FIDIS

Future of Identity in the Information Society

Title:	"D4.11: eHealth identity management in several types of welfare states in Europe"
Author:	WP4
Editors:	Soenens Els and Leys Mark (VUB, Belgium)
Reviewers:	Benoist Emmanuel (VIP, Switzerland)
	Royer Denis (JWG, Germany)
Identifier:	D4.11
Type:	[Final]
Version:	1.0
Date:	Monday, 31 March 2008
Status:	[Final]
Class:	[Public]
File:	WP4-D4.11-final

Summary

This FIDIS deliverable relates to the field of eHealth in general and to the use of health and medical data for various purposes in specific. The use of eHealth tools, such as electronic health records and cards, not only enables the flow of medical data in the 'European Health Information Space'; it also addresses important choices that have to be made by (welfare) states.

The deliverable constitutes of a descriptive part and a discussion section. For the descriptive part, a question list was send to the partners of this deliverable to gather information about European practices in the field.

Subject matters: *eHealth; Electronic health records; Electronic Health cards; medical data; patient mobility; profiling; epidemiological research.*

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 Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	22.12.2007	• First draft (structure and chapters 2-3)
0.2	15.02.2008	• Second draft (including chapters 4-5)
0.3	07.03.2008	• Draft for internal review.
1.0	31.03.2008	• Final Version to the European Commission

Foreword

The text of this deliverable has been written by Els Soenens and Mark Leys (VUB). They made use of the answers provided by the partners based on a question list (for more information about the question list, see later on).

Chapter	*Contributor(s)*
1 (Executive summery)	Els Soenens and Mark Leys
2 (Introduction)	Els Soenens and Mark Leys
3 (Descriptive analysis)	Els Soenens and Mark Leys
4 (Discussion)	Els Soenens and Mark Leys
5 (A agenda for future research)	Els Soenens and Mark Leys

Table of Contents

1 Executive Summary

This deliverable describes eHealth and the use of (health data from) electronic health records and cards in several states in Europe. After an introductory chapter, in which we set the scope and perspective of the study, we present a descriptive analysis of the field. This overview is based on the answers to a question list that the partners of this deliverable received. Issues which are addressed are patient identifiers, access to medical data, the use of medical data for profiling purposes etc. In a following chapter we discuss the results in the light of current development in health care (delivery) systems in welfare states in Europe. Finally, we present some topics relevant to the agenda for future research in the field. We call attention to the fact that further in-depth comparative analyses of social shaping of technology in health care - with a particular attention on profiling - is needed.

2 Introduction

The use of health and health care data is emerging as new societal problem, due to ICT developments. An explosion of the use of ICT in health care (e.g. telemedicine, the Internet, health smart cards) marks the beginning of a wide range of uses of personal health data. Moreover, the use of data is not limited to administrative and medical issues of patients, but the availability of different databases and the potential coupling of these information sources enable to profile individuals. The possibility to use health information in a wide range of contexts beyond the personal clinical relationship should raise social, ethical and legal questions.

In 1999, The European Group on Ethics adopted an Opinion on the ethical aspects of the Information Society. The group listed issues of privacy, confidentiality, the principle of "legitimate purpose", consent, security, transparency and the right for participation & education; these are closely related to the societal problem of profiling.[4] More recently the European funded project 'European Standards on Confidentiality and Privacy in Healthcare' developed a proper framework in which the same principles or put forward.[5]

It is thought that it would be useful for the NoE FIDIS to develop a tentative exploration on how the use of health (care) data, and in particular the development of technological applications, is related to the issue of profiling.

We first explain the scope of the research, including its limitations, the perspective of the study and the formulation of the problem and the operational questions.

2.1 Scope and limitations of the research

In this first exploratory phase on the issue of profiling in health related issues, we concentrate mainly on the collection, storage and use (exploitation) of health data as related to the issue of electronic health records and electronic health cards. Electronic health records and electronic health cards are our core study object. These (different but complementary) tools are currently getting major attention in relation to the development of eHealth (Wilson and Lessens, 2006, 17; Hämäläinen et al., 2007).[6] We look at these tools from a socio-legal perspective.

Our research is comparative. We selected a sample from Northern, Southern, Western and Eastern countries in Europe, in order to get a cross-sectional view of developments in Europe. Switzerland and Norway are included as they are members of the EU i2010 subgroup on health. However, the *selection of countries* is limited. This is due to the fact that we only have a limited number of partners with limited resources to gather information. As a result this study is explorative in nature. The scope of countries is too limited to provide an exhaustive representation of EU states. Further in-depth research is clearly needed. Moreover, our partners all have different backgrounds (such as privacy regulators, IT-universities, law faculties,…). Consequently, the answers to the question list are not homogenous. This makes it difficult and sometimes perilous to put the information in a comparative perspective.

[4] http://ec.europa.eu/european_group_ethics/docs/cp13_en.pdf
[5] http://www.eurosocap.org/eurosocap-standards.aspx
[6] Electronic Health records and electronic health cards are discussed in section 3.2.1.1.

Table 1 gives an overview of the country/-ies and the FIDIS partners responsible for the information provision. Especial thanks goes to the external contributors.

Countries	Responsible FIDIS Partners	External Contributors	Remark
Belgium	Soenens E., VUB (BE)		
Italy	Soenens, E., VUB (BE)		
UK	Dyer, B., LsE (UK)	Prof. R. Jones, Chairman of eHealth of the e-Health Association	
Germany (records)	Raguse, M., ICPP (DE)		
Germany (cards)	Husseiki, R., Sirrix (DE)		
Spain	Daskala, B., IPTS (ES)	Inés Hernando Martin, Coordinator of the Office of Health Affairs, Department of public Services	
Switzerland	Jaquet - Chiffelle, D. – O., VIP (CH)		
Norway	Fischer - Huebner, S., Hedbom, H., Karlstadt (SE)	Kirsi Helkala from the University College Gjövik	
Sweden	Fischer - Huebner, S. and Hedbom, H., Karlstadt (SE)	Rose-Marie Åhlfeld from Skövde University	
Netherlands	Nouwt, S., TILT (NL)		
Bulgaria	Nouwt, S., TILT (NL)		Bulgarian Ministry of healthcare did not react upon the invitation of S. Nouwt to fill in the questionnaire.
Poland	Raguse, M., ICPP		Almost no

	(DE)		information available in English

We now discuss the gathering of information.

Data collection:

The deliverable is based on the information provided by FIDIS-correspondents. Data were collected by means of a common questionnaire (addressing the topics of privacy, profiling, patient identification of electronic health records and cards).[7] The questionnaire was developed as a *frame of reference* to gather as much relevant information as possible. The period for fillling out the questionnaire was set between March 2007 and end of April 2007.

As we will see further, access to information for answering these questions was difficult to obtain within the practical constraints of this workpackage. If any, incompleteness and generality of the answers provided by the partners can to a large degree be explained by the complexity of the field: there is a lack of easy accessible information on a certain topic; it could be because the partners did not find good sources of information. Some national and sub-national organizations and institutions made more efforts than others to provide good access to interesting and relevant information regarding hot issues in the debates and developments.

The partners mostly relied on various national documents on eHealth (e.g. national reports, policy plans, and official communications) and/or information which were provided by third parties.[8] The language barrier was an obvious problem to obtain detailed information for particular countries. Although the co-editors took into account language skills of the partners, sometimes the information available was almost exclusively in the native language of the country. Especially in the case of Poland and Bulgaria, retrieving information relating eHealth seemed to be problematic.[9] Unfortunately information about these countries is lacking.

7 The question list can be consulted at the FIDIS internal portal (http://internal.fidis.net/fileadmin/fidis/workpackages/wp7/eHealth_deliverable_under_wp_4/Question_List-v1.0.doc). The overview document with all answers on the question list is available at: http://internal.fidis.net/fileadmin/fidis/workpackages/wp7/eHealth_deliverable_under_wp_4/Overview_List_ehealth_questions.doc.

8 In this respect, it is important to point out to the discrepancy between policy (documents) and action or deployment of eHealth 'on the field': 'Although the EU health strategy stressed the urge to develop national health roadmaps by the end of 2005, not all European countries have actually such documents (e.g. Belgium). However this does not want to say that there are no eHealth initiatives in Belgium. On the contrary, there are a lot of initiatives in the field of eHealth going on in Belgium. At the other end, it seems that there is often a 'gap between high-level declarations and the delay in practical adoption of eHealth tools': Stroetmann (2007, 32).

9 Relating to Poland, ICPP let know that 'The level of detail you asked for has made it impossible to find appropriate sources in English on the situation in Poland. The sources available are of general nature and do not by far touch questions of encryption, access, control, involved entities, etc but rather a general view on e-health strategies in Poland. Our Polish colleagues were not able to provide help as only resources in Polish exist. Handing the questionnaire to them will be impossible due to limited resources and the estimated time necessary for giving the answers. I am sorry for this.' Related to Bulgaria, TILT informed us of the fact that 'Bulgarian Ministry of healthcare did not complete the question list until now'.

Moreover, in states where health care and eHealth developments are mainly organized on the regional levels, obtaining detailed information regarding differences and similarities in the regions was too time-consuming for the correspondents.[10]

At the moment, no information was communicated regarding the development and use of electronic health cards in Germany (except for some indirect information in the answers on electronic health records).[11]

The state of the art presented in this document is thus necessarily biased and is not offering an exhaustive overview of all information on all topics. The description is based on relevant knowledge from the questionnaires, sometimes complemented with *additional literature & documents*.

Taking into account the particular limitations, some interesting observations on the issue of data collection, storage and use in health care are made, making it worth exploring the issue more in depth in the future. This specific topic could be interesting in relation to other FIDIS initiatives such as the database on Identity Management Systems and the literature collection on AmI, Profiling, Identity and Privacy (D7.10).

2.2 Perspective of the study

This deliverable aimed at sketching the social dynamics within the institutional socio-legal frameworks related to eHealth. It is our aim to understand how personal health data management is fitting into the tradition of welfare states in Europe.

As technology is socially constructed, we want to get a picture of the social construction of technologies related to personal health (care) data. We start from the knowledge that human action shapes technology. The ways in which a technology is used cannot be understood without understanding how that technology is embedded in its social context. In this case we want to get a clearer picture on how eHealth and the use of personal data is embedded in traditions of welfare regimes.

We are mainly interested in the legal, ethical and economical considerations and interest of stakeholders: how do these aspects influence the social construction of the personal health and health care information models in the different countries. We tried to take into account specific normative and cultural elements to welfare states of the countries under investigation.

---

10 For example, in Spain, the 'model is heavily decentralised (Colección Fundación Telefónica (2006) Sociedad de la Información – Las TIC en la Sanidad del Futuro. Informe realizado por Telefónica S.A. y Editorial Ariel S.A.) with each of the 17 Autonomous Communities implementing its own system, resulting in 17 different eHealth system implementations; especially considering that the levels of implementation of the eHealth systems differ from one to the other (in some Communities it is in a more advanced implementation phase than others). This also explains the fragmentation in the answers to the questionnaire.' (…) 'We have sent questionnaires to the responsible persons in the regional government of the Communities of Andalucía, Madrid and Cataluña, but unfortunately we received only reply from our contact in Andalucía. Andalucía is one the largest and most populated region (more than 18% of the whole Spanish state) (Vallejo Serrano, F. (2004) Building the Regional eHealth Network - The Andalusian Experience. Included in e-Health – Current Situation and Examples of Implemented and Beneficial E-Health Applications, Eds. Iakovidis, I., Wilson, P. and Healy, JC, Technology and Informatics, Volume 100, IOS Press). As such, we considered it an important Community to provide input for this study' (answer IPTS).

11 For interesting resource on health cards in Germany, we can refer to the brochure of the Federal Ministery of Health, available at: http://www.die-gesundheitskarte.de/download/dokumente/broschuere_elektronische_gesundheitskarte_engl.pdf.

We aimed at getting a better picture of choices made by different stakeholders on eHealth personal information issues, but the information gathered did not allow for analysing these issues. These aspects will definite require further investigation.

A better understanding of the use of personal health data within the context of welfare states in the Europe is crucial to develop adapted business models for implementing future health knowledge technologies.

The relationship to policy issues is obvious, as choices on the organization and legal frameworks around the development and use of technological infrastructures for capturing personal health data will raise the issue of individual and collective responsibilities. Moreover on a scientific level this deliverable is stepping stone to understand the 'social construction' of patient and health information models and to assess the potential opportunities and challenges related to the technological support tools when dealing with personal health data.

2.3 Formulation of the problem and operational questions

Electronic health records and cards are perceived as useful tools in the realisation of the eHealth vision in Europe (see 3.2.1). Electronic health records and cards create a huge potential to collect, save and use health data of citizens for various purposes. In general terms the current debate on the use of ICT in collecting, storing and using health care data seems to be approached rather from an instrumental way, with major attention on technological standards, interoperability, content issues etc. In addition to this, a rather separate debate seems to get form on the ethical and privacy issues related to health and health care data: but even this debate seems to be approached as a rather 'instrumental' issue that has to be dealt within technological ways.

We do hypothesize that the use of health information and the related profiling issue, is not solely a technological, but to a large extend a sociological issue: it is of utmost importance to study how and to what extent profiling questions are legitimized and what types of societal issues are related to personal health data. Moreover it would be of particular interest of getting a clearer picture on how different policy makers are (not) addressing the topic of personal health(care) data in their policies. Profiling practices in health care could not only affect citizens' privacy and autonomy, but also the groundings of health care in welfare states.

