

United in Diversity: Legal Challenges on the Road Towards Interoperable eHealth Solutions in Europe

Karl A. Stroetmann¹, Jörg Artmann¹, Jos Dumortier², Griet Verhenneman³

¹empirica, Germany

²Time.Lex CVBA, Belgium

³KU Leuven, Belgium

Abstract

The use of IT enabled health services such as an electronic patient summary, ePrescription or telemedicine (commonly called eHealth services) are subject to differing degrees of legal regulation across Europe. This article presents the legal challenges facing further diffusion of eHealth services across Europe, based on the results of a study funded by the European Commission. Challenges of electronic identification and authentication are examples, alongside questions regarding healthcare professional liability, patient consent and data storage. The answers EU Member States have found to these challenges are illustrated in this contribution.

In addition, efforts by the EC funded large scale pilot project epSOS concerning cross-border patient summary and ePrescription services are described, notably the epSOS approach of framework agreements to address challenges resulting from different legal systems at national level.

Keywords

eHealth, legal challenges, patient summary, ePrescription, European Commission

Correspondence to:

Karl A. Stroetmann

empirica Gesellschaft für Kommunikations- und Technologieforschung mbH
Address: Oxfordstr. 2 - 53111 Bonn - Germany
E-mail: karl.stroetmann@empirica.com

EJBI 2012; 8(2):3–10

received: June 20, 2011

accepted: January 16, 2012

published: June 15, 2012

1 eHealth Opportunities and Legal Challenges

Information and communications technology (ICT) based systems and solutions applied in the health sector, loosely defined as eHealth, can be used in a beneficial way when addressing key challenges faced by our health systems [1]. But legal and regulatory issues are among the most challenging aspects when attempting to implement eHealth: privacy, confidentiality, liability and data protection all need to be addressed in order to establish trustworthy and resilient infra-structures which indeed enable a sustainable implementation and use of eHealth applications.

In the following, certain summary results will be reported of a recent study for the European Commission, which surveyed, analysed, and synthesised how far European countries have progressed “on their journey towards national eHealth infrastructures” [2]. It became obvious that a country rarely has a coherent set of laws specifi-

cally designed to address the different aspects of eHealth. In many countries the use of eHealth is currently regulated – if at all – only by the general legal framework, in particular by laws on patients’ rights and data protection. New legislation is often still in the process of being enacted.

It is noteworthy that in March 2011 a EU Directive, the one on patients’ rights in cross-border healthcare [3], not only concerned itself with entitlement and reimbursement of healthcare services across European Union Member States, but also addressed for the first time explicitly the opportunities opened up by interoperable European eHealth systems and services [[3], art. 14].

Here we will focus on European eHealth interoperability efforts at the policy level, which covers also legal and regulatory issues, and the progress Member States have made in creating legal systems that support eHealth services. As national level efforts to regulate eHealth are often limited to specific domains (such as access rights, liability, or reimbursement) and do not cover the full spec-

trum of what is necessary, any future EU efforts to harmonise eHealth related legislation so as to enable cross-border delivery of healthcare, need to acknowledge national diversity and develop from there. Individual country information presented hereafter was chosen by the authors for its illustrative character.

2 The European eHealth Interoperability Policy Environment

eHealth interoperability has been high on the EU policy agenda for several years. Already the eHealth Action Plan of 2004 called for creating the conditions for a seamless flow of information between interoperable systems across Member States and health systems for the benefit of patients [4]. Confidentiality and security issues were already then identified as “major challenges for wider implementation.” A recommended action to be taken on the Member State level, was “[to provide a framework] for greater legal certainty of eHealth products and services liability within the context of existing product liability legislation.”

