Data Protection in Connected Health Ecosystems

Hana Horak [1], Hrvoje Belani [2], Igor Ljubi [2]

[1] University of Zagreb, Faculty of Economics and Business, J. F. Kennedy 6, HR-10000 Zagreb, Croatia; [2] Croatian Health Insurance Fund, Margaretska 3, HR-10000 Zagreb, Croatia
hhorak@efzg.hr, {hrvoje.belani; igor.ljubi}@hzzo.hr

Abstract. The term Connected Health has been coined to encompass various terms that describe different recent advances in ICT-enabled healthcare. In parallel with the efforts to increase availability and quality of the healthcare services while lowering the costs through employing various ICT solutions, special attention should be given to data protection issues in such systems. Naturally, medical data of a person are the most sensitive data, and as such require protection not only by institutions involved in healthcare provision but all the stakeholders in healthcare-related processes. This paper focuses on data protection in Electronic Health Records. We present the legal basis for establishing and maintenance of the EHR in Member States of the European Union. Based on the legislation, we discuss the data protection efforts being done by various Member States, and propose a unified European approach on the protection of personal data in EHRs. As a case study, we present the situation in Croatia, which has recently started the designing phase of EHR implementation. Before the conclusion, we are reviewing challenges that lie ahead in data protection of EHRs and comment suggested workarounds to deal with them.

Keywords: Data protection, Connected health, Electronic health record, Information security, User privacy

1 Introduction

Connected health includes terms such as eHealth, Digital Health, mHealth, tele health, tele care, remote care, and assisted living. It encompasses terms such as wireless, digital, mobile, and tele-health and refers to a conceptual model for health management where devices, services or interventions are designed around the patient's needs, and health related data is shared, in such a way that the patient can receive care in the most proactive and efficient manner possible [1]. All stakeholders in the process are 'connected' by means of timely sharing and presentation of accurate and pertinent information regarding patient status through smarter use of data, devices, communication platforms and people. In connected health technology is vital and exciting – but it is just one part of a much wider context which includes patient care pathways, business and revenue models, data analytics and more. Connected health consolidates information from many different spheres of one person's world to give a more complete picture of their health.

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

Data protection is crucial and the most important issue in process of connecting and consolidating information. European citizens' right to healthcare and protection of personal data [2] are recognised in the Charter of Fundamental Rights of the European Union (EU) [3]. According to the definitions in Action plan [4], eHealth is the use of ICT in health products, services and processes combined with organisational change in healthcare systems and new skills. eHealth covers the interaction between patients and health-service providers, transmission of data from one institution to other, or peer to peer communication between patients and/or health professionals. It should be borne in mind that eHealth is not limited to providing support to healthcare on the national level, but also in great extent facilitates the cross-border healthcare services. Legal and ethical issues are wide and will arise not only in terms of the data sharing, but also in terms of identity certification, professional accreditation and liability for provided care. The legal and regulatory issues include also administrative regulations such as those of reimbursement, and – in the context of cross-border care – the mutual recognition of professional qualifications and the complex issue of entitlement to care [5]. In order to enable all actions within the Member States (abbr. MSs), the European Commission (EC) has established European eHealth Network (eHN) [6]. Regulatory framework has been set up [7] and accompanied for a better implementation with a set of guidelines [8] which are in the form of recommendations, rather than legally binding.

Prior experiences shown that it is always difficult to find the right path when applying the Directive. This is due to the fact that the aim of the Directive is to establish the rules facilitating access to safe and high quality cross border health care on the internal market as well as to ensure mobility of the patients and to promote the cooperation between MSs. On the other hand, this process should fully respect the responsibilities of the MSs for the definition of the social security benefits relating to health and for the organisation and delivery of the healthcare [8]. This two very different aims in its nature are not always easy to achieve [9]. Health services are originally regulated under national legislation. The focus is on the citizen and social benefits (services) provided at national level, but which has to be in line with Treaty on functioning of the EU [10]. The idea on supranational/national level is to remove all existing obstacles and establish interoperability between healthcare systems within EU MSs until 2020. Bringing down the legal barriers should be among the priority actions, since the deep analysis and studies [11] have shown that the main discrepancies are between different regulatory frameworks of the MSs and within the different stages of implementation of EU legal actions on national level [12]. Within the eHN one of the most important issues, beside the data protection, are standardisation of European Health Record systems and laws [13].