We tried to address the issue in some preliminary operational questions that will help to sketch the field:

eHealth in general:

- What is eHealth, the electronic health record and electronic health cards?
- What are the narratives in the debate on eHealth (and especially in relation to the use (the collection, saving and processing) of health/medical data)?

eHealth tools in specific:

- What is the state of art of deployment and implementation of eHealth tools in the questioned countries?

profiling:

- What about the collection of medical data?
- What about saving medical data?
- What about using medical data?
- What are the benefits and risks of electronic health records and cards in relation to profiling practices?

2.4 Summery of main results

There seems to be a *lot of diversity* in the deployment and use of the electronic health records and electronic health cards. Variety can be related to specific necessities in the institutional fields (e.g. primary or secondary line of care, centralized or decentralized systems). Despite the European health insurance card which is mandatory in European countries, little initiatives on electronic health cards were reported. The use of smart health cards to safely access information in electronic health records is promising but actually still in its infancy. Yet it is argued by several countries that, in order to be trustworthy, eHealth systems have to ensure careful access and cautious use of citizens' medical data. Patient and health care identifiers can play a crucial role in this process. Quite a few countries have indicated new initiatives in this field.

Although the countries indicate that the collection and processing of medical data must foremost be seen in the light of simplified communications between healthcare professionals and between healthcare professionals and patients, as well as in the light of cost-effective and efficient health care delivery, it can not be denied that eHealth tools (will) *facilitate profiling practices* to a bigger circle of parties.

In general terms too little attention is being paid to the *particular nature of health care*, as a sociological, cultural, political and economic construct. Health care is not like other industries; moreover it is directly related to welfare issues. Universal access, social justice and quality of the healthcare systems are aspects which must be taken into account before designing and implementing eHealth. Socio-technical choices in health care have to be made within the specific normative, regulative and cultural context of regions or nations. In European democratic societies, this necessarily implies multifaceted balancing practices.

3 Descriptive analysis

3.1 Profiling practices and medical data: what is the issue?

Currently in health care, a lot of attention is being paid to develop tools to capture, monitor and store bio-medical and insurance social data as well as to integrate these data to construct 'health identities', for different purposes. Now it is believed that 'time is right' to reach the 'necessities' of guaranteeing 'quick and easy access to health and insurance data' and of creating more interoperability between the health care (delivery) systems (Directorate General for Research, 2001). This vision enables profiling of health data.

Medical data is understood as 'all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data' (Council of Europe, 1997). The EU published a recommendation for the protection of medical data[12] and in 2007, the Article 29 Data Protection Working Party made efforts to develop a draft framework for the processing of personal data relating to health in electronic health records (Article 29 WP 2007).[13] The Article 29 Data Protection Working Party argued that all data in the electronic patient records must be considered to be sensitive data (Article 29 Data Protection Working Party, 2007). This brings about the duty to foresee additional safeguards when processing the data.

The development of electronic health record systems has 'the potential not only to process more personal data (e.g. in new contexts, or through aggregation) but also to make a patient's data more readily available to a wider circle of recipients than before' (Article 29 Data Protection Working Party, 2007).[14] In sum, we can not ignore that eHealth creates a major bearing surface to (further) process medical (personal) data.

Profiling of health data is a new topic for the NoE FIDIS. As a frame of reference we use the definition of the FIDIS Work Package 7:

"Profiling is 'the process of constructing profiles (correlated data), that identify and represent either a person or a group/category/cluster, and/or the application of profiles (correlated data) to identify and represent a person as a specific person or as member of a specific group/category/cluster;' (Hildebrandt and Backhouse (eds.), 2005, 17).

Following this definition, it could be argued that electronic health records and cards are profiling practices.[15] At least, they are important enablers for profiling. The electronic tools

[12] Council of Europe, Recommendation R (97) 5 on the protection of medical data (13 February 1997)

[13] The working group made recommendations relating to 1. Respecting self determination, 2. Identification and authentication of patients and health care professionals, 3. Authorization for accessing EHR in order to read and write in HER, 4. Use of EHR for other purposes, 5. Organisational structure of an EHR system, 6. Categories of data stored in EHR and modes of their presentation, 7. International transfer of medical records, 8. Data security, 9. Transparency, 10. Liability issues, 11. Control mechanisms for processing data in HER.

[14] Recently, a healthcare professional who did not had any reason to access and look into the medical record of the Yves Leterme Deputy Premier of the Belgian Government, when he was hospitalized, has been fired. Although there was a post-hoc procedure in order to identity the healthcare professional, it could not prevent the access to the medical data of the Deputy Premier.

[15] According to the definition of Hildebrandt and Backhouse (2005, 17), it could be argues that electronic health records are 'correlated data that represent a person': information in the EHR that classify citizens as individual data subjects belonging to

become bearers and new handling techniques of data, which can be used for profiling practices. These are facilitating tools to construct profiles (knowledge) that could be applied onto specific patients or groups/clusters of patients / citizens.

Profiling is thus becoming a mere result than the initial purposes of new ICT initiatives in the area. But within eHealth developments the issue of profiling is seldom explicitly tackled.[16] For instance the debate in eHealth is seldom coupled to debates on e.g. privacy enhancing technologies or debates on the actors gaining access to information. This is particularly striking as eHealth tools such as the electronic health card and the electronic health records smooth the way to process health data enabling profiling practices. For example, practices like risk selection procedures, quality analysis, evidence based health care, and other less innocent health care data related practices such as health (care) behaviour, profit from the collecting and storing of health data (e.g. in records and cards). Some stakeholders (within and outside the health care sector, such as governmental policy makers, research agencies, (health) insurance companies and employers) have clear interests in the availability and use of health related data. Moreover, issues such as integrating health (care) data across a wider range of disparate databases can lead to particular issues such as accidental disclosure or improper use of data.

Whenever personally identifiable information is collected and stored, improper analysis and disclosure can be the root cause for privacy issues, as is clearly discussed in article 8 of the European Convention on Human Rights. The European Commission has therefore proposed a Directive on the protection of personal data in 1998 containing eight key principles that any actor processing personal data must comply with: (1) Fairly and lawfully processed, (2) Processed for limited purposes (3) Adequate, relevant and not excessive (4) Accurate (5) Not kept longer than necessary (6) Processed in accordance with the data subject's rights (7) Secure (8) Not transferred to countries without adequate protection.

The European Data Protection Directive clearly incorporates the concepts of 'obtaining', 'holding' and 'disclosing' information. All EU member states adopted legislation pursuant this Directive or adapted their existing laws, and each country is expected to have its own supervisory authority to monitor the level of protection; and this policy is also clearly related to medical and health (care) data

The issue of handling health care data is a complex one, that cannot be discussed in general “black” or “white” terms of moral justifications for justifying data handling and protection regimes. Some clear work has to be developed on identifying the “field”, specifying which parties and stakeholders are involved, within which normative rules the question of data handling and access to information is developing, on which domains within (medical issues, coordination and collaboration of parties, administrative purposes, insurance aspects) and outside the health care sector (insurance, marketing, justice, …) and for what purposes health care data are handled, including the question of information exchange within and outside health related sectors.

Profiling health data brings about opportunities and risks at the same time. Some of these opportunities and risks will be addressed hereafter.

---

a group or a category. This leads to indirect individual profiling, in the meaning of Jaquet-Chiffelle (2008, 56) who differentiates between direct individual, direct group, indirect individual and indirect group profiling.

[16] Most important publications of the EU on eHealth focus on “instrumental” issues such as the free movement of patients and data (see action plan on eHealth 2002, 2005).

Opportunities:

Under limited and specific conditions[17], the processing of data from electronic health records is allowed in the context of **medical scientific research and government statistics**. The Article 29 Data Protection Working Party stresses that, when possible, these data should be anonymized (or pseudonomynized).

Practices as evidence based medicine, managed care and disease management - profit from the use of eHealth tools. These profiling practices are enabled by 'automatic data extraction from electronic health systems that operate according to Europe's legal requirements on data protection and privacy' (COM (2004) 356 final). In general, recorded health data can be used for 'quality assurance, benchmarking, reimbursement, better management and control; disease surveillance and emergency preparedness, decision support, public health monitoring, knowledge generation and research (Unit ICT for Health in collaboration with the i2010sub-group on eHealth and the eHealth stakeholders' group, 2006). According to several authors, the use of personal health data is fundamental to perform quality research of health (services) (Gostin, Hadley, 1988; Chamberlayne et al., 1998).

The use of health care data is also seen as an opportunity for health services and epidemiological purposes. "Data about the use of medical services in the files and databases of health-insurance companies, or data from medical files or electronic care records maintained by health-care providers, could be merged and analysed. These analyses can result in the description and prediction of the incidence and prevalence of diseases. They also enable epidemiologists to ascertain and find high-risk groups, and to determine relations between chances of recovery from diseases and other – until now as yet unknown – influencing factors, etc.' (Vedder, 2000).

Similarly, data can offer added value for e*vidence based management* & evidence based health care. The EU itself is very active in the domain of Public Health programmes. There are lots of European activities in the domain of health reporting, which is perceived to enable evidence-based health policy. Health risks and necessary treatments of individual patients are based indirect on (individual) profiling.[18]
Disease management has been described as 'a strategy of delivering health care services using interdisciplinary clinical teams, continuous analysis of relevant data, and cost-effective technology to improve the health outcomes of patients with specific diseases. It includes self-care management techniques, patient education, and provider training. Disease management provides individualized care plans based on clinical guidelines to manage individuals with

[17] 'in line with the Data Protection Directive (cf. Article 8 (4) and the corresponding Recital 34): they must therefore be foreseen by law for previously determined, specific purposes under special conditions to guarantee proportionality ("specific and suitable safeguards") so as to protect the fundamental rights and the privacy of individuals.': (Art 29 Working Party, 2007, 16).

[18] See terminology of D.-O. Jaquet-Chiffelle, in Hildebrandt and Gutwirth, (eds), 2008.

treatable chronic diseases.' (National Pharmaceutical Council). Disease management is closely related to the development of managed care. *Managed care plans* are health care delivery models that integrate the financing and delivery of health care. It is an especially American approach to control the use of health care services. It assesses medical necessity of interventions, makes (financial) incentives to use certain providers, and uses the principles of case management. Managed care techniques are most often practised by organizations and professionals that assume risk for a defined population, which implies that managed care organizations generally negotiate agreements with providers to offer packaged health care benefits to covered individuals. *Managed Care* 'implies the provision of information to or by a third party with the objective of creating equilibrium between the need for and the supply of care.' (Hooghiemstra, 1998, 38).

Risks:

Risks of the use of health data for profiling practices relate especially to privacy, individual autonomy and freedom of choice of citizens. In particular when health information is combined with other sources of (medical) information, much more knowledge about the citizens is known (Redigor, 2004). In relation to EHR systems, the Article 29 data Protacction Working Party speaks of a 'new risk scenario' for privacy protection. Even if 'this new risk scenario will be fully realized by most projects only in a future state of full-scale implementation' (Article 29 Data Protection Working Party, 2007, 5), we should already take into account this new risk scenario when designing EHR systems.[19]

eHealth tools can enable easy and widespread access to sensitive information. In the context of information management, third parties have more and more access to this sensitive information. E.g. in most cases of managed care, information management (based on individual patient data) is done by a third party. Managed care can be privacy friendly, but it has to be guided by the rationales of medical secrecy and in accordance with article 6, 1, b of the Data Protection Directive,[20] and in line with the provisions on sensitive data described in article 8 of the Data Protection Directive. PET's can help to 'inscribe' the juridical safeguards into the architecture of databases (Hooghiemstra (ed.), 1998). At least in theory, anonymization and pseudonymization of citizens' data guarantees the privacy of citizens' in profiling practices. Although pseudonymization bears the risk of re-recognition (surveillance of a citizen without actually knowing his or her identity).

It has been argued that profiling of health data not in function of individual or public health issues should be prohibited. For example, when medical practitioners access electronic health records this should be in function of the treatment of a specific patient and not as 'expert for private insurance companies, in litigations, for granting retirement aid, for employers of the

[19] 'Value in technology design' researchers especially stress that political and social implications of technologies are already embedded in technological design. See e.g. the Value in Technology Design Project at the New York University supported by the Ford Foundation's Knowledge, Creativity, and Freedom Program, under directorship of H. Nissenbaum: http://www.nyu.edu/projects/valuesindesign/index.html.

[20] Article 6,1, b of the Directive 95/46/EC: 'Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards'. (Further processing is allowed if there is not re-identification to the individual patients possible.)

data subject etc.' (Article 29 Data Protection Working Party, 2007). However, the secondary use of health (care) data would allow for useful policy issues and support taks to improve health care policies (performance management, evidence based health care, quality monitoring, etc.) There is thus necessarily need for a reflection of the secondary use of the (often fragmented) databases of health care data, including the potential purposes of these forms of secondary use of data. Especially the debate on who is getting access to health care data, under what form, for what purposes has to be discussed more profoundly and embedded in a framework of (legal) guidelines.

3.2 eHealth and processing of health data: a descriptive overview.