Following the eHealth Action Plan, a key document addressing eHealth interoperability is the “European Commission Recommendation of 2nd July 2008 on cross-border interoperability of electronic health record systems” [5]. The Recommendation invites Member States to actively work towards interoperability of EHR systems at four interoperability levels namely the overall political, the organisational, the technical, and the semantic level. It notes in particular that cross-border interoperability of eHealth services also requires “full compliance with national as well as Community legal instruments, in particular for the protection of personal data, including confidentiality and data security. The necessary legal safeguards should be ensured, together with the embedding of data protection safeguards in the design and implementation of electronic health record systems.”

In the EPSCO Council Conclusions of December 2009, legal issues surface as a stand-alone area of interoperability, being previously subsumed under the “political” header. The Council Conclusions of December 2009 provide a strong political mandate for EU eHealth cooperation in four specific areas of interoperability: legal (including regulatory and ethics), standardisation / technical issues, semantics, identification and authentication [6]. These areas correspond to the main priorities of the eHealth Governance Initiative (eHGI) [7]. The EU Digital Agenda, as part of the EU2020 approach and strategy, calls for a recommendation defining a minimum common set of patient data for interoperability of patient records to be accessed or exchanged electronically across Member States by 2012 [8]. Other actions aim at fostering EU-wide standards, interoperability testing and certification of eHealth systems through stakeholder dialogue.

The European Interoperability Framework defines legal interoperability explicitly as “the legislative foundation for interoperability, for example, by providing compatible regulations concerning privacy and access control” [9].

The latest important conceptual development and planning milestone was the Thematic Network Calliope (CALL for InterOPERability) Interoperability Roadmap, which proposes a comprehensive model to address and interlink national and European activities on interoperability. In terms of legal issues, Calliope proposed the concept of an EU trusted domain for eHealth “where national trusted environments for health data exchange are federated through national nodes” [10]. The EC co-funded large scale pilot ePSOS concentrates on developing such a trusted domain through the implementation of framework agreements that enable secure access to patient health information among different European healthcare systems demonstrated on the use cases of interoperable patient summary and ePrescription [11].

In sum, it can be noted that legal issues have permeated every EC policy initiative on eHealth in the last ten years. Security and confidentiality of data have figured as concerns together with liability issues. However, these are embedded in a wider political and technical context that together defines the EU level thinking on interoperability. As can be observed in the next section, national level progress has been made regarding specific areas that affect electronic health records, ePrescribing, and telehealth – among others. However, more legislation is expected to follow increased use of such eHealth applications and systems. Currently, these are still in their infancy i.e. are at a pilot stage in the majority of EU countries or regions [2].

3 EU Member State eHealth Legislation Pertaining to Electronic Health Record Systems, ePrescribing Initiatives, and Telehealth Applications

Strategic eHealth applications as mentioned in the European 2004 eHealth Action Plan are

1. patient summaries and electronic health record (EHR) systems,
2. ePrescription services as well as
3. telehealth solutions.

For each of these applications, key legal issues will be reviewed.

3.1 Patient Summaries and Electronic Health Records

Touted for 20 and more years as the ‘holy grail’ of eHealth, electronic health records (EHR), or more precisely EHR systems, are a consistent element of almost all national strategies and roadmaps. However, whereas EHR-like systems have been implemented or are under development in many healthcare provider organisations, covering patient data from within their own organisational boundaries, and also in various regional healthcare systems, there exist hardly any at the national level. In addition, the urgent clinical need for large-scale national systems is being questioned more and more, as a recent English evaluation noted: “Clinicians’ enthusiasm for electronic health records often related to perceived benefits on their immediate surroundings and did not necessarily relate to the NHS Care Records Service goal of geographically widespread sharing of patient data” [12].

3.1.1 What is meant by patient summary and EHR?

Using the epSOS [13] project’s definition, a patient summary is defined as a minimum set of a patient’s data which would provide a health professional with the essential information needed in case of unexpected or unscheduled care (e.g. emergency, accident), but also in case of planned care (e.g. after a relocation, inter-organisational care path) [14]. Patient summaries, also referred to as core minimum data sets, are usually generated and maintained by GPs. Such a summary was referred to as the “Emergency EHR” in England’s 1998 Information for Health strategy and is the foundation of the Emergency Care Summary (ECS) in Scotland.