2 European Health Record and Data Protection Issues

European Health Record [13] (EHR) has been recognised as a one of the cornerstones of eHealth revolution [14]. EHR *in favorem* of patients facilitate sharing of information, cross border, between all interested stakeholders [15]. On the other hand, data protection issues have been recognised as one of the major challenges in the implementation process of eHealth [4].

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

Despite the opportunities and benefits, major barriers hamper the wider uptake of eHealth. Detected barriers are: (a) lack of awareness of, and confidence in eHealth solutions among patients, citizens and healthcare professionals; (b) lack of interoperability between eHealth solutions; (c) limited large-scale evidence of the cost-effectiveness of eHealth tools and services; (d) lack of legal clarity for health and wellbeing mobile applications and the lack of transparency regarding the utilisation of data collected by such applications; (e) inadequate or fragmented legal frameworks including the lack of reimbursement schemes for eHealth services; (f) high start-up costs involved in setting up eHealth systems; (g) regional differences in accessing ICT services, limited access in deprived areas. As the health records contain the most sensitive information concerning an individual, unauthorised disclosure of a medical condition or diagnosis could impact negatively the individual's personal and professional life. Interoperability [14] of EHRs involves transfer of personal data concerning a patient's health. These data should be able to flow freely from one MS to another, but at the same time the fundamental rights of the individual should be safeguarded. The European Data Supervisor has been established within the Regulation EC 45/2011 [16] and aims to protect the fundamental rights and freedoms [17] of natural persons, and in particular their right to privacy with respect to the processing of personal data.

The fundamental rights in relation with the data protection are contained in several acts, apart from the regulatory framework of the EU, beginning from the European Convention on Human Rights (Art. 8) and restriction laid down in Art. 8.2 of the Council of Europe Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (Art. 10). Convention for the Protection of human Rights and dignity of human being with regard to the application of biology and medicine and also the Case Law of the European Court of Human Rights. On the EU level provisions are contained in TFEU, Art. 16 and the provisions of the Charter of Fundamental Rights, when MSs implementing EU law. Cross border exchange and interoperability of eHealth and related data is enabled within the provisions of Directive 20011/247EU and Directive on ePrescription [18] and the Case Law of the Court of Justice of the EU. According to [15, 19], there is obvious priority to administrative interest rather than giving priority to individuals' right to confidentiality. The main problem arises from the fact that concept of confidentiality [19] is often equated with privacy rights, because both deals with protection of privacy [20]. The conclusion is that relation between confidentiality and privacy must be supported by the full information from the health service provider so patients or healthcare service recipients' autonomy is fully respected.

3 New Proposals for Personal Data Protection

Effective data protection is vital for building trust in eHealth. It is also a key driver for its successful cross-border deployment, in which harmonisation of rules concerning cross border exchange of health data is essential [4]. Beside all the positive effects the room for criticism and organized scepticism should be left. Within the EU legal system we still don't have such a liability mechanism and system of tort litigation like for e.g. in USA [21].

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

The competent authority within the MS lays down a comprehensive legal framework for interoperable EHR systems, that in particular: (a) analyse different personal data protection impacts of organisational alternatives for storing personal data concerning health and establish organisational structures for EHR systems; (b) guarantee the patient's self-determination by allowing for the patient's autonomous and freely taken decision, as to which personal data concerning health are to be stored and disclosed to whom in his or her EHR unless expressly required by national law; (c) establish that EHR systems are designed according to the "least personal data as possible" principle; (d) provide an assessment of the information security risks and personal data protection impacts prior to the implementation of an EHR system; (e) clarify the extent to which categories of personal data concerning health should be made available in electronic form or online; (f) prescribe that processing of personal data in EHR systems must be required and carried out only by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person subject to an equivalent obligation of secrecy; (g) determine the conditions under which health data contained in EHR systems can be lawfully accessed and processed by persons other than the individual concerned; (h) ensure that patients are fully informed on the nature of the data and the EHR structure; (i) provide for special measures to prevent patients from being illegally induced to disclose their personal data contained in EHR systems; (j) make sure that any processing – especially the storage – of personal data in EHR systems takes place within jurisdictions applying Directive 95/46/EC or those with an adequate level of protection of personal data; (k) lay down detailed auditing requirements for the purpose of ensuring compliance with data protection obligations; (l) guarantee the confidentiality of EHR systems as well as provide for appropriate technical and organisational measures, including rules on incident detection and management processes.

