

Identity Management Systems in Healthcare: The Issue of Patient Identifiers

Els Soenens

Vrije Universiteit Brussel, Center for Law, Science, Technology and Society Studies*
Pleinlaan 2, 1050 Brussels, Belgium
Els.Soenens@vub.ac.be

Abstract. According to a recent recommendation of the European Commission, now is the time for Europe to enhance interoperability in eHealth. Although interoperability of patient identifiers seems promising for matters of patient mobility, patient empowerment and effective access to care, we see that today there is indeed a considerable lack of interoperability in the field of patient identification. Looking from a socio-technical rather than a merely technical point of view, one can understand the fact that the development and implementation of an identity management system in a specific healthcare context is influenced by particular social practices, affected by socio-economical history and the political climate and regulated by specific data protection legislations. Consequently, the process of making patient identification in Europe more interoperable is a development beyond semantic and syntactic levels. In this paper, we give some examples of today's patient identifier systems in Europe, discuss the issue of interoperability of (unique) patient identifiers from a socio-technical point of view and try not to ignore the 'privacy side' of the story.

Keywords: eHealth, interoperability, (unique) patient identifiers, identity management, privacy.

1 eHealth and the Need to Identify Patients

Clearly, the urge to identify patients is not something new or exclusive to the domain of eHealth. The importance of correct patient identification for reasons of 'delivery of care, administrative processes, support services, record keeping, information management, and follow-up and preventive care' has been recognized well before eHealth came into the picture [19]. Nevertheless the issue got renewed attention in the light of the idea of eHealth.

* The homepage of this interdisciplinary research group (under directorship of Prof. S. Gutwirth) can be accessed via <http://www.vub.ac.be/LSTS>

eHealth¹ envisions efficient and authorized access to medical data in order to develop patient mobility², patient empowerment³ and enhanced quality of care for citizens. eHealth reflects the idea that Information and Communication Technologies (ICT's) facilitate the access to medical data from various sources on an almost permanent scale. This means that, when necessary, healthcare organizations must be able to exchange and receive medical information about a specific patient. Thus, in order to facilitate the development of eHealth services and applications across Europe, interoperability of patient identification system is crucial [14]. However, when the use of a patient identifier eases the linking of (medical and other) information from several sources to a unique citizen, privacy could be at stake. In other words, whereas correct and easily available patient information is essential to healthcare delivery, it could also entail the risk of breaking off patient safety⁴. The European Commission acknowledges this 'double sword', as can be seen in the recently adopted Communication and proposal for a Council Recommendation on patient safety [21].

Summarized, one can observe at least three important requirements of patient identification systems in an (European) eHealth area: First of all, patients should be *uniquely* identified. Unique identification implies that there is an indisputable association between the medical data and a single individual. Secondly, *interoperable exchange* of patient identifiers (and medical data) should be considered essential. Finally, *privacy and patient safety* should be respected. For the EU, it is crucial that patient identification systems should not endanger the protection of patients' privacy and confidentiality. But aren't these requirements mutually exclusive? Doesn't the use of unique and interoperable patient identification schemes actually impede the protection citizen's privacy?⁵

¹ eHealth in Europe implies the use of information and communication technologies to facilitate safe and efficient healthcare delivery, citizen empowerment, patient mobility, easy access to care and the development of an European market for eHealth applications: [2].

² Patient mobility can be seen in the light of the 'European strive for free movement of citizens and goods. 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)': [1].

³ 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': [22:32]. Patient empowerment reflects the idea that healthcare seekers must be able to make their own choices about treatments. As such, patients become 'active consumers of healthcare': [22]. Recently, the International Council on Medical and Care Compunetics (ICMCC) launched the term '*Patient 2.0 Empowerment*' which underlines the use of ICT: 'the active participation of the citizen in his or her health and care pathway with the interactive use of Information and Communication Technologies.': see <http://www.epractice.eu/document/5162>.

⁴ In the EU patient safety is understood as 'freedom for a patient from unnecessary harm or potential harm associated with healthcare': see http://ec.europa.eu/health-eu/care_for_me/patient_safety/index_en.htm.

⁵ The participants of the 2008 PhD Event (Greece) of the FIDIS project (The Future of Identity in the Information Society) had an interesting discussion about this issue. Some participants, under which lawyers, were convinced of the fact that exchange of interoperable patient identifiers between healthcare contexts is by definition at odds with privacy protection, while others believed that it should be possible to exchange patient information (including identifiers) and still uphold assurance of privacy protection of individuals.

