EJBI 2012 ISSN 1801 - 5603

European Journal for Biomedical Informatics

Volume 8 (2012), Issue 2

Special Topic

Support of eHealth Applications by Legal Systems in Europe

Editors

Petra Wilson and Zoi Kolitsi

An Official Journal of the European Federation for Medical Informatics

www.ejbi.eu

EFMI European Federation for Medical Informatics

Aims and Scope

The European Journal for Biomedical Informatics reacts on the great European need to share the information in the multilingual and multicultural European area. The journal publishes peer-reviewed papers in English and other European languages simultaneously. This opens new possibilities for faster transfer of scientific-research pieces of knowledge to large international community of biomedical researchers, physicians, other health personnel and citizens.

The generally accepted translations of the English version of the paper are to the following European languages:

List of European languages	ISO 639-1 code
Albanian	sg
Armenian	hy
Azerbaijani	az
Belarusian	be
Bosnian	bs
Bulgarian	bg
Catalan	ca
Croatian	hr
Czech	cs
Danish	da
Dutch	nl
English	en
Estonian	et
Finnish	fi
French	fr
Georgian	ka
German	de
Greek	el
Hungarian	hu
Icelandic	is
Irish	ga
Italian	it
Kazakh	kk
Latvian	lv
Lithuanian	lt
Luxembourgish	lb
Macedonian	mk
Maltese	mt
Norwegian	no
Polish	pl
Portuguese	pt
Romanian, Moldavian, Moldovan	ro
Romansh	rm
Russian	ru
Serbian	sr
Slovak	sk
Slovenian	sl
Spanish	es
Swedish	sv
Turkish	tr
Ukrainian	uk

Editors and Management

Editorial Board: National Members

Editorial Board: Representatives of Cooperating Journals

Publisher

EuroMISE s.r.o.
Paprsková 330/15
CZ-14000 Praha 4
Czech Republic
EU VAT ID: CZ25666011

Office

EuroMISE s.r.o.
Paprsková 330/15
CZ-14000 Praha 4
Czech Republic

Contact

Karel Zvára
zvara@euromise.com
Tel: +420 226 228 904
Fax: +420 241 712 990

Instructions to Authors for the Preparation of Contributions

Abstract

The abstract should summarize the contents of the paper and should not exceed 250 words. Authors are requested to write a structured summary, adhering to the following headings: Background (optional), Objectives, Methods, Results, Conclusions.

Keywords

At the end of the Abstract, the contents of the paper should be specified by, at most, five keywords. We recommend using MeSH keywords.

Introduction

Authors are kindly requested to carefully follow all instructions on how to write a paper. In cases where the instructions are not followed, the paper will be returned immediately with a request for changes, and the editorial review process will only start when the paper has been resubmitted in the correct style.

Authors are responsible for obtaining permission to reproduce any copyrighted material and this permission should be acknowledged in the paper.

Authors should not use the names of patients. Patients should not be recognizable from photographs unless their written permission has first been obtained. This permission should be acknowledged in the paper.

In general the manuscript text (excluding summary, references, figures, and tables) should not exceed 5 000 words.

Kindly send the final and checked source and PDF files of your paper to manuscripts@ejbi.org. You should make sure that the LaTeX and the PDF files are identical and correct and that only one version of your paper is sent. Please note that we do not need the printed paper.

Checking the PDF File

Kindly assure that the Contact Volume Editor is given the name and email address of the contact author for your paper. The contact author is asked to check through the final PDF files to make sure that no errors have crept in during the transfer or preparation of the files. Only errors introduced during the preparation of the files will be corrected.

If we do not receive a reply from a particular contact author, within the timeframe given, then it is presumed that the author has found no errors in the paper.

Copyright Transfer Agreement

The copyright form may be downloaded from the "For Authors" section of the EJBI Website: `www.ejbi.org`. Please send your signed copyright form to the Contact Volume Editor, either as a scanned pdf or by fax or by courier. One author may sign on behalf of all the other authors of a particular paper. Digital signatures are acceptable.

Manuscript Preparation

You are strongly encouraged to use LaTeX 2_ε for the preparation of your manuscript. Only if you use LaTeX 2_ε can hyperlinks be generated in the online version of your manuscript. The LaTeX source of this instruction file for LaTeX users may be used as a template.

When you are not able to use LaTeX, please use MS Word or OO Writer and send us the unformatted text. Kindly follow just instructions about preparing figures, tables and references. These instructions are explained for you in the included MS Word document. We are going to convert your text into LaTeX instead of you.

If you use LaTeX together with our template file, `ejbi_template.tex`, your text is typeset automatically. Please do *not* change the preset fonts. Do not use your own macros, or styles.

Please use the commands `\label` and `\ref` for cross-references and the commands `\bibitem` and `\cite` for references to the bibliography, to enable us to create hyperlinks at these places.

Headings Headings should be capitalized (i.e. nouns, verbs, and all other words except articles, prepositions,

and conjunctions should be set with an initial capital) and should be aligned to the left. Words joined by a hyphen are subject to a special rule. If the first word can stand alone, the second word should be capitalized.

Lemmas, Propositions, and Theorems The numbers accorded to lemmas, propositions, and theorems, etc. appear in consecutive order, starting with Lemma 1, and not, for example, with Lemma 11.

Figures and Tables

Attach figures and tables as separate files. Do not integrate them into the text. Do not save your table as an image file or insert a table into your manuscript text document as an image.

Basics of Graphic Composition Less is more! Avoid tables with columns of numbers. Summarise the main conclusion in a figure.

- Annotations belong in a (self-)explanatory legend, do not use headings in the figure, explain abbreviations in the legend.
- Label all axes.
- Use a uniform type size (we recommend Arial 10 point), and avoid borders around tables and figures.

Data Formats

- Submit graphics as a sharp printout as well as a file. The printout and the file must be identical.
- Submit the image file with clear labelling (e.g. Fig_1 instead of joint_ap).

Image Resolution Image resolution is the number of dots per width of 1 inch, the "dots per inch" (dpi). Printing images require a resolution of 800 dpi for graphics and 300 dpi for photographics.

Vector graphics have no resolution problems. Some programs produce images not with a limited number of dots but as a vector graphic. Vectorisation eliminates the problem of resolution. However, if halftone images ("photos") are copied into such a program, these images retain their low resolution.

If screenshots are necessary, please make sure that you are happy with the print quality before you send the files.

Figures and Tables in LaTeX For LaTeX users, we recommend using the *ejbi-figure* environment (Figure 1 shows an example). The lettering in figures should have a height of 2 mm (10-point type). Figures should be numbered and should have a caption which should always be positioned *under* the figures, in contrast to the caption belonging to a table, which should always appear *above* the table (see an example in Table 1). Short captions are centred by default between the margins and typeset automatically in a smaller font.

Table 1: Age, period, cohort modelling of coronary heart mortality, men, 30-74 yrs., Czech Republic, 1980-2004.

No.	Model	D	*df*	*p*-value
0	Interception	355388.0	44	<0.001
1	Age	15148.0	36	<0.001
2	Age-Drift	3255.5	35	<0.001
3a	Age-Age*Drift	2922.5	27	<0.001
3b	Age-Period	388.2	32	<0.001
3c	Age-Cohort	1872.6	24	<0.001
4	Age-Period-Cohort	28.7	21	0.121

Remark 1. In the printed volumes, illustrations are generally black and white (halftones), and only in exceptional cases, and if the author is prepared to cover the extra cost for colour reproduction, are coloured pictures accepted. Coloured pictures are welcome in the electronic version free of charge. If you send coloured figures that are to be printed in black and white, please make sure that they really are legible in black and white. Some colours as well as the contrast of converted colours show up very poorly when printed in black and white.

Formulas

Displayed equations or formulas are centred and set on a separate line (with an extra line or halfline space above and below). Displayed expressions should be numbered for reference. The numbers should be consecutive within each section or within the contribution, with numbers enclosed in parentheses and set on the right margin – which is the default if you use the *equation* environment, e.g.

$$\psi(u) = \int_o^T \left[\frac{1}{2} \left(\Lambda_o^{-1} u, u \right) + N^*(-u) \right] dt \, . \qquad (1)$$

Please punctuate a displayed equation in the same way as the ordinary text but with a small space before the end punctuation.

Footnotes

The superscript numeral used to refer to a footnote appears in the text either directly after the word to be discussed or – in relation to a phrase or a sentence – following the punctuation sign (comma, semicolon, or period). Footnotes should appear at the bottom of the normal text area, with a line of about 2 cm set immediately above them.[1]

[1] The footnote numeral is set flush left and the text follows with the usual word spacing.

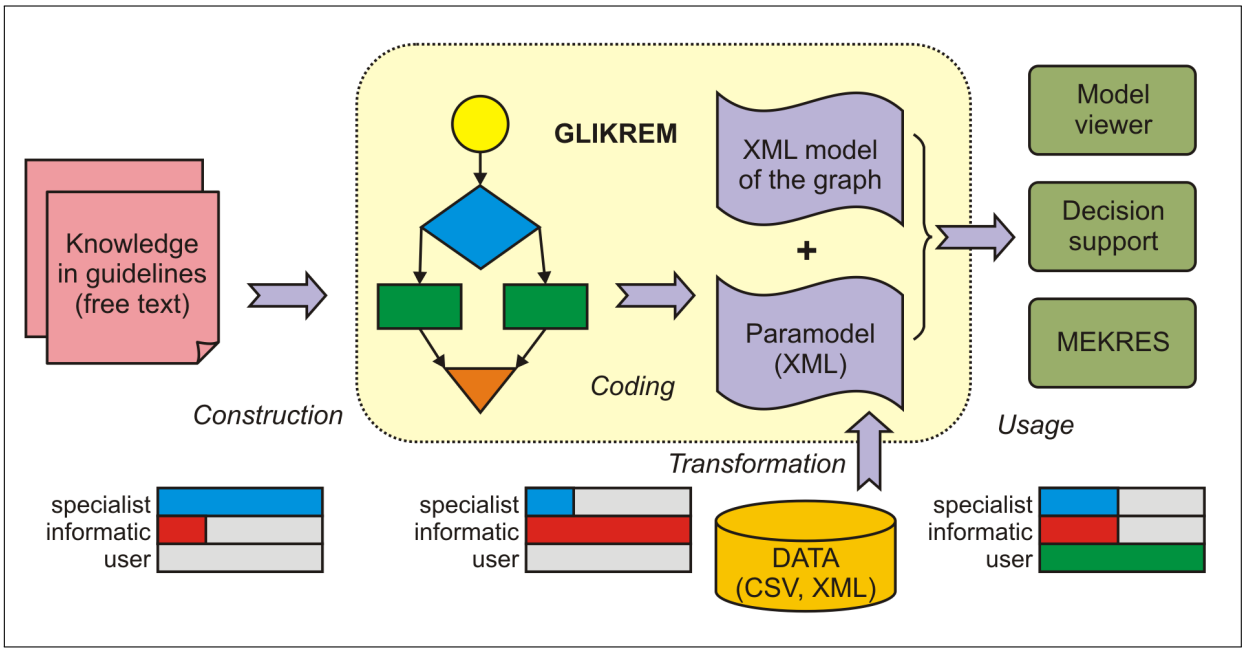

Figure 1: Construction, coding and use of GLIKREM.

Program Code

Program listings or program commands in the text are normally set in a typewriter font, e.g. CMTT10 or Courier.

Citations

The list of references is headed "References" and is not assigned a number. The list should be set in small print and placed at the end of your contribution, in front of the appendix, if one exists. Please do not insert a pagebreak before the list of references if the page is not completely filled. An example is given at the end of this information sheet.

For citations in the text please use square brackets and consecutive numbers: [1], [2, 3, 4]...

In the text number the references consecutively in the order in which they first appear. Use the style, which is based on the formats used by the US National Library of Medicine in MEDLINE (sometimes called the "Vancouver style"). For details see the guidelines from the International Committee of Medical Journal Editors (http://www.nlm.nih.gov/bsd/uniform_requirements.html).

Page Numbering and Running Heads

Please do not set running heads or page numbers.

Acknowledgements

Scientific advice, technical assistance, and credit for financial support and materials may be grouped in a section headed Acknowledgements that will appear at the end of the text (immediately after the Conclusions section).

The heading should be treated as a subsubsection heading and should not be assigned a number.

In case that a financial support of the paper development (e.g. sponsors, projects) is acknowledged, in the year 2012 the fee of 50 EUR will be charged by Publisher. The accepted peer-reviewed papers with an acknowledgement of a financial support, where the fee was not paid, will be published free of charge, but the financial acknowledgement will be withdrawn.

EJBI Online

The online version of the full volume will be available at `www.ejbi.org`.

References

[1] Blobel B. Architectural Approach to eHealth for Enabling Paradigm Changes in Health. Methods Inf Med. 2010; 49(2): 123–134.

[2] Kalina J. Robustní analýza obrazu obličeje pro genetické aplikace. EJBI [Internet]. 2010 [cited 2011 Jun 28]; 6(2): cs95–cs102. Available from: http://www.ejbi.eu/articles/201012/47/2.html

[3] van Bemmel JH, Musen M, editors. Handbook of Medical Informatics. Heidelberg: Springer; 1997.

[4] Zvarova J, Zvara K. e3Health: Three Main Features of Modern Healthcare. In: Moumtzoglou A, Kastania A. E-Health Systems Quality and Reliability: Models and Standards, Hershey: IGI Global; 2010; 18–27.

Contents

Do the Legal Systems of Europe and its Member States Meet the Needs of eHealth?

Petra Wilson[1], **Zoi Kolitsi**[2]

[1] Cisco IBSG, Belgium

[2] Informatics and Information Security Laboratory, AUTH, Greece

The term "eHealth" is used in this special edition of the European Journal of Biomedical Informatics to describe the use of information and communication technology (ICT) in the delivery of healthcare. It encompasses the use of a wide range of ICT applications including *eHealth tools*, such as Electronic Health Records; *eHealth services*, such as the Electronic Prescriptions; and *eHealth devices*, such as the remote monitoring software. The use of these tools, services and devices in the delivery of healthcare is widely acknowledged to be beneficial. They allow for accurate, timely and safe sharing of information so that patients may be better treated and supported.

Core to the efficient functioning of eHealth tools, services and devices is interoperability. Achieving interoperability in eHealth involves a complex set of operations, including *technical interoperability*, which ensures data integrity and authenticity in sharing data between different end points; *semantic interoperability*, so that information may be understood by the end user regardless of the natural language or physical environment in which it is being accessed; *organisational interoperability*, which allows healthcare providers to share information across different internal structures and processes; and *legal interoperability* which allows different jurisdictions to enable secured access to and processing of patient information transferred electronically.

In this special edition four papers are dedicated to different aspects of the legal interoperability which is fundamental to the adoption and implementation of eHealth in Europe. Stroetman [1] and colleagues provide an overview of the state of the art in legal and policy interoperability based in part on the work they undertook within the framework of a European Commission funded study which examined the progress EU Member States had made on the journey towards national eHealth Infrastructures [2].

Stroetman et al examine the current legal frameworks in place in a range of European countries for three core eHealth applications: EHRs, ePrescriptions and telehealth. They conclude that while many countries have made considerable advances in building or adapting legal frameworks for the use of EHRs, much less has been achieved in developing robust legal frameworks for ePrescriptions or telemedicine. They note that most of the legislation currently applied to the use of ICT in healthcare focuses significantly on issues of data protection, measures for ensuring patient consent to the creation and access of records, and administrative measures for ensuring appropriate security in the storage and management of EHRs.

The richness of the legal frameworks necessary to allow the smooth functioning of EHRs within and across healthcare systems is made clear by the two detailed examinations offered in this volume of the legislation on EHRs in Austria and in the Czech Republic. Reimer [3] offers a comprehensive analysis of the wide range of legislation which underpins the use of ICT in healthcare in Austria. His comprehensive paper makes clear that while Austria is still waiting for the enactment of the ELGA legislation which will establish the legal framework for the EHR itself, much of the other necessary legislation is already in place. Austria has for example already established the necessary data security requirements and the information governance framework. Reimer's analysis is significant therefore in underlining that while the EHR is a core element of a functioning eHealth system, it is not the whole story. This will serve as a useful reminder to those who still see the EHR as the Holy Grail which will solve all eHealth problems.

Dostál and Šárek [4] examine the legislation applicable to EHRs in the Czech Republic. Their thorough paper notes that while the Care for Health of the People Act n. 20/1966 Sb Health Record Order provides a good base line for the use of the EHR including guidelines on which data is to be collected, how patients' interests in confidentiality and access are to be guaranteed and how records are archived for future reference. The authors note, however, that the existing legal framework provides very little guidance on technical interoperability issues, and argue that the Czech Republic could do well to follow the model adopted in the USA of appointing an official body that co-ordinate health IT standards.

The fourth paper in this collection broadens the scope of the discussion of legal issues in eHealth away from the EHR to look at the fast evolving range of eHealth devices and eHealth services. Vollebregt [5] examines in careful detail the way in which the Ker-Optika case [5] decided by the ECJ in 2010 begins to clarify the way in which European law will apply to eHealth devices and to the provision of eHealth services on-line. Vollebregt begins by examining the facts in Ker-Optika case and draws clear conclusions that because medical devices are not excluded from the eCommerce Directive, Member States may not prohibit outright the sale of a medical device via on-line retail. However, since that same directive does not cover the modalities of sale, any rules a Member State may wish to impose for public safety or other

reasons must be examined in the light of the general EU internal market rules, which require that any restrictions on the free movement of goods in the internal market must be strictly proportionate to the harm that is to be avoided.

Vollebregt's paper goes on to look beyond the immediate impact of the Ker-Optika case on the on-line sale of medical devices (in that case contact lens were the subject matter) to extrapolate how the reasoning of the court would impact on eHealth software as a service - notably eHealth apps. Here he draws the reader's attention to the 2007 amendment of the Medical Devices Directive (which clarifies that standalone software can be a medical device, which must be duly CE marked) and concludes that "eHealth service providers are fully subject to the internal market clause in article 3 of the e-Commerce Directive".