When it comes to the term EHR, it is much less clear what is meant. Recognising that there is, as yet, no universally accepted standard definition, here a patient’s electronic health record (EHR) is understood to be a shared, integrated or interlinked (virtual) record of all his/her clinically relevant health and medical data independent of when, where and by whom the data were recorded. In other words, it is an account of his/her diverse encounters with the health system as recorded in a variety of medical records maintained by various providers such as GPs, specialists, hospitals, laboratories, pharmacies etc. In some cases, an EHR is understood to contain a patient summary as one of its core elements or artefacts.

3.1.2 EHR systems as an element of national strategies

Across most countries, policy documents mentioning EHRs usually do not contain specific definitions, i.e. it remains unclear what is really meant. It seems that, for implementation purposes, mainly patient summaries

or extended versions thereof are envisaged. Such patient summaries (usually including medication records) as well as ePrescription services are key applications for many Member States and other European countries. Supported by the EC, initially 12 and now 23 of them are currently involved in a large scale pilot, epSOS, for defining, testing and piloting these two services in the cross-border context. These epSOS services will be based on sound elements of legal, security, semantic and technical interoperability. They also need various building blocks like citizen identification and provider identification. All of these issues are being tackled within the pilot. This generates a considerable momentum to move from high-level policy statements to the resolution of concrete challenges in the participating countries and regions.

3.1.3 Legal issues of patient summary and EHR systems

Obligation to keep patient health records Nearly all European countries legally enforce a duty to keep a carefully updated and safely stored health record. This enforcement is often incorporated in patient rights regulation. In a large majority of the countries that recognize the right to a health record, the choice to keep the health record either electronically or on paper is still open. Belgium [15, 16] Greece [17], Lithuania [18], Slovakia [19] and Slovenia [20] for example explicitly enable the maintenance of health records in written or electronic form. If the patient has opted for an electronic form, additional requirements can be set, implying the use of electronic signatures and the adoption of other security related measures. In very few countries the use of an electronic form is already obligatory. It is for example the case in Finland, but only partly. The Finnish Client Data Act [21] requires all public healthcare units to keep all health records in electronic form by 2011. A similar obligation is however expected to arise in other countries, too, as many are currently installing electronic health records that are opt-out based and thus need to be created automatically.

Opt-in or opt-out based electronic healthcare records With EHR projects firmly on the agenda in almost all EU countries, the legal rules governing the creation of individual records can be distinguished as opt-in or opt-out models. The question whether the creation of an electronic health record should be opt-in based or opt-out based, is still one of the most contentioust in many European countries. In Austria and the Netherlands for example it is still being debated what to opt for. In both countries privacy is recognized as the most sensitive aspect of the electronic health record system. Countries like Belgium, France, Italy, Spain, Iceland and Switzerland do require the patient to consent explicitly or in writing before an electronic health record may be created ¹.

¹This consent refers to the national EHR projects and may be different to the creation of medical records in a hospital environment.

In Spain for example the requirement for explicit consent follows from the Health Law read in conjunction with the Data Protection Legislation. In Iceland the Health Sector Database Act, installed in 2002, was heavily criticized for the fact that citizens were identifiable in this opt-out based database. The recently enacted Patient Rights Act now requires the prior consent of the patient before information can be stored in any database. In France an electronic health record can only be created after the consent of the patient, but once created the reimbursement rates are linked to the use of the record. The CNIL (the French Data Protection Authority) did however point out that by linking reimbursement rates to the use of the DMP (Dossier Medical Personnel) the right to consent risked to be compromised [22].