We will argue that they are not. However it certainly calls for a delicate and complex balancing exercise from the countries of the European Economic Area (EEA).⁶

It is the aim of this paper to explore promising solutions for patient identification in today's European eHealth context, taking into account the three requirements summed up above. We start with a non-exhaustive overview of the state of art of patient identification systems across Europe (section 2). We draw on the results reported in deliverable D4.11 of the Network of Excellence 'The Future of Identity in the Information Society' (FIDIS) [1].⁷ Secondly we stress that it is feasible to look at the development and implementation of interoperable patient identification systems as a complex issue combining various technical, social, economical and legal aspects and dimensions (section 3). Thirdly, the requirement of unique identification is focused on. In section 4, we explore existing approaches to uniquely identify patients. Finally, we highlight some of the prospects of patient identification systems that are privacy-friendly and feasible in a cross-border eHealth context (section 5).

2 State of Art Anno 2008

Several EU projects (such as Artemis 'A Semantic Web Service-based P2P Infrastructure for the Interoperability of Medical Information Systems' [3] or RIDE 'A Roadmap for Interoperability of eHealth Systems' [4]); studies [1] [5] and European Commission documents [14] recently indicated a huge variety in the state of art of patient identifiers across Europe. In general differences relate to the reach of the patient identification schemes (hospital specific, national or regional), the purpose of the patient identifier (billing, statistical and/or medical purposes) as well as to the specific content and structure of the identifier (e.g. Social Security Number (SSN) as patient identifier or as building block for one or more unique health care number(s)).

Another major difference between patient identifier systems is that they can be designed to be implemented in one specific healthcare institution or on the contrary, the systems can cover a whole area or nation. In Germany patient identification typically depends on the specific identification system of the hospital [1] whereas national patient identification schemes are implemented in e.g. Denmark, Finland, the Netherlands and the United Kingdom (UK) [5]. In Italy and Spain regional identification schemes exist [6] [1]. However in the latter country, the National Health Service

⁶ Justification: Often, the policy documents on eHealth of the European Commission not only address the Member States of the European Union, but also other countries of the European Economic Area (EEA). Especially in the context of cross-border healthcare and interoperability in eHealth, it is important to take into account these EEA countries.

⁷ The FIDIS D4.11 study was based on information received from FIDIS partners about their home nations (in 2007). As a result the examples in [1] are mainly limited to the following countries: Belgium, Germany and Hungary, Finland, Norway, Spain, The Netherlands. However, when relevant, practices of other (EEA) countries found in literature, are presented as well (e.g. France). Because of this non-exhaustive approach, we suggest interested readers to look into the results of EU projects such as 'A Roadmap for Interoperability of eHealth Systems' (RIDE) (<http://www.srdc.metu.edu.tr/webpage/projects/ride/modules.php?name=Deliverables>) and 'A Semantic Web Service-based P2P Infrastructure for the Interoperability of Medical Information Systems' (Artemis) (<http://www.srdc.metu.edu.tr/webpage/projects/artemis/home.html>) to find more detailed information about other countries.

(NHS) personal identification code links the various system-specific personal identification codes of citizens [1].⁸

There are also major differences that relate to the scope of the identifier used. The (unique) identifier can be used for healthcare related matters only or it can be used for affairs that transcend healthcare. Out of the surveyed countries in the FIDIS study, we found that only the UK use unique national patient identifiers which are specific for the domain of health care [1] [5]. Currently, the British health numbers are still used both for administrative (billing) and medical reasons [5]. Contrary to the UK, some countries use a patient identifier that is not specifically designed for healthcare matters only. In Norway, Sweden and the Netherlands, national citizen identifiers are used to identify patients.⁹ Identity management systems in healthcare can be based on the Social Security Number (SSN) as well. This is e.g. still the case in Belgium, where the diversity in patient identification systems is ‘solved’ in practice by the use of the SSN.¹⁰ In Switzerland, there is a unique identification number for electronic records, which is upon now based on the social security number.

This short non-exhaustive overview of approaches in patient identification systems in Europe not only reveals the huge diversity between regions and/or countries but simultaneously confirms the need for actions by Member States of the EU or by other countries of the EEA to facilitate interoperability in the field. In the following section we emphasise the need to look beyond the technical aspects of the issue of interoperability by addressing a socio-technical point of view.