While Vollebregt's paper looks into the future role of the EU legal framework in regulating eHealth services and eHealth devices, all four papers serve to underline the enduring importance of one of the core principles of medical ethics - that of autonomy. Beauchamp and Childress, in their textbook Principles of biomedical ethics [6], which has for many years been the touchstone of understanding medical ethics around the world, reduce all medical ethics into four core principles: autonomy, beneficence, non-maleficence and justice. Of these the concept of autonomy is most relevant to legal frameworks for eHealth as it is based on the right of every competent adult to make decisions for him or herself.

In health law, a key aspect of respecting the autonomy of the patient is usually upheld by reference to the concepts of consent and privacy. Thus most legislation on health records includes the requirement to seek a patient's consent before collecting, processing, or sharing health related information, and a duty to ensure that the privacy of the record will be maintained. It is not surprising therefore that of the legislative tools most developed in response to eHealth around the world make reference to core legal texts on privacy. The second WHO Global eHealth Observatory Survey [7] completed in 2010 established that most legal systems have enacted legal mechanisms for protecting privacy of medical information. As reported "some 70% of the 113 responding countries reported having legislation providing a basic right to privacy, and the remaining 30% anticipate that such legislation would be adopted by 2015" [8]. The report of the survey noted however that while legislation protecting medical confidentiality was widespread, far fewer countries had adopted specific legislation to protect privacy in EHRs.: only 30% globally reported having such legislation in place. Further analysis of the responses on the use of legislation to ensure privacy in sharing EHRs for treatment or research purposes revealed that very few countries have established comprehensive legal frameworks on EHRs (e.g. only 10% of countries reported having legislation which covers cross-border EHR sharing).

An important contribution towards addressing the paucity of legislative tools addressing EHRs and more particularly the sharing of EHRs across EU borders is made by the epSOS project [9] which establishes a technical and legal framework for sharing Summary Patient Records and ePresciptions between participating nations in the EU. The project provides not only a technical specification for building and sharing such records, but also established the concept of a "circle of trust" based on a common legal framework agreement to create a legal environment in which records can be shared across borders. Stroetman et al, as well as Reimer, make reference to the epSOS project and conclude that the tools and guidelines it develops will greatly assist Europe in developing a more robust legal framework for eHealth.

While the four papers in this collection make clear that Europe still has some way to go in establishing a full legal framework for eHealth, it is worth noting that it is not only the legal framework but also the organisational framework which requires further development. Indicative of this is the fact that the label "eHealth" is used to describe the use of information and communication technology (ICT) based tools in the delivery of healthcare. The very fact that we still use a special label to describe the wide range of ICT applications in healthcare is symptomatic of the fact that we do not yet see it as a core element of healthcare delivery in the twenty-first century, and until it is seen as such a core element it is unlikely that the legislation will be developed to ensure that it can function as such.

The editors of this issue would like to acknowledge and thank the Editor-in-Chief of EJBI for overseeing the process of preparing this special issue.

References

[1] Stroetmann KA., Artmann J., Dumortier J., Verhenneman G., United in diversity: Legal challenges on the road towards interoperable eHealth solutions in Europe. EJBI 2012; 8(2):3–10

[2] full details available at http://www.ehealth-strategies.eu/ (the last access May 2nd, 2012)

[3] Reimer S., Current and future settings of Austrian legislation regarding electronic health records (EHRs) EJBI 2012; 8(2):11–28

[4] Dostál O., Šárek M., Support for Electronic Health Records in Czech Law EJBI 2012; 8(2):29–33

[5] Vollebregt E., Consequences of the EU Ker-Optika Case for e-commerce in Physical Medical Devices and Apps for eHealth Services EJBI 2012; 8(2):34–39

[6] Beauchamp TL. , Childress JF., Principles of biomedical ethics. 6th edition. New York, Oxford University Press, 2001.

[7] For further details see http://www.who.int/goe/en/ (the last access May 2nd, 2012)

[8] Wilson P., Global Observatory for eHealth series - Volume 5 Legal frameworks for eHealth WHO 2012 p. 6

[9] for full details see www.epsos.eu (the last access May 2nd, 2012)

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

Karl A. Stroetmann[1], **Jörg Artmann**[1], **Jos Dumortier**[2], **Griet Verhenneman**[3]

[1]empirica, Germany

[2]Time.Lex CVBA, Belgium

[3]KU 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
recieved: 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 specifically 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 in-corporated 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].

[1] This 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, Scot-land, 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 Regula-tion 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 provision as an element of case manage-ment 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 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

[2] Court 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 merely medical advice by telephone.

[3] Article 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_epsosfileshare/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-lensemble-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 caractere 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 aout 2004 relative a 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 aout 2005 relative a l'organisation de certaines professions de santé et a 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] Arreté 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] Scotish 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 telegeneeskunde 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.

Current and Future Settings of Austrian Legislation Regarding Electronic Health Records (EHR)

Sebastian Reimer[1]

[1]CEO Intelligent Law and Internet Applications, Wien, Austria

Abstract

In the context of the European large-scale pilot on e-health ("epSOS") numerous discussions on the implementation of a pan-European e-health infrastructure have been held. They all proved that differences among the national e-health legislations pose serious obstacles to the European-wide exchange of personal health data. Even if it is very difficult to meet all requirements of the involved countries, this is an absolute pre-condition for a smooth exchange of patient data. The unlawful usage of personal health data can result in the loss of reputation, administrative fines and the need to restructure internal workflows at high costs. Being aware of the current legal framework avoids such. To know about future innovations to the legal framework facilitates strategic decisions and enables to take over leadership in the innovative process.

Recognising this, the aim of this paper is to provide a better understanding of the current Austrian e-health legislation and the innovations to come, inspired by national and European projects. As development is still ongoing at national and European level, the information provided, especially regarding the outlook, is to be understood as of April 2012.

Keywords

computer security, epSOS, electronic health records, health telematics, personal identifiers

Correspondence to:

Sebastian Reimer
CEO Intelligent Law and Internet Applications
Address: A-1030 Wien, Rasumofskygasse 30/1/8
E–mail: office@ilia.ch

EJBI 2012; 8(2):11–28
recieved: June 20, 2011
accepted: February 20, 2012
published: June 15, 2012

1 Status Quo of Austrian E-Health Legislation

The main legal provisions, relevant for the use of personal electronic health data and therefore the establishment of electronic health records (EHR), are to be found in:

- the Data Protection Act 2000 (DPA 2000) [1],
- the Health Telematics Act (HTA) [2],
- the E-Government Act (EGovA) [3],
- the Doctors Code 1998 (DC 1998) [4],
- the General Social Insurance Law (GSIL) [5],
- the Insurance Agreement Act (IAA) [6] and
- the Genetic Engineering Act (GEA) [7].

As these acts are all ordinary statutory law, they have to meet the requirements of higher-ranking law as for example national constitutional law or European law.

1.1 Austrian Constitutional Law Framework

The constitutional provisions of Austria are the highest ranked national provisions and for two reasons of interest: on the one hand they define the binding regulatory framework for future EHR provisions at ordinary law level. On the other hand some of them lay down directly applicable rights, that protect citizens, foreigners and even private law bodies against improper government action ("fundamental rights").

Usually these fundamental rights grant protection solely against infringements by acts of public authorities, as for example rulings, ordinances or ordinary statutory laws. However, there is one fundamental right in Austria – the right to privacy – that also protects against infringe-

ments by private law entities ("third party effect") as for example medical doctors, other healthcare providers or companies. They can be both: plaintiffs and defendants due to privacy infringements. Being informed about basic rights strengthens argumentation, especially when arguing with official authorities. The following fundamental rights are the most relevant ones for e-health:

- the fundamental right to privacy (Sect. 1 DPA 2000 [1]),
- the fundamental right to private and family life (Art. 8 European Convention on Human Rights – ECHR [8]),
- the principle of equality (Art. 2 Basic Law on the General Rights of Nationals – BLGRN [9], Art. 7 FCL [10]) and
- the protection of property (Art. 5 BLGRN [9]).

The **fundamental right to privacy** requires that the use of personal data is proportional, i.e. not excessive. Furthermore the use must:

- serve vital interests of the data subject or third persons or
- serve others' overriding legitimate interests or
- be based upon consent of the data subject.

Laws on EHR need to be legitimated by one of these rationales in order to be compliant with the fundamental right to privacy. The **principle of equality** ensures for example that all patients may receive healthcare under the same conditions regardless whether they opted out of an EHR system or not ("anti-discrimination"). Equal treatment of healthcare providers (HCP) requires that all healthcare providers face the same deadlines for adaption of their systems (hardware, software, organisation, ...) or financial burdens. The **protection of property** prevents that unreasonable financial burdens and risks are imposed on healthcare providers, e.g. high IT infrastructure investments in a short period of time.

Infringements of fundamental rights entitle the persons affected to constitutional legal suits against the government, that enacted the law, in front of the Austrian Constitutional Court. If the court finds in favour of the plaintiff, he can be reimbursed and the contested unconstitutional parts of the law, ordinance, treaty or decision are to be repealed. *Constitutional claims are often the last chance for private companies to avoid unjust burdens, especially financial burdens!*

1.2 Data Protection Law

Sect. 9 DPA 2000 [1] on the usage of sensitive data transposes Art. 8 of the Data Protection Directive (DPD) [11] into Austrian national law. Sensitive data is „data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life" (Sect. 4.2 DPA 2000 [1]).

According to the current legal situation in Austria a specialised law as legal base for the usage of personal health data in the context of EHR does not exist. As a consequence a national EHR, with mandatory participation of all national healthcare providers, is missing. For this reason, only legal entities, that do not perform governmental tasks, as for example medical doctors, hospitals or other healthcare providers according to Art. 3.g of the Patients' Rights Directive (PRD) [12] may take the initiative and introduce or participate in existing EHR systems.

Usage of EHR systems can legally be based upon explicit consent of the patients (Sect. 9.6 DPA 2000 [1]) or medical necessity, especially regarding treatment purposes (Sect. 9.12 DPA 2000 [1]). Some of the healthcare providers, as for example medical doctors may – due to special professional duties – communicate personal data of patients only with their consent (Sect. 51.2 Doctors' Code 1998 [4]).

Working parties on national and European level have been contesting the view, that Sect. 9.12 DPA 2000 [1] on national level or Art. 8.3 DPD [11] on European level could legitimate EHR systems. The Austrian STRING Commission (Kommission für Standards und Richtlinien für den Informatikeinsatz im österreichischen Gesundheitswesen) for example, set up by the Federal Minister for Health and Women (now: Federal Minister for Health) is convinced that Sect. 9.12 DPA 2000 [1], which transposes Art. 8.3 DPD [11] into Austrian law, cannot legitimate the use of EHR, because EHR systems have not yet been in use, when Art. 8 DPD [11] was drafted and therefore cannot cover EHR systems [13].

This argument is false, as it can be verified, that EHR systems have already been discussed in the USA during the 80's of the last century [14]. A similar opinion is shared by the Art. 29 Data Protection Working Party[1] in its Working Paper 131 (WP 131) on EHR systems [16] and its Working Paper 189 (WP 189) on epSOS [17] regarding the non-applicability of Art. 8.3 DPD [11]. Both statements [13, 16] lack detailed explanations of the underlying legal grounds for the non-applicability of Art. 8.3 DPD [11]. They are discussed in more detail below in chapter 2.2.1.

[1]The Art. 29 Data Protection Working Party is an independent advisory body, composed of national representatives of each national Supervisory Authority (Art. 28 DPD [11]) and of two EU representatives. The working party regularly adopts opinions on recent data protection topics [15], among them document WP 131 [16], that deals with EHR issues.

In fact a special law on EHR systems is not necessary from the data protection point of view[2], as both of the above cited general provisions of the DPA 2000 [1], would qualify as valid legal bases for EHR systems. The Viennese Hospital Association (Wiener Krankenanstaltenverbund) – for example – has been operating a network of medical reports since 2008 [21]. Even service providers, as for example in the field of information and communication technologies (ICT), could legally introduce and operate EHR systems based upon either Sect. 9.12 DPA 2000 [1] or Art. 8.3 DPD [11], if the personal health data is decrypted available only to medical staff for treatment purposes or other persons, who are subject to a special obligation of secrecy.

1.3 Health Telematics Law

The Health Telematics Act (HTA) [2] is the most relevant EHR related law, as it explicitly deals with personal health data communicated by electronic means. It is the only Austrian law, to determine the conditions of communicating electronic personal health data in more detail. The HTA [2] is in fact a more specialised and precise part of the Austrian data protection legislation. At the current state the HTA [2] does not provide the legal basis for processing personal electronic health data, but only governs the data security requirements for lawful communication of electronic personal health data. The Austrian Health Telematics Act [2] consists of:

1. general provisions on scope and definitions, e.g. definitions of healthcare provider or health data (Part 1 HTA [2]),
2. special **data security requirements** with regard to e-health (Part 2 HTA [2]),
3. detailed regulations regarding the **e-health directory** (Part 3 HTA [2]),
4. general guidelines for **e-health information governance** (Part 3 HTA [2]) and
5. final provisions, e.g. regarding administrative offences and transitional provisions (Part 4 HTA [2]).

Hereafter the main provisions of the HTA [2] – the core e-health law in Austria – shall be described in more detail.

1.3.1 Personal Scope of the Health Telematics Act: the healthcare providers

The HTA [2] applies to healthcare providers (Gesundheitsdiensteanbieter), who are defined as „data controllers and processors for whom the regular usage of health data is part of their business“ (Sect. 2.2 HTA [2]). The Austrian definition of healthcare providers builds upon the terms of data controllers (Sect. 4.4 DPA 2000 [1])[3] and data processors (Sect. 4.5 DPA 2000 [1])[4] , which are themselves derived from the European Data Protection Directive. Not only medical doctors and their staff are regarded as healthcare providers, but also lawyers specialised on health law or even more important IT companies using personal health data are regarded as healthcare providers in the terms of the HTA [2]. Unfortunately, such a wide definition referring to the regular usage of health data as part of one's business leads to complex discussions what can be deemed "a regular usage of health data" and whether civil servants or public authorities shall also be regarded as healthcare providers or not. Due to data protection the term healthcare provider should be interpreted in an extensive manner: the wider the definition of healthcare provider, the more data controllers and processors are covered and consequently have to comply with the HTA's [2] specialised data security rules, which – in the end – would increase the level of data protection in the health sector. This notion also corresponds with the Austrian legislation on regularity in the context of the legal definition of business according to which "even a singular activity is

[2]If public authorities want to use personal data, they need an accurately formulated legal base at least at statutory law level (Sect. 1.2 DPA 2000 [1]), to be legitimated. Private law entities are regarded too as public authorities in the meaning of Sect. 1.2 DPA 2000 [1], if they can unilaterally determine others' legal positions, in a way typical for public authorities. Based upon a draft of an Austrian EHR law, Mayer [18] argued, that ELGA healthcare providers, as for example medical doctors, will have to enforce the usage of data against the will of the patients and must therefore be regarded as public authorities. Such would require a statutory law in accordance with Art. 8.2 ECHR [8, 17]. This belief is false for the following reasons:

- Medical doctors have always been obliged by law to record medical histories of their patients – in former times by means of paper files – and never have been deemed public authorities, except of course for the public health officers (Sect. 41.1 DC 1998 [4]), who decide, according to specialised provisions of statutory law, for example on the fitness of persons to hold driving permits.
- Patients are entitled to **opt out at any time**, starting one and a half year before ELGA shall be started. Such a possibility to autonomously define one's own legal position does not exist for administrative decisions, that unilaterally define one's legal position, as for example tax assessment notices. Because such decisions were enacted with power of the state (Hoheitsgewalt) it is not possible to rescind or "opt-out". The Austrian Constitutional Court ruled that the ability to issue binding instructions or perform coercive measures is a mandatory requirement for public authorities [19].
- The Austrian Constitutional Court ruled also that the legal relations among citizens are typically regarded civil law matters [20].

[3]Data controller: "natural or legal person, group of persons or organ of a territorial corporate body [German: Gebietskörperschaft] or the offices of these organs, if they decide alone or jointly with others to use data (subpara. 8), without regard whether they use the data themselves (sub-para. 8) or have it done by a service provider (sub-para. 5). They are also deemed to be controllers when the service provider instructed to carry out an order (sub-para. 5) decides to use data for this purpose (sub-para. 8) except if this was expressly prohibited or if the contractor has to decide under his own responsibility, on the basis of rules of law or codes of conduct".

[4]Data processor: "natural or legal person, group of persons or organ of a federal, state and local authority [German: Gebietskörperschaft] or the offices of these organs, if they use data only for a commissioned work".

regarded a regular activity, if one usually would expect a repetition of that activity or the activity takes more time" (Sect. 1.4 Industrial Code – IC [22]).

The national term of healthcare provider differs significantly from the Patients' Rights Directive's (PRD) [12] definition of healthcare provider[5] according to Art. 3.g PRD [12]. The more narrow PRD-term refers only to entities, that factually provide healthcare[6] (Art. 3.a PRD [12]), whereas the Austrian term refers to all entities, that use personal health data. This should be kept in mind, when applying the legal e-health framework in Austria. Medical scientists – for example – dealing with personal health data would qualify as healthcare providers according to Austrian law and would therefore be subject to the national health telematics law. However, they would never qualify as healthcare providers according to the Patients' Rights Directive [12].

1.3.2 Material Scope of the HTA: personal health data

The HTA [2] applies to the communication of **personal health data**, which is according to Sect. 4.1 DPA 2000 [1] defined as personal data about the physical and mental condition of a person, the condition and function of his/her body or parts of it, including data collected during anamnesis, for purposes of preventive medicine or medical treatment, care, settlement of healthcare services or insuring health risks, including but not limited to information:

- about health relevant lifestyle or environmental influences,
- about prescribed or applied medication,
- about methods of diagnosis, treatment or care or
- necessary for the billing of healthcare services.

