delivery, clinical research, public health, and prevention and wellness. To help convey the types of protocols ISO sets in this area, the following are the names of some of ISO's 93 published health information standards: Electronic reporting of adverse drug reactions; Archetype interchange specification; Security; and Interface specification. Part of ISO's activity in e-health involves the rebranding of specifications developed in other standards-setting institutions such as HL7.

6.2 Connectivity

The information exchange and the connectivity between different systems cannot be done without the definition of semantic and common clinical standards to ensure a uniform interpretation of the content of the clinical data at the medical event. International organizations such as as HL7 and IHE provide for the establishment of common semantic framework and clinical standards. These definitions are widely used in the development of healthcare ICT systems worldwide.

Specific initiatives exist addressing the issue of using mobile devices within the processes of care and treatment. HL7 has an internal Mobile Health Work Group that creates and promotes health information technology standards and frameworks for mobile health¹. Moreover HL7 defines and promotes FHIR - Fast Health Interoperable Resources² which represents a new generation of HL7 standard framework proposing components called "resources" that can be combined together to achieve low cost solutions including mobile phones, cloud communications, EHR-based data sharing, server communication in large institutional healthcare providers, and much more.

¹ <http://www.hl7.org/Special/committees/mobile/>

² <http://hl7.org/fhir>

The HL7 FHIR initiative has been welcomed in a positive way by the developer community, since it is expected lower the required effort for application design compared to existing HL7 V3 standards.

IHE has defined a profile MHD (Mobile access to Health Documents) for data access from mobile devices¹ which “defines one standardized interface to health documents for use by mobile devices so that deployment of mobile applications is more consistent and reusable”. The MHD profile reflects the more well-known IHE XDS profile (Cross-Enterprise Document Sharing) to cover simplified access to an XDS domain from mobile devices, considering the limited development potential that such devices require. In particular, the profile defines actors, transactions, and messaging between the actors themselves as in Figure 7.

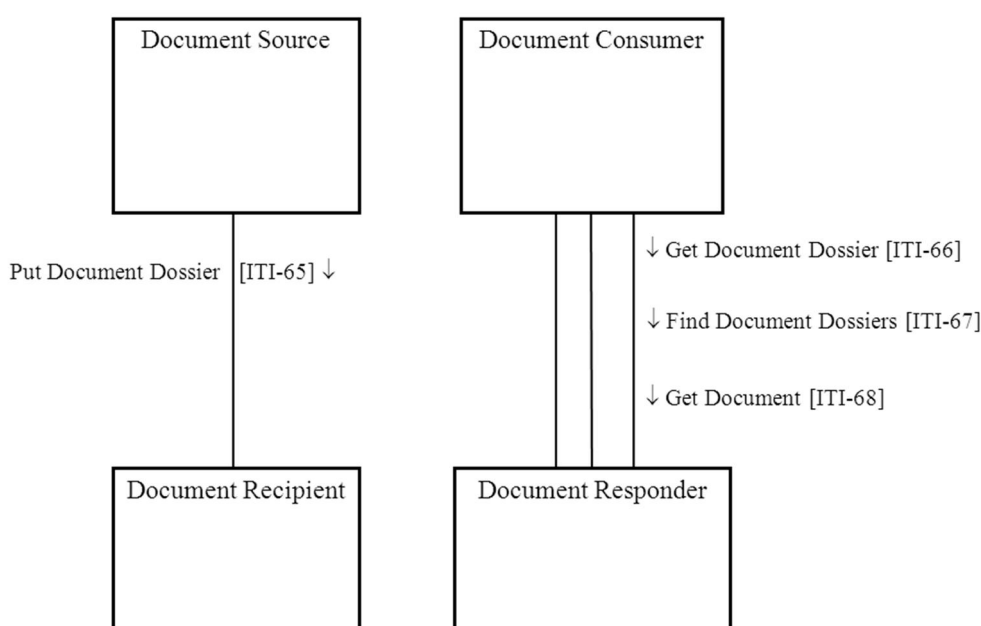


Figure 7. MHD Actor Diagram (IHE)

The epSOS infrastructure supports the document retrieval through the IHE XCF profile (Cross-Community Fetch), which defines a single transaction for accessing medical data between gateways. The XCF profile is applicable to the cross-border access of medical documents.

Concerning PHR’s, there is a need to exchange data via files, either stored on portable media or transmitted by email or other electronic means. The IHE XDM profile (“Cross-Enterprise Document Media Interchange”) addresses such needs. The profile is document format agnostic and defines how the files and the corresponding meta-data shall be organized when stored on media. Possible media types are for example CD-R, USB removable media and email with zip-attachment.

¹ [http://wiki.ihe.net/index.php?title=Mobile_access_to_Health_Documents_\(MHD\)](http://wiki.ihe.net/index.php?title=Mobile_access_to_Health_Documents_(MHD))

6.3 Clinical coding systems

6.3.1 Overview

Internationally agreed clinical codes provide the basis for cross-border semantic interoperability. Clinical coding systems are widely used and they cover well the various domains of clinical care and treatment. The semantic services of epSOS support the following coding systems¹ : EDQM, LOINC, UCUM, ATC, ICD, SNOMED CT, HL7 Code Systems and IHE vocabularies.