3 Interoperability of Patient Identifiers on a European Level

The socio-historical context has changed since eHealth came into the European picture. In the past, the need for interoperability was never so urgent and thus it made

⁸ See 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’: [1].

⁹ 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’: [3]. In the Netherlands the Citizen Service Number (BSN) an unique identification number used throughout the public sector, is recently introduced as personal patient number.

¹⁰ In Belgium, ‘there is no common patient identification scheme used by GP (general practitioners, sic.) 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’: [8]. On several occasions in the past, the Belgian privacy committee condemned the national practice and called for a ‘unique patient identification number specifically dedicated to the processing of personal information regarding healthcare’: [8].

perfect sense for institutions to develop their own software and (privacy-friendly) context-specific patient identifiers [4]. Today however, in several aspects, interoperability has become a condition sine qua non for eHealth [7].

From a technical point of view, both semantic and syntactic interoperability¹¹ are vital. There must be agreed upon a common understanding about patient identifiers and technical standards and platforms must be developed so that patient identifiers can be exchanged in secure ways and provide authorised cross-border access to patient information. From an economical point of view, interoperability of patient identifiers facilitates free movement of people and data smoothing the progress of a European Health Information Space. For business, the 'potential value of recognizing and taking advantage of trends and opportunities in the interoperable exchange of health information among disparate entities is enormous' [4]. From the social point of view, interoperability of patient identification makes it easier for citizen to receive healthcare (at home or abroad) and facilitates public health research and epidemiological studies. From a legal point of view, rules and regulations about interoperability are important to smooth the progress of eHealth business and to avoid legal disputes e.g. about access rights.

The question is thus: How to make patient identification interoperable between organisations and even regions or nations? Although a lack of interoperability in the field is perceived (see section 2), it is without doubt that the topic is getting attention by the EU. Acknowledging the diversity in systems, the necessity for interoperability with regard to eHealth as well as the wish to develop a European Health Information Space by 2015, the European Commission recently launched a recommendation to enhance interoperability in eHealth [14]. The recommendation asks Member States of the EU as well as countries of the EEA to work together, to discuss good practices and to develop a European dynamic in order to make patient identification in Europe more interoperable [14]. These efforts are in line with the Action Plan for a European eHealth Area [10]. In order to find a global and common approach to patient identifiers in Europe, the EU suggests looking at recent developments in the field of standardization¹² and in the context of the European Health Insurance Card.

We argue that interoperability of cross-border patient identification systems (whether on the institutional, the sub-national or supra-national level) should be regarded as a complex issue, in which technical, economical, social, legal and normative aspects all influence the process. Or as the European Commission stated: 'the notion of *eHealth interoperability* used here is not only the technical definition of the term that relates to connecting systems and exchanging information, but also seeks to

¹¹ 'Syntactic interoperability (which we term as messaging layer), involves the ability of two or more systems to exchange information. Syntactic interoperability involves several layers: network and transport layer (such as Internet), application protocol layer (such as HTTP or email), messaging protocol and message format layer (such as ebXML messaging or SOAP), and the sequencing of the messages. Semantic interoperability is the ability for information shared by systems to be understood at the level of formally defined domain concepts': [9].

¹² In Europe, CEN TC251 (The European Committee for Standardization, Technical Committee for Health Informatics), CENELEC (Comité Européen de Normalisation Electrotechnique) and ETSI (European Telecommunication and Standardisation Institute) are working on the domain. These three organisations received a standardisation mandate from the EC [16]. The HISA, EHCRA and Health Level Seven (HL 7) standards are considered as highly useful (see e.g. [17]).

recognise the concept of connecting people, data, and diverse health systems, while particularly taking into account the relevant social, political, regulatory, business/industry, and organisational factors.’ [14]. Looking from such a point of view, the creation of a system for cross-border identification of patients across Europe is perceived as a tremendous task: ‘it could even be argued that the technical requirements for eHealth interoperability are the easy part of the challenge’ [20].

It is especially important to take into account the fragmented and multi-dimensional character of the issue for the reason that the organization of patient identification is subject to the subsidiarity principles of the European Union.¹³ The interoperability process starts from bottom–up, taking into account good practices selected out of existing identification systems in healthcare institutions and regions. However, these systems must be seen as the result of specific needs and practices in a particular socio-historical context.