3.2.1 EU level

3.2.1.1 eHealth, electronic health records and electronic health cards

The European Union's commitment to eHealth started as long ago as 1989 under the label 'healthcare computing' (Wilson and Lessens, 2006). The Advanced Informatics in Medicine Program (1989-1991) already stressed the use of computer technologies for medical practice. Whereas its successor (1991-1994) focused (exclusively) on the needs of health care *professionals*, the following Program 'Telematics Applications for Health Programme' focused rather on 'users' needs' in general (Wilson and Lessens, 2006). Since the 5th RTD framework program (1998-2002) the term 'eHealth' is coined (Wilson and Lessens, 2006). In 2003 the ministers of the EU member states Acceding and Associated countries, as well as EFTA countries met on 22nd May 2003 in the framework of the eHealth 2003 conference organised jointly by the European Commission and the Greek Presidency of the Council. At that event, eHealth was defined as 'the use of modern information and communication technologies to meet needs of citizens, patients, healthcare professionals, healthcare providers, as well as policy makers'. The European perspective on eHealth embodies the wish to fundamentally improve health care in Europe. eHealth should support Member States 'in realizing and sustaining the common values and goals characteristic of Europe's social infrastructure' (Stroetmann, 2007). Although health care is a national responsibility in the European Union, the development of a European health services market and thus the cooperation of the Member States with the European Commission, could help to obtain both the specific objectives of the national health care systems as well as the goals of the European Union (for example in relation to the Lisbon Strategy).[21]

The development and use of electronic patient records (EPRs)[22] and cards are crucial elements to eHealth. An electronic patient record can be defined as a 'comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical

[21] The cooperation between the EU and the member states needs coordination. Therefore, projects as the the eHealth ERA project have the duty 'to coordinate planning of national innovation-oriented research and technology development (RTD) in e-health in the Member States of the European Union.'. See: http://ec.europa.eu/information_society/activities/health/policy_action_plan/i2010subgroup/ehealth_era/index_en.htm. This project has been very informative in the field of ehealth. The final project report 'Deliverable 5.3 in the framework of the eHealth ERA project' by Karl A. Stroetmann (in cooperation with the project partners, 2007), summerises the ten official outputs of the project.

[22] Note: the terms 'electronic patient records (EPR)' and 'electronic health records (EHR)' are used exchangeable throughout the deliverable.

treatment and other closely related purposes.[23]' (Art 29, Data Protection Working Party, 2007). There are so many (small and bigger) differences between electronic health/patient files in and between countries. Some of the major differences relate to the (1) *Content*: e.g. summaries versus 'full' records. (2) *Role of patient*: e.g. patient managed records versus health care professional managed records. (3) *Scope*: e.g. record on a regional level versus national wide. (4) *Use*: e.g. for primary care versus records for secondary care levels.

The current activities on electronic health cards actually concentrate mainly on the implementation and use of electronic health **insurance** cards.[24] It is interesting to differentiate between the two types of cards (although in practice they can be integrated).

Electronic health insurance cards allow 'access to health care' and make 'management and billing easier' (COM (2004) 356). Electronic health insurance cards are 'intended to cover care that becomes necessary whilst in temporarily another Member state for other reasons.'[25] (SEC (2006) 1195/4).

As stipulated by the European Commission, member states should implement the electronic health insurance cards (which replace the E111 files) by 2008.[26]

Electronic health cards 'may carry emergency data (such as blood types, pathologies, treatments) or medical records, or may allow access to these data over a secure network'(COM (2004) 356 final). In the latter case (this is when the electronic health data is not stored on the electronic health card), the card - coupled to the patient identifier -could provide a key to access electronic health records. (Bourret, 2004, 107). The Article 29 Data Protection Working Party also believes that smart cards are a suitable way to access health data (2007). As a result, there is a close link between the development of electronic health records, patient identifiers and health cards.

EPRs and cards could not have been developed without technological developments. But (socio-technological) conditions defining priorities, strategies and values that are believed to be essential for the future of health care and for the European welfare states in general, have an equally important impact. The development and use of electronic patient records and cards are both affected by and affect the health care systems in the European states. As a result, the EHR and electronic card systems must be seen as specific and sometimes unintended outcomes of social, economical and normative *discourses* in health care and society in large.

In the following section, we search for crucial narratives / discourses which play a role in the realization of eHealth and the development of EHR and cards.

3.2.1.2 eHealth discourses

Four issues have dominated the European debate on eHealth in general and health data in specific. These issues are connected but all have their specificity and backgrounds.

[23] 'Medical treatment and closely related purposes' refers to the purposes mentioned in Article 8 (3) of the Directive.

[24] For an overview of the history of the European health insurance card project: http://ec.europa.eu/employment_social/healthcard/coinexpert_en.htm.

[25] This is: you don't go abroad especially for the treatment (patient mobility).

[26] At least this was the ambition of the Commission in February 2003. Actually, the EC acknowledges the huge diversity between national electronic (health) cards and recommends now a more gradual approach 'integrate EU information inside national electronic health cards and therefore harmonise natinal projects in order to try to reach interoperability' (Eurosmart, 2005) (see also action plan 2004).

First of all, the European strive for free movement of citizens and goods has influenced to a large degree the discourse on eHealth. In the context of health care, the free movement refers both to the freedom of citizens to easily and safely seek for health care abroad as well as to the free movement of health data in Europe (under legal-technical restrictions). In several cases at the end of the nineties, the European Court of Justice argued that the internal market should be open for health care provisions.[27] Cross-border health care and patient mobility in specific[28] has become a 'hot topic' on the European agenda.[29] Cross-border health care is a perfect catalyst in the realization of an European Health Information Space: *'In a Europe in which our citizens are increasingly mobile – whether within the borders of their own Member State or among different countries – we need to raise awareness of the pressing need for a more integrated and interoperable European Health Information Space'* (Conclusions of the eHealth Conference, 2005). This requires co-operation on the European level (COM (2004) 301).[30] The European health insurance card and other eHealth related applications to realize this in a safe and efficient way. Such tools can provide the essential information at the right time, at the right place and as such, they help to develop chains in health care beyond national borders. The symbolic value of the card can not be ignored.

A second rationale is found in the consumerist discourse on patient empowerment, a core aspect of Europe's ambitions for health care. It is the idea 'to empower patients with a sense of ownership of their own health care, and to improve communication between patients and clinicians…' (Stroetmann, 2007, 32).[31] Patients have become 'active consumers of healthcare' (Stroetmann, 2007). They autonomously inform themselves, pick and choose a healthcare provider (abroad). In line with the idea of patient empowerment, is the idea to make people more responsible for their own health. The shift in responsibilities is very clear in the 'New

[27] This was the judgment of the ECJ in the Case C-120/95 Decker (1998) ECR I-1831 and the Case C-158/96 Kohll (1998) ECR I-1931; health care is not exempted from the EC Treaty's rules on the free movement of goods and services.

[28] Actually, patient mobility is just one of the four categories of cross-border healthcare. Patient mobility explicitly refers to 'use of services abroad (ie: a patient moving to a healthcare provider in another Member State for treatment)': (SEC (2006) 1195/4). The other categories are: '1) cross-border provision of services (delivery of service from the territory of one Member State into the territory of another); such as telemedicine service, remote diagnosis and prescription, laboratory services. 2) Permanent presence of a service provider (ie: establishment of a healthcare provider in another Member State), such as local clinics of larger providers. 3) Temporary presence of persons (ie: mobility of health professionals, for example moving temporarily to the Member State of the patient to provide services)': (SEC (2006) 1195/4).

[29] The issue has extensively been addressed by the European Commission in a communication titled 'Follow-up to the high level reflection process on patient mobility and healthcare developments' (COM (2004) 301). 'High Level Group on health services and medical care' was establish to perform health technology assessment and to take into account the recommendations of the high level reflection process on patient mobility and healthcare developments (see the 2003 report of the High Level Process of reflection on patient mobility and healthcare developments in the European Union. Available at: http://ec.europa.eu/health/ph_overview/Documents/key01_mobility_en.pdf). Other EU document on the subject: Communication from the Commission to the Council, the EP, the European economic and social committee, and the committee of the regions, 'Modernising social protection for the development of high-quality, accessible and sustainable health care and long-term care: support for the national strategies using the "open method of coordination"', COM(2004) 304 final; Communication of the Commission: 'Consultation regarding Community action on health services' September, 2006; Commission: 'patient mobility in the European Union – Learning from experience (results of the Europe4Patients Project)', June 2006; DG Health and Consumer Protection; Background; Patient Mobility and healthcare development'; Communication from the commission, 'Consultation regarding Community action on health services', SEC (2006) 1195/4.

[30] Health is a matter which is governed by the subsidiarity principle.

[31] This relates also to the idea of minimizing information asymmetry in the relation between the patient and the healthcare provider. Patients are empowered to have insight in their medical records. In case the relation between the patient and healthcare provider is threatened, the right to look at one's medical record empowers the patient vis-à-vis the healthcare professional.

NHS' program in the UK: 'shifting responsibility to the patients and their families the main basis of a 'New NHS' (National Health Service)' (Bourret, C., 2004, 97).

The third discource is grounded in the emerging problem of the scarcity of resources in health care: policy makers look for ways to (fairly) control or reduce costs. eHealth is assumed to contribute to cost-efficiency, in a context of more expensive health interventions and technologies and the greying of society. Recent projections by the European Commission suggest that age-related public expenditures, such as public pensions and health care spending, will raise by 4% of GDP on average for the European Union in about 45 years from now (see e.g. EPC, 2006). Sustainability of the current welfare provisions as we know them is often linked to *cost-effective measures*. Typical economical concepts as quality control, budget planning and economical savings are mentioned in relation to the use of electronic health records. (Stroetmann, 2007; Bourret, 2004, 96).

Finally, within the EU discourse eHealth 'is today's tool for substantial productivity gains, while providing tomorrow's instrument for restructured, citizen-centered health systems and, at the same time, respecting the diversity of Europe's multi-cultural, multi-lingual health care traditions' (Com (2004) 356). The issue of innovation is considered essential in the realisation of eHealth in Europe. The economic aspirations of the EU are remarkably entangled in the domain of eHealth. The market-oriented approach on health is demonstrated as eHealth applications use concepts such as 'B2C' (for example, the patient can find relevant information regarding a healthcare organization, a treatment or illness on the internet); 'B2B' (for example, the 'simplification and acceleration of data transfers between medial institutions' and 'C2C' (for example, the 'possibilities to get informed and comminucate with other patients') (Leys en Potloot, 2004; Scott et al., 2000, 61). This focus on the health care market is striking, as health care in a European tradition has always been linked to the particular traditions of welfare regimes, in which distributive correction mechanisms are core issues in health care market issues to ensure equity, solidarity and fairness.

We briefly sketched some of the narratives currently dominating the EC discourse on eHealth, trying to illustrate that on the European level the debates on technological development is mainly getting form in what could be labelled as the "Lisbon treaty discourse": "economic development, technological innovations and free movement of people" are coming to the fore as core values. However, particularly related to health related issues, it could be questioned whether the dominance of this discourse is not blinding for some other welfare related values and ethical considerations in health and health care, that could be of equal importance when discussing the use of health related data.

Furthermore, we are not blind of the existence of (recent) initiatives of the EU on data protection and privacy related issues. However, we have the impression that this debate is a sectorized one, and not necessarily fully integrated in the local policies on eHealth developments. An explanation for the differences is to a large extent to be sought in the subsidiarity principles of the local member states and Europe in health care related issues. Subsidiarity in health care is the principle that matters ought to be handled by the smaller (or lower) competent authority in the member states. The European treaty literally states: 'In areas which do not fall within its exclusive competence, the Community shall take action, in accordance with the principle of subsidiarity, only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the Community'.

The EU may only act (i.e. make laws) where member states agree that action of individual countries is insufficient. In organisational issues related to health care policy and the organisation of the welfare regimes, this authority is not delegated to the European higher level. However, over time "Europe" has been taking direct responsibility for the selection and implementation of projects and activities related to the European policy level agenda, also in the field of eHealth, but clearly in a different perspective than the one related to the organisation of health care within member states and/or their regions. The division of competencies and the particularities of institution logic are to a large extent explaining the innovation and market-oriented discourse in health related issues on a European level. But it is also clear that the subsidiarity principle in an issue such as health care data within the organisation of health care systems could prohibit a sound discussion on a European level, taking into account the particularities of welfare regimes. Currently, economic principles and issues of technological innovation dominate the debate, but their consequences for health care are hardly taken into account.

3.2.2 eHealth and the use of health data: results of the questionnaire[32]

3.2.2.1 Crucial issues in relation to the development of eHealth as reported by the partners[33]

In most countries the debate on eHealth was initiated top-down (e.g. the Netherlands, Switzerland, Belgium, Spain and Germany). Institutions and organizations that deal with health and welfare in specific (e.g. Ministries or governmental departments on Health) are the fore-runners in this debate (e.g. in Netherlands, Belgium, Spain, Germany, UK). The Swiss answer mentions CEST, a Swiss organization which concentrates on science and technology development as the initiator of the debate. In Italy the Department for Innovation and Technologies, alongside with the Minister of Health, appears to play a major role in the development of eHealth initiatives. People from telematics are other important actors (mentioned by Belgium and Italy) In Sweden the debate seems to be initiated from below (from the level of people working in health provision). In Hungary, the debate on the use of eHealth seems mainly to be initiated from pressure groups of doctors and pharmacists. The Norwegian answer explicitly refers to health enterprises, general practitioners and the National Insurance Service as important players in the development of a debate on eHealth.

There was a lot of agreement on what appear to be the most important **reasons** to implement eHealth (tools). Countries appreciate eHealth because these applications enhance efficiency, quality and security. This 'trio' has been mentioned explicitly by almost all countries. For a lot of countries, eHealth appears to be important to guarantee simplified (centralised) communications between health care providers (Netherlands, Hungary, Belgium, Germany, Italy and UK). Several countries state that stakeholders (e.g. policy makers) stress the ability to be cost-efficient or to reduce costs (Spain, Belgium, Germany, Italy and Hungary). The issue of patient-centressness was mentioned by the Belgian and Italian answer. Patient mobility is mentioned as an important catalyst for eHealth in Spain and Italy (countries where health is a regional responsibility). According to the Swiss answer, eHealth should not only

[32] For an overview of all information provided by the partners we refer to the overview document, available at: http://internal.fidis.net/fileadmin/fidis/workpackages/wp7/eHealth_deliverable_under_wp_4/Overview_List_ehealth_questions.doc.
[33] Question 2 – 4 and 14 of the question list.

facilitate old ways of doing business in health care, it can also bring about some new processes and ways of thinking about the organization of health care.