EDQM (European Directorate for the Quality of Medicines & HealthCare) is a directorate of the Council of Europe. Its aims are to protect public health by enabling the development, supporting the implementation, and monitoring the application of quality standards for safe medicines and their safe use. It provides standard terms related to medication prescriptions, covering dosage forms, routes of administration and containers used for medicines for human and veterinary use.

LOINC (Logical Observation Identifiers Names and Codes)² provides a vocabulary covering laboratory and other clinical observations. The coding system was developed and is maintained by the Regenstrief Institute, a US non-profit medical research organization

UCUM (Unified Code for Units of Measure) is a system of codes for unambiguously representing measurement units to both humans and machines. The code set includes all units defined by ISO, ANSI and HL7, but explicitly and verifiably addresses the naming conflicts and ambiguities in those standards to resolve them.

ATC (Anatomical Therapeutic Chemical Classification System)³ is classification pharmacological substances are divided into different groups according to the organ or organ system which they affect and their chemical, pharmacological and therapeutic properties. The code system is controlled by the WHO Collaborating Centre for Drug Statistics Methodology.

ICD (International Statistical Classification of Diseases and Related Health Problems) is the international standard diagnostic classification of diseases (signs, symptoms, conditions) for all general epidemiological, health management and statistics (death) and clinical use (health records). These include monitoring of the incidence and prevalence of diseases and other health problems. ICD is maintained by the World Health Organization (WHO).

SNOMED CT⁴ (The Systematized Nomenclature of Medicine Clinical Terms) is a systematically organized computer processable collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation and reporting. The nomenclature is used to provide a consistent language that enables a consistent way of capturing, sharing, and aggregating health data across specialties and sites of care. Compared to ICD, SNOMED allows to build more

¹ http://www.epsos.eu/uploads/tx_epsosfileshare/D3.5.2_Appendix_D_epSOS_Master_Value_Set_Catalogue_01.pdf

² <http://loinc.org/>

³ <http://www.who.int/classifications/atcddd/en/>

⁴ <http://www.ihtsdo.org/snomed-ct/>

expressive concepts by grouping together similar diseases and procedures and organize related entities for easy retrieval. SNOMED and ICD can be coordinated. For example the National Library of Medicine (USA) provides a mapping of ICD-9 and ICD-10 codes on the SNOMED nomenclature¹.

HL7 (Health Level Seven) standards (V2 and V3) include data types and vocabularies, which are relevant especially when using CDA documents and its derivatives.

IHE (Integrating the Healthcare Enterprise) has defined vocabularies supporting the IHE profiles².

The "Family of International Classifications"³ by WHO seeks to promote the appropriate selection of classifications for a wide range of healthcare settings⁴.

The FIC is divided into three reference classifications:

- International Statistical Classification of Diseases and Related Health Problems⁵ (ICD), which contains the most used health standards:
 - ICD-9 (9th revision, published in 1977);
 - ICD-9-CM (Clinical Modification, used in the US);
 - ICD-10 (10th revision, in use by WHO since 1994);
 - ICD-10-CM (Clinical Modification, used in the US);
 - ICD-10-PCS (Procedure Coding System, used in the US);
 - ICD-10-CA (used for morbidity classification in Canada);
 - ICD-10-AM (used in Australia and New Zealand);
 - EUROCAT - an extension of the ICD-10 Q chapter for congenital disorders;
- International Classification of Functioning, Disability and Health⁶ (ICF);
- International Classification of Health Interventions⁷ (ICHI) (previously known as International Classification of Procedures in Medicine).

6.3.2 Semantic interoperability aspects of DECIPHER App

The DECIPHER App needs to connect with various systems for retrieving health data. In order to properly combine information from different sources and in order to facilitate automatic localization of medical concepts it is extremely important that the data items are tagged with clinical codes. There are still several challenges in achieving semantic interoperability:

- Different code systems or local versions of them are used in different countries
- International coding systems cover essentially clinical information (not all PHR information)
- Utilization of clinical codes may lead to poor usability in a mobile application

¹ http://www.nlm.nih.gov/research/umls/mapping_projects/snomedct_to_icd10cm.html

² http://wiki.ihe.net/index.php?title=PCC_TF-2/Namespaces_and_Vocabularies

³ <http://www.who.int/classifications/en/>

⁴ http://en.wikipedia.org/wiki/WHO_Family_of_International_Classifications#Other_medical_classifications

⁵ <http://www.who.int/classifications/icd/en/>

⁶ <http://www.who.int/classifications/icf/en/>

⁷ <http://www.who.int/classifications/ichi/en/>

Concerning the needs of the DECIPHER App, the code systems listed in Table 1 seem to be most relevant. These code systems are in wide use by the DECIPHER procuring countries and are proposed to be used by the DECIPHER App. Country-specific implementations of these code systems may exist. The original versions maintained by WHO (for ICD-10, ICPC-2 and ATC) and Regenstrief Institute (for LOINC) should be used instead of country-specific variants where possible.