Analysis provided in [22] shows that within the 28 MSs and Norway there are different approaches regarding the EHRs systems and laws. There are major disparities between countries on the deployment of EHRs as a part of an interoperable infrastructure that allows different healthcare providers to access and update health data in order to ensure the continuity of care of the patient. Regarding the EHRs content and interoperability aspects, the comparative analysis shows that two broad approaches can be distinguished: some countries have set detailed requirements as to the content of EHRs, while others do not specify what should be content [22]. The analysis shows that EHR systems in all countries apply standardised terminology and some form of codification to categorise health data. It is shown that less than half MS have regulated this obligation within respective national regulation. In practice, EHR systems in the MS usually do not use the same standards regarding terminology and coding systems. Also the Overview consider this differences as one of the main barriers to the cross-border transfer of health data. Another problem is that almost half of the countries still don't have specific rules for institutions hosting and managing EHRs. Implemented rules of Directive 95/46/EC, in national regulation is still only rules regulating authorisation requirements. The Overview shows that regarding Patient consent some countries require explicit consent of the patient for the creation of an EHR. Some countries do not require explicit consent for the creation of an EHR but this explicit consent is needed for the

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

inclusion of (data extracted from) this EHR into an EHR sharing system. There are some countries that do not require explicit consent neither for the creation of an EHR nor for the inclusion of (data extracted from) this EHR into a sharing system, but patient consent is needed for the access to the data in the EHR by other healthcare professionals than the one who collected the data [22]. Directive 95/46/EC [22] regulates that the data processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. In the small number of MS that grants the same access rights for different types of health professionals those rights are not in line with Directive 95/46/EC. Half of the MS have different rules for different types of health professionals, depending on the link between the patient and the different health professionals or by assigning to the healthcare providers the task of deciding which health professionals have access to which data. According to the Overview patient's rights over the data in all MS patients are entitled to access their EHRs and in half of them this right covers actually all data contained in EHRs. Unfortunately, as stated before regarding the liability, results of the Overview shows that there are currently no detailed rules on the liability of health professionals with regard to health records in the EU. According to the comparative analysis, only a handful of countries have established specific medical liability rules with regard to EHRs, and these rules are mostly reinforcing or highlighting the general liability regime.

According to some authors when IT meets healthcare, the legal framework have to accommodate rapidly. It is not always easy and it is not that fast in practice when implementing EU rules and harmonising national rules. Beside the remaining issue of standardisation the right balance between national and supranational public health policy remains the challenge [23]. From the findings of the Overview it is obviously that in the EU MSs the regulation on data protection is based on Data protection Directive 95/46 and possibility that comes from the implementation of directive as a legal instrument [24] [25], different national laws and ways of implementation led to almost 28 different levels of data protection. EU General Data Protection Regulation [26] allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Personal data in documents held by a public authority or public body may be disclosed by that authority or body in accordance with Union or MS law regarding public access to official documents, which reconciles the right to data protection with the right of public access to official documents and constitutes a fair balance of the various interests involved.

4 Croatian Perspective on Electronic Health Records

Back in 2011, the Academy of Medical Sciences of Croatia has published the „Declaration on eHealth“ in order to alert all stakeholders (patients, health professionals, institutions, government bodies, suppliers) to use the immense potential of information and communication technologies and solutions for improving health care in Croatia [27]. The Declaration draws attention to the areas of infrastructure, such as: education, regulation and standardization, medical and health informatics as a profession, the obligation of institutions, government bodies and suppliers.