Other countries choose to install an opt-out based system. Examples thereof are: Estonia, Scotland, Slovakia, Sweden and Poland. In Estonia the Amendment Act lays down the general principles for the management of health information and sets ground for the automatic creation of electronic health records in the central Health Information System unless the patient objects to it. In Scotland there is no explicit provision for the consent of the patient with regards to the creation of a health record. The dominant view in Scotland is that although the Scottish Data Protection Act does require explicit consent, this does not preclude obtaining consent on an opt-out basis. In Slovakia the Act on Health Care states that maintaining medical records is an integral part of the healthcare provision and therefore, consent from the patient is not necessary in order to create a medical record, whether written or electronic.

Three storage types of electronic healthcare record systems In terms of storage of EHRs, three types of approaches can be distinguished in Europe: centralised, decentralised or host-based. In Belgium and The Netherlands for example – two countries that opt for a decentralised system – specific laws are created to install a national “traffic control” platform [23, 24] Spain also opted for decentralised storage, but enforces the decentralised storage through its data protection legislation. In countries where it was opted for a centralized system, legislative changes often proved necessary in order to install the central/national repository.

This was for instance the case in Czech Republic and Finland. In Finland the Act on Experiments with Seamless Service Chains in Social Welfare and Care Services [25] was issued in 2000 with the aim to gain experience of arranging seamless service chains and of ways to optimize the use of information technology. This Act was followed by for example the Client Data Act covering archive services, encryption and certification services in 2007 [26] and the Act on the Use of Electronic Prescription in 2008. France, last but not least, is the best example of a country that opted for a third option: a host-based electronic health record system. French users are free to choose a data-host for their health record. As prescribed by the

French Decrees on Data hosts [27] and Confidentiality [28], data hosts can only deal with health data after having obtained certification.

3.2 ePrescription

Only a few European countries have implemented a fully operational national primary care ePrescription service. But the majority of Member States (sixteen) reported it as an element of their national eHealth strategy and/or implementation plan already for 2006, a number which has increased to twenty-two by 2010. At the national level, a full ePrescription process is used routinely only in Denmark, Estonia, Iceland, and Sweden. The Netherlands has established routine use of ePrescription in some regions, at different levels of penetration depending on the GP or hospital environment. At a national level, only Denmark provides patients with access to their medication profiles and enables them to re-order certain repeat medications themselves, e.g. via a web service.

3.2.1 What is meant by ePrescription?

ePrescription is understood as the process of the electronic transfer of a prescription by a healthcare provider in a primary care or community health centre setting to a pharmacy for retrieval of the drug by the patient. A necessary condition for this to occur is the recording of medications in the prescriber’s office Electronic Medical Record (EMR) or other system in order to generate an electronic document, the medication prescription, to be transferred via communications connections to a specific pharmacy or a regional or national ePrescription repository. More advanced capabilities include the use of computer decision support to assist in the medication ordering process before the electronic transmission of the prescription.

The ePrescription process in primary care needs to be distinguished from the use of computer technology in hospitals to facilitate the medication prescription and administration process. In those types of settings, the gold standard is a closed loop medication administration system which may include medication reconciliation and adverse drug event monitoring. Closed loop medication systems usually include an electronic medication administration record (eMAR) as well as the use of Computerized Provider/Physician Order Entry (CPOE) by physicians and/or other clinicians and support staff.

3.2.2 Legal issues in ePrescription

In some countries, ePrescription in primary care is not being used in part due to national legislation forbidding or not addressing the electronic transmission of prescriptions and the use of electronic signatures. The legal requirements concerning ePrescription mostly deal with authentication and electronic signatures, patient consent, the possibility to obtain a paper copy, and in some countries the obligation to prior clinical examination.

In Wales, e.g., the new National Health Service (Pharmaceutical Service) Amendment Regulation of April 2010 [29] requires that advanced electronic signature procedures must be applied for ePrescription purposes. The ePrescribing process must be based on modalities that the signatory can maintain under its sole control. Any subsequent change of data must be detectable.