Questions were asked on the crucial issues in the development and use of eHealth tools. Some interesting (socio-ethical) aspects relate to the position and role of insurance companies in the health information space (mentioned by Germany, Spain and Netherlands). Health insurance companies already know a lot about our medical history. The electronic health record systems and especially the use of unique national identifiers could enable the access and processing of medical data by health insurance companies. A lot of countries wonder how to organize the identification of patient and of health care providers. Should this preferably be done by using national social security identifiers or rather by using health care-specific ID number) (issue on identification is mentioned by Netherlands, Belgium, Hungary and Germany)? In Belgium there seem to be discussion about possible changes in the doctor-patient relation due to the conflict of eHealth tools with healthcare professionals' duty of medical secrecy. Germany and Hungary explicitly mention the question on how eHealth could organize transparency in health care. Protection of privacy and identity of citizens is a big concern to the questioned countries. When looking at the country answers, it seems that this worry calls for technical and legal measures. Several countries mention the need for technical standards for interoperability and storage of data and the development of secure and effective telematica platforms (e.g. Germany, Belgium, Sweden, Italy, UK and Norway). Access control is an important technical-legal issue. Other legal issues at stake are the issue of consent and the applicability of data protection legislation (e.g. Switzerland, Netherlands, Spain, Belgium, Germany and Italy) [34]

The countries mention various **actors** involved in the development of eHealth records. Obviously, national or regional governmental bodies and (organizations of) healthcare professionals are mentioned. Other frequently mentioned actors are the social security organizations, insurance companies and product industry. Only a few countries explicitly mention the institutions that deal with data protection and privacy protection (Norway and Belgium). However in most countries, and especially in Germany, the actors in the legal field have to be considered as important actors. Institutions such as the Norwegian KITH and Swiss TARMED are mentioned as important actors in the development of technical standards for eHealth applications (e.g. in the area of the records, resp. medical billing).

According to Newman and Bach (2004), there seems to be a country-specific relationship between the national regulatory system for health matters and the way data protection authorities are organized: 'unitary governmental systems like the U.K. have a centralized data protection authority while federal governmental systems like Germany rely on a decentralized network of regulators at the federal and state levels.' Central regulatory authorities seem to be favored for public sectors such as health. However, since public– private cooperation is growing in the health care sector, decentralized networks ('primarily engaged in advising legislators and the private sector' (Newman, Bach, 2004) do have an important supportive and co-operative role in the field as well.

[34] In the following sections (3.2.2.3 - 3.2.2.5) we tackle several of these issues more in detail.

3.2.2.2 State of art of deployment and implementation of eHealth tools[35]

3.2.2.2.1 Electronic health records

Several states already implemented electronic health records as tools to support eHealth (see also the results of Hämäläinen et al. (2007)). Concepts as 'electronic health record', 'electronic patient file', 'patient health file', 'electronic medical records' (Netherlands), 'electronic locum record for GPs' (Netherlands), 'electronic case record' (Germany), 'electronic medical file' (Belgium), 'virtual patient record' (Italy), 'citizen-managed personal electronic health record' (Germany, under preparation), 'central electronic health record' (Germany), 'summarised electronic health record' (Belgium), 'NHS care record' (UK), … all refer to the electronic health or medical records. A lot of initatives are still in the implementation stage (see also Stroetmann (2007, 29), Wilson and Lessens (2006, 19) and Nouwt (2007, 161)). In Germany a 'citizen-managed personal electronic health record' is currently under preparation. In the Netherlands the 'electronic medication file' (EMD)[36] and 'observation file generalist' (WDH)[37] are in test phase in pilot regions. In Switzerland, the electronic patient record will be used only from 2015.

A lot of countries report great differentiation in health records (system specific use of systems depending on the needs of the level of health care, the type of organizations and the region of deployment). The Health Information Network Europe survey confirms this differentiation in the levels of sophistication between European countries as well.

As a result of the highly diverse standards and types of records, integration between health records is currently not that common (for example Switzerland, Germany). Regions/countries try or plan to enhance interoperability and communication between the Health Records (the Dutch AORTA, Swedish harmonisation efforts, the example of the German region Rhine-Westphalia, the Belgian BeHealth platform and decentralised FLOW, the Spanish Plan Avanza). The UK Map of Medicine is another example of a decentralized way of merging information from health records. Some countries explicitly mention the efforts to create (national or regional) standardization in the use and development of health records (for example the Swiss national health strategy, Swedish Carelink project, Hungarian Standardization Committee; Spanish plan Avanza, the Communicating for health program in the UK). According to CEN (The European Standards Committee) this does not mean that European states have to make all electronic health records uniform in every detail.[38]

The operational advantages of health record systems in health care are mentioned as important purposes by our partners. According to the answers of the partners, the intended use of electronic health records must mainly be seen in relation to the enhancement of communication between healthcare professionals and between healthcare professionals and

[35] Question 8, 9.1, 28 and 29.1 of the question list.
[36] Elektronisch MedikatieDossier
[37] WaarneemDossier Huisartsen
[38] According to (CEN) the most suitable European EHR architecture is '… a model of the generic features, necessary in any electronic healthcare record in order that the record may be communicable, complete, a useful and effective ethic-legal record of care, and may retain integrity across systems countries and time. The Architecture does not prescribe nor dictate what anyone stores in their healthcare records. Nor does it prescribe nor dictate how any electronic health care record is implemented. (it) places no restriction on the types of data which can appear in the record, including those which have no counterpart in paper records. … Details like 'filed size' coming from the world of physical databases, are not relevant to the electronic healthcare record Architecture.' (Garland, 2002).

patients. Electronic health records are used make an overview of the the medical history of patients within particular health care settings (Norway, Netherlands, Spain, Italy, UK...). Electronic health records are also assumed to enhance quality and continuity in the delivery of health care to a specific patient inside a specific context (hospitals or 'locum GPs' (see Netherlands)). The Belgian answer also stresses the symbolic function of electronic records (General Practitioners are put at the centre of first line care). Next to the benefits for the communication and efficiency, electronic records are assumed to be useful for administrative purposes (e.g. billing). Switzerland and Hungary explicitly refer to the role of insurance funds in the development of centralised patient information from the electronic record. In Hungary the EHR system is used to deal with the problem of defaulters to pay their insurance membership. The use of health records for epidemiological reasons has been mentioned as well. The Belgian, Spanish and Italian (Jhospital system) answers point out to the use of health record data on the aggregated level to investigate and optimize the delivery, quality and organization of health care. The emergence of clinical pathways and health trajectories has become an important field of research.

3.2.2.2.2 Electronic health cards

In general, we received little information on the state of the art on electronic health cards in the selected countries. Several countries report that no electronic health cards exist (Norway, Netherlands and Sweden). However, the European health insurance card, introduced by a decision of the European Council of Barcelona 2002, has been implemented in the European Economic Community since 2004 - 2005. Next to the European health insurance card, some countries mention other electronic health (insurance) cards. Belgium has a SIS (social identity) card for all citizens and a SAM (secure access module) card for healthcare professionals. In Spain, each community/region has its own eHealth card. In Italy (Lombardy), the CRS (carta regionale del servizi) for citizens and the SISS (Health Care Information System) card for healthcare professionals are perceived as corner stones of a 'Healthcare extranet' that links professionals, social services, organizations and citizens and enables tracking of all the events in the context of patient treatment and the provision of value added services.[39]

The minimization of administrative efforts for insured citizens is mentioned as an important purpose by Switzerland, Italy and Belgium. E.g. the Belgium SIS card is used for authentication of the insured in health care[40]. In the Basque Country (País Vasco), e.g. 'the card allows for a number of procedures through the Internet, offering an advanced security level, utilising the electronic card exactly as it happens with the doctor, in the case for example of requesting a second medical opinion, clinical records, clinical episodes and data of medical leave.' (European Commission, annex Spain, 2007). Sometimes the card is used to update data (e.g. the health card of Galicia, Spain).

[39] The development of the Lombardy CRS-SISS project has been one of the first integrated strategies on eHealth in Europe. Because this eHealth project started in 1 region and is now being implemented in other Italian regions (under the umbrella of INCO-Health), it is perceived as an important example for the development of eHealth in Europe.

[40] 'to check insurability rights of the patient and allow – when possible – third party payment' (https://portal.health.fgov.be). Authorized parties which are not part of the network of the 'Kruispuntbank', can have access to insurance related personal data by the use of the SIS card of the patient.

3.2.2.3 Collection of health data

In the question list, we asked for the mechanisms for collecting health care related data.

According to the Article 29 Data Protection Working Party, medical data shall in principle be obtained from the data subject. However, there are a lot of exceptions. First of all, medical data can be collected (and processed) if it's provided for by law for public health reasons or other important public interests. It is also permitted by law for preventive medical purposes or for diagnostic or for therapeutic purposes with regard to data subjects or a relative in the genetic line, to safeguard the vital interests of the data subject or a third person, for the fulfillment of specific contractual obligations or to establish, exercise or defend a legal claim. Also, when consent is given by the data subject (for one or more purposes), other parties can also give the medical data of the data subject, in so far as domestic law does not provide otherwise (Council of Europe, R (97) 5, 1997).

A particular issue in data collection is related to the issue of quality of the data (correct (valid and reliable), up to date, and specified for the purposes of use of data). Wrong or incomplete medical information can lead to medical errors which entails financial losses (Frost and Sullivan, 2004). Especially in a context where databases can be connected through health care networks vast amounts of health care data can be handled. Moreover reflections have to be made on the usability of the systems to bring in reliable and valid data in the databases: 'the relevant step forward is that information is gathered during routine patient treatment, not during activities explicitly dedicated to scientific research within universities or research institutes' (Kell)'[41]

Two important topics for the collection of health data get more attention in this section. These are (1) patient (and healthcare) identifiers and (2) the question of the ownership of health data and health records.

3.2.2.3.1 Patient identifiers[42]

Patient identifiers enable the identification of the medical data to the citizen and are therefore essential but also privacy-invasive tools of eHealth. Member states of the EU have the duty 'to determine the conditions under which a national identification number or any other identifier of general application may be processed' (article 8 (7) Directive). The unique identifier can either be used exclusively for identification and authentication in the domain of health care or can be used in broader contexts (e.g. e-Government). General identification number are welcome 'to render the management of administration more efficient, to save costs and to reach a good level of accuracy in the identification of the data subject' (Rouillé - Mirza, Wright, 2004, 158). On the other hand, general identification numbers bear risks because administration can link various information to one number, this brings about 'a huge power of identification' (Rouillé -Mirza, Wright, 2004, 158).

The contributing partners report that most healthcare institutions use their particular identification approaches for patient identification. Often patient records have been assigned ad hoc unique numbers randomly because the identification number is depending on the particular application/software used. Citizen identifiers or social security numbers enable identification could be a tool to linking data as an essential element for operational and

[41] http://www.kell.it/telemedicineteleeducation/downloadable-files/JH-pres-eng.pdf
[42] Questions 9.11, 9.12, 32.1, 32.2 of the list.

epidemiological information systems. In Germany control numbers are used in the epidemiological cancer registries 'to allow record linkage of anonymised records that describe cancer cases and are collected independently from multiple sources' (Thoben, Appelrath, &Sauer, 1994). But in Germany too, there is strong controversy on 'identifiers'. It is one of the main stumbling blocks in the development of national health card project. In the UK as well, the use of patient health card is debated in the context of public liberty.

In the Netherlands, the Citizen Service Number (BSN) will be used for the EMD and WDH and it will replace the social security number as key identifier in administrative matters. The unique social security number is used in Sweden and Belgium.[43] On several occasions, the Belgian privacy committee contemns the national practice and calls for a 'unique patient identification number specifically dedicated to the processing of personal information regarding healthcare' (HEPI – GO final report, 2006). This is already the case in the UK, where a *unique national patient* number is used. In Switzerland, there is a unique identification number for electronic records, which is now based on the social security number. The national citizen identifier is used in Norway.[44] In Spain the NHS personal identification code links the various system-specific personal identification codes of citizens: 'regulation RD 183/2004 which regulates the individual health card: The regulation was approved in order for all NHS beneficiaries to have a unique personal identification code that would provide good service and would permit obtaining the appropriate medical information at every point of the public health system. The assignment of the NHS personal identification code is realised at the moment of the inclusion of the relative data to every citizen in the database protected by the NHS, developed by the Ministry of Health, and acts as the link for the different autonomous personal identification codes that every person may be assigned during his/her life.'

Several states are currently developing new initiatives in the context of patient identification. We aready referred to the Dutch Citizen Service Number (BSN). Switzerland will introduce a new social security number (after July 2008). This number will no longer entail sensitive information - it will be a totally random number.[45] Belgian's HEPI GO project favours the idea of a Health Electronic Patient Identifier (HEPI). HEPI would be an irreversibly transformation of the citizen's social securtiy number. Interestingly, the project plans two test phases: first a 'primary HEPI' which is not 100% anonymous will be implemented, whereas in the second phase they use a 'secondary HEPI' (using pseudonyms and Trusted Third Parties to garantuee the anonymity of the citizen/patient) (HEPI – GO final report, 2006).