Table 1. Clinical code systems proposed for DECIPHER App

Code system	Description	Languages
ICD-10	Classification of diseases and health problems	Translated to 42 languages (incl. English, Spanish and Italian)
ICPC-2	Classification of diseases and health problems for primary care	Translated to 19 languages (incl. English, Spanish and Italian)
ATC	Classification of drugs	Several (including English, Spanish and Italian)
LOINC	Identification of laboratory and clinical observations	Translated to 6 languages (incl. English, Spanish and Italian)

The clinical code systems provide little support for identifying concepts related to wellness activities, such as life-style monitoring. In such cases the DECIPHER App should use other openly available vocabularies where possible. Some wellness-related code systems already exist and their usage in DECIPHER App should be considered. An example of such systems is the Compendium of Physical Activities (University of Minnesota) which provides a classification of physical activities by rate of energy expenditure¹.

While the use of coding systems is essential for semantic interoperability perspective it is important to maintain good usability. Usability may be degraded e.g. when vocabularies need to be downloaded or updated during a slow internet connection. This kind of aspects should be taken into account in the application design.

6.4 Authentication

Authentication of the end-user is needed in order to control the access to the DECIPHER App, which contains medical records and other personal information.

6.4.1 Authentication methods

Table 2 lists currently used approaches for authentication in web applications, such as PHRs and PHR based services.

¹ <http://www.ncbi.nlm.nih.gov/pubmed/8292105>

Table 2. Approaches for end-user authentication

Method	Usage	Examples of standards / defacto standards / products	Advantages	Disadvantages
Service specific username and password	Widely used in global internet services.	Basic or form-based authentication (over HTTPS), Digest authentication.	Simple implementation.	Password difficult to remember. Not a strong authentication method.
Federated web-authentication based on username and password	Widely used in global internet services, especially in social media services.	Google (OpenID), Microsoft account, Facebook	Simple implementation. User-friendly (same password for many services).	Not a strong authentication method.
Challenge question / response	Used as an additional security measure typically in the context of username/password authentication.	-	Simple implementation.	Provides additional security to other methods, but is not secure enough as the sole method.
One-time passwords	Widely used in online services with high security demand e.g. in network banking.	Mostly national (e.g. TUPAS in Finland) and proprietary (e.g. SecurID).	Misuse of password is difficult as it is constantly changing.	More elaborate to use compared to username/password
Smartcard PKI authentication	Widely used in national services.	PKCS #11, X.509	Strong authentication method.	Efforts needed for acquiring the smart card and smart card reader.
Mobile (SIM-card) PKI authentication	Some implementations exist (e.g. Finland)	ETSI-MSS, X.509	Attractive for mobile apps with high security demands.	Not yet widely in use.
Biometric authentication	Biometric authentication is used in some personal devices (phones, tablets, laptops)	ISO/IEC 24745 (biometric information protection)	User-friendly approach, since the authentication identifier is always present (e.g. fingerprint)	Not a secure enough used as the sole method. Identifiers are not anonymous and can not be revoked.
Device authentication	Hardware or software based solutions can be used for authenticating the user platform.	Intel Identity Protection Technology. SecureKey.	User friendly approach bringing additional security.	Hardware based solutions are not available in all platforms.

The combination of username and password is the most commonly used authentication method in web services and mobile applications. It is simple to implement and use. The method has several weaknesses. "Simple" passwords can be easily broken by brute-force methods. On the other hand, long passwords are difficult to memorize and users need to store them on paper where they may be exposed to unauthorized access.

One of the problems of username/password authentication is the need to use passwords in different services, which makes usage of on-line services tedious and forces the users to keep passwords in paper notes. Federated identity refers to the linking of the user's electronic identity across different services. It enables the user to be authenticated by one service and then access resources at another service (single sign-on). This approach has become widely used in the context of social media services (Facebook, Google, Microsoft), which use username/password authentication. These services have published open single sign-on interfaces. Other services can

exploit these interfaces and, thereby avoid implementing their own authentication and identity management functionalities.

The security of username/password method is sometimes enhanced by additionally using the challenge question/response method¹. The challenge question/response method requires the user to answer a question, which the user has previously defined. The response is typically related to the individual's personal life and is therefore easy to memorize for the user.

One-time passwords² provide considerable improvement to basic username/password authentication. In this approach the password is continuously changed. The passwords can be provided for the user through multiple channels. Short message service (SMS) is an attractive method due to the fact that a phone is a personal device and conveniently available for use. Another, widely used approach is to provide a list of passwords to the user by ordinary mail. Password lists are largely in use e.g. in network-banking, where they are used also for confirming transactions. The approach of exploiting an additional "channel" (SMS, voice connection, ordinary mail) for authentication is sometimes referred as "out-of-band authentication".

The most secure authentication methods are based on digital certificates and a Public Key Infrastructure (PKI)³. The PKI is an arrangement, which binds the public key of the user with the user's identity by means of a certificate authority. Typically, the user's certificate and private key are installed on a smartcard. The smartcard represents a secure processing environment, which can internally execute the necessary cryptographic functions, and thereby the private key can always stay within the smartcard chip. Another option is to store the private key and certificate in a SIM-card (Subscriber Identity Module), which also provides a secure execution and storage environment. The SIM-card resides in a mobile phone which provides the required "smartcard reader functionality". Smartcards, on the contrary, need a smartcard reader to be operational. Some mobile phones include the so called Nearfield Communications (NFC)⁴ functionality, which enables them to connect with specific NFC enabled smartcards⁵. When this technology spreads into wider use, it will be possible to use the mobile phone as a smartcard reader.