In Finland, the Act on the Use of Electronic Prescriptions [30] and a Decree of the Ministry of Social Affairs and Health concerning electronic prescriptions state that the patient's consent is not required for issuing an electronic prescription, but the patient will have the right to receive the prescription on paper. When the prescription is electronic, the patient furthermore needs to be informed about the national database service so that s/he is aware of the data exchange and archiving operations that will take place. In France, the Healthcare Insurance Act [31] allows prescription by email only after the healthcare professional has performed a prior clinical examination.

The introduction of electronic pharmaceutical services usually requires that specific legislation be passed. In France the law no. 2007-127 [32] introduced a pharmaceutical record for every beneficiary of social health insurance. Contrary to the nation-wide electronic health record, which is opt-out based; the pharmaceutical record is optional and is thus opt-in based. The patient has the right to refuse the update of the record with specific drug information, refuse access to it, and close it. In Belgium, the Royal Decree containing instructions for the pharmacist was amended in 2009 [33], introducing an obligation by law for the pharmacist to register certain data related to prescribed medication. It also introduced a more elaborate opt-in based pharmaceutical record.

3.3 Telehealth

Telehealth applications may concern service delivery from a healthcare provider or wellness service to a citizen, among health professionals, or among citizens and family members. European Commission services defined it as “the delivery of healthcare services through the use of Information and Communication Technologies (ICT) in a situation where the actors are not at the same location”. In its 2009 Communication on telemedicine for the benefit of patients, healthcare systems and society, the Commission emphasised the value of this technology for health system efficiency and the improvement of healthcare delivery [34]. It was mentioned as a key application domain already in the 2004 eHealth Action Plan [4].

3.3.1 The telehealth landscape in Europe

All European countries surveyed report at least small local telehealth or telemedicine pilots. This concerns mostly telemonitoring applications for chronically ill patients, access to care from a distance in scarcely populated areas, sharing of patient data and coordination of services between health and social care providers, or telecare pro-

vision as an element of case management for particularly expensive patients.

3.3.2 Legal issues in telehealth

The amount of legal and regulatory documents available on telehealth is considerably smaller than on electronic health record implementations. Two causes for this can be identified: first of all telehealth applications are less advanced than electronic health record systems, and secondly there is a tendency to regard the use of telehealth services to be less problematic under current legal frameworks, so that the usefulness of legal provisions dealing with telehealth specifically is questioned. In Belgium, the Czech Republic, Greece, Italy and the Netherlands no major legal obstacles for the use of telehealth applications appear, even though no specific regulations were passed. On the other hand, a number of countries report that legal issues are still an obstacle towards wider deployment (e.g. Austria, Cyprus and Hungary).

The three most common regulatory issues with respect to telehealth are: a) the requirement to treat a patient in person, i.e. in direct face-to-face contact; b) accreditation is not available for professionals, and c) the liability of the provider of telehealth services is uncertain.

Treatment in person The requirement to render medical services face-to-face means that telehealth services from professionals to patients are not allowed (e.g., Austria) [35]). The Polish Act on the Professions of Physician and Dentist [36], too, requires that a diagnosis is made only after personally examining the patient. However, the Austrian guideline on ‘Physician and Public’ [37] specifies that the use of telemedicine can be accepted in case of an emergency. In Malta, on the other hand, online interaction or telephone-based consultations by the family doctor are not accepted as professional practice. In some countries these rigid requirements are now under discussion, and revisions may be expected. In England, the question whether a doctor is obliged to physically attend a patient arose in another than telemedicine context, but it was concluded that there is no general principle requiring the physician to do so.

Accreditation The issue of accreditation and relevant training arose in particular in England. The British Medical Association therefore issued in 2007 its own recommendations with regard to the need for training in supporting self and home-care by ICT facilitated means. Their recommendations state that education in rendering telehealth services should be included in the medical curriculum and that healthcare professionals should be rewarded for undertaking learning and skills development.