If such data is communicated by healthcare providers the rules of the HTA [2] apply. Mere processing without communicating data does not entail applicability of the HTA [2] (Part 2 of the HTA [2]). The definition of health data has been heavily criticised during the parliamentary process by privacy institutions [23, 24, 25] but not regarded unconstitutional. So did, however, the Austrian Medical Association years later (sic!) during the preparation of an Austrian EHR law in April 2012 [26]. Allegedly the definition of personal health data is according to the AMA not accurate enough [26]. The AMA is convinced, that the definition does not conform to relevant judgments of the Austrian Constitutional Court on accuracy of legal terms. According to these judgements the terms "severe breach of duty" [27], "excellent job performance" [28], "important service interests" [29] or the "economically justified price" [30] are sufficiently determined. Contrary "usually" for example has not been found sufficiently determined [31]. In these premises, the allegation of the AMA appears unsupported.

1.3.3 Special Laws on Data Security

Part 2 of the HTA [2] specifies concrete data security measures, which prevail over the more general data security measures laid down in Sect. 14 DPA 2000 [1]. In contrast to the DPA 2000 [1] the HTA's [2] data protection provisions are limited to data security. Other aspects of data protection, as for example the legitimacy of data usage, are not governed by the HTA [2]. Even more detailed provisions than the provisions of the HTA [2] on data security are laid down in the Health Telematics Ordinance [32], that itself is based upon the HTA [2]. The HTO's [32] special data protection rules concern:

- proof of identity and role as precondition for communication of electronic personal health data (Sect. 3 HTA [2] and Sect. 1 HTO [32]),
- verification and proof of the involved healthcare providers' identities and roles (Sect. 4 and 5 HTA [2], Sect. 1 and 2 HTO [32] and Annex 1 HTO [32]),
- protection of confidentiality and integrity of the communicated health data (Sect. 6 and 7 HTA [2], Sect. 3 and 4 HTO [32] and annex 2 HTO [32]),
- documentation of the applied data security measures (Sect. 8 HTA [2] and Sect. 5 HTO [32]),
- administrative penalties of up to EUR 5.000 EUR[7] to ensure compliance with the HTA's [2] data security requirements (Sect. 17 HTA [2]) and
- transitional provisions to balance the interests of data and investment protection (Sect. 19 HTA [2]).

1.3.4 Verification and Proof of Identity

The identity of healthcare providers has to be proven primarily (Sect. 4.1 HTA [2]) by means of certificates[8] (Sect. 2.8 Electronic Signature Act [33]) and identity data. These identity data must be collected in a way compliant to the Austrian E-Government Act (EGovA) [3], i.e. by means of the citizen card (Sect. 2.10 and Sect. 4 et sqq. EGovA [3]) and/or the e-government registers (Sect. 6.2 and 6.3 EGovA [3]). Subsidiary proof of identity may also be carried out:

[5] Healthcare provider: "any natural or legal person or any other entity legally providing healthcare on the territory of a Member State".

[6] Healthcare: "health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices".

[7] The abusive use of the e-health directory's data is fined up to 50.000 EUR.

[8] Certificate: "an electronic confirmation, that assigns signature-verification data [German: Signaturprüfdaten] to a particular person and confirms her identity".

- via access of the e-health directory (Sect. 4.2 HTA [2]),
- by means of server certificates (Sect. 4.3 HTA [2]),
- via login details, if the use of certificates or the e-health directory appears inappropriate from either the technical or the economical point of view (Sect. 4.4 HTA [2]),
- in form of personal or phone contact, contractual agreement or via electronic professional registers access, if proof of identity according to Sect. 4 HTA [2] is unreasonable due to inappropriate technical expenditure (Sect. 19.1 HTA [2]) or
- in any other form, provided that
- confidentiality of data transfer is assured,
- the link between identity data of the healthcare providers and transferred health data cannot be changed without a trace and
- confusion between the involved healthcare providers can be ruled out (Sect. 1.2 HTO [32]).

1.3.5 Verification and Proof of Roles

Basically the same rules apply to verification and proof of roles: primarily they have to be proven by means of certificates (Sect. 5.2 HTA [2]). Healthcare providers choose their roles out of the 46 roles[9], defined in the HTO [32] and have them confirmed by so called registration bodies, which are according to Sect. 2.2 HTO [32] the Austrian Medical Association, the Austrian Dental Association, the Austrian Chamber of Pharmacists, the Austrian Midwives Committee as well as the Federation of the Austrian Social Security Institutions (Hauptverband der österreichischen Sozialversicherungsträger) and the Austrian Federal Minister for Health. Evidence that the correct roles are used may be given:

- via access of the e-health directory (Sect. 5.3 HTA [2] or Sect. 2.5 HTO [32]),
- via login details (Sect. 5.5 HTA [2]) or
- in the form of personal or phone contact, contractual agreement or via electronic professional registers access, if proof of roles according to Sect. 5 HTA [2] is unreasonable due to inappropriate technical overhead (Sect. 19.1 HTA [2]).

In case of automated exchange of data, evidence must be given basically only prior to the first use of health data (Sect. 5.4 HTA [2]). Roles other than those provided for in Annex 1 HTO [32] must not be used (Sect. 1.1 HTO [32]).

1.3.6 Confidentiality: Legitimacy of Fax and E-Mail

The confidentiality of communicated personal health data has to be ensured by means of encryption. The procedures and algorithms applied must resist attacks, that can be performed with economically acceptable effort (Sect. 6.1 HTA [2]). According to Annex 2 of the HTO [32] the procedures and algorithms laid down in the Electronic Signature Ordinance [34] as well as the symmetric encryption algorithms AES[10] and TripleDES[11] may be used for ehealth purposes. For performance reasons the obligation to encrypt the data is limited to identifiers or any other information, allowing to track down the data subject, as well as any login details (Sect. 3.2 HTO [32]).

Unencrypted mailing of personal health related data is forbidden by law[12]. Faxing is nonetheless permitted according to Sect. 19.3 HTA [2], provided that:

- the fax is access-restricted,
- the phone numbers are verifiably kept up-to-date,
- automatic forwarding and remote maintenance functions are deactivated and
- the device's security features are activated.

Until December 31st 2015 the requirements of the HTA [2] regarding confidentiality do not apply to wireless communication of rescue services (Sect. 19.7 HTA [2]). This exemption is the last and now only transitional provision with a fixed deadline. This is owed to the fact, that former transitional provisions regarding the technical pre-requisites needed continuous amendment[13], because technical development and dissemination of innovations

[9] These roles comprise: all kinds of medical doctors (Annex [Anx] 1.1 to 1.5 HTO [32]), all kinds of therapists (Anx. 1.6 to 1.9 and 1.11 HTO [32]), midwives (Anx. 1.10 HTO [32]), nursing staff (Anx. 1.18 to 1.20 HTO [32]), various legal entities, as for example hospitals, penal institutions (Anx. 1.24 HTO [32]), pharmacies (Anx. 1.26 HTO [32]), tissue banks (Anx. 1.27 HTO [32]), patient transport (Anx. 1.36 HTO [32]), health administration (Anx. 1.44 HTO [32]), patient advocacy (Anx. 1.45 HTO [32]) and – due to the wide definition of the term "healthcare provider" according to Sect. 2.2 HTA [2] – a general role called "health service provider" (Anx. 1.46 HTO [32]).

[10] Advanced Encryption Standard (AES) is an encryption procedure published in 2000.

[11] Data Encryption Standard (DES) is an encryption procedure officially confirmed by the US government in 1976 and the predecessor of AES.

[12] The prohibition of unencrypted mailing can be drawn from Sect. 19.1 HTA [2], that is a transitional provision for all data security requirements except confidentiality according to Sect. 6 HTA [2]. Sect. 19.3 HTA [2] again limits the strict confidentiality requirement of Sect. 6 HTA [2] only with regard to faxing, but not with regard to mailing. Hence no exemption from confidentiality is stipulated, that would allow unencrypted mailing.

[13] All amendments to the HTA [2], from 2008 to 2010 [35], have been driven by the idea to extend the fixed deadlines of the transitional provisions. The underlying problem is still hard to resolve, because the conflicting interests of data protection on the one hand and cost awareness of the healthcare providers ("investment protection") on the other hand need to be balanced. Based on risk assessment the last amendment [36] introduced a completely revised version of transitional provisions.

were not and still are not predictable. For this reason a "smooth" deadline, depending on the factual deployment of privacy enhancing technologies has been introduced in 2010 (Sect. 19.5 HTA [2]). As a result the Federal Minister of Health may terminate the transitional phase by means of ministerial ordinance, if the data security requirements can be met by commonly available and affordable technology, after having heard the relevant stakeholders[14].

1.3.7 The E Health Directory: a Register of Healthcare Providers

The e-health directory is a register of healthcare providers to promote the electronic exchange of health data, to increase information on healthcare services and to improve policy making in the field of e-health (Sect. 9.1 HTA [2]). Healthcare providers exercising their profession in Austria – including of course foreign healthcare providers – can be registered regardless of their citizenship. Registration is free of costs, voluntary (Sect. 11.1 HTA [2]) and accomplished by registration bodies (Sect. 13 HTA [2]). For the purposes of the e-health directory the following data are collected and processed (Sect. 10.1 HTA [2]):

- name and unique identification according to Sect. 8 EGovA [3] of the healthcare provider,
- contact details (postal and electronic),
- Object Identifier (OID) according to ISO[15]/IEC[16] 9834 respectively DIN[17] 66334,
- role(s) of the healthcare provider,
- information on geographic localisation of the healthcare provider,
- uniform resource locator (URL) of the public key[18] for encryption of health data,
- name of the registration body,
- date of registration and latest amendment to registration as well as name of the performing registration body.

The data of the e-health directory must not be published, but may only be used by the healthcare providers concerned, the registration bodies and government bodies competent in public health (Sect. 9.3 HTA [2]).

1.3.8 E-Health Information Governance

The HTA's [2] provisions on e-health related information governance were introduced in 2004, with unfortunately remaining some of them without considerable practical impact up to now. One of these provisions deals with the reporting system on health telematics (Sect. 14 HTA [2]), that would in fact cover very interesting information on:

- the availability of technical infrastructure for health telematics,
- the nature and scope of applications and procedures employed in the field of health telematics,
- the type and amount of personal health data, that has been electronically communicated as well as
- the general economic conditions of health telematics.

For the purpose of this monitoring, data of the e-health directory may be used (Sect. 14.2 HTA [2]).

Furthermore, the Federal Minister of Health is entitled to issue guidelines regarding the quality of health-related online information [37]. These guidelines shall include provisions on complaints management and be published – together with the results of the complaints management – in the Information Centre (Sect. 16 HTA [2]), which is online at [38]. Main objective of this publicly available Information Centre is to raise awareness in the field of health telematics, e.g. by informing about new procedures and methods of health telematics ("best practices") or national or international standards as for example ICD-10[19].

1.4 Austrian E-Government Law: Data Protection Compliant Identification

Main goal of the Austrian E-Government Act (EGovA) [3] is to provide a data protection compliant and accurate way of identification of entities[20] by means of personal identifiers.

Accurate identification creates trust and is therefore an essential pre-requisite for electronic communication of delicate personal data, as for example health data or legal relevant information. Unambiguous identification of both patients and healthcare providers is necessary to ensure quality of e-health services: health information assigned to the right patients prevents maltreatment, whereas correct identification of healthcare providers allows traceabi-

[14] E.g.: Austrian Medical Association, representatives of hospital operators or advocates for patients.

[15] International Organisation for Standardisation.

[16] International Electrotechnical Commission.

[17] German Institute for Standardisation (Deutsches Institut für Normung).

[18] Public keys are used in asymmetric encryption, the function of which is based upon two different keys: one for encryption and one for decryption. If information shall be hid the encryption is done with the public key, published by the potential recipient of encrypted data. If information shall be electronically signed the encryption is done with the private key. The public key is usually published in the certificate of the signatory and can be used by any recipient to decrypt the transmitted information. Thereby the recipient verifies that it could have been only the holder of the private key, who encrypted the information.

[19] ICD-10 (International Classification of Diseases version 10) is an international standard issued by the World Health Organisation (WHO) "for all general epidemiological, many health management purposes and clinical use" [39].

[20] Entities according to EGovA [3] include natural and legal persons, as well as other entities.

lity and quality control, especially relevant in cases of law suits.

Nonetheless, personal identifiers are often regarded as harmful[21], as they can be used for profiling of people. To overcome this problem the accurateness of a unique identifier is combined with a structure representing the different fields of activity. Public services are divided into at least 35 sectors and private services into sectors for each data controller.

This separation guarantees that activities of one data subject cannot be traced over different sectors, because the different unique identifiers of one and the same person can – due to encryption – not be derived from each other. The central register of residents number – CRRN (Zentrale Melderegister-Zahl) serves as the before mentioned unique identifier. It is strongly[22] encrypted to generate the so called sourcePIN (Stammzahl) according to Sect. 2.8 EGovA [3].

Then this sourcePIN is concatenated with individual tokens for each sector and the resulting term is hashed with a one-way hash algorithm[23] to calculate the sector specific personal identifier – ssPIN (bereichsspezifisches Personenkennzeichen) according to Sect. 9 EGovA [3]. The use of such one-way functions assures that ssPINs can only be derived from the sourcePIN of a data subject but not from other ssPINs of the data subject. As the sourcePIN is the only means to calculate ssPINs, the usage of the sourcePIN is subject to strict limitations. sourcePINs must not be used directly for identification purposes (Sect. 12 EGovA [3]) or stored outside the data subjects' citizen cards.

Solely the ssPINs may lawfully be kept by data controllers. The citizen card does not need to be a smart card in the common understanding, but can be any technical device, as for example a mobile phone. The only pre-condition is that the device provides an electronic signature function and allows the storage of an identification data set (identity link) that is electronically signed by the sourcePIN Register Authority[24].

National personal identifiers, that are at the same time accurate and data protection compliant, will be extremely important for patients, as such identifiers allow patients to manage their health data online, for example via a national health portal. Entities without residence in Austria can also participate in the Austrian identity management by applying for registration in the supplementary register [44]. Even powers of attorney can be managed [45].

1.5 Doctors' Code 1998: the Medical Secrecy

Fundamental provisions, whether data may be used or not, are laid down in the Doctors Code 1998 (DC 1998) [4], in particular Sect. 51.2 DC 1998 [4]. According to this provision medical doctors may process personal health data necessary for the patients' treatment and communicate this data to other healthcare providers, if patients have agreed to such, or social security institutions.

Secret information that has been revealed to medical doctors in the course of their professional activities must not be communicated ("medical secrecy[25]"), except for the following:

1. other laws require the communication of health data (Sect. 54.2.1 DC 1998 [4]),
2. communication of health data is necessary for sickness insurance institutions to perform their duties (Sect. 54.2.2 DC 1998 [4]),
3. the data subject gave consent (Sect. 54.2.3 DC 1998 [4]),
4. communication is necessary to protect prevailing public interests regarding public health or jurisdiction (Sect. 54.2.4 DC 1998 [4]),
5. communication is necessary for settlement of medical costs and costs for drugs or medical aids (Sect. 54.3 DC 1998 [4]) or
6. in cases of serious crimes, e.g.: sexual abuse, maltreatment or neglect of minors or incapacitated persons or bodily harm leading to serious injury or death (Sect. 54.4 to 54.6 DC 1998 [4]).

A similar provision for dentists is Sect. 21 Dentists' Code [46], which differs from the general medical secrecy of Sect. 54 DC 1998 [4] in particular in the absence of legitimating communication in cases of serious crime. Both secrecies also protect third persons [47] – e.g. information about the spouse's mental illness – and do not presume a valid treatment contract [47], but are directly effective due to the cited law provisions.

[21] According to Art. 8.7 DPD [11] "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed".

[22] The strong encryption is required by law (Sect. 6.2 EGovA [3]) and currently achieved using Triple DES [40] in CBC (Cipher Block Chaining) mode [41, 42].

[23] A one-way hash algorithm allows to compute a digital fingerprint (hash-value) that represents the original data. This hash-value is usually a fixed-digit number, that changes after re-calculation, if the original data has been altered. Whereas the hash-value can always be calculated if the original data is known, the inversion, i.e. the calculation of the original data from the hash value, does not work.

Hashing can be used to generate checksums for data. An example for a one-way hash function is the MD5 algorithm, that creates 128 bit hash values.

[24] According to Sect. 7 EGovA [3] the Austrian Data Protection Agency acts as the sourcePIN Register Authority [43].

[25] The term "secrecy" in the Austrian legal language refers to the duty of persons to not actively communicate data, whereas "confidentiality" refers to the obligation to prevent even passive, i.e. accidental, communication or loss of data, e.g. by using encryption techniques and checksums.

1.6 General Social Insurance Law

1.6.1 The Electronic Management System ELSY

In 1999 an amendment to Sect. 31a [48] of the Austrian General Social Insurance Law (GSIL) [5] introduced the electronic management system "ELSY", to support the administrative processes among insurance holders, employers, contractual partners and insurance carriers. Part of the ELSY are the e-cards for patients, the a-cards for pharmacists and the o-cards for physicians. All these cards are key cards, meaning that by default no data except for identification and authentication purposes are stored on these cards. Additionally the citizen card can be used as e-card (Sect. 31a.2 GSIL [5]). Till December 31st 2010 all cards should have been access protected by use of passwords or biometrics, which did not happen till now [49]. As a result issues of liability could be raised in cases of loss and misuse of e-cards.