Biometric authentication uses a scan of fingerprint, face, iris, voice or other characteristic of the user for identification. These methods are user-friendly, since the "authentication device" (e.g. fingerprint) is always present. Fingerprint authentication is already available e.g. in the iPhone 5S phone. Biometric authentication is, however, not secure enough as a sole method - an additional pin-code or password is needed. Additionally, biometric identifiers are not anonymous and they can not be revoked.

Additional security dimension to authentication can be brought by secure identification of the personal device (e.g. laptop, tablet or phone). This identification can be based on specific solutions

¹ http://en.wikipedia.org/wiki/Challenge%20%80%93response_authentication

² http://en.wikipedia.org/wiki/One-time_password

³ http://en.wikipedia.org/wiki/Public-key_infrastructure

⁴ http://en.wikipedia.org/wiki/Near_field_communication

⁵ <http://www.smartcardalliance.org/pages/smart-cards-applications-nfc>

included in the device hardware, like the Intel Identity Protection Technology¹. Also software based solutions are available². Connected with a reliable mapping between devices and users this approach can be used to make basic person-level authentication more reliable. This approach is particularly interesting for enterprise applications, since the usage of device types can be harmonized and a reliable mapping between users and devices is available by default.

6.4.2 Authentication and identity aspects of PHRs

Username/password based methods can be easily used in global services and with certain enhancements (see 6.4.1) they can be relatively secure. The main problem is that it is difficult to confirm the real identity of the person. When, the real identity of the person is needed, the authentication method shall be bound to a subscription process for the verification of the real identity of the subject. For example, the customer may need to visit a mobile operator's shop in person and identify himself, before a SIM-card or smartcard with a personal certificate is given to him. Such authentication methods and processes are typically country-dependent and they are mostly targeted for enabling secure online access to services in the home country.

In healthcare applications, the real identity of the person is typically required. For example, successful transfer of patient data between PHR and an external application (e.g. DECIPHER App), can be most easily achieved if both systems are aware of the real identity of the patient. In case the external application is using a username/password method, the true identity of the user may not be definitely known. In such case information may still be conveyed between the systems if the user confirms the connection by using the secure method by the PHR system. This confirmation process may create a credential which can be used in subsequent data retrievals. The Taltioni³ platform exploits this kind of approach and the OAuth2⁴ protocol for establishing secure connections with external services.

In order to facilitate quick access to core DECIPHER App data, one option is to use an "emergency login" approach as is the case e.g. in the Vivaport PHR⁵. While logged in to the application the user may generate an access code, which enables a view of core patient data relevant in emergency situation. This access code can then be printed and carried along. Also camera-readable 2-dimensional bar (matrix) codes can be utilized in this kind of mechanism.

Strong authentication methods in Table 2 refer to mechanisms where at least two factors are needed. For example, the user is expected to: (1) have the smartcard and (2) memorize a pin-code to use it. Another example is biometric authentication, e.g. based on fingerprint, combined with a pin-code or a password.

From the strong authentication methods listed in Table 2 SIM-card based authentication can be conveniently applied for mobile applications. Since SIM-card based authentication is not yet

¹ <http://ipt.intel.com/Home>

² <http://securekey.com/>

³ <http://www.taltioni.fi/en>

⁴ <https://developers.google.com/accounts/docs/OAuth2>

⁵ <https://vivaport.eu/>

widely available, the DECIPHER App may need to use other methods for authentication in the first phase. Even the username/password method may be sufficiently safe when properly implemented (e.g. using the HTTPS protocol for the exchange of authentication messages and long enough passwords). A flexible design allowing the adoption of alternative authentication methods is recommended.

Federated web authentication based on commonly used platforms (Google, Facebook, Microsoft) would be welcomed by many users. In principle, this approach would be equally safe as DECIPHER App's dedicated username/password –based authentication. However, this option should be carefully considered. Connection with social networks – although only for the purposes of authentication – may give the impression that DECIPHER App's data could be unintentionally shared in social networks, which could lead to hesitation towards the application by the users.

6.5 Patient summary

The patient summary contains a core data set of the most relevant administrative, demographic, and clinical information about a patient. Patient summary provides the essential set of data needed in order to treat the patient, e.g. in the cross-border setting addressed by the epSOS project.

Continuity of Care Document (CCD) defined by HL7¹ in co-operation with ASTM², is an XML-based markup standard intended to specify the encoding, structure and semantics of the patient summary. The definition of CCD was made taking into account the existing Continuity of Care (CCR) record standard³ by ASTM. Therefore, conversions between the two formats are possible.

The CCD specification is based on the HL7 CDA R2 document standard, which can be used in a wide spectrum of different clinical applications. The CCD specification is effectively a set of constraints which define how CDA R2 is used to formulate a patient summary document. CCD has been widely applied to PHR systems. Table 3 lists the contents of a CCD file indicating the usage of content categories in different contexts. HITSP/C32 is a CCD-based patient summary defined by the HITSP partnership⁴. Blue Button⁵ is a mechanism embedded at a health portal or PHR user interface allowing users to view, download and print their health data. The Blue Button was first used in 2010 by U.S. Department of Veterans Affairs in their My HealthVet service⁶. epSOS uses the CCD specification for its patient summary service. Also the IHE's XPHR content profile is based on CCD⁷.

