FIDIS

Future of Identity in the Information Society

Title:	"D4.9: An application of the management method to interoperability within e-Health"
Author:	WP4
Editors:	James Backhouse (LSE) Bernard Dyer (LSE)
Reviewers:	Vashek Matyas (MU) Denis Royer (JWG)
Identifier:	D4.9
Type:	[Deliverable]
Version:	4.0
Date:	Monday, 26 November 2007
Status:	[Final]
Class:	[Public]
File:	fidis-wp4-del_D4.9_application_to_e-health.doc

Summary

This deliverable is concerned with developing interoperable identity management systems, within the e-Health sector, throughout and between EU states. To achieve comprehensive, practical, and cost effective systems that work together throughout the EU there are many challenges which need to be addressed including:

- A need for a common policy on interoperability throughout the EU
- Development and maintenance of an integrated e-Health network that brings together patients, professionals, providers, regions, and nations
- A need to incorporate identity management, including FIDIS research, into existing and proposed information systems
- The increased movement of EU citizens around the Union for purposes of travel, study, work and retirement
- Establishment of standard data sets for all aspects of health records
- Full cooperation between Member states, the many stakeholders involved and personnel performing a wide range of disciplines

It is envisaged that the work being performed in WP4 will assist practitioners in meeting these challenges in a methodical and comprehensive way.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieked Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
1.0	July 2007	Preparation (James Backhouse and Bernard Dyer)
2.0	August and September 2007	Continuous development. Contributions to this document: VUB: Development of e-Health within the EU (D4.11); KUL and TILT: Conceptual Framework for Identity Management in e-Government (D16.1); Health practitioners of e-Health within the UK
3.0	October 2007	Draft version sent to reviewers for comments. Vashek Matyas (MU): Contribution on the structure and content of the document. To include previous work so that it is complete, and helpful to readers who are new to the work of WP4; Denis Royer (JWG): Contributions on the content of the script; Discussions with representatives at the 3rd Strategic Work Plan Workshop in Frankfurt
4.0	November 2007	Final version incorporating comments from the reviewers

Table of Contents

1 Executive Summary

This deliverable is aimed at supporting the development of interoperable identity management systems within the e-Health sector, both throughout and between EU states. Creating comprehensive, practical, and cost effective systems that work together throughout the EU, requires a number of key challenges, discussed in this report, to be addressed and resolved. This report seeks to illustrate how FIDIS research in the area of interoperability of identity management systems can be assimilated and exploited for this purpose.

When developing this report the work undertaken in two related FIDIS deliverables has been represented within the models proposed and in the application of the management principles. The relevant deliverables are

- ***D4.11*** – which explores the development of e-Health in the EU and reviews the processes for introducing e-Health applications in the different European States.
- ***D16.1*** - whose main aim is to find agreement within the different disciplines, represented in FIDIS on the basic terminology needed to support dialogue on the very specific research field of privacy-friendly identity management in e-Government.

This report furthermore extends the work of three previous deliverables of Work Package 4 on interoperability which may be found on the FIDIS website:

- ***D4.6:*** "Draft best practice guidelines"
- ***D4.7:*** "Review and classification for a FIDIS identity model"
- ***D4.8:*** "Creating the method to incorporate FIDIS research for generic application"

To enable the practical adoption of the management method we have proposed a FIDIS portal to assist with the dissemination and exploitation of the FIDIS research. The portal will be specified in Deliverable ***D4.10***: "Specification of a portal for interoperability of identity management systems".

It is envisaged that the work being performed in WP4 will assist those seeking to develop interoperable eHealth systems in meeting the many challenges, in a methodical and comprehensive way, and will be suitable for performing the recommended e-Health applications, within an EU interoperability framework, as highlighted in the following EC reports:

- "European Interoperability Framework for Pan-European e-Government Services"
- "Connected Health – Quality and Safety for European Citizens".

2 Introduction

One of the most important services governments have to deliver is health care to citizens, and computerised applications in the field of health, especially e-Health, can significantly improve health service delivery. For example, electronic access to core patient data can improve both ongoing and emergency treatment and electronic prescriptions transferred directly, from the doctor to the chemist, can save time and costs. The ideal situation is to provide the right *information,* at the right *time,* at the right *place,* to the right *people.* Governments therefore need to harness information and communications technology (ICT) to deliver high-quality health care for all. The European e-Health Action Plan of April 2004[4] provided a roadmap for the development of interoperable e-Health services in and across Member states.

This deliverable is concerned with developing interoperable identity management systems, within the e-Health sector, throughout and between EU states. To achieve comprehensive, practical, and cost effective systems that work together throughout the EU there are many challenges which need to be addressed including the:

- need for a common policy on interoperability throughout the EU
- development and maintenance of an integrated e-Health network that brings together patients, professionals, providers, regions, and nations
- need to incorporate identity management, including FIDIS research, into existing and proposed information systems
- increased movement of EU citizens around the Union for purposes of travel, study, work and retirement
- establishing of standard data sets for all aspects of health records
- full cooperation between Member states, the many stakeholders involved, and personnel performing a wide range of disciplines

The EC report[5] "Connected Health – Quality and Safety for European Citizens" outlines priority issues which must be pursued vigorously in order to meet all the challenges described above – improve patient safety, encourage well-informed citizens on health matters, and create high-quality health systems and services. It focuses on the overriding theme of comprehensive e-Health interoperability.