The identification of healthcare professionals received new attention because of eHealth applications. This practice can help to guarantee the secure access to patients' records for example. In the Netherlands, reference can be made to the UZI card and server cerificate as

[43] In Belgium: 'there is no common patient identification scheme used by GP or hospitals. Many medical software applications introduce their own proprietary identifiers. Such schemes are generally limited to the assignment of a random number, which only guarantees uniqueness within that particular application. In practice, the identification issue is solved through the comparison of administrative information and often inclusion of the INSS. Belgian's Unique Social Security Number (INSS) is an extension of the national numbering scheme. (HEPI – GO final report, 2006).

[44] In Norway they use Control numbers. A control number is 'a national person identifier that is commonly used as the index key for medical records': (Eichlberg et al., 2005).

[45] Now, 'the number contains 11 decimals, from which the first three are computed from the family name, the next three from the birth date together with the gender, the next two from the citizenship (Swiss or foreigner) and a "running number", and the last decimal is a check digit.': (Swiss-9.11).

means to identify health professionals. In Belgium healthcare providers and some social institutions have a SAM card (secure access module card), distributed by the RIZIV, the federal institute for sickness and invalidity insurances. The code of the SAM card is depending on the category of healthcare providers and constitutes of logistic and a serie number (this link between these numbers is protected by the crossroad bank for social security). In the Andaloucian region, health professionals are uniquely identified with a unique user identifier / password and with digital certificates. Health professionals working in the Lombardian SSIS system need to proof their identity with an e-signature. The next generation of Jhospital records will be secured with PKI infrastructure and certificates. In the UK health professionals as well as managerial/clerical and secretarial staff are uniquely identified with a user number and user name and (varied) password.

According to Hämäläinen, one would assume that in region-driven countries where 'the architectural choice for an eHealth service network with interoperable connections is favoured more than an integrated information system' **(**Hämäläinen, 2007, 10), patient identification is even more essential. However, the study reports that patient identification and health cards are deployed in all insurance-based systems but 'in region-driven countries this is not such a strong priority' **(**Hämäläinen, 2007, 10).[46] However, the Spanish the NHS identification code, 'the central node which manages information streams between regions' (Spain – 12) as part of 'Plan Avanza' provides a counter-example.

Beside patient and healthcare identification, the ownership of medical data is another crucial topic, closely linked to the collection of health data by means of eHealth tools.

3.2.2.3.2 Ownership of medical data[47]

Some countries see the data controller (health care organization) as owners of the health information (Norway, Sweden). Other countries/regions stipulate that the patient is the owner of the information (Switzerland, Flanders, Andaloucian Region). As the rightful owner, the patient decides what happens with his medical data: 'the authority to decide upon the use of medical data shall remain with the citizens and the principle of voluntarism of medical data retention shall be upheld' (Germany – 1). In Spain, 'the doctor is the owner of the 'Subjective Observations' (comments made by the doctor), which may not be accessible by the patient, if the doctor indicates so' (Spain - 9.7) The Dutch answer shows that control over the data (regardless if they are owned by the patient or the healthcare organization) is diffuse: '(relating, sic) EMD: Sometimes, the healthcare professional is considered to be the owner of the health information. However, the healthcare professional only has certain control over the health information: he is responsible for the storage and quality of the data. The patient also has control over the health information: he has a right of access and a right to delete his own health information. Finally, the healthcare establishment (hospital) has control: the hospital often determines the means of processing the health information and is often the owner of the

[46] Some background on the study: 'For the purposes of contrasting the policy and deployment situation, countries where assigned to one of three country groups. The first group was formed by countries where the state is the main player organising the health care system with a national health service or similar; the second group was one where the national insurance system is the main player, and the third was a group of countries where regions or other areas with great autonomy are the main organizers of health care. Differences among these groups are very small and there are so few cases in each group that statistical comparison can not be done, however the simple frequencies suggest the same conclusion that an educated guess would give': (Hämäläinen et al., 2007, 69).

[47] In particular, question 9.7 of the question list.

health information system' (Netherlands – 9.7). In the answer of the UK doubts about the ownership of health information on health cards and records are related to the fact that there has been a transition from paper records to digital records (UK- 9.7).

According to the Article 29 Data protection Working Party, 'in the legal provisions introducing an EHR system, it should be laid down as a rule that entering data into a EHR or accessing such data such be governed by an incremental system of opt-in requirements (especially when processing data, which are potentially extra harmful such as psychiatric data, data about abortion etc.) and opt-out possibilities for less intrusive data' (Art 29 Data Protection Working Party, 2007).

The explicit consent of the patient is needed to include personal health related information into records and databases. However, the notion of explicit consent differs along the national laws.[48] According to the Norwegian Personal Health Data Filing System act, it is sufficient that 'consent is asked when the database is first established' ('written' or 'explicit' are not mentioned). In the Belgian FLOW project, an explicit consent to include information in an electronic medical file of a patient is needed, who is in an independent position. This written explicit consent can be withdrawn at any moment.

In order to consent to the use of one's health data, sufficient knowledge about the data processing is essential. However, in practice this is very hard.[49] Maybe, as Dierks (2003, 177) suggests, 'there is a need for an evaluation of necessary minimum information that is required for informed consent'. A patient does have the right to withdraw his or her consent. But how can this be done and how can we turn back the clock if we withdraw our consent? This poses a lot of practical difficulties. Actually, the fact that patients must provide consent to collect and use health related data at the time of contact with healthcare provider is, from the ethical point of view, unjustified because there is no informed consent without the purpose being specified in advance. Another example of unjustified consent is the way health data is processed in the electronic individual health system in Flanders: in the operational system, 'there is an automatic input from the regular individual health care file to the electronic version of the file. The consent of the patient regarding the data exchange in the operational information system is assumed but not asked explicitly**.** This is not in line with the Federal law on patient rights. Explicit consent has to be given by patient.' (Belgium –9.6)

3.2.2.4 Storage of health data[50]

Secure saving of health data is a conditio sine qua non for eHealth. Technicians, experts and commercial partners are always looking for new ways to do this. However, both paper based systems as well as highly technological systems bear the risk to loose health data. Recently, there have been several cases of losses of stored medical data in the UK (see box).

[48] Differences in the 'national laws in relation to the type of consent requirements for processing sensitive data: explicit consent in Portugal, Sweden and UK; express consent in Finland, the Netherlands; written consent in Belgium, Greece, Hungary, Bulgaria; express reference in Germany; explicit and written in Spain; Approval of Supervisory Authority in Italy.': (Beyleveldt et al., 2007, 152).

[49] 'informing about all the explicit details of such a procedure tackles the limits of the physician's and the patient's mental and timing capacities. The kind of data and the purpose will have to be specified. The infrastructure needs to be described. Procedures, like public key infrastructure and electronic signatures, their security and significance will have to explained' (Dierks, C., 2003, 117).

[50] Question 9.2, 9.13, 29.3 and 30 of the question list.

'NHS smartcard losses aren't being monitored', Tash Shifrin, Computerworld UK, 19/10/2007.

'Personal details of 16000 children lost in hospital data disks blunder, the Daily Mail, 12/12/2007.

'Boston hospital data stolen' by Nicola Dowling, Manchester Evening News, 23/12/2007.

'Exclusive: Hospital Test data found in the street', Peter Truman, Your Local Guardian, 9/01/2008.

'Doctors encourage patients to opt-out after NHS data losses', SA Mathieson, Infosecurity News, 4/01/2008.

Little correspondents indicated that countries use health cards to store health information or to provide access to patient data. Detailed health related data are seldom stored on the card itself:

The Swiss electronic health smart card, foreseen to be introduced in 2008, can contain 'information to improve the medical attendance', such as: blood type, immunization and transplantation data, allergies, medication, information about an already existing living will. Here as well a PIN code can protect the data. Medical data can be put on the (future) Swiss card, but only if the patient agrees. A record of medicines is optional on the Swiss cards and mandatory on the social security card in Italy

In the Lombardian SISS system clinical data for emergencies is saved on the CRS, the smart card. The holder can block data entries with a PIN code and the card allows updating data.

The Andalausian cards contain basic medical information but fingerprint protection of the holder. The Belgian and Spanish cards do not put information of prescribed medicines onto the record.

The European health insurance card contains the following information; code of country of membership of insurance, name and first name of holder, data of birth, registration number, identification number of the relevant institution, logic number of the card and information of the institution re the logic number, end date of card. The card has no other data on the card than the data visible on the document (except if the card is integrated in another national electronic card).

Once the German eGesundheitskarte will be deployed, 'patients shall be entitled to decide which of their medical data will be included on the card and which will be deleted' (the joint declaration of 3 May 2002 announcing the introduction of the eGk the Federal Ministry of Health and the stakeholder organisations in the health sector) (Germany-16).

3.2.2.4.1 What data are saved on records and cards?[51]

There is agreement on some generally categories of information (although the type of information is depending on the purposes of the record). These categories are: 1. patient contact information (administrative part – patient ID), 2. Patient medical information (non-exhaustively: information on treatments, health history or medication data…), 3. Patient's rights information (does patient want blood transplants e.g.) and sometimes 4. A non patient

[51] Question 9.2 and 29.3 and 30 of the question list.

related information part (supportive part: flyers related to 'mainstream' medical conditions, follow up rules…). According to the information provided by the countries, emergency data is included in the Norwegian hospital records, in health records of medical institutions in Switzerland (although not as a special data set), in the Belgian Electronic health file (SUMEHR), in the Andaloucian health record and in the UK health record.

The choice between a centralized and a decentralized system to save health data in is very important. Both have pros and contras. Bourret observes a link between the way health data are stored and two common visions on electronic health records: 'the first older one views EHR as an electronic safe, it is often connected with the idea of a standardized EHR. The second view, which is more recent and innovative, has emerged with the Internet technologies: the shared EHR' (Bourret, 2004, 106). The latter vision, where the electronic health record 'is made up of documents and also includes links to documents at remote site' has the advantage that the 'data deposits remain in the sites where they are collected' (Bourret, 2004, 106). The shared EHR is therefore interesting for organising the health networks (e.g. between hospitals and primary care). Some countries (Germany e.g.) state very explicit that 'no central register or data base with patients' data shall be implemented' (the joint declaration of 3 May 2002 announcing the introduction of the eGk the Federal Ministry of Health and the stakeholder organisations in the health sector) (Germany-16). The Belgian FLOW healthcare network (which is a voluntary and open platform to share information) wants to provide an alternative for the closed and centralised alternatives in medical dossiers. (Belgium – 9.1) According to the UK answer, 'there is no linkage between eRecord and any social care record' (UK-2).

Member states of the European Union have to follow the legal rules of the EU but they have some freedoms, e.g. in limiting the period of saving health data. In the Netherlands, it has long been argued that medical records should be stored for only 10 years.[52] Contrary, specific archival legislation in Scandinavian countries, determines very long retention periods for health data for scientific research.

3.2.2.5 Access of health data

The access to health data is essential for healthcare professionals, for patients and for third parties. However, the control on the access to medical data in records and cards is an essential safeguard to citizens' privacy. According to the Swedish correspondent, 'there is a **tendency to increase the access to the records** (to be able to supply better care rather than a debate about privacy)' (Sweden -15).

Access and use of the health related data is guided by (legal and technical) procedures: there should always be a log system in order to verify (post-hoc) who has accessed what data, when en why. The German correspondent provided some clear examples of access control: 1. 'to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used', 2. 'to prevent data processing systems from being used without authorization', 3. 'to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access' and 4. 'that personal data cannot

[52] However, in the light of profiling health data (for managed care e.g.), there has been a discussion since 2000 to amend the Dutch law in order to elaborate extensively the retention period of medical data (at least up to 30 years) (see http://www.gr.nl/samenvatting.php?ID=921&highlight=retention).

be read, copied, modified, or removed without authorization in the cause of processing or use and after storage' (Germany-2, according to vGeneral provisions on data security and technical measures to ensure privacy protection are laid down in Article 9 BDSG and the annex to Article 9).

We differentiate between (1) access of the citizen to his or her health information, (2) access of the healthcare provider and (3) access of third parties.

(1) **Patient access**

Patients have the right to access the medical data relating to them. This does not have to be direct access, although this can boost patients' trust in electronic health record systems. In general, people can view at least certain parts of the patient record (e.g. in the Swedish and UK case you can ask for a print-out (at your own cost)). In Germany, 'patients and insurance holders shall be entitled to fully access all data stored relating to them' (the joint declaration of 3 May 2002 announcing the introduction of the eGk the Federal Ministry of Health and the stakeholder organisations in the health sector) (GE-16). Sometimes the right to look into one's record can only be done in the company of a health worker (in case of Norway). Sometimes a written request – without motivation - is necessary (the individual health file in Flanders) (Question 9.3). The Belgian answer stresses the fact that the patient does not have open access to all parts of the record. For example: comments and notes of the healthcare professional are not available to the patient (BE-9.10) (this has been mentioned by the Andaloucian report as well (ES - 9.7 on 'subjective observations'). In Belgium the access granted by the patient is depending on the type of the specific record (Morbé, 2003, 94-96). According to the answer of Norway, Norwegian patient can not change nor delete data from their files. Contrary, Andalusian patients can request a change or deletion of information but only when it is not correct. Dutch patients have a (general) right to delete his own health information in the electronic medical record and his/her electronic GP record. In the Flemish case, patients can exclude information from databases/ records but only in 'severe reasons and special cases and when the information was not generated in the case of voluntary participation to a preventive program'. The patient also has the right to object to the nation-wide availability of his health information through the electronic general practicer record (right to block the access to his health information for other healthcare professionals).