As seen in Table 3, the CCD includes the essential contents needed in the care of acute diseases and is therefore relevant concerning the corresponding use cases of the DECIPHER App. In the most desirable case the DECIPHER App can read CCD files from a PHR system by using a web

¹ <http://hl7.org>

² <http://astm.org>

³ <http://www.aafp.org/practice-management/health-it/astm.html>

⁴ http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=32

⁵ <http://bluebuttonplus.org/>

⁶ <https://www.myhealth.va.gov/index.html>

⁷ http://www.ihe.net/Technical_Framework/upload/IHE_PCC_TF_Vol2.pdf

service interface. In any case, it should be possible to download a CCD file (e.g. by using the Blue Button mechanism) and import the data to the DECIPHER App.

Table 3. CCD sections and their usage in different contexts

Content	HL7 / CCD	HITSP C32	Blue Button	Epsos	IHE / XPHR	Description	Template code ref.
Advance directives	x	x	x		x	Living wills, resuscitation	LOINC 42348-3
Allergies (Alerts)	x	x	x	x	x	Allergies, adverse reactions	LOINC 48765-2
Encounters	x	x	x		x	Interactions between patient and HCP's	LOINC 46240-8
Family history	x				x	Diseases of family members	LOINC 10157-6
Functional status	x		x	x	x	Abilities needed for daily life	LOINC 47420-5
Healthcare provider info	x	x	x	x	x	Healthcare providers for the patient	
Immunizations	x	x	x	x	x	Immunization status and history	LOINC 11369-6
Medical equipment	x			x	x	Implanted or external medical devices	LOINC 46264-8
Medications	x	x	x	x	x	Medication list (including past)	LOINC 10160-0
Patient contacts	x	x	x	x	x	Family members and other contacts	
Payers	x	x			x	Payment sources (insurances, self-pay)	LOINC 48768-6
Person information	x	x	x	x	x	Basic demographic information	
Plan of Care	x	x	x	x	x	Pending interventions, encounters, services ...	LOINC 18776-5
Problem	x	x	x	x	x	Current conditions being monitored	LOINC 11450-4
Procedures	x	x	x	x	x	Past surgeries and treatments	LOINC 47519-4
Results	x	x	x	x	x	Laboratory, imaging etc. results	LOINC 30954-2
Social history	x		x	x	x	Life style factors, marital status	LOINC 29762-2
Vital signs	x	x	x	x	x	Blood pressure, heart rate etc. observations	LOINC 8716-3

6.6 Security and privacy

Due to the sensitive nature of personal health information there are several security and privacy issues which need to be taken into account in the provision of PHR's and PHR-based applications such as the DECIPHER App. Confidentiality of personal information shall be maintained both during transfers between service components and services as well as during storage.

Listings of security vulnerabilities (e.g. OWASP¹) are commonly exploited in application development phase in order to ensure secure application design. Top vulnerabilities include flaws allowing an attacker to inject malicious code to database queries (injection flaws), to compromise credentials (broken authentication and session management flaws), or to make the server accept malicious code to be sent to the user's browser (cross-site scripting flaws). Good design and coding practices (e.g. proper treatment of input data and encryption of data) are needed to protect towards the multitude of possible attacks. Increasingly, open source web frameworks and toolkits are used in application development. This approach brings the benefit of community-based detection and fixing of vulnerabilities in software components.

A basic security measure in applications transferring confidential user data is to protect the information channel by the HTTPS protocol (Hypertext Transfer Protocol Secure) and server certificates. HTTPS takes care of encryption of the transferred data by using SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocol. Server certificates provide identification of the server being connected.

During storage, the corresponding service provider is responsible for the protection of the confidential information. The required processes and procedures are guided by legislation and quality standards.

Patient data stored in EHRs is protected by national laws and the Data Protection Directive (95/46/EC) (see also Section 3.4.2). These define the specific requirements which the *controller* of the personal data registry shall fulfil. Concerning EHRs, the controllers are healthcare service providers, which typically employ trusted partners for carrying out the operational duties of IT system management. The spectrum of PHRs is wider. There are PHR services which comply with Data Protection Directive (95/46/EC) while many PHR services do not.

Quality management is important for both the provider of the health service and the developer or vendor responsible for the software components. The Medical Device Directive may be applicable (see 3.4.3) in which case a quality certification is needed for the product.

The ISO 9000 standards family (in particular the ISO 9001 standard) addresses the quality management systems of organizations. The Information Technology Infrastructure Library (ITIL) is a set of practices on aligning IT services with the needs of business. Service providers are increasingly using external services (e.g. cloud services) to host services and user data. Also in such cases the service provider is responsible for the service and shall be assured by about proper data management through appropriate contracts.

¹ https://www.owasp.org/index.php/Main_Page

6.7 Accessibility

Web accessibility refers to the application design taking into account the diverse range of user's hearing, movement, sight, and cognitive ability. Web accessibility features can be useful to all application users, not only by people with disabilities or the elderly. The Web Accessibility Initiative (WAI) of the W3C provides a wide range of resources on different aspects of web accessibility standards, education, implementation, and policy¹. The Web Content Accessibility Guidelines (WCAG) provide a practical list of issues to take into account in designing web applications². These guidelines have been compiled from the perspective of conventional web applications, but can be applied also to mobile applications along with the W3C Mobile Application Best Practices³.