The proposals outlined in a second EC report[6], "European Interoperability Framework for Pan-European e-Government Services" also need to be taken into account, particularly those relating to technology, when considering e-Health services within and across Member states.

To progress towards interconnected and collaborative e-Health services at the local, regional, national and pan-European levels, a structured approach is recommended.

[4] The European e-Health Action Plan of April 2004 – Communication (2004) 356 – e-Health

[5] Connected Health – Quality and Safety for European Citizens ISBN 92-79-02705 – EC 2006

[6] European Interoperability for Pan-European e-Government Services ISBN 92-894-8389-X - EC 2004

When developing this report the work undertaken in two FIDIS deliverables has been represented, within the proposed models and application of the management principles:

- ***D4.11*** which explores the development of e-Health in the EU and reviews the processes for introducing e-Health applications in the different European States.
- ***D16.1*** whose main goal is to find an agreement within the different disciplines, represented in FIDIS, on the basic terminology needed to allow dialogue on the very specific research field of privacy-friendly identity management in e-Government.

This report extends the work of previous deliverables of WP4, which may be referred to on the FIDIS website[7]:

- ***D4.6:*** "Draft best practice guidelines"
- ***D4.7:*** "Review and classification for a FIDIS identity model"
- ***D4.8:*** "Creating the method to incorporate FIDIS research for generic application"

It is envisaged that the proposed FIDIS interoperability management method and framework (described in deliverables ***D4.6, D4.7 and D4.8***) will be suitable for performing all of the applications discussed in the EC reports. Interoperability means systems and services that are connected and can work together easily and effectively, while maintaining patient and professional confidentiality, privacy and security.

2.1 Aims of the deliverable

The aims of this deliverable are:

- To apply the proposed FIDIS management method and framework, in broad terms, to e-Health within and across Member states
- To make recommendations on how the work of FIDIS can be integrated into other initiatives particularly e-Government
- To propose a structure for the European interoperability network, relating to e-Health within and between Member states

[7] http://www.fidis.net/

3 Application of the management method to e-Health

As stated in earlier deliverables of FIDIS Work Package 4, the interoperability management method is separated into four domains, as shown in Figure 1 namely the requirements domain; the business modelling domain; the information management principles domain; and the system specification domain.

This section outlines how the proposed management method may be applied, in more detail to that described in deliverable ***D4.8***, to interoperability within e-Health.

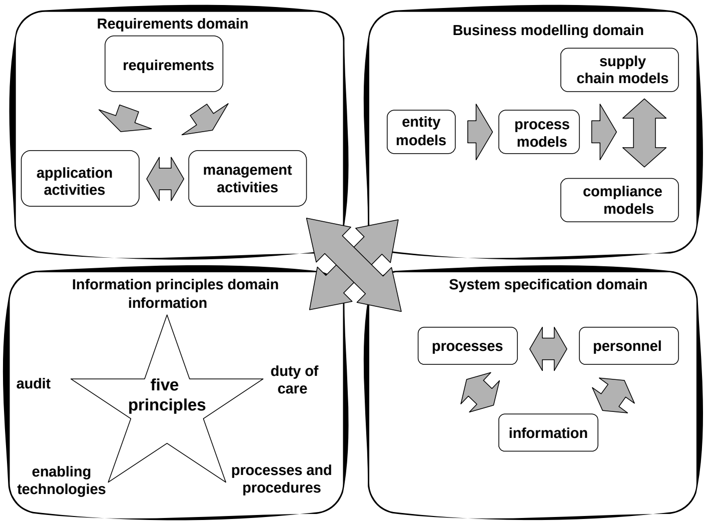


Figure 1: Domains of the Framework

2.2 Requirements domain

The requirements, brought together from literature reviews, EU directives and discussions with medical practitioners, are divided into two main areas: those specifying the e-Health application activities, and those specifying the management activities.

2.2.1 Operational / application activities include:

- Provide health care to all citizens within and across Member states
- Ensure identity management is incorporated into ICT systems within e-Health sectors
- A activity of paramount importance is to ensure that the identity of the citizen, or patient, is completely secure and strictly confidential to those who are authorised to access and use this information

- Provide and manage medical practitioners such as doctors, surgeons, nurses and records managers, who have been vetted for security purposes and verified for their relevant skills by their qualifications and experience
- Supply and monitor funds to develop and maintain the network
- Keep up-to-date the medical records of doctors, patients, biological data, etc

2.2.2 Management activities

The requirements for management activities should specify the tools, such as project management techniques and procedures, which have to be employed to ensure that all the information, roles and responsibilities, processes and technologies are in place to manage identity issues in a secure manner. These requirements should include the management of projects, finances, human and technology resources.

2.3 Business Modelling Domain

The following models have been developed, within the report, to assist practitioners in all disciplines, including Information Communication and Technology (ICT), to establish e-Health applications within and across Member states.