Liability Sometimes, liability issues are complicating the delivery of telehealth and telemedicine services. However, when telemedicine is used at the national level, most

countries seem to apply their general regulatory framework by analogy. This is for example the case in Denmark. The Danish Board of Health concluded in its legal guidelines [38] regarding the liability and other legal matters in connection with the provision of telehealth services by practitioners that the usual legal rules apply as well. In Belgium jurisprudence ruled that the laws applied to the liability of physicians who provide medical advice to patients by phone are the same as those for traditional liability for negligence ².

Both in England and Scotland, NHS Direct services make heavy use of nurse telephone advisers for consulting patients. The Scottish NHS service came under scrutiny in 2008 when a patient died who had been wrongly diagnosed after a telephone consultation. In legal terms, however, the fact that the advice was given by telephone rather than in a face to face situation would not per se impact upon the existence or extent of liability [39]. The misdiagnosis was not only made by the NHS 24 advisor, but also by the GP visited at the Primary Care Emergency Centre.

Whereas at the national level few barriers seem to exist, the lack of clarity concerning liability rules when practicing telemedicine in a cross-border context seems to cause some restraints to offering cross-border telemedicine services. Although EU private international rules such as the Rome I [40], Rome II [41] and Brussels I [42] regulations are in place to determine the national applicable laws and competent courts under normal circumstances, the virtual cooperation of several actors in the field of medicine and social security, under several liability rules, causes confusion. As a consequence social security services were excluded from the scope of Brussels I ³. The numerous guiding factors in these regulations, which patients can use to determine where and what type of complaint they want to issue, complicate the delineation of liabilities by healthcare practitioners or companies [43]. The confusion is furthermore enhanced by the often complicated controller – co-controller – processor relationships. It is therefore not surprising that no examples of such cross-border services were recorded in the country reports.

4 Conclusions

Considering the large diversity of national-level legislation regarding patient summary/EHR systems, ePrescribing or telehealth services, a promising approach towards enabling cross-border exchange of patient summary and ePrescription information as well as delivery of cross-border telehealth services seems to be the trusted domain approach adopted by the epSOS project through national framework agreements. This domain is considered to be an extension beyond national or regional territories where

²Court of Appeal Liege 3 October 1995; Jurisprudence de Liege et Mons 1996, page 742: a physician was held liable for the death of a child who had eaten poisonous mushroom; the court considered that the physician committed a serious professional fault by giving

epSOS Services are physically provided. The function of the framework agreement is to ensure provide the epSOS national contact points with a legal basis upon which to contract with their local healthcare professionals and healthcare organisations. It is notably designed to ensure “that suitable systems of security exist [and] that data cannot be accessed by unauthorized parties, and that patients’ rights of informed consent to data sharing are duly respected by all parties” [44].

At the more general level, the analysis showed a rather disturbing lack of legal regulations and thereby of a trustworthy base for both health providers and patients when engaging in eHealth facilitated services. A prime requirement to achieve their wider acceptance and diffusion is the Europe-wide establishment of interoperable eHealth infrastructures as a public backbone for eHealth. This calls for tackling the lack of governance structures and for more pronounced leadership in the respective regions and countries in order to provide the legal framework to govern the legitimate uses of individual medical data. Particularly, well established data protection and security rules and supportive technologies are needed to achieve a high level of acceptance from both the public and from health service providers.

Together, European actors need to develop a tighter framework addressing security, access (including patients) and consent aspects as well as other related legal issues. Furthermore, the sometimes envisaged centralisation of ‘sensitive’ data causes a great deal of discussion, e.g. whether this collection of individual data is necessary and where the limits for collection will be set, and needs greater attention as well.

Finally, to reap the full benefits from eHealth systems, the legitimate re-use use of data, e.g. for clinical research, clinical trials, epidemiological studies or public health objectives, needs to be addressed. Here nuggets of information and knowledge can be found or newly derived from advanced data-mining techniques, which would improve diagnosis and treatment, patient safety and the quality of care.