The patients' health card, called e-card, is an electronic health insurance certificate and replaces the former paper version. Thereby red tape is cut, as a defined goal of ELSY (Sect. 31a.1 GSIL [5]). According to Sect. 31a.3 GSIL [5] the e-card may exclusively hold the following data:

1. name, date of birth and sex of the card holder,
2. insurance number,
3. card number, date of issuance and name of card issuer as well as
4. any other data, that shall be stored on the e-card by law.

Patients may also have their emergency data[26] written on their e-cards (Sect. 31a.5 GSIL [5]). Strict rules on the usage of data guarantee a high level of data protection, e.g.: the ban to link patients' claims to the fact whether patients agreed upon the use of their e-cards or not (Sect. 31a.4a GSIL [5]) or the restriction of purposes, for which ELSY may be used (Sect. 31a.4 GSIL [5]). As an additional safeguard, the misuse of emergency data stored on e-cards is fined up to 18 890 EUR.

1.6.2 The Obligation to Cooperate in ELGA Affairs

Sect. 31d GSIL [5] obliges the Federation of the Austrian Social Security Institutions (FASSI – Hauptverband der österreichischen Sozialversicherungsträger) to engage in the conception and implementation of a national EHR, called ELGA. The FASSI is one of the three shareholders of the "ELGA-GmbH", which shall introduce and implement ELGA. The other two shareholders are the federal government and all state governments together. The division into three shareholders is owed to the constitutional law fact, that the distribution of competences among the federal and states governments is not absolutely clear. The main competence "health affairs" resides with the federal level. However, it is to a large extent restricted by the state governments competences regarding infrastructure and operation of hospitals. Due to this lack of clarity the federal and state level need to closely co-operate.

1.6.3 Electronic Exchange of Data

Data between hospitals and insurance carriers must be exchanged electronically (Sect. 148.6 GSIL [5]) as well as the settlement of accounts needs to be done by electronic means of communication (Sect. 340a, 342a, 348g and 349a GSIL [5]). The social insurance number (SIN) may be used as personal identifier for purposes of social and unemployment insurance (Sect. 460d GSIL [5]).

In case that personal details, e.g.: SIN, name, birth date, sex or citizenship, need to be changed or updated, these changes have to be communicated to the matching table[27] of the Federal Minister of the Interior (Sect. 460d GSIL [5]).

Although this matching table does not hold health related information, it is an important pre-requisite to calculate the ssPINs for the health sector, as it eases the transformation from SINs to CRRNs, which are the mathematical base for calculating the ssPINs. For statistical purposes the Federal Minister of the Interior is legitimated to match the CRRNs against the SINs by comparing sets of personal data from the central register of residents and the FASSI's central partner database (Zentrale Partnerverwaltung).

1.7 Insurance Agreement Act: Usage of Insurance Data

The Austrian Insurance Agreement Act (IAA) [6] provides a framework for e.g. conclusion, rights and duties, pre-requisites of validity and termination of insurance agreements or the profession of insurance brokers. Addressees of the IAA [6] are insurers under private law. Public insurers as for example the Regional Health Insurance Fund of Vienna (Wiener Gebietskrankenkasse) are not subject to the IAA [6] but to the GSIL [5]. According to the HTA's [2] definition of healthcare providers (Sect.

[26] Unfortunately there is no explicit definition of the term emergency data, which was introduced by the 59th amendment [50] to the GSIL [5], although Sect. 31a.5 GSIL [5] empowers the Federal Minister for Social Security and Generations (now: Federal Minister for Labour, Social Affairs and Consumer Protection) to specify by ministerial ordinance the use of emergency data in more detail. The only hint, what can be referred to by "emergency data", gives Sect. 31a.5 GSIL [5] itself, by referring to the data "being of vital interest for the data subject in case of medical emergency". This does not specify the data types as for example, blood group, drug intolerances or status of vaccination, but remains on a very abstract and thus open level, which could be necessary for example for people with rare diseases. For them specific emergency data could insofar be relevant as the knowledge of these data could have decisive influence on the ongoing treatment.

[27] The legal foundation of the so called matching table (Gleichsetzungstabelle) is laid down in Sect. 16b of the Registration Act 1991 [51].

2.2 HTA [2]), insurers are regarded healthcare providers, and hence subject to the special data protection requirements set forth in the HTA [2].

Sect. 11a IAA [6] is the most relevant IAA-provision with regard to e-health. It determines how health data may be used by insurers. The only valid purposes for which insurers may use personal health data are:

1. assessment whether and subject to which conditions insurance agreements are entered into or amended (Sect. 11a.1.1 IAA [6]),
2. administration of valid insurance agreements (Sect. 11a.1.2 IAA [6]) and
3. assessment and settlement of claims arising from insurance agreements (Sect. 11a.1.3 IAA [6]).

All methods of data collection are limited to methods, that involve the data subjects and take into account their will (Sect. 11a.2.1 to 11a.2.4 IAA [6]) or concern otherwise lawfully collected data, provided that the data subjects are informed about this way of collection (Sect. 11a.2.5 IAA [6]). As a consequence, any collection of personal health data by insurers requires in some way or another the data subjects' involvement.

Health data may only be kept as long as necessary (Sect. 11a.5 IAA [6]) with the statutory limitation period as an upper limit. The general civil law limitation periods of three respectively thirty years, are altered by Sect. 12.1 IAA [6] to three years after termination of the agreement, at the latest ten years, if third-parties are beneficiaries and not aware of their contractual entitlements.

1.8 Genetic Engineering Act: Usage of Personal Genetic Data

Another relevant provision regarding the usage of personal health data is Sect. 67 of the Genetic Engineering Act (GEA) [7]. It absolutely bans the usage of personal data related to human genetic data by employers and insurers. The provision reads as follows:

„Ban on enquiry and use of genetic analyses' results for particular purposes

§67. Employers and insurers including their appointees and employees must not enquire, require, receive or otherwise use the results of genetic analyses relating to their employees, job-seekers, insurance holders or prospective insurance holders. According to this ban it is also prohibited by law to ask for or accept body substances for purposes of genetic analyses."

All other persons, not mentioned in Sect. 67 GEA [7], may – subject to the provisions of the DPA 2000 [1], HTA [2], HTO [32] and EGovA [3] – use genetic data, also in electronic form.

2 Outlook

In the next few years Austria is facing some fundamental improvements to its e-health sector. Some innovations are nationally inspired, as for example the national EHR, called ELGA (Elektronische Gesundheitsakte), while others, as for example the European Patients Smart Open Services (epSOS) [52] large scale pilot or the voluntary networks according to Art. 14 PRD [12], are European initiatives.

2.1 Expected National Innovations: ELGA and Telemedicine

Since several years an amendment to the HTA [2] has been under discussion. The new provisions shall introduce a legal framework for ELGA. This will be the most important step ever taken regarding Austrian e-health legislation.

2.1.1 ELGA in a Nutshell

ELGA is designed as an IT-infrastructure, that is made up of centralised and decentralised components (figure 1). The centralised components will be the Master Patient Index, the ELGA Healthcare Provider (HCP) Index, the Access Control Centre (ACC – Berechtigungssystem), the logging system and the internet portal. The decentralised components are the document registries and the document repositories. Both **indexes** shall guarantee valid identification of ELGA participants[28] and ELGA healthcare providers. One of their features will be to convert internal identifiers, e.g. of a local hospital in Vienna, into nation-wide valid ssPINs, as provided by the EGovA [3]. The **Access Control Centre** enables the ELGA participants to define individual rules, which data can be accessed by which ELGA healthcare providers. Functionality of the Access Control Centre is provided to the ELGA participants either online, by means of the ELGA portal, or offline via the ELGA ombudsmen. The **logging system** logs every single processing step of data usage in the context of ELGA, as for example access of the indexes, registries or repositories. The **document registries** are collections of links to the actual health data, which is stored in **document repositories**. The reasons and advantages of this decentralised approach are explained below in chapter 2.1.3.

If a request is sent to the ELGA system, the IDs of the ELGA participant and the ELGA healthcare provider are checked against the indexes. According to the rules stored in the Access Control Centre the request is either forwarded to the document registries or not. The registries determine which of them holds the necessary information

[28] As patients are not obliged to participate in ELGA, the ones, who did not opt out are called ELGA participants to distinguish them from other patients, that opted out of ELGA.

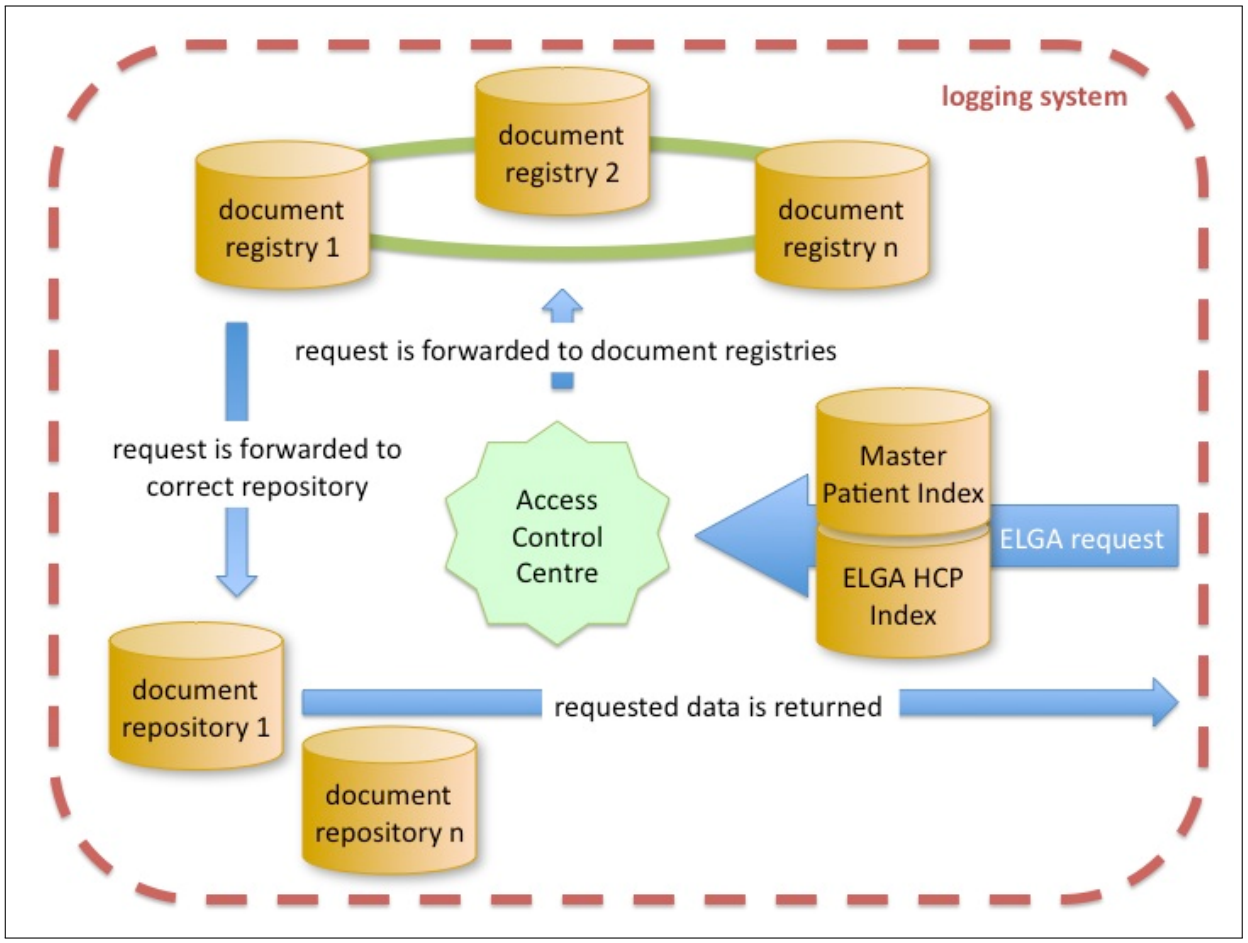

Figure 1: Fundamental structure of ELGA.

and then forwards the request accordingly to the right document repository, from where the requested data is retrieved and returned.

The document registries are linked databases of links. As already mentioned, they do not hold any health data, but only technical information about the documents, as for example addresses and IDs of the document repositories, where the health data are saved, keywords, IDs of ELGA healthcare providers, IDs of ELGA participants or versioning information. The decentralised approach reduces vulnerability of ELGA, as the data of ELGA participants is not stored at one central place, but at many different places.

2.1.2 Main Principles of ELGA

ELGA is based upon the following principles:

1. the legitimate usage of ELGA is exclusively granted to the ELGA participants and their representatives, ELGA ombudsmen and **ELGA healthcare providers**, i.e. medical doctors and supporting medical staff, if and as far as these persons do not act on behalf of national, regional or local governments in their sovereign capacity (Hoheitsgewalt);
2. usage of health data is strictly limited to purposes of medical treatment or exercise of the ELGA participants' rights;
3. patients may opt-out of their participation in ELGA at any time;
4. patients may declare to participate just in particular ELGA applications, as for example the e-medication services;
5. patients may declare that their data is not to be included within ELGA ("right to object") at any time and
6. patients keep clear control over their data via the Access Control Centre.

It is important to note that not all healthcare providers according to Sect. 2.2 HTA [2], will be addressees of the ELGA provisions. Only a little subset of them, the so called ELGA healthcare providers, will be subject to ELGA regulations. By doing so healthcare providers, that are no ELGA healthcare providers are excluded by law from using ELGA. Conversely all ELGA healthcare providers are "normal" healthcare providers, which means that they have to adhere to the data security requirements of Part 2 HTA [2].

2.1.3 The Net-Based Concept of ELGA: Protecting Data and Investments

Hospital information systems are de facto standard in Austria. Additionally, some hospital co-operations use shared data pools, as for example the Viennese Hospital Association. To put it another way: major investments in shared IT-infrastructure have already been made and these expenditures should not be frustrated by new laws. The expected costs have been the main reason for the lengthy discussion on the data security provisions of the HTA, which finally resulted in the transitional provision of Sect. 19 HTA [2]. One outcome of this discussion was the decision that faxing should be a legally accepted way of communicating personal health data, as explained above in chapter 1.3.5.

To not give rise to such discussions again, it was considered to set up ELGA upon existing infrastructure and introduce a flexible system, that is based upon decentralised document registries and document repositories. This approach facilitates the re-use of existing registers. Another benefit of this solution is, that a longstanding calling of data privacy activists for decentralised storage of personal health data, is satisfied [13].

2.1.4 Participation in ELGA: Opt-In, Opt-Out or Mandatory Participation

One of the main legal issues in the Austrian discussion on national EHR systems has been the question whether participation in ELGA should be mandatory or not. As already mentioned above in chapter 1.1, the fundamental right to privacy is constitutional law and may according to Sect. 1.2 DPA 2000 [1] only be restricted, in case of:

1. vital interests or
2. consent given by the data subject or
3. overriding legitimate interests of others.

At least one of these three requirements has to be met by a future EHR law, because otherwise its provisions could easily be suspended[29] by the Austrian Constitutional Court due to non-conformity to the fundamental right to privacy. Due to the higher rank of constitutional law an ordinary statutory law based upon "overriding legitimate interests of others" cannot rule out "vital interests" or "data subject's consent" [53] as legal base for the usage of personal data. That means, that the consent of the data subject may also legitimate usage of data, which is not regulated by the future "normal ranked" EHR law.

Participation can either be stipulated in form of an opt-in, opt-out or mandatory participation. The first two approaches would take the will of the data subject, i.e. the patient, into account, whereas a mandatory approach would oblige all patients to be ELGA participants, regardless of their intention to participate or not[30].

According to the Data Protection Directive a national ELGA law could basically be based upon:

- explicit consent[31],
- necessity for healthcare purposes (Art. 8.3 DPD [11]) or
- substantial public interests (Art. 8.4 DPD [11]).

The potential legal bases for a national ELGA law are illustrated in figure 2, both on EU and Austrian constitutional law level. To be compliant with EU law each legal base for processing data according to Art. 8 DPD [11], must be covered by a correspondent legal base of the Austrian fundamental right to privacy. Otherwise the fundamental right to privacy would breach Art. 8 DPD [11]. Figure 2 shows how the legal bases for data processing correlate on European and national level and that for example the usage of data for healthcare purposes allowed at European level by Art. 8.3 DPD [11], must be a legitimate overriding interest at national level according to Sect. 1.2 3rd case DPA 2000 [1].

The Art. 29 Data Protection Working Party believes that "opt-out solutions will not meet the requirement of being 'explicit'" [17], so only the necessity for healthcare purposes (Art. 8.3 DPD [11]) or substantial public interests (Art. 8.4 DPD [11]) could justify opt-out solutions. Concerning the usage of data for healthcare purposes, the Art. 29 Data Protection Working Party is not convinced that Art. 8.3 DPD [11] can serve as sole legal basis for a national EHR law [17]. This seems a bit too strict and unfounded, as especially the e-medication tools of EHRs can increase drug security remarkably [55] and thus save

[29] Judicial review (Normenkontrolle) is one of the most important tasks of the Austrian Constitutional Court. That means, that the court may repeal any law or ordinance, that contradicts or interferes with higher ranking law.

[30] Mayer [18] criticises that an opt-out approach cannot replace the requirement for the data subjects' consent, because data is already processed before the data subjects, i.e. the patients, have the possibility to decide, whether they opt out or not. This is definitely not true for the current draft of the ELGA law, as the transitional provisions require that ELGA participants are entitled to opt out from summer 2013 onwards, whereas ELGA is intended to start in January 2015. So ELGA participants have one and half year of time to declare, that they are not willing to participate in ELGA, without having any personal health data about them processed in ELGA during this time. Even after the 1st of January 2015 patients can effectively avoid to have their personal health data included in ELGA, by opting out before their first healthcare encounter or even later by exercising their right to object during the healthcare encounter and opting out afterwards. Also Frohner [54] acknowledges the opt-out approach, as suggested by the EHR law draft, as an appropriate safeguard according to Art. 8.4 DPD [11].