2.3.1 Integration and interoperability

Figure 2 shows the different elements that need to be addressed when integration and interoperability are brought together:

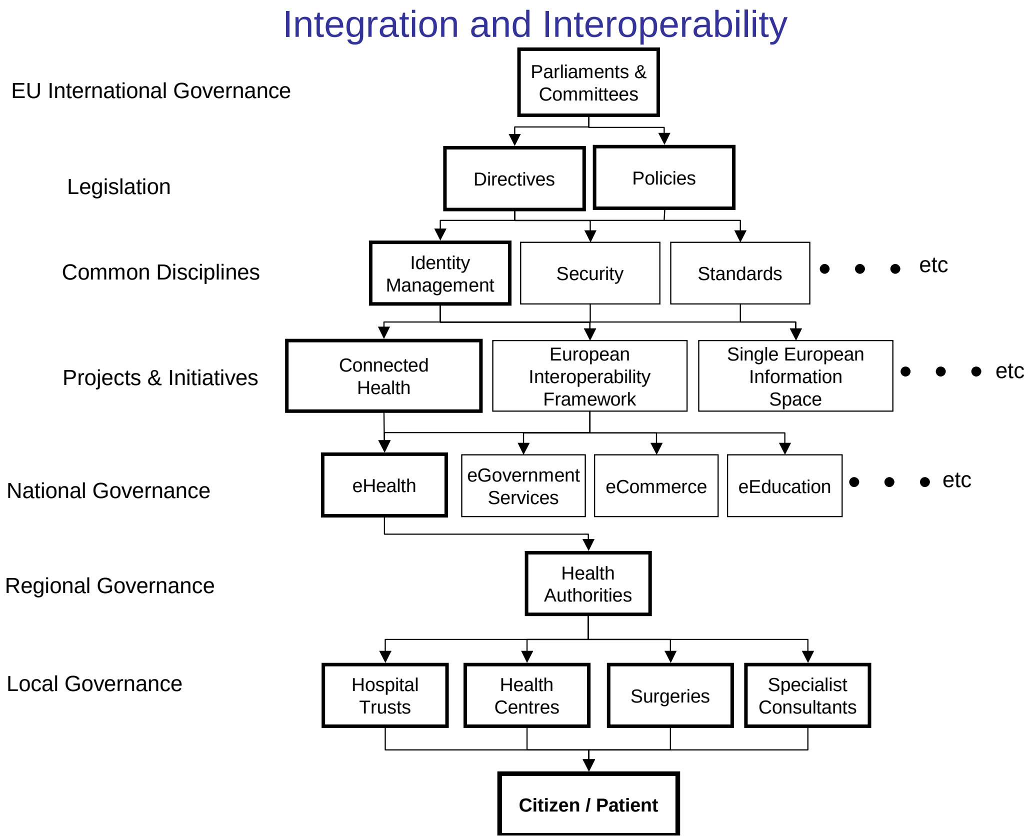


Figure 2: Integration and Interoperability

The following paragraphs briefly describe the areas of interest in the model:

- **EU International Governance**

  - **Parliaments**

EU governance is directed at the highest level through the European Parliament and the parliaments of the EU countries. Each parliament operates under a parliamentary system of government in which the executive or cabinet, as in the case of the UK, is constitutionally answerable to the parliament. The government in office is responsible for establishing the various departments, such as those dealing with law and order, treasury functions and health, and ensuring that they operate effectively in terms of efficiency, services to citizens and cost.

  - **Committees**

Committees have been set up by the EC to determine policies for particular areas of interest. The Health Telematics Working Group of the High Level Committee on

Health[8], established by the EC reviewed the introduction of ICT in the health sector, the factors promoting or inhibiting its development, and areas where Community legislation could be beneficial. It paid particular attention to applications of ICT in e-Health namely health cards, virtual hospitals and provision of health-related information to health professionals and patients. Reports on their findings and recommendations are published yearly.

The i2010 High Level Group was set up to study Information Space, Innovation & Investment in R&D inclusion, throughout Member states. It published a report "The Challenges of Convergence" in December 2006[9].

- **Legislation**

To establish Directives and Policies, for common legislation and regulations within Member states, Directive 95/46/EC[10] covers the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- **Common Disciplines**

Identity management cannot be seen in isolation. Systems need to incorporate other disciplines such as security, information management and data protection. National and international standards have been written for many of these disciplines such as security[11] and records management[12], to ensure standardisation whenever they are applied.

- **Projects & Initiatives**

The EU projects and initiatives which need to be taken into account when considering e-Health include:

- Connected Health – Quality and Safety for European Citizens (see earlier)
- European Interoperability Framework for Pan-European e-Government Services (see earlier)
- Single European Information Space whose aim is to establish a Single European Information Space offering affordable and secure high-bandwidth communications, rich and diverse content and digital services (the first objective of i2010 HLG) .

- **National Governance**

[8] Yearly Reports of the High Level Group on Health Services and Medical Care to the EPSCO

[9] I2010 HLG – Convergence Discussion Paper (12th December 2006

[10] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[11] ISO/IEC 17799, Information technology – Code of practice for information security management

[12] ISO/TR 15489, Information and documentation – Records management- Guidelines

The government in each state is responsible for putting in place policies and departments, to develop and administer such services as e-Government, e-Health and e-Education.