Acknowledgements

This paper is based on a report [2] commissioned by the European Commission (EC), Directorate General Information Society and Media, Directorate ICT Addressing Societal Challenges, ICT for Health Unit, Brussels, Belgium. The authors thank national correspondents, EC colleagues of the ICT for Health Unit, numerous representatives and experts of the countries surveyed, and various colleagues for their valuable input, contributions, and critical reviews of the study report, country reports, and other preparatory documents. Neither the European Commission nor any person acting on behalf of the Commission is merely medical advice by telephone.

³Article 1, c) Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

responsible for the use which might be made of the information presented. The views expressed are those of the authors and do not necessarily reflect those of the European Commission.

References

- [1] Stroetmann, K.A., et al., eHealth is Worth it, The economic benefits of implemented eHealth solutions at ten European sites. 2006, European Commission: Bonn.
- [2] Stroetmann K., A.J., Stroetmann V.N. et al. European countries on their journey towards national eHealth infrastructures. 2011.
- [3] European Union, Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. 2011, Official Journal of the European Union: Brussels.
- [4] European Commission, e-Health - making healthcare better for European citizens: an action plan for a European e-Health Area. 2004, European Commission: Brussels.
- [5] European Commission, Commission Recommendation on cross-border interoperability of electronic health record systems 2008, Official Journal of the European Union. p. 37-43
- [6] European Council, Council Conclusions on Safe and efficient healthcare through eHealth. 2009: Brussels.
- [7] European Commission. eHealth Governance Initiative. 2011 [cited 2011 20.06.2011]; Available from: http://ec.europa.eu/information_society/activities/health/policy/ehealth_governance_initiative/index_en.htm.
- [8] European Commission, A Digital Agenda for Europe. 2010: Brussels.
- [9] epSOS, D3.3.3 epSOS Interoperability Framework. 2010.
- [10] Calliope Thematic Network, EU eHealth Interoperability Roadmap. 2010: Brussels.
- [11] epSOS. epSOS D2.1.2 Legal and Regulatory Constraints on epSOS Design: Participating Member States 2010; Available from: http://www.epsos.eu/uploads/tx_eposfiles/D2.1.2_Standard_Contract_Terms_for_MS_Document_for_engagement_of_pilot_sites_01.pdf
- [12] Robertson, A., et al., Implementation and adoption of nationwide electronic health records in secondary care in England: qualitative analysis of interim results from a prospective national evaluation. *BMJ*, 2010. 341: p. c4564.
- [13] epSOS. Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription.; Available from: www.epsos.eu.
- [14] epSOS, D3.2.2 Final Definition of Functional Service Requirements – Patient Summary. 2010.
- [15] Royal Decree, Arrêté royal déterminant les conditions générales minimales auxquelles le dossier, visé à l'article 17quater de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre. 2006: Brussels.
- [16] Royal Decree, Arrêté royal du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre. 1999: Brussels.
- [17] Greek Government, Law 3418/2005 on the Code of Medical Ethics. 2005: Athens.
- [18] Lithuanian Government, Law on Patients' Rights and Compensation for Health Damages (No. I-1562, 3 October, 1996, last amended in 2005). 1996: Vilnius.
- [19] Slovakian Government, Act No. 576/2004 Coll. of 22 September 2004. On healthcare, healthcare-related services and on the amendment and supplementing of certain laws. 2004: Bratislava.
- [20] Government of Slovenia, The Patients Rights Act (Zakon o pacientovih pravicah, ZPacP), Official Journal of the Republic of Slovenia, Nr. 15/2008, 11 February, 2008. 2008, Official Journal of the Republic of Slovenia: Ljubljana.
- [21] Finnish Government, Act 159/2007 Laki sosiaali- ja terveydenhuollon asiakirjojen sähköisestä käsittelystä (in Finnish, content in English: legislation on eArchiving). 2007: Helsinki.
- [22] Commission Nationale Informatique et Libertés (CNIL). La CNIL autorise le déploiement du dossier médical personnel sur l'ensemble du territoire. 2010 20.06.2011; Available from: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-autorise-le-deploiement-du-dossier-medical-personnel-sur-l-ensemble-du-territoire/>.
- [23] La plate-forme eHealth. Bienvenue sur le site portail de la plate-forme eHealth [Welcome to the portal site for the eHealth platform]. 2008 16.09.2010; Available from: <https://www.ehealth.fgov.be/fr/homepage/index.html>.
- [24] NICTIZ. Landelijke infrastructuur. 2011 [cited 2011 20.06.2011]; Available from: <http://www.nictiz.nl/page/Landelijke-infrastructuur>
- [25] Finnish Government, Act on Experiments with Seamless Service Chains in Social Welfare and Health Care Services and with a Social Security Card. 2000: Helsinki.
- [26] Finnish Government, Act on the electronic processing of client data within social welfare and health care 2007: Helsinki.
- [27] French Government, Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires) 2006: Paris.
- [28] French Government, Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires) 2007: Paris.
- [29] National Assembly of Wales, The National Health Services Regulations (Pharmaceutical Services) (Amendment) (Wales) Regulations 2010. 2010.
- [30] Ministry of Health and Social Affairs, Laki sähköisestä lääkemääräyksestä [Law on ePrescription]. 2007, Finlex: Helsinki.
- [31] Loi n°2004/810 du 13 août 2004 relative à l'assurance maladie [Healthcare Insurance Act]. 2004, Legifrance: Paris.
- [32] Assemblée Nationale, Loi no 2007-127 du 30 janvier 2007 ratifiant l'ordonnance no 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique. 2007.
- [33] Arrêté royal portant instructions pour les pharmaciens (du 21 janvier 2009), Agence Fédérale des Médicaments et des produits de santé, Editor. 2009.
- [34] European Commission, Communication on telemedicine for the benefit of patients, healthcare systems and society. 2008: Brussels.