[31] Art. 8.2.a DPD [11] reads as follows: "Paragraph 1 [ann: which generally prohibits the use of 'sensitive data'] shall not apply where: (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent".

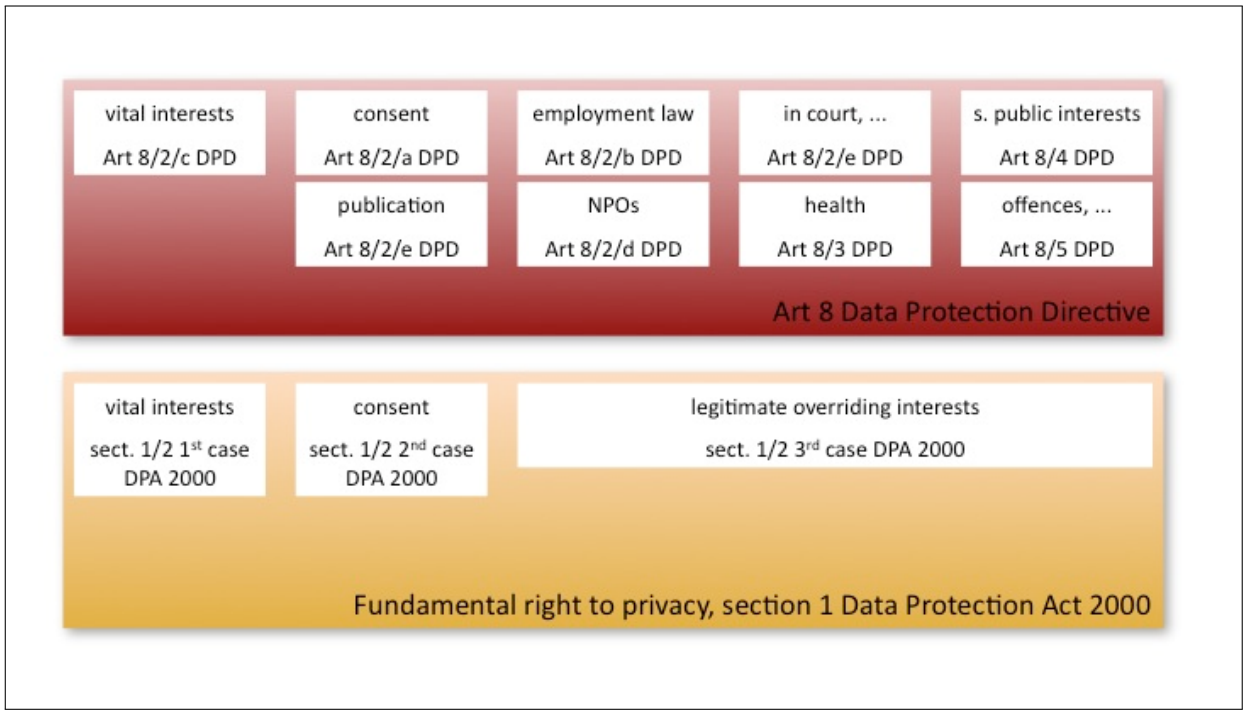

Figure 2: Legal bases for data processing at European and national level.

human lives[32]. These facts indicate medical necessity in the meaning of Art. 8.3 DPD [11], and substantial public interests in the meaning of Art. 8.4 DPD [11], even more when referring to the rulings of the Austrian Constitutional Court, that acknowledged the interest to guarantee financial viability of public health as a substantial public interest [60].

2.1.5 Securing the Patients' Freedom of Choice: the Access Control Centre

Patients' freedom of choice, whether to join an EHR or not, is one of the strongest arguments [13, 61] against ELGA in Austria. Having that in mind a system has been developed that allows full control of the patients over their health data. Compared to the currently used paper documents, an electronic system eases traceability of single steps of data usage and improves transparency for the patients.

At present state the Access Control Centre is designed to store and manage two levels of access rights:

- the abstract access rights, explicitly laid down in the ELGA law and
- the individual access rights, defined individually by each ELGA participant.

The **abstract access rights** make up a binding framework of general entitlements, that must not be extended by the individual access rights. Healthcare providers that are not entitled to use data according the abstract access rights, can also not be authorised by means of individual access rights. Task of the abstract access rights is only to provide standard settings for an optimal balance between data protection, usability and quality of healthcare. Medical doctors and medical staff of hospitals for example are basically entitled to access all personal health data, whereas pharmacists are limited to the medication relevant subset of health data. The abstract access rights can only be limited by the individual access rights, but not extended.

At the level of the **individual access rights** the ELGA participants may further restrict the abstract access rights of their ELGA healthcare providers. Additionally ELGA participants can define for how long their authentication, which can for example be done via e-card, will remain valid. During this period, which is by default 28 days, ELGA healthcare providers do not need to re-authenticate their "ELGA patients" for accessing their ELGA data.

This shall ease usability of ELGA, because the validity period can be extended beyond the 28 days of the standard rule, which benefits ELGA participants, that are hospi-

[32] A meta analysis of 39 US studies on hospitalised patients revealed, that fatal adverse drug reactions (ADRs) account for 0.32 percent of deaths among hospitalised patients [56]. According to a Swedish study of 2001 based upon 1574 study subjects, fatal ADRs cause approximately 3 percent of all fatalities [57]. Even though the percentage of fatal ADRs differs significantly, fatal ADRs gain increasing importance as the Adverse Events Reporting System (AERS) of the U.S. Food and Drug Administration persuasively demonstrates. According to the AERS the number of fatal ADRs increased by a factor 4 between 2000 and 2010 [58]. 9 percent of the ADR deaths are assumed to be preventable in any case, with only 28 percent assessed to be unavoidable [59].

talised for a longer period of time. Aim of the individual access rights is to strengthen the ELGA participants' autonomy and serve as an appropriate safeguard according to Art. 8.4 DPD [11].

2.1.6 Telemedicine

For the purpose of this article, "telemedicine" should be understood as the provision of healthcare services by means of information and communication technologies (ICT) without simultaneous presence of the persons involved. Apart from Sect. 49.2 DC 1998 [4] there are no explicit rules in Austrian legislation on telemedicine.

The above cited Sect. 49.2 DC 1998 [4] reads as follows:

"Treatment of patients and care for healthy people

(1) [...]

(2) The medical doctor has to exercise his/her profession directly and in person and, if necessary, in co-operation with other medical doctors. He may draw upon auxiliary staff, provided that these persons act upon his exact instructions and under his constant supervision."

On the one hand the requirement to "exercise his profession directly and in person" could be interpreted to rule out telemedicine. On the other hand the authorisation to co-operate with other medical doctors, relaxes this apparent restriction substantially. Actually this is the crucial statement: the co-operation of medical doctors is legally allowed, thus also allowing for online consultation or other forms of ICT based co-operation of medical doctors, provided that at least one physician providers his services in person.

The transmission of data necessary for telemedical treatment is also subject to the HTA [2] as any other transmission of personal health data as for example the communication of x-ray images.

2.2 Expected European Innovations: epSOS

The European large scale pilot epSOS[33] "attempts to offer seamless healthcare to European citizens. Key goals are to improve the quality and safety of healthcare for citizens when travelling to another European country. Moreover, it concentrates on developing a practical eHealth framework and ICT infrastructure that enables secure access to patient health information among different European healthcare systems" [62]. Legal key strategy of epSOS is the so called "circle of trust" or "web of trust" constituted by the National Contact Points (NCPs), which act as gateways and confirm identity, qualification and authorisation of healthcare providers involved as well as compliance with national and international standards on data protection and data security.

2.2.1 The "Opt-In Problem" of epSOS

Since the project was started in July 2008 intense discussions on the **legal bases of data processing** have been held. Currently two approaches are conceivable: either the patients' consent ("opt-in" according to Art. 8.2.a DPD [11]) or processing of personal data for healthcare purposes (Art. 8.3 DPD [11]). As "never touch existing legislation"[34] has always been one of epSOS' guiding principles, the opt-in approach was chosen. Though this is basically comprehensible from the legal point of view, the practical downsides are a logical consequence: likelihood of real use cases is dramatically reduced, as three different "opt-ins" are required: the participation of each epSOS healthcare provider in the patient's home country (country A) and in the country of treatment (country B) as well as the general participation and concrete consent of the epSOS patient himself. This reduces the chance for real-life use cases, which in fact epSOS would essentially need, dramatically. Given an unrealistic high acceptance of 10 percent among patients and doctors such a policy would lead to an overall chance of one per mill (0.1 x 0.1 x 0.1 = 0.001) of all cross border incidents. Considering the little number of cross border encounters another solution should have been chosen to have at least a few use cases for the epSOS pilot.

2.2.2 epSOS and the Art. 29 Data Protection Working Party

The argument of the Art. 29 Data Protection Working Party against EHR systems, that "the mere 'usefulness' of having such personal data contained in an EHR would not be sufficient" [17] to meet the requirements of **Art. 8.3 DPD** [11] is not an EHR-specific argument, but also an argument against "traditional" paper-based medical histories. Art. 3.1 DPD [11] sets the scope of the DPD [11] to the processing of data by automatic means and "the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system". Accordingly the DPD [11] is basically also to be applied to paper-based medical histories, as for example defined in Sect. 10.2 of the Austrian Hospitals- and Sanatoriums Law (HSL) [63]. The medical history definition of Sect. 10.2 HSL [63] covers inter alia: information about anamnesis, current physical condition (status praesens), course of disease (decursus morbi), applied medication and treatment, donation of tissues and organs or living wills. This personal data is processed without consent of the patients. If the arguments of the

[33] epSOS is an acronym for European Patients Smart Open Services [52].

[34] This refers to national as well as international/European level.

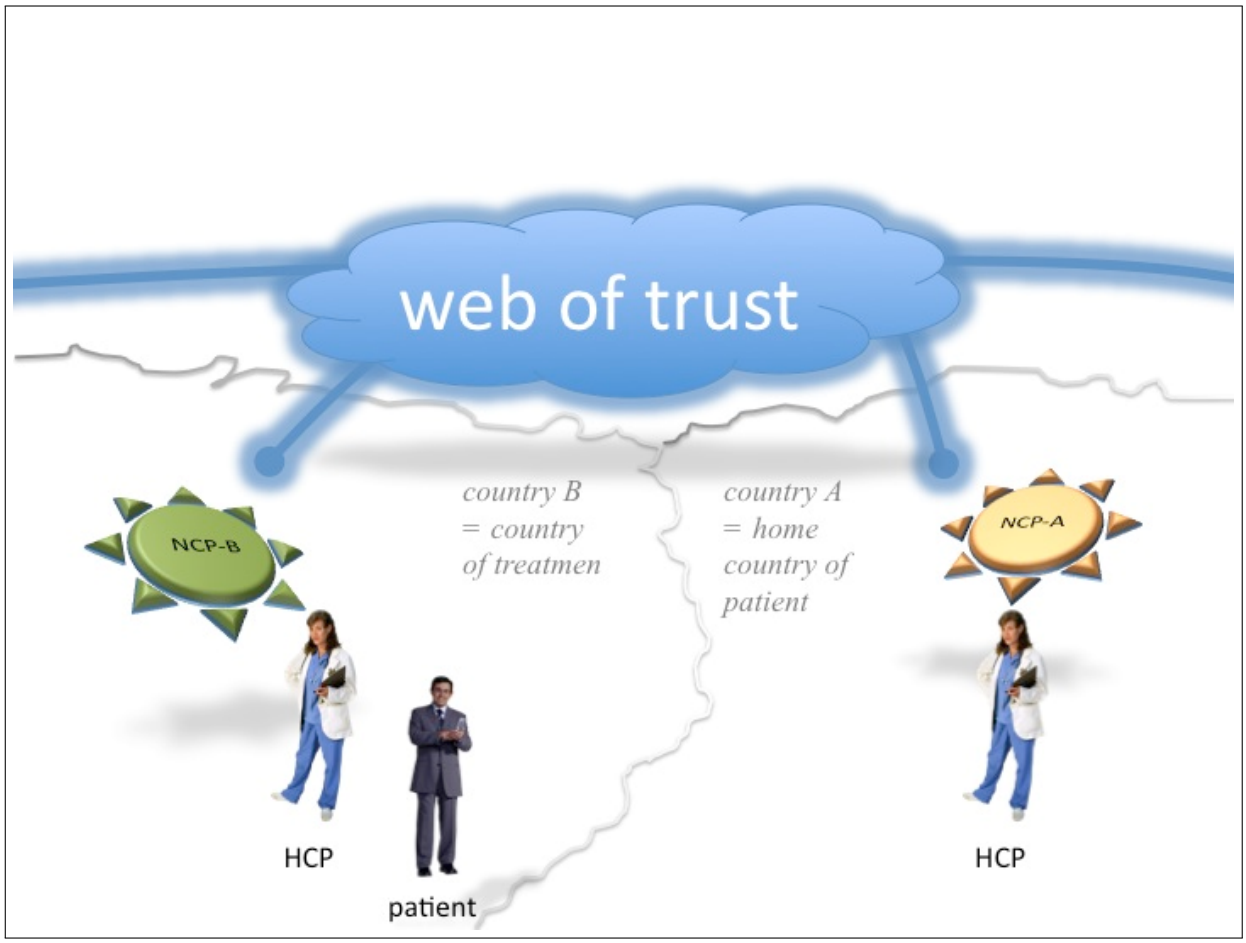

Figure 3: Structure of epSOS.

Art. 29 Data Protection Working Party were true, all medical histories, that are kept without consent of the patients, would be illegal, due to the fact that there is definitely some data collected, without being used once again. Nevertheless *collecting such data, is not just* ***useful****, but* ***necessary*** *in terms of treatment*, as neither the course of diseases nor secondary diseases can be foreseen. Due to the reference to "vital interests" (Art. 8.2.c DPD [11]), that may suspend data protection under distinct circumstances and Art. 8.3 DPD [11] itself, the obvious precedence of health over privacy interests are clearly expressed in the DPD [11].

Another deficiency of the documents [16, 17] of the Art. 29 Data Protection Working Party is, that the fundamental question regarding the application of the DPD [11] have not even been asked. However, *applicability of the DPD [11] cannot doubtlessly be assumed*, as Art. 3.2 DPD [11] excludes the processing of personal data "in the course of an activity which falls outside the scope of Community law" from the scope of the DPD [11]. According to Art. 168.7 of the Treaty on the Functioning of the European Union (TFEU) [64] the "Union action shall respect the responsibilities of the Member States [...] for the organisation and delivery of health services and medical care". For the first time, the European Court of Justice ruled upon the applicability of the DPD [11] in the case "Rechnungshof vs ORF" [65] and concluded, that the DPD [11] applies to the publication of remunerations of the public broadcasting's employees, even though this kind of publication might be "an activity which falls outside the scope of Community law" according to Art. 3.2 DPD [11]. The decisive argument has been, that Art. 100a of the Treaty establishing the European Community (TEC) [66] on the approximation of laws and legal base of the DPD [11] "does not presuppose the existence of an actual link with free movement [...] in every situation referred to by the" DPD [11]. The European Court of Justice ruled similarly in the case "Lindqvist" [67], when it had to decide whether the publication of personal health data on a website for private purposes is subject to the DPD [11] or not. The court affirmed the application of the DPD [11], because a "contrary interpretation [of Art. 3.2 DPD] could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws" [67].

Legal situation is however different regarding health services and medical care (Art. 168.7 TFEU [64]). The competence to approximate laws is only applicable insofar as not otherwise provided in the treaties (Art. 114.1

TFEU [64]). The regulation, that the competences regarding health services and medical care remain with the member states in Art. 168.7 TFEU [64] is explicitly enough, to assume that:

- legal foundations for activities in such areas cannot be harmonised according to Art. 114 TFEU [64] and
- such activities fall outside the scope of EU law according to Art. 3.2 DPD [11].

Being sure about the applicability of the DPD [11] is a pre-requisite to derive legal consequences from it. An objective answer, that meets academic requirements, should be given by the Art. 29 Data Protection Working Party. Knowledge about the scope of the DPD [11] with regard to health affairs is *extremely important for national legislation*, in particular when specialised provisions on new developments shall be enacted, as for example *regarding EHR systems or bio banks*.

2.2.3 Implementation of the epSOS Framework Agreement

epSOS' legal centrepiece is the so called Framework Agreement (FWA) [68]. This is a blueprint for national contracts to establish on the one hand the epSOS NCPs and on the other hand to shape the framework for the legal relationships between NCPs and epSOS healthcare providers. Some countries, among them Austria[35], established their NCPs by assigning the NCP role not by contract but ministerial decision, ordinance or directive. In these countries the only contracts needed for the implementation of epSOS are the contracts between the NCP and the epSOS healthcare providers. The patients' rights and the duties of the NCP and epSOS healthcare providers are governed by these NCP-HCP contracts as laid down in the FWA [68]. Healthcare providers, especially physicians, that are interested in participating in epSOS, can register online [69].

epSOS is a pilot project and therefore it is very likely that due to new experiences gained, the FWA [68] requires amendments in near future. Therefore Art. 9 of the FWA [68] implements a **general amendment procedure**. According to this procedure the decisions taken by the epSOS Project Steering Board[36] (PSB) shall be published nationally within four weeks, after the PSB's decision. Within sixteen weeks following the PSB decision the national contracting partners (pilot sites) have the right to rescind the national contracts, therewith guaranteeing that the pilot sites are not subject to provisions, they could not accept (Art. 9.2 FWA [68]).