- **Regional Governance**

Regional governance of e-Health services will normally be administered by Health Authorities within the regions.

- **Local Governance**

Local governance will normally be managed and administered by hospital trusts or boards to deliver medical services by health centres, surgeries and specialist consultants, to the local community.

- **Citizens and patients**

The governance described above is all put in place to provide the best possible health services, throughout Member states, to citizens and patients.

2.3.2 Stakeholders

A stakeholder model for e-Health is shown in Figure 3 which represents a “typical” structure of a national health service. The government policies are determined by parliament and performed by the various departments and agencies. The Connected Health initiative considers the “requirements of e-Health interoperability which aim to provide systems and services that are connected and can work together easily and effectively, while maintaining patient and professional confidentiality, privacy and security”.

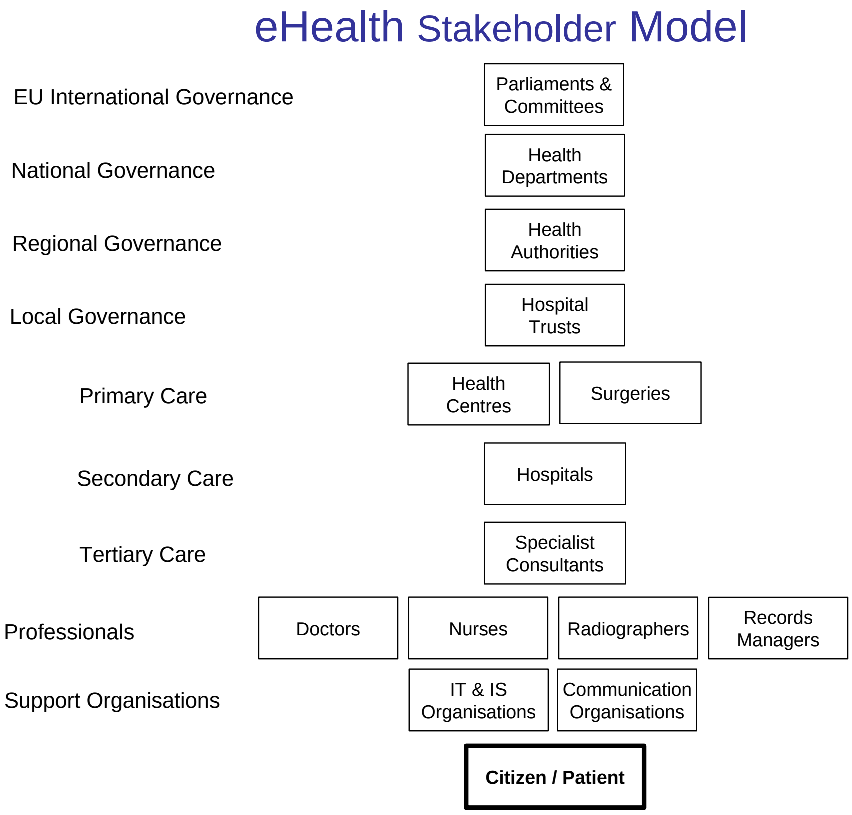


Figure 3: Typical stakeholders within health sector

The following paragraphs briefly describe the areas of interest in the model.

- **EU International Governance**

As described earlier

- **National Governance**

As described earlier

  - Health departments

Departments of health aim to improve people’s health and wellbeing through responsibility and accountability for the health and social care system within their particular country.

- **Regional Governance**

In order to manage e-Health effectively the country may be divided into Regional Health Authorities. They in turn may divide their region into local areas which provide governance of the medical services within their region.

- **Local Governance**

As described earlier

  - **Primary care**

Primary care covers the following establishments:

- Health Centres house local medical services or the practice of a group of doctors
- Surgeries provide medical practitioner that treat or advise patients

  - **Secondary care**

Secondary care covers hospitals which provide medical and surgical treatment and nursing care for sick or injured people.

  - **Tertiary Care**

Tertiary care provides specialist consultants to treat patients with exceptional health conditions.

- **Professionals**

Medical practitioners such as consultants, doctors, nurses and radiographers, as well as administration and support staff, such as records managers

- **Support organisations**

Information Technology (IT) and Information Systems (IS) organisations assist in the development and support of information systems and communication networks.

- **Citizen and patients**

The stakeholders described above aim to provide the best possible health services, throughout Member states, to citizens and patients.

2.3.3 Networks and information flows

There is a wide diversity in the mechanisms currently in place in the Member states for e-Health services, and it is considered that cooperation at the EU level is essential. The fundamental aim is to enable personal and medical information be made available to patients, and health practitioners, within and between Member states. Considering cross-border care, there is at present a lack of data and consideration must be given to collect complete and comparable data. As well as managing medical data Member states must collect and monitor data on health professionals' and patients' mobility throughout Europe.