Modern smartphone models have a variety of in-built accessibility features, including:

- screenreader (read text aloud from display)
- speak selection (select phone functions by speech commands)
- dictation (dictation converted to text by speech recognition)
- zoom (magnify display in steps on demand)
- large text (use larger font in all texts)
- invert colors (inverting colors for better contrast)
- video calls (high quality video enables usage of sign language)
- visible and vibrating alerts

7 Access to the EHR systems of the DECIPHER partners

Based on this survey the most critical issue concerning the DECIPHER App is the access to EHR data, which varies from country to country. Even, in the case when epSOS infrastructure is available, the solutions for patient access are variable and not implemented in all countries.

Although, the DECIPHER App will not be directly accessing information in the EHR's, it will rely on the availability of EHR data through PHR's or the epSOS Patient Access System. Therefore it is highly important for the DECIPHER PCP project that access mechanisms to EHR systems are existing.

Patient data is stored in regional and national EHR systems. Some PHR services (tethered PHRs) provide the individual with possibility to view the EHR data. However, it is not always possible to extract medical records in structured digital form to be used in another service. The situation concerning the procuring partners of DECIPHER PCP project is summarized in Table 4.

¹ <http://www.w3.org/standards/webdesign/accessibility#wai>

² <http://www.w3.org/WAI/WCAG20/quickref/#guidelines>

³ <http://www.w3.org/TR/mwabp/>

The situation in Catalonia is favourable due to the availability of the Personal Health Channel (PHC) which allows the access to clinical data for citizens. The access to the PHR-S available in Catalonia containing structured medical data is authorised by using software digital certificates or smart cards. During the last trimester of 2013 access using user and password will be allowed to the PHC, after a process where the user provides the mobile phone number where a one time code is sent to access the PHC and the password is created by the user. An Interoperability Framework is also in place to facilitate the integration of applications with the PHC.

In Tuscany, the EHR system (FSET) is already available for users to view after smartcard-based authentication (personal Health Card - CNS). The CNS smart card contains a micro-chip that contains a digital authentication certificate. Furthermore, the strong authentication system which is required for access to FSET and other online services of the Tuscany Region, operates through a single sign-on system released by the region based on Authentication, Role definition, Profile assignment and Access, hence the acronym in Italian: ARPA. This infrastructure allows the direct or federated authentication through open and secure SAML protocols. The Tuscany Region is currently working on a project that aims to provide user access to online services that require strong authentication, including FSET, from personal mobile devices. The on-going project will provide user access to the FSET from personal mobile phone that has been previously paired to the personal Health Card. The DECIPHER application could use this mechanism for accessing the medical record.

In UK/Manchester, the possibility to use the HealthVault service is being investigated. There are on-going NHS's development activities such as the the My Health Locker¹ (South London and Maudsley) and the My Health Record² (University Hospital Southampton). UK/Manchester should benefit from the lessons-learned in these NHS's units.

¹ <https://www.myhealthlockerlondon.nhs.uk/>

² <http://www.uhs.nhs.uk/AboutTheTrust/Myhealthrecord/Myhealthrecord.aspx>

Table 4. Possibility to access EHR data through open interfaces.

Country	PHR-EHR interface (ref: Figure 1)	PHR- interface (ref: Figure 1)	Conclusion / recommendation
Spain/Catalonia	Yes. PHC is connected with EHR.	Yes. Applications can be connected by PHC complying with the profiles defined in the Interoperability Framework.	Connectivity with PHC should be required from the DECIPHER App. The rules and API for connecting shall be made available in the DECIPHER Call For Tender.
UK/Manchester	No. However, the interface exists in other HealthVault-based implementations of NHS.	No. However, the interface exists in other HealthVault-based implementations of NHS.	Connectivity with HealthVault should be required from the DECIPHER App. Connection with NHS units running HealthVault-based services shall be established for information sharing.
Italy/Tuscany	The FSET EHR can be currently accessed by the EHC smartcard. On-going project to facilitate federated OAuth2.0 access by mobile apps.	This interface is not needed if access to EHR will be available for mobile applications through the OAuth2.0 mechanism.	DECIPHER can provide an interesting use case for piloting the federated FSET access. Specifications for the API shall be made available in the DECIPHER Call For Tender.

In addition to the recommendations listed in Table 4, it is appropriate that the DECIPHER App includes mechanisms for entering EHR data manually and reading it from standard file formats, such as the CCD (the File interface shown in Figure 1).

8 Conclusions

The objective of the DECIPHER architecture is to enable a set of basic functionalities as outlined in Section 3.2. Most importantly, the DECIPHER App requires access to EHR data residing in national health records. There are many challenges – both technical and privacy-related - in accessing the EHR records of patients (citizens) by other applications. Therefore applications accessing EHR systems are typically tethered – e.g. solutions provided by the national authorities. In the DECIPHER App a realistic approach has been chosen: the application is not connecting EHR systems directly, but relies on PHRs, which are already existing or being developed in different countries, or through the epSOS Patient Access Service when available. The DECIPHER App shall include the necessary functionalities in order to connect with these national services and exchange information with them as required by the addressed use cases.