2.2.4 Liability and Enforcement Issues

epSOS duration and number of participants were extended in 2011. Among the new participating nations there are also two third countries, Switzerland and Turkey. This raises new legal questions in the field of data protection and liability for e.g. regarding medical malpractice. Whereas the European data protection framework offers clear answers – Switzerland has been confirmed by decision of the EU Commission [70] to share the same level of data protection as the EU member states do or standard contractual clauses could be used for the exchange of personal health data with Turkey – things are not that clear with regard to international private law issues, especially enforcement. The main three questions regarding international private law are:

1. Where is the place of jurisdiction? (jurisdiction)
2. Which law is to be applied? (choice of law)
3. How and where can judgements be enforced? (foreign judgements)

In the context of jurisdiction and foreign judgements the so called Brussels regime[37] is to be applied among the EU member states and Switzerland. Austria and Turkey concluded an agreement on recognition and enforcement of judgements in civil and commercial matters [74]. Among the EU member states the choice of law is governed by the EU regulations Rome I [75] and Rome II [76].

From the Austrian point of view the international private law issues seem to be solved for the moment. Nonetheless in case that other third countries join, these issues may become important again.

2.3 Proposal for a General Data Protection Regulation

By the end of January 2012 a proposal for a general data protection regulation [77] has been published by the EU Commission. The most evident innovations to the current European data protection law in the field of e-health would be:

1. the explicit statement that consent is not the only legal foundation for processing personal health data, thus *allowing explicitly opt-out approaches*; [38]

[35] The NCP-AT, i.e. the NCP for Austria, is the Austrian Federal Ministry of Health (Bundesministerium für Gesundheit).

[36] The epSOS Project Steering Board is the highest decision-making committee of epSOS.

[37] The Brussels regime consists of the Brussels Convention [71], the Lugano Convention [72] and the Brussels I regulation [73]. The differences between these three documents are marginal – the Brussels Convention [71] was the first to be agreed in 1968, the Lugano Convention [72] twenty years later to allow for the integration of the European Free Trade Association (EFTA) member states and last but most important the Brussels I regulation [73], supplanting more or less the Brussels Convention [71]. Due to its EFTA relevance and in contrast to the Brussels Convention [71], the Lugano Convention [72] is still relevant in cases relating to EFTA states.

[38] Recital 123 of the proposal [77] states that "the processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject [, ...] meaning all elements related to [...] resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing".

2. the *definition of health data at European level*: Art. 4.12 of the proposal [77] defines "'data concerning health' [as] any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual";

3. the legal empowerment of the EU Commission to *harmonise the implementation of data security* requirements according to Art. 30.4 of the proposal [77]. This is of great importance for the international exchange of personal health data, as differing national data security requirements are one of the biggest show-stoppers for international projects like epSOS; and last but not least

4. a special provision on the processing of personal data concerning health, laid down in *Art. 81 of the proposal* [77]; Art. 81.1.a of the proposal [77] for example, is very similar to the existing Art. 8.3 DPD [11], that focuses on the usage of health data for treatment purposes by healthcare providers, subject to a special secrecy obligation; genuine innovations are

   (a) the reference to "ensuring high standards of quality and safety" which is acknowledged as public interest, possibly legitimating e-medication (Art. 81.1.b of the proposal [77]) and

   (b) Art. 81.2 of the proposal [77], that even allows the usage of personal data concerning health for scientific research purposes.

The impact of the Proposal for a General Data Protection Regulation [77] as of January 25th 2012 would be enormous on international as well as national level. At national level most of the data protection legislation would need to be repealed and at international level a new level of harmonisation, even regarding technical details as for example the data security measures, could be achieved.

3 Conclusion

Austrian legislation has *already resolved* crucial questions arising from the field of e health, above all by its Health Telematics Act [2] (chapter 1.3), that defines on the one hand the minimum data security requirements for exchange of electronic personal health data and introduces on the other hand an information governance framework (chapter 1.3.7). Administrative fines ensure that the requirements of the HTA [2] are obeyed.

An important cornerstone regarding e-health in Austria is the E-Government Act [3] (chapter 1.4), that provides basic rules for a national identity management system. This allows an unambiguous and data protection compliant identification, not only of Austrian citizens, but also foreign citizens and entities.

The *next steps to be taken* at Austrian level are first and above all the enactment of the ELGA law (chapter 2.1). This would inaugurate a new e-health era in Austria. Trust would be provided by fundamental rules regarding data protection and investment protection. Further challenges come from the European level in the context of international exchange of patient data in the course of the EU funded large scale pilot epSOS (chapter 2.2). Special attention is drawn to the opt-in issue on national level regarding ELGA (chapter 2.1.3) as well as on European level regarding epSOS (chapter 2.2.1). Another important approach to assure the patients' freedom of choice is the Access Control Centre of ELGA (chapter 2.1.5), that will give patients full control over their data.

Acknowledgements

I would like to express my thanks to Mascha Glomb and Valerie Kainz for their assistance in structuring and preparing the German translation.

References

[1] Data Protection Act 2000 (DPA 2000 – Datenschutzgesetz 2000) Federal Law Gazette, Part I No. 165/1999 as amended by Federal Law Gazette, Part I No. 135/2009. In German.

[2] Health Telematics Act (HTA – Gesundheitstelematikgesetz) Federal Law Gazette, Part I No. 179/2004 as amended by Federal Law Gazette part I no. 103/2010. In German.

[3] E-Government Act (EGovA – E-Government-Gesetz) Federal Law Gazette, Part I No. 10/2004 as amended by Federal Law Gazette part I no. 111/2010. In German.

[4] Doctors Code 1998 (DC 1998 – Ärztegesetz 1998) Federal Law Gazette, Part I No. 169/1998 as amended by Federal Law Gazette, Part I No. 61/2010. In German.

[5] General Social Insurance Law (GSIL – Allgemeines Sozialversicherungsgesetz) Federal Law Gazette, No. 189/1955 as amended by Federal Law Gazette, Part I No. 24/2011. In German.

[6] Insurance Agreement Act 1958 (IAA – Vertragsversicherungsgesetz 1958) Federal Law Gazette, No. 2/1959 as amended by Federal Law Gazette, Part I No. 58/2010. In German.

[7] Genetic Engineering Act (GEA – Gentechnikgesetz) Federal Law Gazette, No. 510/1994 as amended by Federal Law Gazette, Part I No. 13/2006. In German.

[8] European Convention on Human Rights (ECHR), Federal Law Gazette, No. 210/1958 as amended by Federal Law Gazette, Part III No. 47/2010. In German.

[9] Basic Law on the General Rights of Nationals (BLGRN – Staatsgrundgesetz) Imperial Law Gazette, No. 142/1867 as amended by Federal Law Gazette, No. 684/1988. In German.

[10] Federal Constitutional Law (Bundes-Verfassungsgesetz) Federal Law Gazette, No. 1/1930 as amended by Federal Law Gazette, Part I No. 127/2009. In German.

[11] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive – DPD). OJ L 281, 23.11.1995, p. 31-50.

[12] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare (Patients' Rights Directive – PRD). OJ L 88, 4.4.2011, p. 45-65.

[13] String-Commission. Electronic lifelong Health Record (EHR) – A privacy impact assessment – Version 1.0. Vienna: String-Commission; 2003. In German.

[14] Berner ES, Detmer DE, Simborg D. Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States. Journal of the American Medical Informatics Association 2005 Jan-Feb; 12(1): 3-7.

[15] http://ec.europa.eu/justice/policies/privacy/workinggroup /wpdocs/index_search_en.htm [cited 2012 Feb 20].

[16] Article 29 Data Protection Working Party. Working Document on the processing of personal data relating to health in electronic health records (EHR) [internet]. Brussels: Article 29 Data Protection Working Party; 2007; WP 131 [cited 2012 Mar 20]. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs /2007/wp131_en.pdf.

[17] Article 29 Data Protection Working Party. Working Document 01/2012 on epSOS [internet]. Brussels: Article 29 Data Protection Working Party; 2012; WP 189 [cited 2012 Mar 20]. Available from: http://ec.europa.eu/justice/data-protection /article-29/documentation/opinion-recommendation /files/2012/wp189_en.pdf.

[18] Mayer H. Legal opinion on the draft of an "Electronic-Health-Records-Framework Act – EHR-A" [internet]. Vienna: Medical Association of Vienna; 2012. p. 5 [cited 2012 Feb 12]. Available from: http://www.aekwien.at/media/ELGA-Gutachten.pdf. In German.

[19] Austrian Constitutional Court. Ruling 16.342/2001 of 2001 Nov 26. In German.

[20] Austrian Constitutional Court. Ruling 11.760/1988 of 1988 Jun 24. In German.

[21] http://www.wienkav.at/kav/ikt/ZeigeText.asp?ID=28413 [cited 2012 Feb 7]. In German.

[22] Industrial Code (IC – Gewerbeordnung) Federal Law Gazette, No. 194/1994 as amended by Federal Law Gazette, Part I No. 111/2010. In German.

[23] Austrian Data Protection Council. Opinion on the draft of an Health Telematics Act. 6/SN-341/ME of the 21st Austrian legislative term. [cited 2012 Feb 20]. p. 1 et sqq. Available from http://www.parlament.gv.at/PAKT/VHG/XXI/ME /ME_00341_06/imfname_000000.pdf. In German.

[24] Arge Daten. Opinion on the draft of an Health Telematics Act. 27/SN-341/ME of the 21st Austrian legislative term. [cited 2012 Feb 20]. p. 2 et sqq. Available from http://www.parlament.gv.at/PAKT/VHG/XXI/ME /ME_00341_27/imfname_000000.pdf. In German.

[25] Federal Chancellery. Opinion on the draft of an Health Telematics Act. 29/SN-341/ME of the 21st Austrian legislative term. [cited 2012 Feb 20]. p. 1 et sqq. Available from http://www.parlament.gv.at/PAKT/VHG/XXI/ME /ME_00341_29/imfname_000000.pdf. In German.

[26] Huber M. EHR law: Unconstitutional! Journal of the Austrian Medical Association 2012 Apr; 7a: 10. In German.

[27] Austrian Constitutional Court. Ruling 18.405/2008 of 2001 Mar 6. In German.

[28] Austrian Constitutional Court. Ruling 15.447/1999 of 1999 Mar 4. In German.

[29] Austrian Constitutional Court. Ruling 14.573/1996 of 1996 Sep 24. In German.

[30] Austrian Constitutional Court. Ruling 10.313/1984 of 1984 Dec 12. In German.

[31] Austrian Constitutional Court. Ruling 14.936/1997 of 1997 Oct 1. In German.

[32] Health Telematics Ordinance (HTO – Gesundheit-stelematikverordnung) Federal Law Gazette, Part II No. 451/2008 as amended by Federal Law Gazette, Part II No. 464/2010. In German.

[33] Electronic Signature Act (Signaturgesetz) Federal Law Gazette, Part. I No. 190/1999 as amended by Federal Law Gazette, Part I No. 75/2010. In German.

[34] Electronic Signature Ordinance 2008 (Signaturverordnung 2008) Federal Law Gazette, Part II No. 3/2008 as amended by Federal Law Gazette, Part II No. 401/2010. In German.

[35] Federal Law Gazette, Part I Nos. 23/2008, 36/2009 and 103/2010.

[36] Federal Law Gazette, Part I No. 103/2010.

[37] https://www.gesundheit.gv.at/Portal.Node/ghp/public/files /Ueberblick_Qualitaetskriterien.pdf [cited 2012 Feb 5]. In German.

[38] https://www.gesundheit.gv.at [cited 2012 Feb 7]. In German.

[39] http://www.who.int/classifications/icd/en [cited 2012 Mar 30].

[40] http://en.wikipedia.org/wiki/Triple_DES [cited 2012 Mar 30].

[41] SourcePin Register Authority. Creation of sourcePINs for natural persons [internet]. Vienna: Austrian Data Protection Commission [cited 2012 Mar 30]. Available from: http://www.stammzahlenregister.gv.at/site/6001 /default.aspx#sz. In German.

[42] http://en.wikipedia.org/wiki/Cipher_block_chaining - Cipher-block_chaining_.28CBC.29 [cited 2012 Mar 30].

[43] http://www.stammzahlenregister.gv.at/site/5109/default.aspx [cited 2012 Feb 2]. In German.

[44] http://www.stammzahlenregister.gv.at/site/6085/default.aspx [cited 2012 Feb 2]. In German.

[45] http://www.stammzahlenregister.gv.at/site/5983/default.aspx [cited 2012 Feb 2]. In German.

[46] Dentists Code (Zahnärztegesetz) Federal Law Gazette, Part I No. 126/2005 as amended by Federal Law Gazette, Part I No. 57/2008. In German.

[47] Leitner H. §54. In: Emberger H, Wallner F, editors. Commentary on the Austrian Doctor's Code. 2nd ed. Vienna: Verlagshaus der Ärzte; 2008. p. 259-68. In German.

[48] Federal Law Gazette, Part I No. 172/1999. In German.

[49] Milisits C. Wesentliche Neuerungen im Gesundheitsbereich. In: Karl B, Marko-Herzeg, Herausgeber. Jahrbuch Sozialversicherungsrecht 2010. Wien: Neuer Wissenschaftlicher Verlag; 2010. S. 83-104. German.

[50] Federal Law Gazette, Part I No. 1/2002. In German.

[51] Registration Act 1991 (Meldegesetz 1991) Federal Law Gazette, No. 9/1992 as amended by Federal Law Gazette, Part I No. 135/2009. In German.

[52] http://www.epsos.eu [cited Feb 3].

[53] Reimer S. The consent according to the data protection law. St. Gallen: Intelligent Law and Internet Applications; 2011. p. 65 et sq. [cited 2012 Feb 20]. Available from http://www.ilia.ch/downloads/20110205_ilia_ch_version.pdf. In German.

[54] Frohner J. Privacy and E-Health. In: Bauer L, Reimer S, editors. Manual on Austrian Data Protection Law. Vienna: Facultas; 2009. p. 253-71. In German.

[55] Reeve JF, Tenni PC, Peterson GM. An electronic prompt in dispensing software to promote clinical interventions by community pharmacists: a randomized controlled trial. British Journal of Clinical Pharmacology 2008; 65(3): 377-85.

[56] Lazarou J, Pomeranz BH, Corey PN. Incidence of Adverse Drug Reactions in Hospitalized Patients, JAMA 1998; 279(15): 1200-5.

[57] Wester K, Jönsson AK, Spigset O, Druid H, Hägg S. Incidence of fatal adverse drug reactions: a population based study. British Journal of Clinical Pharmacology 2008; 65(4): 573-9.

[58] US Department of Health and Human Services, US Food and Drug Administration. AERS Patient Outcomes by Year. Silver Spring: US Department f Heath and Human Services; 2010. [cited: 2012 Feb 16]. Available from http://www.fda.gov/Drugs /GuidanceComplianceRegulatoryInformation/Surveillance /AdverseDrugEffects/ucm070461.htm.

[59] Lee A. Adverse Drug Reactions. 2nd ed. London: Pharmaceutical Press; 2006.

[60] Austrian Constitutional Court. Ruling 17.500/2005 of 2005 Mar 10. In German.

[61] Constitutional Service of the Federal Chancellery. Opinion on the draft of an EHR Framework Act. Vienna: Constitutional Service of the Federal Chancellery; 2011; BKA-601.349/0001-V/5/2011. p. 4 et sqq. [cited 2012 Feb 20]. Available from http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00260_24/imfname_210643.pdf. In German.

[62] http://www.epsos.eu/home/about-epsos.html [cited 2012 Feb 16].

[63] Hospitals- and Sanatoriums Law (Krankenanstalten- und Kuranstaltengesetz) Federal Law Gazette, No. 1/1957 as amended by Federal Law Gazette, Part I No. 147/2011. In German.

[64] Treaty on the Functioning of the European Union [consolidated version]. OJ C 83, 30.3.2010, p. 47-199.

[65] European Court of Justice. Case "Rechnungshof vs ORF" C-465/00, of 2003 May 20.

[66] Treaty establishing the European Community [consolidated version]. OJ C 325, 24.12.2002, p. 33-184.

[67] European Court of Justice. Case "Lindqvist" C-101/01, of 2003 Nov 6.

[68] epSOS. Framework Agreement on National Contact Points in the context of the Smart Open Services for European Patients Project (epSOS) – (version 2) [internet]. [cited 2012 Feb 20] Available from http://www.epsos.eu/fileadmin/content/pdf/Framework_Agreement_on_National_Contact_Points_V2.pdf.

[69] http://www.epsos.eu/for-health-professionals/how-can-health-professionals-participate.html [cited 2012 Mar 30].

[70] Commission Decision pursuant to Directive 95/46/EC on the adequate protection of personal data provided in Switzerland, 2000/518/EC. OJ L 215, 25.8.2000, p. 1-3.

[71] Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters [consolidated version]. OJ C 27, 26.1.1998, p. 1-27.

[72] Convention on jurisdiction and the enforcement of judgments in civil and commercial matters; done at Lugano on 1988 September 16, 88/592/EEC [consolidated version]. OJ L 319, 25.11.1988. p. 9-28.

[73] Regulation (EC) No. 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. OJ L 12, 16.1.2001, p. 1-23.

[74] Federal Law Gazette, No. 571/1992 as amended by Federal Law Gazette, No. 949/1994. In German.

[75] Regulation (EC) No. 593/2008 on the law applicable to contractual obligations (Rome I). OJ L 177, 4.7.2008, p. 6-16.

[76] Regulation (EC) No. 864/2007 on the law applicable to non-contractual obligations (Rome II). OJ L 199, 31.7.2007, p. 40-9.