A possible network configuration for supplying e-Health services throughout Europe is illustrated in two scenarios:

- Scenario 1: A national information database for e-Health (Figure 4)
- Scenario 2: An EU information database for e-Health (Figure 5)

Both scenarios have the following structure:

- **Level 1: Institutional database**

When a citizen or patient registers at a surgery, health centre or hospital, his or her identity credentials, specified in Table 1, are recorded on the institution's database. If treatment is required, at any time, at any of these institutions, then the patient's medical records, specified in Table 2 are updated on the institution's database.

- **Level 2: Local community database**

Databases, relating to medical care of all patients, who have had or are receiving treatment in the medical institutions within the local community, may be transferred for amalgamation into a local community medical database.

- **Level 3: Regional database**

All of the medical institutions within a region, determined by the state, may transfer the medical records of all citizens residing in the region for amalgamation into a regional database.

- **Level 4: National database**

The regional databases containing the medical records of all citizens, within the state, may be transferred for amalgamation into a national medical database.

- **Level 5: EU database for e-Health**

The national medical databases containing the medical records of all citizens, within the EU, may be transferred for amalgamation into an EU database for e-Health.

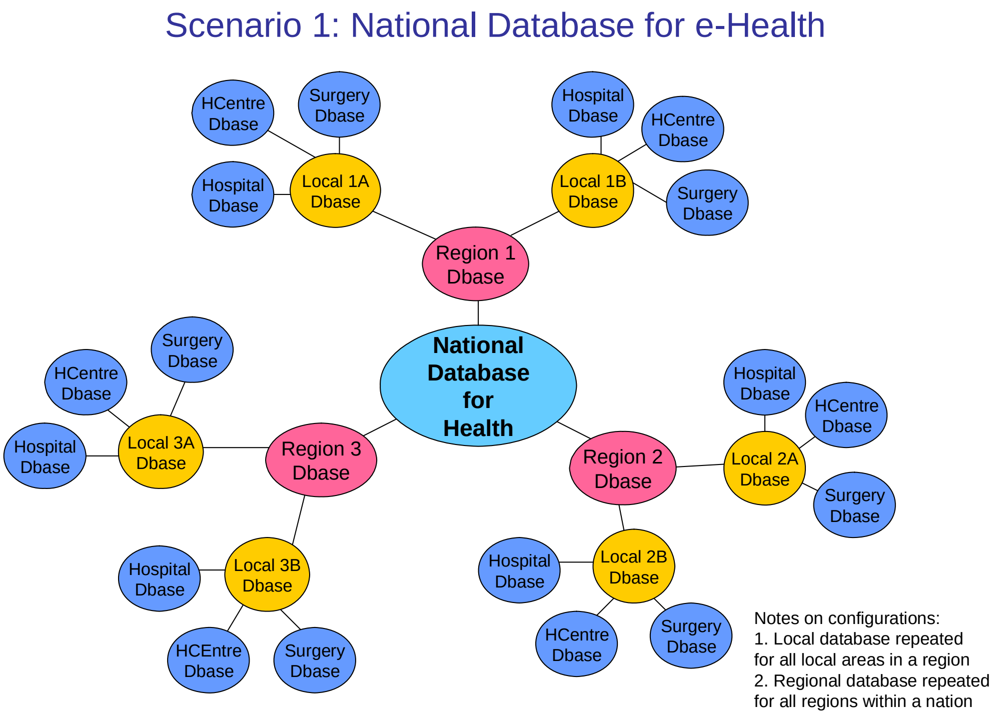
Because it is such an extremely large and time consuming task to develop such networks of medical databases, which contain medical records of many millions of people, it is considered that a staged and structured approach is essential. The level-by-level approach, outlined above may assist with the development of such networks. States may choose to combine some of the levels together, depending on the size of the country and the number of citizens involved, but the basic principles remain the same. Issues of control and ownership may vary between member states and the consensus may be against a massive national database in which secure management procedures are difficult to ensure. The alternative is for local control and ownership with protocols that govern the exchange of information.

The funding for developing and maintaining the databases and networks will normally be provided by the Member state. Each stakeholder, within the various levels of governance, will be responsible for managing their allocation of funds to ensure that the health services they provide are efficient and cost-effective.

Member states have appreciated that implementing e-Health interoperability is a long term process requiring a sustained commitment with respect to political involvement and resources. Interoperability is probably only achieved gradually by developing application by application.

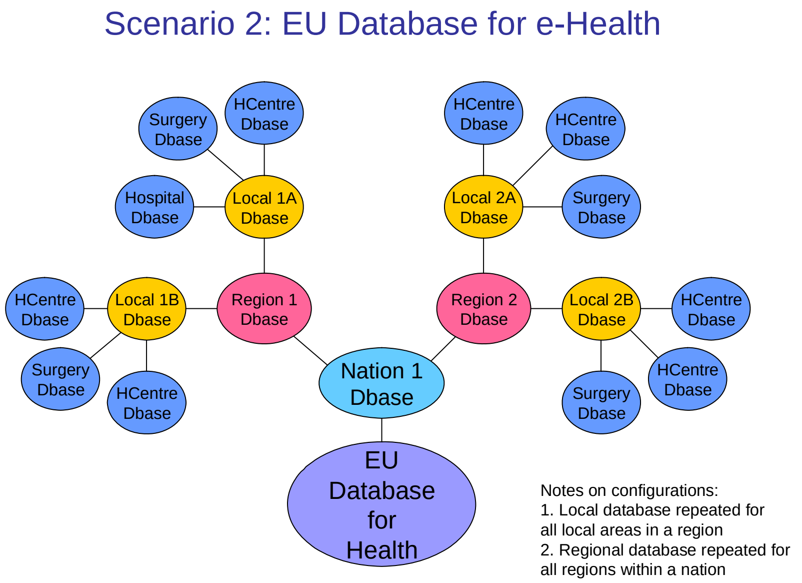
Very often citizens have to travel abroad, or to other regions within their country, for business or pleasure purposes. If they become ill, or are involved in an accident, then they may require medical treatment from a medical institution, anywhere within the EU. Once the EU e-Health networks are in place then authorized personnel within the institution will have access to the medical records of the EU citizen needing treatment.