The main conclusions of this state-of-the-art report concerning the relevant technologies for the DECIPHER App are:

Several EU-level activities addressing cross-border health are on-going. The most important activity, from the architectural perspective is epSOS, which has been able to define and

Public

demonstrate a working infrastructure for cross-border health. The Patient Access Service is highly relevant from the DECIPHER perspective especially since it provides a mechanism for automatic language translation. The epSOS project is ending by the end of 2013 and it is currently being planned how the development and deployment of the infrastructure will continue. The DECIPHER project shall closely follow epSOS and other related EU-projects in order to be informed about the plans concerning epSOS and its successors. Complementary mechanisms for language translation should be considered in DECIPHER to cover situations where epSOS interfaces are not available.

Mobile health applications are largely available for various areas ranging from personal wellness management to chronic disease management. Applications are most typically not connected to EHR systems, although also tethered mobile applications exist. Many apps support several languages, but none of the found applications were known to support language translation mechanisms based on clinical codes. This functionality, to be included in DECIPHER App will evidently exceed the state-of-the-art of current apps.

Existing PHR-platforms are increasingly available. Microsoft's HealthVault is most important of the commercial global platforms. It provides a technologically viable solution for connecting PHR's with clinical EHR data. So far, however, there is little evidence of existing operational usage of HealthVault for EHR-PHR integration. Anyway, since there are on-going HealthVault-based pilots in UK, it seems to be currently the most likely mechanism for accessing personal health data in UK. In Catalonia and Tuscany, there are regional services, which provide Patient Access to medical records. These services will be used by the DECIPHER PCP project.

Connectivity of health information between service components (PHR systems, EHR systems and related service components) is highly important. There are several existing standards addressing this area. Concerning Europe, most important are HL7 standards and IHE profiles. Concerning PHR interfaces, it seems to be most important that health information content follows HL7's Continuity of Care Document (CCD) standard, since this is most widely applied in PHR systems and also epSOS compatible.

Usage of clinical code systems is important in order to enable semantic interoperability and automatic language translation of coded terms. This is another feature of DECIPHER App which is expected to exceed the state-of-the-art of current apps. The usage of clinical codes seems not to be common in current mobile applications based on the available information. Concerning EHR systems in Europe especially ICD-10, ICPC-2 and ATC are widely used and should be supported. Additionally LOINC, which provides the main structure of the CCD file should be supported. The usage of SNOMED CT is considered by some European countries and may need to be supported at a later stage.

Authentication is an important functionality, which affects both security and user experience. Certificate-based mobile authentication (certificate on SIM card) are emerging in some countries, but are not yet widely available. While this is the case, it is likely that password based authentication is currently the best choice for mobile apps. Latest phone models are offering advanced technologies, such as fingerprint authentication, which can improve user experience while maintaining a high level of security.

9 Definitions

Term	Description
Country of Affiliation	This is the country (Country A) which holds information about a patient, where the patient can be univocally identified and his or her data may be accessed.
Country of Treatment	The country (Country B) where cross-border healthcare is provided when the patient is seeking care abroad. This country is different from country A, in which healthcare related information about a patient is held.
Electronic Health Record	The data repository for storing patient information needed for care documentation. Electronic Health Record is primarily used by the healthcare professionals. Access to view EHR contents is permitted to patients in some implementations.
Health record	Personal health information covering both Personal Health Records and Electronic Health Records.
Electronic Health Record System	The term is used instead of Electronic Health Record to highlight the functionality for using and managing the information stored in the Electronic Health Record.
DECIPHER App	The cross-border mobile application to be developed by the DECIPHER project.
Patient Access Service	An epSOS extension phase service providing the patients the access to their health record.
Personal Health Channel	The Catalan public PHR service.
Personal Health Record	A data repository for personal health-related information. Personal Health Record (PHR) contains information owned and managed by the individual citizen.
Personal Health Record System	The term is used instead of Personal Health Record to highlight the functionality for using and managing the information stored in the Personal Health Record.
Taltioni	A Finnish nation-wide PHR platform service.

10 Abbreviations

Acronym	Meaning
API	Application Programming Interface
ASTM	American Society for Testing and Materials
ATC	Anatomical Therapeutic Chemical Classification System
CCD	Continuity of Care Document
CCR	Continuity of Care Record
CDA	Clinical Document Architecture
CEN	European Committee for Standardization
CNS	Personal Health Card (Italy)
EDQM	European Directorate for the Quality of Medicines & HealthCare
EHIC	European Health Insurance Card
EHR	Electronic Health Record
eID	Electronic Identification
FDA	Food and drug administration
FHIR	Fast Health Interoperable Resources (HL7 activity)
FIC	Family of International Classifications (WHO)
FSET	Fascicolo Sanitario Elettronico regione Toscana
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSMA	GSM Association
HCP	Healthcare professional
HITSP	Healthcare Information Technology Standards Panel
HL7	Health Level Seven
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICD	International Statistical Classification of Diseases and Related Health Problems
ICPC	International Classification for Primary Care
ICT	Information and Communication Technologies
IHE	Integrating the Healthcare Enterprise
ISO	International Organization for Standardization
ITIL	The Information Technology Infrastructure Library
JSON	JavaScript Object Notation
LOINC	Logical Observation Identifiers Names and Codes
MDD	Medical Device Directive
MHD	Mobile Access to Health Documents (IHE profile)
MTD	Master Translation/Transcoding Catalogue (from epsOS)
MVC	Master Value Set Catalogue (from epsOS)
NFC	Nearfield Communications
PAC	Patient Access Service (from epsOS)
PHC	Personal Health Channel
PHR	Personal Health Record