Several provisions of the data protection directive can limit patient access. Access right can be denied e.g. in the context of article 13 (1) of the Data Protection Directive, 'to protect the rights of freedom of others'. Examples can be found in the legislations of Bulgaria, Finland, Italy, the Netherlands, Norway, Poland, Spain and the UK.[53] This exception shows that in a democratic society the 'balancing exercise' is an important check. Also, exemptions to the right to information (article 10-11) are rather common. First of all, this can happen in the context of art 11 (2)[54] 'where providing information to the data subject is impossible or would require a disproportioned effort, and appropriate safeguards are observed, the data controller or his/her representative would not have to provide any information' (Rouillé-Mirza and Wright, 2004b, 203). Countries as Belgium, Germany, the Netherlands[55] and Spain have

[53] See Rouillé-Mirza and Wright (2004b, 205-207) for more information.
[54] This relates to processing for statistical purposes or for the purposes of historical or scientific research and only if the data has not been collected directly from the data subject.
[55] The Dutch 'medical treatment contracts acts' states that medical data are particularly protected and (…) informed consent (involving information to be provided to the data subject) has to be obtained from the data subject before the disclosure of such data outside a medical team': (Rouillé-Mirza and Wright, 2004, 220).

included this exemption in the context of scientific research / purposes in their domestic law. Without explicitly referring to the context of scientific research or purposes, the exemption has been included in Finland, Italy, Norway and the UK as well. In Hungary[56], the exemption is not included in domestic law (Rouillé-Mirza and Wright, 2004b, 220-221). Secondly, the exemption can be allowed in the context of art 13 (1). For example in Norway, there is an 'exemption to the information provisions where it is inadvisable for the data subject to gain such knowledge, out of consideration for the health of the person concerned or for the relationships with persons close to the person concerned (Section 23 c of the Norwegian Persona Data Act (14/4/2000 No. 31).

(2) **Access of healthcare professionals**

'An NHS primary care trust has warned of a new risk to the confidentiality of medical records under the National Programme for IT (NPfIT); after more than 50 staff viewed the electronic records of a celerity admitted into hospital', Tony Collins, 'ComputerWeekly.com, 17/09/2007.

In the context of the doctor-patient confidentially, it is crucial that healthcare providers can only consult health data if this is necessary for the treatment of a specific patient. Transmission control is an important aspect in this context: 'to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged' (Germany-2)[57].

In the countries questioned, closed records with selective access limited to well-defined circumstances seem to be the standard (Norway, Switzerland, Netherlands, Sweden, Spain and Belgium). As a result, only information from the health record which is necessary and relevant can be consulted and the access depends on the relation of the healthcare provider with the patient. The secrecy of duty of the health care provider and the protection of the doctor – patient relation is perceived to be essential (Question 9.6). According to the Dutch answer, selective access by the healthcare provider is supported by authentication and authorization. In contrast, the Swedish answer points out to the fact that selective access is foremost a *legal restriction instead of a technical one* (logs can be consulted to check if the selective access has been used correctly but this is not checked in a consistent manner)! (Question 9.10) The answer of the UK shows that evidence of breaking the stipulation of privacy and confidentiality which are included in the contract of clinical and managerial/clerical or secretarial staff, can lead to 'immediate suspension and possible dismissal'. In the Netherlands, **"**Well Managed Healthcare System" (GBZ) criteria are established for access of healthcare provisioners to the electronic medical record and authorization guidelines for the GP record "lead takers". The German penal code (Article 203[58]) and the professional code of conducts[59] serve as general rules for the patient record system NEXUS.MedFolio®. In German, 'legal provisions exist on collection, transmission

[56] As well as in Bulgaria, Estonia, Greece, Slovakia and Slovenia (Rouillé-Mirza and Wright, 2004, 221).
[57] 'General provisions on data security and technical measures to ensure privacy protection are laid down in Article 9 BDSG and the annex to Article 9': (Germany- 2).
[58] Available at http://www.gesetze-im-internet.de/stgb/__203.html.

[59]See template at the German Medical Association at http://www.bundesaerztekammer.de/page.asp?his=1.100.1143.

and storage of medical data by health care providers. Strict purpose binding provisions apply and sector specific information must not be linked (question 16)[60]. The Italian J-Hospital system 'has a module that performs advanced check on user data entry.' (question 9.6)

Several countries state that the exchange of information between healthcare organizations is arranged in a standardized way.[61] Old-fashioned way of information sharing (document sent by fax or email) and paper-based approaches do still exists (e.g. UK), next to more advanced ways of sharing of information as for example, the Dutch secure storage approach (use of UZI card) and the Italian Jhospital system (question 11).

(3) Access by third parties:

Since informational privacy and medical secrecy must be ensured, neither patients nor doctors can be put under pressure to provide health related information to third parties (e.g. insurance companies, employers, (governmental) health organizations…). At least in principle, (direct) access of medical information from patient records by third parties is not allowed. However, in the context of medical-scientific research and government policy (statistics), an exception can be made.[62]

Citizens must understand the workings of the data controller in order to develop trust in the system. The data controller[63] is responsible for the management of the data. He or she has to 'implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.' So it is the duty of the data controller to 'choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures' (art. 17 of the D 95/46/EC). (Authorized) people working under the authority of the controller or the processor can only process data when required by law, or when they received instructions from the data controller. This means that not only the head of a healthcare institute or department is responsible, but also all authorized employees working with the data of the electronic health care (clinical professionals). As a result, professionals on the health care *and* the administrative levels can be put responsible. An electronic signature or another authentication measure can be used to verify in real time or post-hoc who gathered, maintained or stored the data. This is important in liability issues.

---

[60] 'Statutory Health Insurance companies receive accounting data of statutory insured patients. According to Article 295 section 1 SGB V the treating doctor must transmit the ICD-10 key for the specific diagnose and the date of treatment to the regional association of SHI-accredited physicians which then transmits data to the Statutory Health Insurance companies (Article 295 Section 2 SGB V). All other health care providers (for example hospitals and pharmacists) transmit accounting and medical treatment data directly to the Statutory Health Insurance companies' (the joint declaration of 3 May 2002 announcing the introduction of the eGk the Federal Ministry of Health and the stakeholder organisations in the health sector)': (GE-16).

[61] Other countries as Swizerland, Sweden and Hungary do not (yet) have a standardized exchange of information between organizations.

[62] In that case the safeguards of article 8 (4) of the Directive have to be ensured.

[63] 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 or the specific criteria for his nomination may be designated by national or Community law; organizations.'

Some countries work with central nodes to exchange health related information between organizations. This means that there are no centralized database of information but there are specific structures or/and organizations that connect information from various databases and provide the information to those (authorized ones) who need it. As a result, the organizations 'on top' of the exchange system can access a lot of information, but the information remains at the source location. Examples are available in the Netherlands (National Switch Point), in Belgium (cross-road bank, FLOW, BeHealth), in Spain (central node of NHS) and in Germany (Statutory Health Insurance (SHI) company). The answer of the UK shows a discrepancy between the companies providing system for data exchange and the users of those systems. The first offer centralized systems in order to organize the exchange information between healthcare organizations. The latter believe a 'disseminated open architecture that allows data to stay where it was created but be accessed by appropriate clinical carers' is the best option (Question 10). Nevertheless, 'summarising and sharing with others then it can only be done with the explicit written agreement of the patient on every occasion. For example, the provision of information for life insurers or health care insurers' (UK -16).

According to the results of Hämäläinen (2007, 10) there is a relation between the type of national health information system and the way health is organized in a specific country: 'having an integrated national health information system, seems to be a higher priority in state-centred systems than in others', Also 'in region-driven countries the architectural choice for an eHealth service network with interoperable connections is favoured more than an integrated information system. Promoting and deploying standards is a higher priority in groups other than the state-driven group, which is understandable since the use of standards is essential in multi-player systems' (Hämäläinen, 2007, 10).

3.2.2.6 Use of health information

The European legal framework shapes the conditions for on the use of health data.[64] At least in theory, Member States have an obligation to prohibit the processing of health related data (article 8 (1) D95/46/EC).[65] However, European states can make use of various exceptions to this general prohibition to allow the processing of personal data in the context of eHealth. When possible, we refer to the answers to the question list.

First of all, there are exemptions to the prohibition of processing sensitive data in the context of article 8 of the Data Protection Directive.

[64] Note that we focus mainly on the general data protection framework set out in D 95/46/EC. Besides the EU directives on data protection, the legal framework on electronic medical records furthermore consists of (European) regulations by Article 8 ECHR; the treaty of the Council of Europe to protect persons against the automatic processing of personal data (Strasbourg Treaty 108-in particular article 6); the Additional Protocol to the Convention for the Protection of Individuals with regards to automatic processing of personal data, regarding supervisory authorities and Transborder Data Flows, European Treaty Series No. 181; Recommendation R (97) 5 of the Council of Europe on the protection of medical data (13/02/1997); article 8 of the Charter of fundamental rights of the European Union (2000/C 364/01); Directive 2002/58/EC on Privacy and electronic Communications. The recommendations described in the 'working document on the online availability of electronic health records' of the International Working Group on Data Protection in Telecommunications (6-7 April 2007 Washington are also of importance to the EU (various recommendations have been integrated in the recommendation (97) 5 of the Council of Europe. Regulations and directives on 'Trade and Competition' and well as on 'Products and Services liability' make the picture complete (see eHealth fact sheet 'legally eHealth': the legal and regulatory context', available at: http://ec.europa.eu/information_society/activities/health/docs/projects/project_of_month/200702legally-ehealth.pdf).

[65] Data concerning health is part of a 'special category of data' (article 8 D 95/46/EC) and according to the Article 29 WP group, all data in the medical record is senstive data.

In the context of article 8 (2a): when the data subject has given his or her explicit consent to process the data. But, Member States can lay down in law 'that the prohibition referred to (...) may not be lifted by the data subject's giving his consent'.

In the context of article 8 (2c): when processing the data is necessary to 'protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent'.

In the context of article 8 (3): for preventive medicine and medical diagnosis (and medical research in general).[66] In the UK it is explicitly allowed to process sensitive data in the context of medical research, medical diagnosis and preventive medicine (The UK 1998 Data Protection Act Chapter 29, Schedule 3, Paragraph 8 (2))[67]. This entails a rather wide interpretation of article 8 (3). Although not mentioned explicitly in other countries, processing of sensitive data for could be allow if it's put under the purpose of science or preventive medicine or medical diagnosis.

In the context of art 8 (4): public interest: it is possible for States to use article 8 (4) of the Data Protection Directive, instead of article 8 (3), in order to allow the processing of sensitive data in the context of scientific (and thus medical) research.). However, states have to provide 'suitable safeguards'.[68] In the UK and the Netherlands among others the prohibition to process is ignored when processing is done for scientific research that has 'substantial public interest'.[69] It is unclear what is meant with the latter concept. In Norway for example, the public interest has to clearly exceed 'the disadvantages or risks it might entail for the data subject' (Rouillé-Mirza and Wright, 2004b, 218). According to Rouillé-Mirza and Wright (2004b, 218-219), 'it is not rare to see the (pre-2004, sic.) NAS providing an exemption to the prohibition of processing sensitive data for medical research for particular processing, which could be seen as being of public interest, and also when the safeguards required are in place. This latter remark is interesting, since it shows that the pre-2004 New Assigned States have been following the same logic as the European Member States.

Additional exceptions relating to the data protection principles (article 6 (1)) are also possible in the following contexts:

In the context of article 6 (1b): for historical, statistical or scientific purposes.

In the context of Article 13 (1g): the article on the protection of the data subject or of the rights and freedoms of others can be used to restrict the application of article 6 principles in relation to medical research.[70] The UK[71] once again and the Netherlands[72] provide proof for this exemption based on article 13 (1).

---

[66] In principle, the exception on the prohibition does not refer to medical research in general but the Directive does not specify whether medical research can be put under preventive medicine and medical diagnosis. However there seems to be proof for the fact that medical research can generally be used in the context of article 8 (3) D 95/46/EC (See UK, See Beyleveld et al., 2004).

[67] In Sweden, Luxembourg and Ireland.

[68] In the PRIVIREAL study, only Bulgaria did not have these safeguards included in their law.

[69] UK: Statutory Instrument 2000 No. 417 – The data protection 'processing of sensitive personal data) order 2000, article 2 paragraph 9. Netherlands: Personal Data Protection Act – Rules for the protection of personal data 25 892, passed by the Upper House on 3/7/2000 (Stb. 2000, 302), article 23 (2a).

[70] 'Results of medical research can protect the data subject and that medical research is both a right and a freedom, generally': Rouillé-Mirza and Wright (2004b, 199).

In relation to the purpose principle, there is an exemption for scientific reasons. However, in Belgium, Finland, Italy, Slovakia and Spain, no safeguards are provided 'to ensure that there are no measures or decisions regarding any particular individual' (Rouillé-Mirza and Wright, 2004b, 211). This means that the legislation of these countries is not compliant with the Directive![73] Safeguards are provided by law e.g. in the UK, Germany, the Netherlands and Poland. However the Directive does not specify the content of these safeguards.

In the context of article 18 (2) of Directive 95/46/EC, the Supervisory Authority has not to be notified about automatic processing.[74] This exemption can be used for medical research purposes but it seems not many countries make use of it. However Finland, the Netherlands (as well as Greece and Sweden) do.