It is critical that the data within the network is secure at all times and can only be accessed by authorised personnel. The security applies not only to technical aspects but also to the personnel who are managing and administrating the data. Staff need to be fully aware of their responsibilities in managing and administrating security and should be trained accordingly. The problems of security increase rapidly when databases are combined together as the volumes of data grow substantially, particularly at the level of a national medical database. In the UK alone the National Health Service has a goal of having 60 million patients on a centralised electronic health record by 2010. If an EU database is established then it will contain more than a billion records.



Notes on configurations:
1. Local database repeated for all local areas in a region
2. Regional database repeated for all regions within a nation

Figure 4: National Database for e-Health



Notes on configurations:
1. Local database repeated for all local areas in a region
2. Regional database repeated for all regions within a nation
3. National database repeated for all nations within EU

Figure 5: EU Database for e-Health

Personal Identifiers / Credentials include:

Identity	Principles of Information Management							
	Information				**Roles & Responsibilities**	**Processes & Procedures**	**Enabling Technologies**	**Audit & Control**
	Identifier / Credential	**Importance**	**Held by person**	**Held by other stakeholders**				
Person	Name (n)		Yes	All stakeholders	Secure and protect: Information Computer systems Ensure stakeholders & representatives are bona fide Protect: Passwords Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Authorisation Confidentiality Security Interoperability	Paper Electronic Web E-mails Mobiles Caads Etc RFID	Ensure all items are bona fide: Stakeholders & their representatives Documents and copies Compliance with statutes & regulations
	Signature		Yes	All stakeholders				
	Insurance Number			Government				
	Citizen Service Number			Government				
Location	Address (n)		Yes	All stakeholders				
	Location address (n)		Yes	All stakeholders				
	Phone Numbers (n)		Yes	All stakeholders				
	e-mail address (n)		Yes	All stakeholders				
Next of Kin/ Contacts	Name (n)		Yes	All stakeholders				
	Address (n)		Yes	All stakeholders				
	Location address (n)		Yes	All stakeholders				
	Phone Numbers (n)		Yes	All stakeholders				
	e-mail address (n)		Yes	All stakeholders				

Table 1

Health Sector – Identifiers / Credentials

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
Medical	Doctor (n)		Yes	Govn't (Health)	Secure and protect: Information Computer systems Destroy out of date information Ensure stakeholders & representatives are bona fide Protect: Passwords Delete unsolicited emails Monitor regularly: Information Computer systems Vetting of personnel Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Accuracy Authentication Authorisation Confidentiality Security Interoperability Identification Matching checks	Paper Electronic Web E-mail Cards Voice Face to face Images RFID Databases	Ensure all items are bona fide: Person (n) Stakeholders & their representatives Documents and copies Scans match with originals Computer systems Compliance with statutes & regulations
	Hospital (n)		Yes	Govn't (Health)				
	Medical records (n)		No	Govn't (Health)				
	Condition (n)		Yes	Govn't (Health)				
Biological	Gender		Yes	Govn't (Health)				
	Eye colour		Yes	Govn't (Health)				
	Height		Yes	Govn't (Health)				
	Fingerprint		Yes	Govn't (Health)				
	DNA		Yes	Govn't (Health)				
	Retina		Yes	Govn't (Health)				
	Iris		Yes	Govn't (Health)				
	Face		Yes	Govn't (Health)				
	Handwriting		Yes	Govn't (Forensics)				
	Voice		Yes	Govn't (Forensics)				

Table 2

To develop such a network is an extremely challenging task, taking many years to achieve because of the very large number of citizens and the vast amount of medical data involved.

This challenge has also been considered by the High Level Group on Health Services and in Annex 1 of their 2006 Report it outlines options for procedure for identification and development of European Reference Networks (ERN). These are summarised in the following table.