The efforts to enhance interoperability should of course take into account the existing data protection requirements as well as the specific underlying normative attitudes of healthcare system, the role of insurance companies, the existing approaches in the field of identity management etc.¹⁴ For example in some countries, due to legal and socio-historical reasons, there exists no national identification number (Germany, Hungary) whereas in other countries such as Norway, Sweden or Turkey a national personal identifier is common and often used as an index key for medical records [3].

Rather than creating a whole new method to identify patients throughout Europe, the European Council suggests allowing Member States to maintain their own (national, regional) patient identification number systems. Only at a later stage, interoperability should be developed at the European level. An alternative solution would be to create a European Patient Identifier (EPI), which can easily and safely be used for matters of cross-border healthcare delivery and European public health statistics and which would be interoperable with existing national health identifiers [5].¹⁵

In this section we mainly focused on the examples mentioned in the FIDIS deliverable [1] but of course there are a lot of other efforts going on in the field of eHealth interoperability that relate to patient identification. Leaving aside the necessity of interoperability, eHealth applications and services count on unique identification of patients.

4 Unique Identification of Patients

In the context of eHealth, patient identifiers must be able to *uniquely identify* citizens across healthcare organizations. Unique identification is essential for integration of information across healthcare contexts, for creating a long-life view of one’s health and for the development of a Health Information Space. Patient identifiers can either be unique or not. The former are permanently assigned and unique across the entire

¹³ According to the Article 8 (7) Data Protection Directive 95/46/EC, Member States have the duty ‘to determine the conditions under which a national identification number or any other identifier of general application may be processed’.

¹⁴ Although it is very interesting to investigate in further detail how specific healthcare and insurance models influence patient identification systems, this falls outside the scope of the paper.

¹⁵ See further section 5.

(cross-border) healthcare environment whereas non-unique patient identifiers depend on the healthcare provider, the system or/and the time [19]. Examples of unique patient identifiers are e.g. the SSN and biometric identifiers. As seen in the previous sections, the SSN is indeed often used to uniquely identify patients. This poses privacy questions (see also next section). But what if a Member State opposes the use of such a unique health identifier for each citizen in Europe? Interestingly, unique identification can be done by using a unique identifier or alternatively by the use of non-unique identifiers. The Artemis project developed a 'Patient Identification Process (PIP) Protocol' suitable for cross-border for interoperability without the need to use unique identifiers [3].¹⁶ This PIP protocol provides a solution for locating and accessing prior clinical records facilitating continuity of care, an aspect that is likely to become very important in the healthcare sector. The HL7 MPI mediation standard can be mentioned as another example of unique identification of patients without using unique identifiers [19].

In any case, throughout the process of creating interoperable identifiers that uniquely identify patients, important choices influencing the privacy side of the story are made. In the following section we discuss this topic.

5 What about Privacy?

Without doubt, patient identifiers are 'essential but also privacy-invasive tools of eHealth' [1]. Privacy can be at risk if interoperable patient identifier systems facilitate exchange and access of sensitive information. However, Hippocrates' Oath still remains and is reflected in today's privacy framework (e.g. in the Directive 94/46 EC).¹⁷ Existing privacy regulatory frameworks ensure the protection of personal data and define the conditions under which processing of personal data is allowed.

We argue that privacy protection of patients is depending on administrative, technical, legal, social and organizational measures. Regarding security, there should be a differentiation between the identification function and access control function (for audit trails and /or preventive actions). The design of the patient identifier should be content free and irreversible to guarantee anonymity. Finally, staff and user training seem to be absolutely preconditional for privacy [19].

In the following several concrete suggestions for privacy-friendly patient identification systems are made. First of all, privacy-friendly patient identification schemes must be able to assure that citizens have individual control over who uses their data and for what purposes. It is therefore suggested by [12] that 'voluntary, patient-controlled system of unique identifiers is the only way to ensure acceptable levels of safety and accuracy when exchanging medical information through an electronic national network'. However, unique identifiers have the potential to link data from electronic health records with other data sources. Especially the use of the Social Security Number (SSN) as a patient identifier can imply serious privacy risks. When using the SSN as a patient identifier,¹⁸ health related data can easily be linked with other personal information, creating a bearing surface for profiling practices.

¹⁶ For more information we refer to the Artemis deliverables: [18].

¹⁷ For a detailed overview of legal aspects of eHealth, we refer to [11].

¹⁸ As is the actual practice in Belgium and Switzerland.