- [35] Bundesgesetz, mit dem ein Bundesgesetz über die Ausübung des ärztlichen Berufes und die Standesvertretung der Ärzte (Ärztegesetz 1998 - ÄrzteG 1998) erlassen und das Ausbildungsvorbehaltsgesetz geändert wird, Bundesgesetzblatt, Editor. 1998: Wien.
- [36] Law of 5th December 1996 on professions of a physician and a dentist (Journal of Laws of 2008, No 136, item 857) 1996.
- [37] Österreichische Ärztekammer (Austrian Chamber of Physicians), *Arzt und Öffentlichkeit (Werberichtlinie)*, A.C.o. Physicians, Editor. 2004: Vienna.
- [38] Sundhedsstyrelsen, *Vejledning om ansvarsforholdene mv. ved lagers brug af telemedicin [Instructions on physician liability in the use of telemedicine]* (No. 9719 of November 9th 2005). 2005: Copenhagen.
- [39] Scottish Parliament Region: Glasgow and Central Scotland, Cases 200502301 200600457: NHS24 and Lanarkshire NHS Board (Summary of Investigation).
- [40] EC Regulation, Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations. (Rome I). , Official Journal of the European Union L 177 (4.7.2008), Editor. 2008: Brussels.
- [41] EC Regulation, Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), Official Journal of the European Union L 199/40, Editor. 2007.
- [42] Council of the European Union, Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J.o.t.E.C.L. 12/1, Editor. 2001.
- [43] S. Callens, J.T.H., *Juridische beschouwingen bij telegenesekunde Tijdschrift voor Gezondheidsrecht*, 2000(1999-00): p. 316.
- [44] Framework Agreement on National Contact Points in the context of the Smart Open Services for European Patients Project (epSOS) - Preamble. 2011.