[77] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [internet]. COM(2012)11 final. [cited 2012 Feb 19] Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Support for Electronic Health Records in Czech Law

Otto Dostál[1], **Milan Šárek**[2]

[1] Masaryk University, Institute of Computer Science, Brno, Czech Republic

[2] Institute of Computer Science AS CR, Department of Medical Informatics, Prague, Czech Republic

Abstract

The spreading use of the e-Health applications in healthcare raises questions about the legal aspects of this development. In this paper, we wanted to look into such questions related to one of the most basic elements of any e-Health solution - electronic health records - in Czech law. The article aimed to create a review of the national legislation related to electronic health records currently in force (which means primarily the Care for Health of the People Act n. 20/1966 Sb.), and to identify possible legal issues that could be preventing the deployment of e-Health Applications. The article shows that the Czech law indeed allows usage of electronic health records, and sets relatively detailed rules in some areas such as what information must be included inside it, and how to archive the data. However, it offers little guidance regarding some other situations, like it is ignoring the question of technical standards for interoperability. The briefness of the Act leaves lot of the decisions related to the development of the e-Health applications up to the individual healthcare facilities.

Keywords

e-Health, electronic health record, legal framework, Care for Health of the People Act, advanced electronic signature

Correspondence to:

Otto Dostál
Masaryk University, Institute of Computer Science
Address: Botanická 554/68a, Ponava, Brno, Czech Republic
E–mail: ottodostal@gmail.com

EJBI 2012; 8(2):29–33
recieved: June 21, 2011
accepted: January 16, 2012
published: June 15, 2012

1 Introduction

The incorporation of various information technology tools in medical practice brings opportunities related to improvement of quality and availability of services and other benefits. However, the spreading use of the e-Health applications in healthcare also raises questions about the legal aspects of this development. In this paper, we would like to look into such questions related to one of the most basic elements of any e-Health solution - electronic health records - in Czech law.

The legal framework for the management of electronic health records forms the basis both for the successful design of electronic health records, and for the subsequent management of the whole process of documentation. The process of documentation starts from the creation of the data in medical facilities and continues with its storage and subsequent archiving, but includes also the transfer of medical data extramural outside the hospital information system. This article aims to create a review of the national legislation related to electronic health records currently in force, and to identify possible legal issues that could be preventing the deployment of e-Health Applications. The article would also like to possibly arouse discussion on this crucial issue. Discussion could contribute to the further development of e-Health applications, which could then facilitate the implementation of EU priorities promoting the mobility of EU citizens as described for example in the report of the EU on e-Health infrastructures from January 2011 [1].

2 Relevant Statutes

The legal framework in the Czech Republic related to the problematic of electronic health records consists of several acts [2], primarily the n. 20/1966 Sb. Care for Health of the People Act, the n. 101/2000 Sb. Personal Data Protection Act and the n. 227/2000 Sb. Digital Signature Act.

In this article, we will concentrate mostly on the n. 20/1966 Sb. Care for Health of the People Act (hereinafter referred only as "Care for Health of the People Act" or "Act"). The reason for this is, that the n. 101/2000 Sb. Personal Data Protection Act and the n. 227/2000 Sb. Digital Signature Act are more general types of statutes, while Care for Health of the People Act incorporates the core of the legal regulation of health records, including the electronic variant. Also, the n. 101/2000 Sb. Personal Data Protection Act and the n. 227/2000 Sb. Digital Sig-

nature Act are heavily influenced by the European Union legislation they are implementing (Directive n. 95/46/ES on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3, 4] and Directive n. 99/93/ES on a Community framework for electronic signatures respectively), while the Care for Health of the People Act is not expressly implementing any EU legislation. Therefore we believe that the more detailed analysis of the Care for Health of the People Act might reveal some more unique issues, which could eventually be interesting for example when considering if some new EU legislation in this area might be sensible.

To the Care for Health of the People Act an implementing n. 385/2006 Sb. Health Record Order (hereinafter referred as "Order") has been later passed.

3 Electronic Health Records under the Care for Health of the People Act

The Care for Health of the People Act (that is its § 67a and following) is not defining the term "health record". However, it at least states, what such a health record consists of. That is:

1. personal data of the patient in the scope necessary for identification of the patient and assessment of the anamnesis [5] (It is explicitly specified, that it can contain the birth certificate number of the patient.) and

2. information about the illness of the patient, about the process and results of examinations, treatments, and other significant circumstances related to the health state of the patient and the procedure during health care delivery.

3.1 Three Possible Legal Ways of Having the Health Records in the Electronic Form

The Care for Health of the People Act expressly permits keeping the health record in electronic form (literally saying in its § 67b article 5 that, „Health record can be kept on a medium either in a text, graphical, or audio-visual form".). It even allows for several ways how this can be done:

(A) Health records can be first kept in paper form and the data from them transferred to the electronic form only later. It this case, it is not necessary to attach the advanced digital signature to the electronic variant of the record, but it is necessary to archive those former paper documents. This way even old records created before the switch to electronic health records can be transformed to the electronic form.

(B) Health records can be first kept in the electronic form and then transformed to the paper. In such a case the person that made the record must also log the date on it and sign it and such a printout must be archived. The printout is considered a separate part of the health record (§ 67b article 6) and as such it must include the personal data of the patient in the scope necessary for his/her identification and the specification of the medical facility that created it (§ 67b article 3). It this case it is also not necessary to use the advanced digital signature.

(C) Health records can be kept in the electronic form exclusively. In such a case the Act stipulates following rules:

   (a) All separate parts of the health record include the advanced electronic signature of the person that made the record,

   (b) safety copies of files are made at least once each working day,

   (c) after the expiration of the lifetime period of the record a transcript of the archival copies is secured,

   (d) the storage of archival copies that are made at least once a year is done in a way preventing additional changes to them.

3.2 How to Apply These Rules to Different Types of Records

The question can be to what extent some of the mentioned rules (especially the rule to transform to the paper form under the alternative B and rules mentioned under alternative C) apply only to records in form of text and to what extent also to records in graphical or audio-visual form.

In practice these rules are not interpreted strictly. In our opinion though, it is necessary to apply the same rules as in the case of text records. That is, because the law is not talking about any differences and the opposite conclusion would be hardly acceptable, as it would in essence mean, that a document kept only in electronic form does not have to fulfil rules under alternative C. This should not be too hard to technically implement anyway, as from the point of the digital signature algorithms, there is essentially no difference between digital signing of text, picture or video (although with the larger data files it will obviously take more computing power to process).

The current legal state therefore seems such, that every graphical or audio-visual document about a patient in a digital form that is not going to be transferred to a paper form fall within the scope of the alternative C, that is, the rules concerning the backup procedures and usage of digital signature.

3.3 When to Apply the Advanced Electronic Signature

The Act stipulates, that every "separate part" of the health record must include the personal data of the patient in the scope necessary for his/her identification and the specification of the medical facility that created it, and, if health records are to be kept in the electronic form exclusively, all "separate parts" of the health record must also include the advanced electronic signature of the person that made the record. In this situation we found it necessary to consider the term "separate part of the health record" itself.

The law does not define it, but it can be inferred, that not every document in the health record must necessarily be signed by the advanced digital signature. Otherwise, the legislator would not use the term separate part of the health record, but it would link the rules directly to the term "record". This conclusion is also supported by the wording of the implementing Order, which defines in its supplement n. 1 "the minimal content of the separate part of the health record". This is not a list of parts of health record that are already separate, but instead of parts that might become separate (see § 3 article 2 of the Order) and for which special necessities are defined. In relation to these necessities the list is taxative, but as for the term separate part of the health record it is demonstrative. The point is, that every part of health record that is being detached, for example during its sending to another medical facility, should be signed by digital signature and marked with necessary identification data.

Such detaching and sending can be possible with virtually any kind of content of the health record (whether it is a X-ray picture or something else). For the fulfilment of the requirements it is enough if the document is signed with the digital signature (and the mentioned identification data are included in it) at the phase in which it is being sent (e. g. it is becoming separate). Of course though, that it must be the signature of the person responsible for the content of the document; if other person would be the one sending it, the signature of such a person would not be sufficient (see the wording "the electronic signature of the person that made the record").

From this reason it seems more practical to have the documents in health record already signed right from their creation and not only when they have to be sent somewhere. Also the wider usage of digital signatures can be generally recommended, anyway, to improve credibility of the given system. Besides, for documents that are already stored in a way prescribed for separate parts of health record, it opens a way to consider the possibilities to exchange them in such a style that there would be no more necessary to send a request between medical facilities that someone must answer, but based upon a password and other security measures the system could evaluate the request itself and allow access to the data.

3.4 Concerning the Rules Related to the Archiving of the Data

Let's have a look at other rules under the alternative C. Rules b) and d) should not cause, although their fulfilment will of course require some financial and other expenses, bigger legal or technical problems. Each workday a backup of data must be made, during which all new records (e. g. new documents and changes of the older ones) must be archived compared to the previous backup (that must have been performed the day before). This rule will be of course fulfilled by usage of even higher standard, when all changes on one data-storage are immediately mirrored on another data-storage. Besides that, the law prescribes creation of additional backup of the records that must be performed at least once a year. In case of this backup, the storage must be done in a way preventing additional changes to them. As for the documents signed with digital signature this rule is, thanks to its attributes, fulfilled. The second option might be to use non-rewritable mediums (such as DVD-R). The question of eventual other ways and additional details how to store the data without the possibility of future changes to them the Act does not answer and leaves it to the individual subjects, or rather their employees, particularly the computing experts.

Significantly more difficult to analyse are the rules under letter c) "after the expiration of the lifetime period of the record a transcript of the archival copies is secured". This provision seems rather unintelligible. Not only that it might not be clear to everybody what is "the lifetime period of the record", but doubts arose also from the term "transcript" (if it is a copy, why the Act uses different word?), the term "archival copies" (which is the same expression as under letter d), but ordering, that is placement of rule c) higher, does not correspond to the sameness) and strange is the instruction to do it "after" (when the record is not, or might be not, readable anymore?!).

The intention of the lawmaker has probably been though, to set some standard of reliability for the data-storage of the health record. Therefore only such data-storage should be used, for which the lifetime period set by its manufacturer or provider has not yet expired, and a transfer to another data-storage ahead of such time must be done (Doing it "before" instead of "after" will not be a violation of the law - argumentum a minori ad maius.).

This obligation logically relates primarily to the main backup, but considering the evident need to keep both backups usable, it seems fitting to apply it to them as well. In case of archival copies according to letter d) it is not necessary to infer this in such a way, as the Act deals with them specifically and somewhat more clearly. According to § 67b article 8 "While keeping archival copies of data on memory mediums of computer technology an access to the data and their readability (usability) must be guaranteed at least for the time prescribed for the archiving of health records".

3.5 Other Formal Requirements

We already described some rules concerning what must be included as an information with health records, such as that each separate part of the health record must "include the personal data of the patient in the scope necessary for his/her identification and the specification of the medical facility that created it". However, the Act, for all ways of keeping of the health record, prescribes some other rules that we should also mention at least briefly.

According to § 67b article 4 each record "must include date of its creation, identification and signature of the person that made the record. Corrections in health record are done by new record that must include date of its creation, identification and signature of the person that made the correction. The former record must stay readable". A question might be, what is "the signature" according to this provision. In the context of the Act it is nevertheless clear, that the lawmaker meant only the paper version of health record and in case of electronic health record that does not have to include the advanced digital signature (variants A and B) it is apparently sufficient to list the person that made that record.

In the last quoted § we can note, that the records in electronic health record should not be completely erased, but an access to the corrected part must remain possible.

3.6 Right of the Patient to Access the Health Record

The Act after its amendment n. 111/2007 Sb. finally [6] introduces the right of the patient to access the health record (§ 67b article 12). In relationship with the topic of this article we would like to emphasize that in case of existence of electronic health records, the patient now obviously has the right to be provided with corresponding digital copy. The way to consider the possibilities of the on-line access to the health record by the patient himself opens too.

As a side note, we would like to remark that we would recommend to establish also the right of the patient to access the automatically generated logs about the access to the health record, which would future support their significant contribution to the protection of the records from unauthorized access.

4 Discussion and Conclusion

Above we described the core of the national legislation related to electronic health records and analysed the meaning and appropriate implementation of some parts of its text. We have found the current text of the Care for Health of the People Act to be sometimes problematic and inconsistent, and thus we believe that it should be rewritten to be clearer and more comprehensive. Nevertheless, as we could see, the legal framework in the Czech Republic indeed allows the usage of electronic health record, which is the basic requirement for deployment of various e-Health applications.

What the authors of this article are finding concerning is what the Care for Health of the People Act does not say. The text of the Act is rather brief and obviously is not covering all aspects of implementation of electronic health records in detail. While we were talking about the Care for Health of the People Act we did not mention anything about any legally binding technical data standards set by law concerning the transfer of the digital data between different medical facilities. Neither had we talked about any legally created dedicated body entitled with establishing of such standards and policies (Such as the Office of the National Coordinator for Health Information Technology and the HIT Standards Committee in USA [7]). The reason is that there is no such a thing. There exists a certain standard called "Data Standard of Ministry of Health of the Czech Republic", but this standard is not legally binding and despite its officially sounding name the Ministry of Health is letting it being developed mostly in an informal cooperation between various private companies. This standard is now widely used in the country, yet it is not accepted by all healthcare facilities, and the other problem is, that many of the facilities are using several years old versions of the standard, as they are not forced to update it, despite the authors of the standard are urging them to do so. Besides its problematic enforcement, we would also like to stress out, that it is a purely national standard, which does not even have any ambition [8] for compatibility with foreign facilities, e. g. to support transfers of electronic health records across the borders of the country. We believe this to be an issue, especially for a country that is a member of the ever more integrating European Union.

The briefness of the Act leaves a lot of the decisions related to the development of the e-Health applications up to the individual healthcare facilities. For example, as we could see, the Act sets rules as to when the advanced electronic signature has to be used; however, it does not set any detailed rules about the certification-service-provider. On one hand the usage of the advanced electronic signatures is mandatory, but on the other hand, it is not necessary for these signatures to be based on qualified certificates. Healthcare facilities thus might use a certification-service-provider that does not have any accreditation, or theoretically even create their own certification-service-provider. Obviously, such decisions are connected with responsibly towards the patients in case of some problems.

It might be argued, that it is actually a good thing, that the legal regulation sets only some basic rules to allow the existence of electronic health records and that is not too detailed, as the rapid development in the field of e-Health could in such a case quickly render the text of the statutes obsolete, and the too precise legal rules might limit the possibilities of development and deployment of various new technological solutions and services. The authors of this article are of such opinion though, that the Czech government should take more active role, and pro-

vide some more guidance in the processes we discussed, like in the area of creation and enforcement of interoperability standards.

References

[1] Stroetmann K. et al. European countries on their journey towards national eHealth infrastructures. Brussels: European Commission, Information Society Media Directorate-General, eHealth Strategies Report; 2011. Available from: http://www.ehealth-strategies.eu/report/eHealth_Strategies_Final_Report_Web.pdf.

[2] Dostál Otto, Brechlerová Dagmar. Selected legal aspects of health records and telemedicine (in Czech). Prague: EuroMISE centrum; 2005.

[3] Mates Pavel. Ochrana soukromí ve správním právu. Praha: Linde; 2004. In Czech.

[4] Matoušová Miroslava, Hejlík Ladislav. Osobní údaje a jejich ochrana. Praha: ASPI Publishing; 2003. In Czech.

[5] A diagnosis is reached by the examination of the patient. This consists in the obtaining of the history (anamnesis) and in the objective examination (status praesens). - Georg Klemperer. The Elements of clinical diagnosis. The Macmillan Co.; 1904. p. 1.

[6] Buriánek Jan. Lékařské tajemství, zdravotnická dokumentace a související právní otázky. Praha: Linde; 2005. p. 54 and following. In Czech.

[7] Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, § 2.A.III B.4.

[8] Seiner Miroslav, Zámečník Miroslav. Současný vývoj a záměry rozvoje datového standardu MZ ČR. ISSN 1803-8115, p. 235-248. In Czech.

Consequences of the EU Ker-Optika Case for e-commerce in Physical Medical Devices and Apps for eHealth Services

Erik Vollebregt[1]

[1] Partner, Axon Lawyers, Amsterdam, the Netherlands

Abstract

This article analyses the reasoning of the European Court with respect to the interpretation of the e-commerce directive and the free movement of goods provisions to the Internet sale of medical devices as goods in the Ker-Optika case. It draws conclusions from that analysis for e-commerce in medical devices as goods in the EU, which are extrapolated to the sale of medical devices as services such as apps for home treatment or monitoring in the context of eHealth services.

The article finds that eHealth services constituting medical devices are regulated identically under EU law to physical medical devices and analyses the consequences of this.

Keywords

apps, software, medical devices, e-commerce, on-line sales

Correspondence to:

Erik Vollebregt
Partner, Axon Lawyers, Amsterdam, the Netherlands
Address: Piet Heinkade 183, 1019 HC Amsterdam, The Netherlands
E–mail: erik.vollebregt@axonlawyers.com

EJBI 2012; 8(2):34–39
recieved: June 20, 2011
accepted: March 31, 2012
published: June 15, 2012

1 Introduction

As medical devices are becoming more of a commodity and self-care medical devices proliferate, the question arises to what extent EU member states can regulate clinical supervision of the delivery of medical devices. Just like with medicinal products there are medical devices that member states regulate as prescription medical devices (such as hip implants and pacemakers) whereas there is a growing category of medical devices that consumers purchase without prescription and apply for themselves, such as contact lens fluid. While European medicinal products regulation makes a clear distinction between prescription medicinal products and non-prescription medicinal products for the purpose of distribution and sales to consumers, the medical devices directives[1] presently do not.

This makes the regulatory freedom that member states have to define what clinical supervision they may exercise on the delivery of medical devices a subject of the free movement of goods. The modalities of sale (e.g. online via website) are not prescribed for medical devices on a European level as they are in the level of detail of medicinal products. Consequently, the same questions come up as with regulation of delivery of medical devices: to what extent are EU member states allowed to regulate modalities of sale for medical devices? Both of these questions have been addressed in a judgment delivered by the European Court of Justice concerning online sales of contact lenses. This article will discuss the legal reasoning in this case and subsequently extrapolate it to another field of medical devices that is rapidly developing: that of apps used for treatment and diagnosis, whether or not in the context of provision of eHealth services.