We therefore suggest not the use the SSN as a direct patient identifier to provide access to information in medical records. However, the SSN can be used as the basis for the creation of a unique patient identifier but only when irreversibility and thus anonymity is guaranteed. By using a ‘double hashing method’ (a first coding from SSN to health identification number (for health portal) and a second one (for data processing shelter) [6]), the privacy risks can be minimized. This is so because there is an irreversible transformation of the SSN. This approach has been proposed by the Belgian HEPI GO project. Interestingly, two test phases were planned: first a ‘primary HEPI’ which is not 100% anonymous will be implemented, whereas in the second phase they want to use a ‘secondary HEPI’ (using pseudonyms and Trusted Third Parties to guarantee the anonymity of the citizen/patient) [8].¹⁹ The double hashing method has also been suggested by [6] for interoperable yet privacy-friendly patient identification numbers in France.²⁰ As a thumb of rule, reversible encryption techniques should be avoided when using the SSN as a patient identifier [5]. The approach of Quantin et al. ensures factual interoperability at the European level by including a family-component in the hashed SSN [6].²¹ This is very important for realizing a Health Information Space in Europe and for public health research and epidemiological studies in general. The approach could facilitate the use of a Unique European Health Identifier in compliance with the existing data protection framework. The already mentioned approach developed by the Artemis project also shows that it is possible to have interoperable unique patient identification that allows undirected searches for patient records without violating data protection requirements [3].

It has also been suggested that a high level of confidentiality of the medical data in electronic patient files can be reached by differentiating the access modalities of various actors (healthcare providers, administrative levels, public bodies, insurances). This could be done by separating the overall unique patient identifier into several unique identifiers that are purpose-specific. This means e.g. that administrative levels use a purpose-specific identifier which allows them to see only the information necessary for billing purposes and not the medical information [1].

¹⁹ Recently however the Belgian privacy commission permitted the classic SSN to be used as a means of obtaining access to citizens’ medical data through the Belgian eHealth platform. The commission’s new position represents a 180-degree turn on its previous stance; it may jeopardize the current level of privacy protection of Belgian citizens [13].

²⁰ Method utilizing a derived social security number with the same reliability as the social security number. We show the anonymity techniques classically based on unidirectional hash functions (such as the secure hash algorithm (SHA-2) function that can guarantee the security, quality, and reliability of information if these techniques are applied to the Social Security Number). Hashing produces a strictly anonymous code that is always the same for a given individual, and thus enables patient data to be linked. Different solutions are developed and proposed in this article. Hashing the social security number will make it possible to link the information in the personal medical file to other national health information sources with the aim of completing or validating the personal medical record or conducting epidemiological and clinical research. This data linkage would meet the anonymous data requirements of the European directive on data protection.’: [6]. See also [15] and [16].

²¹ The Hashed SSN alone can not provide enough input for the creation of a European Health Information Space. See [6].

Also, content-free patient identification numbers are useful against privacy – intrusions. In other words, no information about the sex, age or place of birth of the patient should be revealed by the patient identification number [5]. For example, 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.

6 Conclusion

In the context of eHealth, (unique) patient identifiers are critical but also privacy - invasive tools. Actually, a lot of efforts are made to discuss good practices and to develop a common understanding and vision about interoperability of patient identifiers in Europe. Although the time seems right for European Member States to develop more interoperability between patient identification systems, evidence shows that the road is still long.

Accepting the fact that existing patient identification systems in healthcare institutions, regions or nations should be seen as a particular outcome of specific socio-economical, legal and historical circumstances, it is without doubt that there are a lot of other aspects besides semantic and syntactic interoperability that have to be dealt with. For example: Do Member States want to use something as a (unique) European Patient Identifier for medical purposes? How to create interoperability between national patient identifiers if not all countries are used to have unique identifiers for citizens and some legislations explicitly prohibit this? Alternatively, interoperable solutions that do not rely on the use of unique national identifiers are proposed.

Interoperability of patient identification systems is crucial for realizing the prospects of eHealth at the individual level as well as at the community level. During the process of making patient identifiers in Europe interoperable, important choices have to be made. This will have consequences (even unintended) on the future use of medical data. We therefore believe it is essential to strive for interoperable solutions to uniquely identify patients throughout Europe that ensure strong privacy guarantees.

Acknowledgement

Research done by the author was funded by FIDIS (Future of Identity in the Information Society, Network of Excellence, FP 6 of the European Union, www.fidis.net) for FIDIS deliverable 4.11, edited by Soenens and Leys (2008).

The author thanks the participants of the FIDIS/IFIP Summer School 2008 to whom a draft version of this paper was presented for their feedback and insightful questions.