Options	Advantages	Disadvantages
Option 1 – Adapting existing mechanisms	• Does not require major structural changes • Relatively easy to execute in short-term perspective	• Very limited in terms of budget and time • Does not guarantee long term sustainability for the networks • Does not address related practical, financial and legal issues which are specific for ERN
Option 2 – New specific mechanism for European reference networks	• Provides long-term sustainability for the networks • Opportunity to address specific practical problems of ERN, including financial and legal issues • Distribution of competence at all levels within the implementing structure	• Requires new specific instrument, so lengthy institutional negotiations • Requires specific allocation of resources fro Community budget • Creation of implementing structure requires more time and resources than Option 3
Option 3 – concentrated procedure	• Provides long-term sustainability for the networks • Opportunity to address specific practical problems of ERN, including financial and legal issues • Less time and resources needed for creation of implementing structure than Option 2	• Requires new specific instrument, so lengthy institutional negotiations • Requires specific allocation of resources fro Community budget • Distribution of competence at al levels within the implementing structure is less transparent than in Option 2

2.4 Information management principles domain

2.4.1 Information

Information may be represented in different forms and on different media including:

- **Electronic Health Records (EHR)**

An electronic health record (EHR) refers to an individual patient's health record in digital format. Electronic health record systems co-ordinate the storage and retrieval of individual records with the aid of computer systems. EHRs are usually accessed on a computer system, often over a network. It may be made up of electronic medical records (EMRs) from many locations and/or sources. A variety of types of health care-related information may be stored and accessed in this way. Electronic medical records may include:

- Patient demographics
- Medical history, examination and progress reports of health and illnesses
- Medicine allergy lists
- Immunisation status
- Laboratory tests
- Medication information, including side effects and interactions
- Recommendations for specific medical conditions

Identifiers/Credentials of the patient/citizen were specified in Tables 4 and 5 of deliverable ***D4.7*** and include:

- Patient name
- Address
- Date of birth
- Next of kin
- Family doctor
- National Insurance Number or National Identity Number
- Insurance scheme

Electronic systems should increase medical practitioners' efficiency, reduce costs and promote standardisation of care. To support interoperability it is fundamental to have common data sets, formats, and semantics, specified within recognised standards, which are some of the aims of deliverable ***D16.1.***

- **Health Cards (Chip-cards)**

Medical information must travel with the patient to ensure correct treatment in different countries and for good continuity of care when the patient returns home, so Health Cards have been introduced in several countries, including Belgium, Spain and Italy. Switzerland is introducing them in 2008.

All existing Health Cards, carried by citizens, contain information on the card but this information differs between the various cards in the different countries, so to provide interoperability they need to be standardised. Personal data is provided on all cards and includes:

- Name
- National Insurance Number or National Identity Number
- Date of birth
- Sex
- Name and identifier of the insurance company
- Identifier of the card
- Expiry date of card
- Blood type
- Immunization data
- Transplant data
- Allergies
- Diseases
- Special entries
- Medication
- One or more contacts for any emergency

- **European Health Insurance Card**

The European health insurance cards aim to enable mobility of insured people in Europe diminishing administrative efforts for people travelling in other European Member States and enhance the access to health care throughout Europe. The existing European Health Insurance Card contains no patient health data, and is not yet therefore a complete EU passport to health.

- **General considerations**

  - Medical data is a special category of data is which is protected by Article 8 of Directive 46/95/EC[13]
  - There is a need for well-structured information management, and efficient and economic administration
  - Hashing and encrypting data should be applied to prohibit the identification of patient data
  - All records should include the information which is important for patient's rights, e.g. patient does not want to be vaccinated, does not want to have a blood

[13] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

  - transfusion or patient has seen the record and noticed there is a mistake and asks it to be corrected
  - Statement of who is responsible for the management of the record
  - There is no standard European medicine prescription and this can prevent patients from obtaining the right medicine
  - When a patient leaves hospital in one country there is no standard discharge letter to ensure good continuity of care back in the patient's home country

- **Standards**

It is important that dissemination of the research achieved in FIDIS continues with the standards bodies, including ISO/IEC JTC 1/SC 27/WG 5, especially with respect to Identity Management, Privacy and Biometrics. FIDIS has a liaison with ISO/IEC JTC 1/SC 27/WG 5 and with EG5. Of special interest are the Working Drafts; 24760 "A framework For Identity Management"; 29100 "Privacy Framework"; 29115 "Authentication Assurance" and to a lesser degree 24745 "Biometric template protection". However, ongoing work in ISO/IEC JTC 1/SC 27/WG 5 might generate other Working Drafts of interest. This work is discussed in Chapter 3 of ***D4.7:*** "Review and classification for a FIDIS identity management model".

Such an endeavour will contribute substantially to the dissemination of the FIDIS results beyond academia and directly to standardisation bodies, and through these to industry and to governmental bodies.

2.4.2 Duty of care

The following roles and responsibilities have been agreed by the Member states:

- The data controller is responsible for all records, according to the directive 95/46/EC.
- "The controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller of the specific criteria for his nomination may be designated by national or Community law; organizations"
- All countries agree that access has to be authorized.
- The secrecy of duty of the doctor and the protection of the doctor – patient relation is a central rationale
- Ownership of the data varies within Member states
- Member states should consider appointing a clearly defined contact point for patients who seek information about access to health care across borders.
- The national or regional contact points could form a network in order to share experiences and information related to cross-border care. The contact details of the participants in the network could be made available through an EU Health portal and

the commission could provide assistance to the network by raising awareness about the EU legislation.