Public

PKI	Public Key Infrastructure
RTD	Research and Technological Development
RDF	Resource Description Framework
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SIM	Subscriber Identity Module
SMS	Short Message Service
SNOMED	Systematized Nomenclature of Medicine
SSL	Secure Sockets Layer
TAS	Terminology Access Services (from epsOS)
TSL	Transport Layer Security
UCUM	Unified Code for Units of Measure
USB	Universal Serial BUS
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WCAG	Web Content Accessibility Guidelines
WHO	World Health Organization
XCF	Cross-Community Fetch (IHE profile)
XDM	Cross-Enterprise Document Media Interchange (IHE profile)
XDS	Cross-Enterprise Document Sharing
XML	Extensible Markup Language
XPHR	Exchange of Personal Health Record Content (IHE profile)

11 Appendix 1: Examples of mobile health applications

Name and URL	Scope	Type	Platform	Connections	Languages
Chronic disease management					
BodyTel System https://secure.bodytel.com/en	Multiple measurement types	Server-connected mobile app.	Android, Java/Symbian	Stand-alone PHR. Data transfer from compatible meters to portal (BodyTelCenter)	German, English, Dutch
Capzule PHR http://www.capzule.com/	Multiple measurement types	Mobile app	iOS	Stand-alone PHR.	English
HealthPAL™ i http://medapps.net/healthpal.html	Multiple measurement types	Server-connected device		Stand-alone PHR. Data transfer from compatible meters to portal (CloudCare platform)	English
t+ Medical http://www.obsmedical.com/	Multiple measurement types	Server-connected mobile app.		Stand-alone PHR. Back-end server (connection with healthcare providers)	English
Sports and Wellness support					
Diet Assistant http://dietassistantapp.com/	Nutrition, weight management	Mobile app	Android	Stand-alone PHR	English

Public

Livescape™ for Windows Phone http://livescape.mobi/	Nutrition, health and wellness data	Server-connected mobile app	Windows	Interconnected PHR / HealthVault Facebook, Twitter	English
NewBalance http://nbmonitors.com/gps-enabled-monitors/nx990-gps-cardio-trainer/	Heart rate data	Sport watch	Sport watch	Stand-alone PHR + PC software	English
NIKE+ SportWatch GPS http://nikeplus.nike.com/plus/products/sport_watch/	Heart rate data	Sport watch		Stand-alone PHR + PC software	English
Suunto Ambit2 http://www.suunto.com/en-GB/Products/sports-watches/Suunto-Ambit2-S/Suunto-Ambit2-S-Graphite/	Heart rate data	Sport watch		Stand-alone PHR + PC software	Multiple languages
Wellmo http://www.wellmo.com/	Generic wellness	Server-connected mobile app	Android, iOS, Windows, Symbian	Interconnected PHR / Wellmo Service portal and Taltioni-platform	English, Finnish
Management and access of personal health data					
Gazelle - Mobile Health Application http://mygazelleapp.com/	Generic health data	Server-connected mobile app	iOS, Android, Blackberry	Interconnected PHR / Quest Diagnostics (lab data) HealthVault	English
Health Choices http://www.3chillies.co.uk/health-choices	Finding and managing health services	Server-connected mobile app	Windows, Android and iOS	Interconnected PHR / HealthVault	English

Public

Health nexus Lab Tracker https://www.healthnexus.com/iPadApps/labTracker-Index.cgi	Laboratory test results	Server-connected mobile app	Browser iOS	Interconnected PHR / HealthVault	English
HealthVault Client App https://itunes.apple.com/us/app/microsoft-healthvault/id546835834?mt=8	Generic health data	Server-connected mobile app	Windows, iPhone	Interconnected PHR / HealthVault	English
How are you? https://en-gb.howareyou.com/	Generic health data, messaging	Server-connected mobile app	iOS	Standalone/tethered PHR / NHS N3 network	English
Medical Wallet http://www.windowsphone.com/en-us/store/app/medical-wallet/b697a49e-d2ad-4fcc-a8e3-d6500fc94f22	Generic health data	Server-connected mobile app	Windows, iOS, Android	Interconnected PHR / HealthVault	Several
MediTrack http://www.iphonehealthapps.net/2009/09/25/MediTrack/	Medication tracking	Mobile app	iOS	Stand-alone PHR	English
MotionPHR http://motionphr.com/	Generic Health Data	Mobile app	iOS, Android	Stand-alone PHR. Server (back-up)	English
MyChart http://www.epic.com/software-phr.php	Access to EHR	Server-connected mobile app	Browser, iOS, Android	Tethered PHR / Epic EHR	English