References

1. Soenens, E., Leys, M. (eds.): eHealth identity management in several types of welfare states in Europe. FIDIS Deliverable D4.11 (2008), <http://www.FIDIS-project.eu>

2. Wilson, P., Lessens, V.: Rising to the challenges of eHealth across Europe's regions. Report of the High Level Conference on eHealth, Malaga (2006), http://ec.europa.eu/information_society/activities/health/docs/events/ehealth2006malaga/ehealth2006rising_challenges_ehealth_europe_regions.pdf
3. Eichelberg, M., Aden, T., Thoben, W.: A Distributed Patient Identification Protocol based on Control Numbers with Semantic Annotation. *Int'l Journal on Semantic Web & Information Systems* 1(4), 24–43 (2005), http://www.srdc.metu.edu.tr/webpage/projects/artemis/publications/ijswis_eichelberg.pdf
4. RIDE: Publishable Final Activity Report D1.1.6 (2008), http://www.srdc.metu.edu.tr/webpage/projects/ride/deliverables/D1.1.6RIDEPublishableFinalActivityReport-v1.1.doc#_Toc189556115
5. Quantin, C., et al.: Unique Patient Concept: a key choice for European epidemiology. *International Journal of Medical Informatics* 76, 419–426 (2007)
6. Quantin, C., et al.: Building Application-Related Patient Identifiers: What Solution for a European Country. *International Journal of Telemedicine and Applications* 2008, article ID 678302, 5 pages (2008), <http://www.hindawi.com/GetArticle.aspx?doi=10.1155/2008/678302&e=cta>
7. High Level Group on Health Services and Medical Care: Report from the High Level Group to the Employment, Social Affairs, Health and Consumer Protection Council on 6-7 December 2004. HLG/2004/21 FINAL (2004)
8. HEPI-GO Project Belgium: Final Project Report (2006)
9. Dogac, A., et al.: Key Issues of Technical Interoperability Solutions in eHealth and the RIDE project. *eHealthNews.EU Portal* (2007), <http://www.ehealthnews.eu/images/stories/pdf/ride.pdf>
10. European Commission: eHealth making healthcare better for European citizens. COM(2004)356 final (2004)
11. European Commission: Legally eHealth. Putting eHealth in its legal European Context (Study report prepared by Van Dosselaere C. et al.) 14–16 (2008)
12. Medical News Today: Creation Of Voluntary Unique Patient Identifiers For Exchanging Electronic Health Records Called For. *Medical News Today* (December 2007), <http://www.medicalnewstoday.com/articles/91766.php>
13. De Morgen: Vragen rond privacy bij eHealth (30/05/2008)
14. European Commission: Recommendation of 2nd July 2008 on cross-border interoperability of electronic health record systems (COM(2008)3282 final) (2008), http://ec.europa.eu/information_society/activities/health/docs/policy/20080702-interop_recom.pdf
15. Quantin, et al.: Proposal of a French Health Identification Number Interoperable at the European Level. In: *Medinfo Proceedings of the 12th World Congress on Health (Medical) Informatics; Building Sustainable Health Systems*, pp. 503–507 (2007)
16. European Commission, DG Enterprise and industry: Standardisation mandate addressed to CEN, CENELEC and ETSI in the field Of Information and Communication Technologies. M/403 (2007), http://www.ict.etsi.fr/Activities/Documents/Mandate403_eHealth.pdf

17. Patient identity in eHealth: Project fact sheet 'patient identity in eHealth. Exchange of good practices in eHealth' (2005),
http://ec.europa.eu/information_society/activities/health/docs/studies/patientehealth-fp6book.pdf
18. Artemis: Building interoperability into medical information systems,
<http://www.srdc.metu.edu.tr/webpage/projects/artemis/publications/istresults.doc>
19. Appavu, S.I.: Analysis of Unique Patient Identifier Options. Final Report prepared for the Department of Health and Human Services (1997),
<http://www.ncvhs.hhs.gov/app0.htm>
20. European Commission: Connecting eHealth Services. Europe's Information Society Portal,
http://ec.europa.eu/information_society/activities/health/policy/interoperability/index_en.htm
21. European Commission: Press Release 'Commission takes steps to promote patient safety in Europe', IP/08/1973, December 15 (2008)
22. Stroetmann, K.: Final project report Deliverable 5.3 in the framework of the eHealth ERA project (September 2007)