Member states of the EU can take supplementary measures (next to those stipulated in the D 95/46/EC framework) to ensure the protection of personal data of their citizens. Yet they have also the freedom to allow additional exceptions to the general prohibition of processing those data. There seems to be a difference between what is possible by law and what the practice by institutions is. The law of Spain for example, provides several possibilities for the use of personal data in the light of epidemiological research. However in the Spanish practice there is a rather limited interest in the use of personal data for such research.

71 In order to safeguard the interests of the data subject or the rights and freedoms of any other individual, the Secretary of State can make an exemption from the first data protection principle in the context of processing for health, education of social work (Sections 38 (1) and (2)).

72 'There is an exemption to the incompatibility principle to protect the rights and freedoms of others' (Rouillé-Mirza and Wright, 2004b, 202).

73 In that the 'scientific purpose can only be viewed as not incompatible with the initial purposes provided that the country furnish appropriate safeguards': Rouillé-Mirza and Wright (2004, 211).

74 But in the case of the Flemish individual health file, 'further processing of data from the end file without anonymisation, can only after the Commission allows it'.

4 Discussion

This section addresses some important concerns in the field of processing health data. We discuss following aspects:

- EHR systems are pushed by technological developments but it is essential that they are deployed to achieve higher rationalisation of the health care industry. How can this 'double' (economic) potential be fulfilled?

- Since private partners become central partners in health care (delivery), how can we balance privacy protection of citizens against (other) interests of these private stakeholders? What role does the EU and national governments play herein?

- Crucial choices have to be made by governments to generate the future of the social welfare states in Europe. How will eHealth affect the character of the social welfare state?

- Patient empowerment is an important rationale in the European vision on eHealth. However, patients risk being subject of risk analyses in higher degrees.

- Necessitate (and lack of attention) to stress organisational matters besides pure technological needs. How can this be taken into the development of eHealth?

As stated before, our overview is too limited to make a comparative picture on how different types of European welfare countries are socially constructing eHealth records and cards. However, based on the information made available, we have indications of *diverging debates*. Moreover, the debate on health profiling seems in most of the countries embryonic and more related to technological and legal issues. The discourse on eHealth and profiling is mainly developed from different viewpoints.

Technology push, economic value and innovation perspectives are dominant in the discourse on eHealth developments. The European ambition to play a prominent role as dynamic knowledge-based economy is currently an important driver in eHealth. Whether we call it 'knowledge-based economy', information society', 'service economy', or even 'information economy'[75], information and knowledge become more and more a profitable and valuable source for economy.[76] In this context and in line with the ambitions of the Lisbon Declaration (European Council, 2000) and the i2010 Initiative, there is a huge economic potential in eHealth: 'e-Health is emerging as the new *industry*[77] alongside pharmaceuticals and the medical devices sector' (Com (2004), 356 final).[78] The ambition of a European Health Information Space has to be understood from this perspective. The link between the

[75] There is some overlap between the concepts 'information economy' and 'service economy': in a service economy there is an increase of the importance of the service sector and in such a post-industrial economy, the value of information becomes more important. Marc Uri Porat (1977) launched the term 'information economy' in his dissertation (see Porat, Marc U and Rubin, Michael R. 1977, The Information Economy (9 volumes), Office of Telecommunications Special Publication 77-12, US Department of Commerce, Washington D.C.).

[76] Newman and Bach (2004) warn for the 'marketization of privacy protection' and the influence this has on citizens' privacy and identity?

[77] Emphasis added by us.

[78] By 2010, eHealth will take up 5 times the amount of the health budget in comparison with 2000 (Note: comparison between the 25 member states in 2010 and the 15 in 2000): 'Health Information Network Europe (2003)'.

management of information and its economical value was also mentioned by the German correspondent: 'Economization of information administration' (GE-2).

In the particular domain of EHR, it has become clear that cards are mostly defined and approached as technological enablers of efficiency and quality of health care (delivery). They accelerate the flows of information and are seen as enablers for free movement of people and data, which they are. However, fundamental social, ethical and legal questions are slowly being integrated in the debate. The Article 29 Data Protection Working Party makes us explicitly aware of the 'new risk scenario' emerging out of the use of eHealth tools. Without taking the position of a technological pessimist, more concerns should rise on the way eHealth in general and the handling of health care related information. Andreassen et al. (2007) warn for 'unintentional consequences' which could emerge because of the use of electronic systems in health care.[79] Because of the phenomenon of technology push – economical and human losses for eHealth applications can be quite high.

eHealth is emerging as 'a vehicle for health reforms' (Rossing). As mentioned by the Swiss partner, the whole organisation of health care has to be reconsidered: '*Not the reproduction of existing structures is the target subject. Conjunction, simplification and interoperability of existing in order to create new, improved processes are the main reasons*'. Since welfare states at least have the *ambition* to make available health for all, they urgently look for ways to provide new efficient and qualitative care. However, it is not that easy to radically change systems. Changes are not that new, they still are the outcome of the past.[80] But very little is currently debated on health care reforms related to the issue of eHealth. This debate is necessary in order to sketch the role of health information systems within these contexts, especially since health care service configurations are divergent between the European countries.[81] The balancing of privacy against other rights is a very difficult task with unpredictable outcomes, as the national background and history of the specific welfare state certainly play a role. Healthcare systems are influenced by the organizational and cultural differences of member states (COM (2004) 356, 13) and in turn, 'certain features of health care system structure might have an effect in eHealth policy and deployment priorities' (Hämäläinen et al., 2007, 10). Comparative, multi-country research has been underutilised as a means to inform health system development. For the EU, it remains important to try to find

[79] 'This divide (the digital divide, *sic*) (…) affects the society as a whole. Through the use of mass media, like the Internet, there is also the potential of creating needs in the population, a well known strategy in marketing and advertising.' The authors also refer to the process of 'medicalization of modern society (Conrad, 1992, Illich, 1976)': Andreassen, et al. (2007, 7).

[80] The British respondent: 'There a number of primary care systems available and these have evolved with appearance and disappearance of both products and providers. The transfer of data from one system to another has proved difficult with poor technical support by the companies involved. My own experience is of the use of threatened litigation to ease the path toward successful data transfer. This inhibits progress as new systems evolve. Present systems have evolved out of earlier systems and are therefore very similar in their functionality. Improving standards are pushing providers toward generic systems and standardising coding. Early systems were text driven and coding was limited. Early coders lost whole data records because of inadequate coding translation. Neither government, EU nor providers seem to want to carry the cost of resolving the difficulties' (UK – 8).

[81] For readers interested in the different organizational models in the European countries, we refer to http://www.euro.who.int/observatory/Hits/TopPage where general descriptions can be found on the organisation of health care systems in Europe.

'common values and principles in EU health systems', to build upon (Ministers at the Health Council on 1 June 2006).[82]

The current reforms in European health care create more opportunities for private partners to take up central roles. These types of reforms should urge to discuss the issue of public and private information: in general we can assume that governments and public agencies have to act according to specific regulations and laws dealing with the collection, storage and utilization of health data. From the information we obtained from our correspondents it is clear that important reflections are still underway in several countries in the particular case of electronic health cards and records. However, due to changes in the organisation of welfare regimes, more and more private agencies will be taking up roles in the collection, storage and use of health related data. Very little specific information from our national correspondents came through on how private (for profit or not-for profit) agencies will be held responsible and sanctioned when (ab)using health information, what will be considered as purposive use, how informed consent matters will be dealt with etc. We assume that government protections on this level are still very limited in scope, while IT developments clearly have taken the trajectory of public-private cooperation. However the EU has an important role to play in this field: only with a strong (supra-national) policy citizens can be protected against possible privacy intrusions of multinationals.

In the perspective of previous observation, the issue of access and use of health data is a normative issue. What do we want to do with health data? Should it be accessible and used for public health research, even without people being aware of the use of (their) health data? 'The use of personal information without the individual's consent violates Kant's categorical imperative that human beings are ends and not means' (Redigor, 2004, 1977). Next to this deontological point of view, utilitarian theories provide more support for the use of health related information for public health research (Coughlin, 2006).

However, in practice there are often conflicts between principles.[83] How do we weight the importance of autonomy against justice, or against beneficence? Redigor (2004, 1977) concludes that there is a moral justification for using personal data without informed consent in research, 'the benefits to society weigh more than the harm attributable to the invasion of privacy, so long as the use of personal data without informed consent is the only way to answer a research question, and confidentiality and personal integrity remain intact.' However, moral evaluations are (more and more) subordinated to the rule of law. Both in the United States as in the European Union, the use of personal data from medical records in the context of epidemiological research has been restricted by law.[84] Melton (1997) points out to the fact that – because of all those legal restrictions on the use of personal data – important advantages regarding monitoring health, disease management and effectives can be lost.

Besides technological and legal protective measures, very little reflections and documentation is found on organisational measures creating a context for profiling based on health information. Organizational policies and practices are at least as important as other measures.

[82] New member states are in a special position. On the one hand, they might have stressed other values and principles than those of the health systems of 'old member states'. But on the other hand, experiences of the healthcare systems of the latter states could inspire new member states.

[83] Conflicts between generally accepted principles are: Respect for autonomy, non-maleficence, beneficence and justice (Beauchamp and Childress, 1994).

[84] Wukadinovich and Coughlin (1999) describe the situation in Lousiana.

An important part of data-handling is not solely a question of technological and legal issues but also related to behavioural and cultural aspects on how to handle personal data. Clear guidelines and protocols for people involved in the handling of personal health data should be considered as necessary, but this kind of debate seems not to very prominent in the current reflections on health cards and health records. Operational policy statements regarding information use and flows should attempt to balance the need for providers, payers, researchers, and others to access health information against patients' desires for privacy. Policies with health care agencies regarding information use and flows are to be formalized in specific policy documents on security, confidentiality, protection of sensitive health information, research uses of health information, and release of health information.

The issue of patient empowerment in combination with the increased focus on individual responsibility in health is in both ways affecting the way thoughts are being developed on health information systems. Stroetmann pointed out to the parallel between the growing use of ICT in healthcare provisions and the emphasis on health rather than care (Stroetmann, 2007, 24). The emphasis on patient empowerment seems to introduce a twist away from the paternalist protective vision on health care towards a 'participative state' (Klamer, H. et al., 2005). Patient empowerments is going hand in hand with the access to (personal) health information and information on health care provision. However, one question is to what extent eHealth tools will be deployed to support policies for the wellbeing of (all) citizens or to endorse the individual responsibilities. The introduction of disease management programmes and the changing health insurance field (away from solely public insurance) could lead to a new approach of the citizen, using health information and profiling techniques for risk selection When health insurance institutions and other (private) companies have access to data, they could make abuse of it enlarging the information asymmetry, instead of deploying a participative model of the welfare state.

Internationally, the increased attention for international comparisons and benchmarking, performance and quality measurement, the upcoming evidence based health care, the need to assess the cost and funding related issues, all urge to be able to make use of better deployed health information systems. Governments have the double duty in this process. First of all, they have to ensure the rule of law, including the right to privacy, and secondly, they are the forerunners of the (proactive) development of the welfare state. For the latter, massive amounts of personal data have to be (automatically) processed in order to guarantee the effective implementation of activities in the field of taxation, public health, etc. This double duty asks for a correct balance between the use of personal information and the protection of it. Some others are surprised by the fact 'at a time when mankind is experiencing the greatest developments in information technology, we are limiting the use of personal information that can be used for the common good' (Redigor, 2004, 1978)[85]. The idea of using personal information for the common good risks to undermine the balance in favor of the (unlimited) processing of personal data against the protection of peoples' privacy (e.g. when profiles are used to categorize people). But always, there has to be found a balance between the protection of peoples' privacy and the advantages of processing personal data for the 'public good'. When processing health data, member states are bounded by the general data protection principles. Data protection is important in the context of the individual freedom, at least in

[85] According to Redigor (2004, 1978), there are 'reductionist conceptions of health research' and 'subjective or irrational arguments about the methodology and risks involved in the use of data in research' (that) have played a major role in the limiting the use of personal information for the common good.

Western democracies. However, 'communitarian perspectives may favor limiting individual autonomy for the sake of the common good or public interest [7]' (Coughlin, S.S., 2006, 17). According to Regidor (2004) and Capron (1991) if confidentiality (of the information derived from the medical records) is maintained, the use of information from medical records can be justified.[86] In some cases this is could be true. A clear example is that the patient does not have to give his or her informed consent each time a healthcare professional makes use of the information from his or her medical record for treatment and diagnosis. However, in the context of managed care, 'information management by a third party can damage a doctor-patient relationship of trust and threaten the protection of medical data', despites the workings of data protection legislations (Hooghiemstra, 1998).

[86] 'Discrimination due to the inappropriate use of any kind of personal information does not depend on the existence of stored personal data, but on the lack of the necessary mechanisms to protect confidentiality, and on the absence of sanctions when this type of information is accessed or revealed for ends other than those which society believes are appropriate': Redigor, (2004, 1981).

5 Agenda for future research

It is clear that information technology and eHealth developments are becoming increasingly important as a support tool on different health care levels. In relation to two particular eHealth applications - eHealth records and eHealth smart cards - the discussion seems to limit itself to technical and legal instrumental issues. A rather aggressive approach to improve the security of health information is needed, without being opposed to the use of sensitive health information in health care.

But the current approach is too reductionist. In general terms too little attention is being paid to the particular nature of health care, as a sociological, cultural, political and economic construct. Health care is not like other industries; moreover it is directly related to welfare issues. Universal access and quality are aspects which must be included in implementing eHealth. Socio-technical choices in health care have to be made within the specific normative, regulative and cultural context of regions or nations.