This software represents a huge developing market[2] and the EU has put it beyond doubt that such apps are considered medical devices regulated under the medical devices regulations [2]. Software is not a good, however, especially not if it is purchased online and delivered online

[1] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ L 169, 12.7.1993, p. 1–43, Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices, OJ L 189, 20.7.1990, p. 17–36 and Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices, OJ L 331, 7.12.1998, p. 1–37

[2] For example, the global telemedicine market is expected to grow from $9.8 billion in 2010 to $11.6 billion in 2011, and to $27.3 billion in 2016, a compound annual growth rate (CAGR) of 18.6% over the next five years. The telehospital/clinic market segment was worth $8.1 billion in 2011. This is expected to grow to $17.6 billion in 2016, demonstrating a CAGR of 16.8% between 2011 and 2016. The telehome segment is growing faster than the telehospital/clinic segment. This market segment was valued at $3.5 billion in 2011, and this revenue is expected to grow at a CAGR of 22.5%, reaching $9.7 billion in 2016. [source BCC Research, January 2012]

to a consumer's computer or handheld device. In that case the medical device would constitute a service for the purpose of EU internal market law. Given the developments of medical devices in the form of software as service, it is interesting to investigate if the reasoning applied in the case discussed also applies to medical devices as services.

2 Judgment of the Court

The Ker-Optika case [1] concerned a dispute about the legality of Hungarian legislation that reserves the sale of contact lenses to shops that specialise in the sale of medical devices and, consequently, prohibits the sale of contact lenses via the Internet. The European Court held that EU member states are not under all circumstances allowed to restrict the sale of medical devices to only physical outlets that specialise in medical devices. It ruled on two points of law important to members of the medical devices industry seeking to sell medical devices to consumers in the EU online:

1. the scope of the e-commerce directive with respect to the national rules prohibiting Internet sales of certain medical devices (in this case contact lenses),

2. the restrictions that general EU free movement of goods rules impose on national requirements to sell certain medical devices only from brick-and-mortar shops with qualified personnel.

3 Scope of the e-commerce Directive

First, the Court clarified the scope of the e-commerce directive [3] with respect to the national rules prohibiting Internet sales of contact lenses. It held that national rules relating to whether or not medical devices can be sold via the Internet fall within the scope of the e-commerce directive because medical devices are not excluded from its scope. However, national rules that seek to regulate how medical devices are supplied to the end user (e.g., only after a prior examination for fitting) fall outside the scope of the e-commerce directive and, consequently, cannot be assessed by the rules that the e-commerce directive imposes. Those national rules have to be assessed under the general EU internal market rules on free movement of goods. Given that the sale of medical devices via the Internet falls within the scope of the e-commerce directive, the European Court ruled that Internet sales as such cannot be prohibited, even in cases where a prior examination by qualified staff would be necessary, because that examination can be separated from the subsequent Internet sale.

4 Permitted National Law Restrictions under Free Movement Rules

What then are the restrictions that general EU free movement of goods rules impose on national requirements to sell certain medical devices only from shops with qualified personnel? First of all, these rules hinder access to the market of the member state that has those rules more for foreign traders than for local traders, the court reasoned, with reference to the DocMorris case [4] concerning Internet sales of medicinal products.

That restriction must therefore be justified if the member state wants to be able to maintain it. However, the European Court finds that the type of devices in question does not justify this type of restriction for three reasons (paraphrased wording from the judgment):

1. In regards to the requirement that the customer must be physically present to have his eyes examined by an optician at the sales outlet, it must first be observed that precautionary examinations carried out for investigative purposes can be undertaken by ophthalmologists in places other than opticians' shops. However, there was no requirement that an optician must make every supply of lenses dependent on a precautionary examination or on medical advice having first been obtained or that those conditions are imposed, in particular, on each occasion when there is a series of supplies of lenses to the same customer.

   Accordingly, undergoing such examinations and obtaining such advice must be held to be optional, and consequently it is primarily the responsibility of each contact lens user to make use of them, while the task of the optician in that regard is to give advice to the users. If that is the case, customers can be advised, in the same way, before the supply of contact lenses, as part of the process of selling the lenses via the Internet, by means of the interactive features on the Internet site concerned, the customer's use of which must be mandatory before he can proceed to purchase the lenses.

2. Member states can require that the determination of which type of contact lenses is the most appropriate be undertaken by an optician, who is under an obligation, at that time, to check the positioning of the lenses on the customer's eyes and advise the customer on the correct use and care of the lenses. However, that is normally only required when contact lenses are first supplied. At the time of subsequent supplies, there is, as a general rule, no need to provide the customer with such services. It is sufficient that the customer advise the seller of the type of lenses which was provided when lenses were first supplied, the specifications of those lenses having

been adjusted, where necessary, by an ophthalmologist who has issued a new prescription which takes into account any change in the customer's vision.

3. While the extended use of contact lenses must be accompanied by supplementary information and advice, those can be given to the customer by means of the interactive features of the website of the Internet sales provider (e.g., through a qualified optician whose task is to give to the customer, at a distance, individualised information and advice on the use and care of the contact lenses). The provision of such information and advice at a distance may, moreover, offer advantages, since the lens user is able to submit questions that are well thought out and pertinent, and without the need to go out.

In summary, because the legislation in question was not proportionate for regulation of the sale of contact lenses via the Internet, it was contrary to the general rules on free movement of goods.

5 Consequences for e-commerce for Medical Devices as Goods

This judgment has important consequences for national rules governing Internet sales of medical devices in the EU. Any restriction on Internet sales, even if it is intended to protect consumer health, must also be proportionate to that goal, and whether that is the case will differ from device to device. Even in cases concerning devices for which initial clinical/fitting advice would be prudent, EU member states are not allowed to completely ban Internet sales of the devices. The same is true for national advertising rules that impact the advertising of medical devices sold via the Internet. Medical device companies that experience difficulties with their (intended) Internet sales in EU member states should now definitely have an interest in taking a good look at whether the legislation concerned is proportionate.

Another important point of this case is that the European Court seems to view medical devices (at least OTC devices) as different from medicinal products, because it held in the DocMorris case that a categorical ban on Internet sales of both prescription and non-prescription medicinal products could not be justified altogether, although it did state that the supply of prescription medicinal products needs to be more strictly controlled [5]. It will be interesting to see if the European Court rules along the same lines in the case of prescription or high-risk medical devices. This seems however likely to happen.

[3]Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689

6 Intermezzo: Are Software and eHealth Services Medical Devices?

The foregoing analysis has important consequences for the eHealth services industry in the EU, because eHealth services and specifically the software provided for the therapeutic and/or diagnostic functionalities may very well constitute medical devices in the meaning of Directive 93/42 ("MDD") as amended [6]. In fact, many eHealth services and software provided for the provision thereof have characteristics that cause them to fall within the scope of the concept of 'medical device' as defined in the MDD. Any software provided as service or software application provided to an end user for diagnostic and/or therapeutic purposes will normally constitute a medical device caught with the scope of the MDD [7]. Indeed, with the adoption of Directive 2007/47 amending the MDD it has been clarified beyond doubt that standalone software can also constitute a medical device [8]. This has been recently supplemented by a new MEDDEV guidance document of the European Commission about standalone software under the MDD. That means that eHealth services constituting a medical device (software as service) or involving a medical device (locally installed app to provide the service) must be CE marked as required under the MDD and the local national implementation of that directive, because otherwise they are on the market illegally. In practice however many eHealth services and applications do not meet this requirement and the level of awareness of regulatory compliance on the part of developers of such products and physicians prescribing them is very low [9].

Typical candidates for inclusion in the scope of medical devices are for example remote monitoring tools that monitor the physical condition of a patient via the internet and include a software algorithm that warns a physician if the patient's parameters give cause for this. Another candidate would be remote readout and interpretation of blood values, like glucose or other critical values allowing a patient to adjust medication to the readout. As I have argued on other occasions, prime candidates are Internet websites that allow individuals to assess their health risks [10] or apps that psychiatric patients can use on their iPad to condition themselves for and report to their psychiatrist about otherwise threatening situations that may provoke panic attacks [11]. Another good example is a medical decision support system running on a central server provided to physician.

And finally many of the telemedicine applications mentioned in the Commission's Communication on telemedicine for the benefit of patients, healthcare systems and society[3] will fall within that scope. In my view therefore the legal situation with respect to telemedicine is a lot less unclear than the Commission states in its Communi-

[4]Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 8

cation on telemedicine for the benefit of patients, healthcare systems and society[4], because telemedicine services and their constituent software will largely be an information society service regulated under the e-Commerce directive and the MDD when provided at a distance. The software installed locally or running on servers will constitute standalone software in the scope of the MDD.

7 Consequences for eHealth Services Offered Online

Because the e-Commerce Directive also applies to the provsion of services, it applies likewise to medical devices that are sold through the internet as an eHealth service, as has been confirmed by the European Commission in the Explanatory Memorandum to the Cross-Border Healthcare Directive[5] and in the Communication on telemedicine for the benefit of patients, healthcare systems and society [6].

If we apply the reasoning in the Ker-Optika judgment, this means that EU member states cannot restrict the provision of eHealth services in general with the sole argument that the physical presence of the patient and the health professional in the same place is required at all times. This is for example one of the major obstacles to telemedicine mentioned in the Commission's Communication on telemedicine for the benefit of patients, healthcare systems and society.[7] This obstacle seems to have been removed by the Ker-Optika judgment. However, an EU member state could prescribe that (certain) eHealth services can only be offered after initial expert clinical intervention, e.g. after initial prescription by a physician or after an initial consult to define the parameters of the eHealth service.

In addition, in case of cross-border eHealth services EU member states may restrict the freedom to provide those on grounds of the protection of public health [12], provided however that

- the eHealth service concerned prejudices public health or presents a serious and grave risk of prejudice to those objectives and that
- the measures taken are proportionate to those objectives [13] and that
- the EU member state has concerned has asked the member state in which the provider is established to take measures and the latter did not take such measures, or they were inadequate, and notified the European Commission and the EU member state in which the provider is established of its intention to take such measures [14].

The Commission has indicated in its Communication on telemedicine for the benefit of patients, healthcare systems and society that

> "for business-to-business (professional-to-professional) telemedicine services, such as teleradiology, the country of origin principle applies: the service offered by the professional must comply with the rules of the Member State of establishment. In the case of business-to-consumer activities (which might be relevant to telemonitoring services) the contractual obligations are exempted from the country of origin principle: the service might need to comply with the rules of the recipient's country."[8]

It is unclear to me why the Commission would want to make this distinction between B2B and B2C eHealth services, as there is no clear basis for that in the e-Commerce directive.

As explained above, national rules on how medical devices may be provided fall within the scope of the rules on the free movement of goods. This does not however apply to eHealth services in the same way. In the Ker-Optika case the Court held that this was an unregulated field under the e-Commerce directive because "requirements applicable to the delivery of goods" were explicitly stated to be outside the coordinated field pursuant to article 2 (h) (ii) e-Commerce directive [15]. Consequently, the Court held, the national rules which relate to the conditions under which goods sold via the Internet may be supplied within the territory of a Member State fall outside the scope of that directive [17]. Article 2 (h) e-Commerce Directive that defines the coordinated field of the e-Commerce Directive does not contain a similar limitation of the scope of the directive for information society services, so these are fully within the scope of the e-Commerce directive. This means that eHealth service providers are fully subject to the internal market clause in article 3 of the e-Commerce Directive (free provision of services provided that the provider meets the requirements for the activity concerned of the member in which it is established). Those member states may pose requirements with which the service provider has to comply in respect of:

- the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification, and
- the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or

[5] See the explanatory memorandum to the Cross-Border Healthcare Directive, COM(2008) 414 final, p. 6

[6] Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 9

[7] Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 8

[8] Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 9

requirements concerning the liability of the service provider [16].

This means that it is very attractive to engage in forum shopping in the EU, because an eHealth services provider would logically establish itself in the EU jurisdiction with the most favourable eHealth regime and subsequently export that to the other member states via the internal market clause. Larger companies can choose out of which of their subsidiaries they will conduct their activities.

In their implementation of EU directives, member states have to observe the basic freedoms granted under the TFEU and the requirements that they may impose within the coordinated field have to be proportionate (see for example [18]). Member states have to be able justify the proportionality of their rules. Since the provisions on the free movement of services are highly similar (and some might argue identical) on the point of restriction of market access and possible justifications for them, the reasoning of the European Court in the Ker-Optika case would arguably be similar when applied to eHealth services. Whether or not a restriction in the form of a prior mandatory examination in person by a physician (as opposed for example to a video conference consultation) is justified, will depend on the risks associated with the condition that the eHealth service seeks to treat. Conversely, the fact that there is a high safety risk for users and patients if the eHealth service fails, is not as such an argument to prohibit an eHealth service for a particular purpose altogether but rather to require better risk management.

Finally, since the EU is not entitled to regulate healthcare as such [19], the scope and content of healthcare services will remain member state competence.[9] However, the Commission has stated that as a general principle the classification of specific telemedicine services as medical acts should ensure that these meet the same level of requirements as equivalent non-telemedicine services (e.g. teleradiology vs. radiology).[10] This principle ensures that adequately regulated health services are not replaced by less regulated telemedicine services and it avoids discrimination between providers of the same service, which would be incompatible with the e-Commerce Directive.[11] This principle is also reflected in the intention of the EU to regulate diagnostic testing services provided from outside the EU in the new EU medical devices regulation which is currently in preparation [20].

One other important point is that any member states' rules that have an impact on eHealth services are most likely technical regulations caught under Directive 98/34/EC as amended by Directive 98/48/EC. This directive establishes a procedure which imposes an obligation on Member States to notify the Commission and each other of all draft technical regulations "concerning products and Information Society Services, including telemedicine"[12], before they are adopted in national law. If this has not taken place the European Court has ruled "that breach of the obligation to notify renders the technical regulations concerned inapplicable, so that they are unenforceable against individuals" (see for example [21] and [22]) As a result, eHealth providers have a strong instrument to use against technical measures impacting on eHealth services that have not gone through the notification procedure correctly and were duly scrutinized by the European Commission.

8 Conclusion

The Ker-Optika case confirms many of the legal assumptions that the Commission has previously made about the legal status of e-Health services. eHealth services that constitute medical devices fall within the scope of the e-Commerce directive. As a result, advertising and sales of these services are covered by that directive. Also the way the services are provided is harmonised under the e-Commerce directive and although it may still be regulated by EU member states in certain detail, such regulation must meet the proportionality requirements for restrictions on the free provision of services. If member states take measures to regulate e-commerce in eHealth services, they must notify these to the European Commission for them to be enforceable against companies and private persons.

References

[1] C-108/09 of 2 December 2010, not yet published

[2] MEDDEV 2.1/6 January 2012, Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices

[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 2000 L 178/1

[4] C-322/01 of 11 December 2003, [2003] ECR I-14887; see for discussion of the case Vollebregt, E.R.: Vrij verkeer van goederen en geneesmiddelenverkoop via het internet, Nederlands tijdschrift voor Europees recht 2004 p.65-70; Koenig, Christian; Meurer Friederike; Engelmann, Christina: Das EuGH-Urteil "Deutscher Apothekerverband/Doc Morris", Europäisches Wirtschafts- Steuerrecht - EWS 2004 p.65-72; Lang, Richard: Common Market Law Review 2005 p.189-204 and Mand, Elmar: Internationaler Versandhandel mit Arzneimitteln, Gewerblicher Rechtsschutz und Urheberrecht, internationaler Teil 2005 p.637-647

[5] C-322/01 of 11 December 2003, [2003] ECR I-14887, point 117

[9] Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 9

[10] Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 9

[11] Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 10

[12] Commission Communication on telemedicine for the benefit of patients, healthcare systems and society, 4 November 2008, COM (2008) 689, p. 9

[6] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ L 169, 12.7.1993, p. 1–43, Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices, OJ L 189, 20.7.1990, p. 17–36 and Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices, OJ L 331, 7.12.1998, p. 1–37

[7] Vollebregt, E.R., Kluemper, M., "The Regulation of Software for Medical Devices in Europe", Journal of Medical Devices Regulation (JMDR), May 2010, p. 4-13, see http://medicaldeviceslegal.com/tag/software/

[8] Vollebregt, E.R., Kluemper, M., "The Regulation of Software for Medical Devices in Europe", Journal of Medical Devices Regulation (JMDR), May 2010, p. 4-13 See http://medicaldeviceslegal.com/tag/software/ and COCIR's decision tree on software as medical device at http://www.cocir.org/uploads/documents/-48-cocir_medical_software_qualification_as_medical_device_-_22_nov_2010.pdf

[9] http://www.eucomed.org/blog/84/59/eHealth-applications-and-websites-developed-by-clinicians-there-are-rules-for-that-33/

[10] http://medicaldeviceslegal.com/2011/01/13/ehealth-and-clinicians/

[11] http://www.eucomed.org/blog/84/59/eHealth-applications-and-websites-developed-by-clinicians-there-are-rules-for-that-33/

[12] Article 3 (2) juncto article 4 (a) (i) 2nd indent Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 2000 L 178/1

[13] Article 4 (a) (ii) and (iii) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 2000 L 178/1

[14] Article 4 (b) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 2000 L 178/1

[15] C-108/09 of 2 December 2010, not yet published, point 29

[16] Article 2 (h) (i) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 2000 L 178/1

[17] C-108/09 of 2 December 2010, not yet published, point 30

[18] C-315/92 Clinique [1994] ECR 317, point 17

[19] Article 168 TFEU

[20] Presentation of Jcqueline Minor of DG SANCO, European Commission at the DIA Euromeeting on 26 March 2012

[21] C-194/94 CIA Security International [1996] ECR I-2201, point 54

[22] C-303/04 LIDL Italia [2005] ECR I-7865, point 23