- Member states should take the necessary measures for the compilation and registration of data allowing at least a view on the medical, financial and administrative information related to cross border care.
- Member states should ensure that identity management is incorporated into all e-Health systems
- FIDIS Work Package 7 is researching and reporting on national and international sources of law (treaties, EU regulations, statutes and regulations, profiling and ambient law)

2.4.3 Processes and procedures

All Member states need to ensure that they:

- Identify, document and describe all processes and procedures related to e-Health
- Monitor and control changes to standard procedures using the documented descriptions of its operations
- Provide training to staff working in the various disciplines, when necessary, and at the appropriate level

2.4.4 Enabling technologies

All Member states need to cooperate with one another to install communication networks within and between other states. They should liaise with ICT organisations to develop appropriate computer systems for their e-Health operations. States should adopt the use of smart and medical insurance cards so that the medical information may travel with the patient to ensure correct treatment in different countries.

The work being developed within FIDIS in WP3 and WP11 should contribute to advances in enabling technologies:

- **WP3**
  - Mechanisms, methods and tools
  - Network protocols
  - Biometrics
  - Standards
  - Models for privacy
  - RFID

- **WP11**
  - Mobile communication networks
  - Private and public access
  - Mobility and identity

2.4.5 Audit

Member states must ensure that they employ appropriate measures to monitor and document its e-Health operations and any deviations from its designated standards and methods of operation as established by EU directives and policies.

2.5 System Domain

In the 5th Work Plan ***D4.12*** focuses on developing a demonstrator, representing an interoperability portal specified in ***D4.10*** "Specification of a portal for interoperability of identity management systems", for disseminating the FIDIS results. The portal will guide actors responsible for developing interoperable identity management systems, especially within sectors such as e-Health and e-Government..

3 Conclusions and future work

Work Package 4 is one example of the transverse perspective that goes across the full spectrum of FIDIS work and integrates the research to ensure the success of the FIDIS NoE. WP4 investigates the interoperability of identity. It is envisaged that the proposed FIDIS interoperability management method and framework, described in deliverables ***D4.6, D4.7***, and ***D4.8*** and applied in this report to e-Health in Europe, will be suitable for performing many of the applications discussed in the EC reports "Connected Health" and "European Interoperability Framework for Pan-European e-Government Services".

Interoperability means systems and services that are connected and can work together easily and effectively, while maintaining patient and professional confidentiality, privacy and security. Common policies and related initiatives concerning interoperability throughout the EU are identified and discussed.

An integrated e-Health network is proposed that brings together patients, professionals, providers, regions, and nations. There is a need to incorporate identity management, including FIDIS research, into existing and proposed information systems by actively participating in developing standards and liaising with other research initiatives and projects. Dissemination of the results of FIDIS research, through the FIDIS journal and proposed interoperability portal is extremely important in this task.

3.1 4th FIDIS Work Plan

To enable the practical adoption of the management method, we have proposed a FIDIS portal, to assist with the dissemination and exploitation of the FIDIS results. The portal will be specified in Deliverable ***D4.10***: "Specification of a portal for interoperability of identity management systems".

3.2 5th FIDIS Work Plan

In the 5th Work Plan ***D4.12*** focuses on developing a demonstrator, representing an interoperability portal specified in ***D4.10***, for disseminating the FIDIS results. The demonstrator portal has the aim of supporting management decision-making in this area by making accessible the work of FIDIS. The work will embrace the various relevant research areas in FIDIS Work Packages.

It will be designed to incorporate and embed the taxonomy and concepts elaborated within FIDIS into the internal structures of the portal. This reinforces the value of the conceptualisations constructed by the NoE.

The demonstrator tool will aid users in the resolution of issues that are raised when developing and implementing identity management systems, such as the classification of identifiers and the application of technology. It will address directly 2 aims established in the 2004 Description of Work – “Making results available on the FIDIS web pages in a form that allows citizens and SMEs to make use of them” as well as “Promoting Interoperability of Identity management systems”.

4 References

FIDIS D4.6: “Draft best practice guidelines”

FIDIS D4.7: “Review and classification for a FIDIS identity model”

FIDIS D4.8: “Creating the method to incorporate FIDIS research for generic application”

FIDIS D4.11: “Overview of reflections and models underlying the health identity management of different types of welfare states in Europe”

FIDIS D16.1: “Conceptual framework for Privacy-Friendly Identity management for e-Government”

The European e-Health Action Plan of April 2004 – Communication (2004) 356 – e-Health

Connected Health – Quality and Safety for European Citizens ISBN 92-79-02705 – EC 2006

European Interoperability for Pan-European e-Government Services ISBN 92-894-8389-X - EC 2004

Yearly Reports of the High Level Group on Health Services and Medical Care to the EPSCO

I2010 HLG – Convergence Discussion Paper (12th December 2006)

Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

ISO/IEC 17799, Information technology – Code of practice for information security management

ISO/TR 15489, Information and documentation – Records management- Guidelines

ISO/IEC JTC 1/SC 27/WG 5, and EG5 Working Drafts:
24760 “A framework For Identity Management”;
29100 “Privacy Framework”; 29115 “Authentication Assurance”
24745 “Biometric template protection”.