Following Orlikowksi[87], IT research can benefit from policy, organisational and health services studies, especially from institutionalism (with institutional forces acting both as enablers and constrainers of actions) to understand 'how institutions influence the design, use, and consequences of technologies, either within or across organizations'. Orlikowski has used Giddens' Theory of Structuration to underscore the duality of IT as objective reality and as socially constructed product. Underlying assumptions, expectations, and interpretations of technology (technological frames) are central to understanding technological development, use and change in social contexts. The mutual adaptation of technology and social context involves reciprocal causation. Orlikowski focuses on organisations, but the line of reasoning can be broadened to policy contexts too. Technological frames of key groups in society are significantly different and very little knowledge is currently being developed on how to integrate and handle the different perspectives on eHealth in general and personal data management in particular.[88] Information infrastructures are shaped and socially constructed within social contexts. Information infrastructures and more particularly, the design and implementation processes that lead to their construction and operation, have to be approached as complex interaction processes which are embedded in larger, contextual domains. Regulative, normative and/or cognitive elements[89] transform not only the delivery and organization of health care, they reflect and affect at the same time how health related personal data is valued, used and abused.

Therefore a future in-depth comparative analysis of social shaping of technology in health care with a particular attention on profiling is needed. This in-depth study would be of added value for 'late starters' and would enable to make an inventory of concerns and measures taken by early starters, taking into account the organisational principles of the respective welfare regimes.

[87] See http://ccs.mit.edu/wanda.html.
[88] For a quick introduction on social constructionism, we refer to http://en.wikipedia.org/wiki/Social_constructionism and to http://en.wikipedia.org/wiki/Science_and_technology_studies.
[89] Regulative aspects relate to rules, laws and sanctions. They show what is allowed and what is prohibited in a specific institution or institutional field. This level has to do with regulative elements in institutions such as the control systems, power systems, protocols, standards and procedures. Normative elements relate to social beliefs, norms and values. Guidelines, strategies, roles, positions and authority systems are examples of normative aspects of institutions. At last, cognitive aspects – symbols, ideas and interpretations – show who we are and what we do.

In 2007 the Article 29 Data Protection Working Party made efforts to develop a draft framework for the processing of personal data relating to health in electronic health records.[90] It is argued by some authors that 'additional legislative measure need to be developed in order to ensure medical data protection on a multinational level and enable health telematics on a larger scale in accordance with the free movement of goods and services' (Dierks, 2003, 120). This type of 'reactive' actions should be accompanied by 'proactive regulatory input' (Dumortier and Goemans, 2004). Focusing on 'privacy by design' means that privacy protection requirements should be implemented 'at the earliest framing of programs or services and in all successive activies', rather than focus on 'data controller's compliance with privacy protection' (Dumortier and Goeman, 2004, 12).[91] The idea of proactive regulatory input provides opportunities for European countries that not yet (fully) implemented an electronic medical record system, to think about the privacy by design for eHealth applications.

[90] The Article 29 Working Group made recommendations relating to 1. Respecting self determination, 2. Identification and authentication of patients and health care professionals, 3. Authorization for accessing EHR in order to read and write in HER, 4. Use of EHR for other purposes, 5. Organisational structure of an EHR system, 6. Categories of data stored in EHR and modes of their presentation, 7. International transfer of medical records, 8. Data security, 9. Transparency, 10. Liability issues, 11. Control mechanisms for processing data in EHR.

[91] See also Recital 30 of the EU Directive 2002/58/EC: 'systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'.

6 Glossary

6 Glossary

EHR – Electronic Health Record

EPR – Electronic Patient Record

PET's – Privacy Enhancing Technologies

GP – General Practitioner

7 Bibliography

Andreassen, H.K., Sorensen, T., Kummervold, P.E., Project Report 'eHealth trends across Europe 2005 – 2007. WHO/European survey on e-Health Consumer Trends', NST Report 09-2007. Available at: http://www.telemed.no/

Article 29 Data Protection Working Party, Working document on the processing of personal data relating to health in electronic health records (EHR)', 00323/07/EN, WP 131/. Adopted on 15/02/2007. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf

Beauchamp, T.L., Childress, H.T., *Principles of biomedical ethics*, New York, Oxford University Press, 1994.

Berghman, Jos et al., **'**Dynamics of social security in Europe: summary', Project SO/01/010, Brussels : Science Policy Office, 2003 (SP1240).

Beyleveld D., Townend D., Rouillé-Mirza S., Wright J. (eds.), *The Data Protection Directive and Medical Research Across Europe: PRIVIREAL*, Ashgate Publishing Limited, UK, 2004.

Bourret, C., 'Data concerns and challenges in health: networks, information systems and electronic records', Data Science Journal, Vol. 3, 17/09/2004.

Capron, A., 'Protection of research subjects; Do special rules apply in epidemiology?', Journal of Clinical Epidemiology, Vol. 44 (Suppl I), 1991, 81S -89S.

Chaquet – Chiffelle, D.O., 'Reply: Direct and Indirect Profiling in the light of Virtual Persons', in Hildebrandt, M. and Gutwirth, S., *Profiling the European Citizen, A cross-disciplinary perspective*, Springer Dordrecht Netherlands, 2008, 56.

Coughlin, S.S., 'Ethical issues in epidemiologic research and public health practice', *Emerging Themes in Epidemiology*, Vol. 3, 2006, 16-26. Available at: http://www.ete-online.com/content/3/1/16

Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (13/02/1997).

Directorate General for Research, STOA, 'A European health card. Final study', *Working document for the STOA Panel*. Luxembourg, March 2001, PE 296.7.1/Fin. St.

Dierks, C., 'Data subject's consent and cross-border data processing', in Callens, S. (ed.), *E-Health and the Law*, Kluwer Law International and International Bar Association, 2003, 111-120.

Dumortier, J., Goemans, C., 'Legal Challenges for Privacy Protection and Identity Management', in *Proceedings of the NATO/NASTEC Workshop on Advanced Security Technologies in Networking*, Bled (Slovenia) 15-18 September 2003, Springer, 2004, p. 191-212.

Eichlbergh et al., 'A Distributed Patient Identification Protocol based on Control Numbers with Semantic Annotation' *International Journal on Semantic Web and Information Systems*, Vol. 1, No. 4, 2005, p. 24-43.

Eurosmart, 'Eurosmart position on the EU Health Cards', November 2005.

EurActiv.com, 'Patient Mobility', 17/11/2005, updated 22/03/2007.

European Commission, 'eEurope 2002. An Information Society for all', Action Plan prepared for Feira European Council, 14.06.2000.

European Council, 'Presidency Conclusions', Libon European Council, 23-24 March 2000.

European Commission – Information Society and Media, eHealth priorities and Strategies in European Countries eHealth ERA report – Towards the establishment of a European eHealth research area, March 2007. Available at: http://ec.europa.eu/information_society/activities/health/docs/policy/200703ehealthera-countries.pdf.

European Commission, 'eEurope 2005: An Information Society for all', Communication from the Commission to the Council, the EP, the Economic and Social Committee and the Committee of the regions, An Action Plan to be presented in view of the Sevilla European Council, COM (2002) 263 final, 2002.

European Commission of the European Communities, Information Society & Media DG, 'Connected Health: Quality and Safety for European Citizens', Report of the Unit ICT for Health in collaboration with the i2010 sub-group on eHealth (formerly known as the eHealth working group) and the eHealth stakeholders' group, 2006.

European Commission of the European Communities, Information Society & Media DG, 'e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area', Communication from the Commission to the Council, the EP, The Economic and Social Committee and the Committee of the regions**,** COM (2004)356 final, 2004. Available at: http:europa.eu.inf/information_society.

eHealth conference 2005 Tromsdo, Conference Conclusions. (www.ehealth2005.no)

Frost and Sullivan, 'The European electronic medical records markets', *Healthinformatics Europe*, BJHC Ltd, 2004. available at: www.hi-europe.info/files/2004/9979.htm.

Garland, A., 'Electronic Health records in Europe. A shared vision for tomorrow. Paper presented at the Midwest Instruction and Computing symposium April 2002n Ioawa, USA.

Gutwirth, S., *Privacy and the Information Age. Critical Media Studies - Institutions, Politics and Culture*. For the Rathenau Institute. Translated by Raf Casert, Rowman and Littlefield Press, 2002.

Hämäläinen, P., et al. (eds.), 'The European eHealth policy and deployment situation by the end of 2006', Del. 2.2 *eHealth ERA project*, Nov. 2007.

Hildebrandt, M. and Backhouse, J. (eds.), 'Descriptive Analysis and Inventory of Profiling Practices', FIDIS Deliverable 7.2, June 2005.

Hooghiemstra, mr. drs. T.F.M., 'Privacy & Managed Care', *Registratiekamer, Achtergrondstudies en Verkenningen*, 12, december 1998.

Kell, 'J-Hospital'. Available at: http://www.kell.it/telemedicineteleeducation/downloadable-files/JH-pres-eng.pdf.

Kivisto, P., *Key Ideas in Sociology*, Pine Forge Press, 1998.

Klamer, H., Dolsma G., Braak. J-W. van den, *Perspectief op een participatiemaatschappij; op weg naar een duurzaam sociaal stelsel*, Van Gorcum, 2005.

Leys, M., Potloot, L., 'Stand van zaken E-gezondheid in Vlaanderen. Voorstudie van maatschappelijke vraagstukken met betrekking tot e-health in Vlaanderen', Vakgroep Medische Sociologie, Vrije Universiteit Brussel, 2004.

Lassey, M., Lassey, W., Jinks, M., *Health Care Systems Around the World, characteristics, issues, reforms*, Prentice Hall, New Jersey 1997

Melton, L.S., 'The threat to medical-records reserarch', *The New England Journal of Medicine*, Vol. 337, 1997, 1466-1470.

Morbé, E., De wet betreffende de rechten van de patient, UGA Heule, 2003.

National Pharmaceutical Council, 'Disease management and Medicaid health outcomes management'. Available at: http://www.npcnow.org/resources/issuearea/diseasemanagement.asp

Newman, A.L., Bach, D., 'Privacy and Regulation in a Digital Age', in Harry Bouwman, Brigitte Preissl, and Charles Steinfield, (Eds.), *E-Life After the Dot.Com Bust* (Springer Verlag), 2004, 249-270.

Nouwt, J., 'Juridische aanbevelingen voor Elektronische Patiënten Dossiers', *P&I*, afl. 4, augustus 2007, 160 – 164.

Orlikowski, W.J. & Barley, S.R., 'Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other?', *MIS Quarterly*, 25, 2001, p. 145-165.

Penchenon, D., 'What's next for evidence-based medicine', Editorial, *Evidence-Based Healthcare and Public Health*, Vol.9, n° 5, 2005, 319-321.

Redigor, E., 'The use of personal data from medical records and biological materials: ethical perspectives and the basis for legal restrictions in health research', *Social Science and Medicine*, Vol. 59, 2004, 1975-1984.

Richardson, R., 'eHealth for Europe', *Eurohealth*, Vol.8, No. 2, Spring 2002.

Rossing, N., 'the Challenges of setting up a Pan European eHealth Network'. Available at: http://www.ehealthinternational.org/archive.htm

Rouillé -Mirza, S., Wright, J., 'Comparative Study on the Implementaion and Effect of the Directive 95/46/EC on Data Protection in Europe: General Standards', in Beyleveld, D. et al. (eds.), *The Data Protection Directive and Medical Research across Europe, PRIVIREAL*, Ashgate Publ. Limited, UK, 2004a, 125-187.

Rouillé -Mirza, S., Wright, J., 'Comparative Study on the Implementaion and Effect of the Directive 95/46/EC on Data Protection in Europe: Medical Research', in Beyleveld, D. et al. (eds.), The *Data Protection Directive and Medical Research across Europe, PRIVIREAL*, Ashgate Publ. Limited, UK, 2004b, 189-230.

Scott, W.R., et al., *Institutional Change and Healthcare organizations. From Professional Dominance to Managed Care*, University of Chicago Press, Chicago and London, 2000.

Sackett, D.L., Rosenberg, W.M., Gray, J.A., Haynes, R.B., Richardson, W.S., 'Evidence based medicine: what it is and what it isn't', *BMJ*, 312 (7023), 1996, 71-2.

Stroetmann, K., 'Final project report Deliverable 5.3 in the framework of the eHealth ERA project', September 2007.

Taylor-Gooby, P., 'Trust and Welfare State Reform: The Example of the NHS', *Social Policy & Administration* (OnlineEarly Articles) doi:10.1111/j.1467-9515.2007.00592.x

Taylor, P., *From Patient Data to Medical Knowledge. The Principles and Practice of Health Inforamtics*, Blackwell Publishing, 2006.

Thompson, D., Wright K., *Developing a Unified Patient Records. A practical guide*, Radcliffe Medical Press, 2003.

Vedder, A., 'Medical data, New Information Technologies and the Need for Normative Principles Other than Privacy Rules', in M. Freeman and A. Lewis (ed.), *Law and Medicine.* (Series Current Legal Issues). Oxford: Oxford University Press, 2000, 441-459.

Wilson P., Lessens, V., 'Rising to the challenges of eHealth across Europe's regions', *eHealth 2006*, eHealth and Health policies. Synergies for better Health in a Europe of regions. High level conference, exhibition and associated events, Malaga, Spain, 10-12 May 2006

Wukadinovish, D.,M., Coughlin, S.S., 'State confidentiality laws and restrictions on epidemiologic research: a case study of Louisiana law and proposed solutions', *Epidemiology*, Vol. 10, 1999, 91-94.