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

Regarding the data protection legislation in Croatian eHealth, general regulations are implemented. The authorised users are obliged to assure the confidentiality of medical data according to the relevant regulations set in the Data Protection Law and the Law on protection of personal data. The Law on Protection of personal data prescribes that the following offences will be charged with a fine. Central Information System of Croatian Healthcare (Abbr. CEZIH in Croatian) is a centralized information system which is based on the following guidelines:

- System is using virtual private network (VPN) to interconnect every medical practices of the primary healthcare with the Croatian Health Insurance Fund (CHIF) and Croatian Public Health Institute.
- Medical doctors and nurses gain access to the system through the applications installed in their practises, and two institutions have made their information systems interoperable with CEZIH
- Every application from the medical practices have to be certified by CHIF.
- Training process to work with the software in the medical practices is the responsibility of its respective manufacturers.

We are currently implementing the Central EHR, which uses the data which are currently being exchanged through the CEZIH system from the following mechanisms: ePrescription, eReferral for Laboratory diagnostics in Primary Health Care, eReferral (to specialist diagnostics or care, once it will be implemented), reports after examinations (for four specialist groups), and report on work absence.

Legislation in Croatia relevant to health data protection: (1) Law on Health Protection; (2) Law on Medical Practice; (3) Law on Protection of patient rights; (4) Law on Protection of Personal Data; (5) Law on Data Protection; (6) Law on Access to Information. On the basis of the Law on Data Protection, the Law on Protection of Personal Data and the Law on Access to Information the Managing Committee of the Croatian Health Insurance Fund has approved, as an internal act, the Act on data protection and the right to access information of the Croatian Health Insurance Fund. The management, storage, assembly and use of medical information belonging to a patient with mandatory health insurance in the Central Information System of Croatian Healthcare (abb. CEZIH in Croatian) as well as the management of the personal health records in electronic form have been regulated by the below mentioned Acts: (1) The Act on managing, storing, assembly and use of medical documentation of patients in the Central Information System of Croatian Healthcare; (2) Act on use and protection of data from the medical documentation of patients in the Central Information System of Croatian Healthcare; (3) Act on Managing the personal healthcare record in electronic form. The appropriated sanctions to be implemented in the case of breach of the data protection procedures have been prescribed in Art. 21 of the Act on Data Protection which states that in the case an employee should breech the rules of the aforementioned act, this would be treated as a gross misconduct. The Law on Medical practice prescribes sanctions for physicians in the case that they do not manage and/or use medical documentation according to the relevant legislation. The Law on Protection of Personal Data prescribes sanctions in all other cases.

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

Data from the insured person's personal EHR are electronically submitted to the CEZIH for safekeeping. The architecture of the CEZIH allows doctors to view both the medical and the personal data of their patients. Communication between practitioners and other institutions is ciphered, and the medical data completely separated from the administrative data. In such a way the system itself is assuring that the institutions get only depersonalised information on various medical conditions that they track. Furthermore, only authorised personnel from the institutions (CHIF, CPHI, Ministry of Health, etc.) have access to the data stored in CEZIH. They can then only use the data to create reports which are needed based on the legislation, or to make statistical analysis with the medical data. Authorised persons are obliged to maintain the data confidentiality during and beyond their employment in their respective institutions. The physician is responsible to upkeep precise, detailed and dated medical documentation according to procedures of managing medical documentation of patients, which can, in any moment, provide relevant information on the medical condition of the patient and the status of its treatment. The physician and/or the responsible person of the healthcare institution are obliged to safe keep the data on medical treatment of the patients up to 10 years after the treatment has been finished. After that period, they have to perform actions defined in the proceedings on medical documentation. For research and reporting purposes, various mechanism for data obfuscating have been employed, making it virtually impossible to re-identify the patient. To be fully compliant with both national and European legislation, the patient will be offered a written consent by which he/she will authorise medical practitioners (other than their family doctors) to gain access to the most relevant data in their EHR. Also there will be a possibility to take back the access authorisation, also in a written form. However, data from the transactional mechanisms such as ePrescription and eReferral will be transferred to the EHR database for every patient, whether he/she have gave consent to access to the data to some medical practitioner or not. In such a way it is insured that, if the patient decide to give to authorisation to a practitioner afterwards, all the relevant data about his health status is already in the system. The obligation for managing informational consent of subjects of care is clearly stated in the ISO 27799:2008 international standard on Health informatics – Information security management in health using ISO/IEC 27002, where data protection is one of the main information security guidelines for the health sector. Security and data protection mechanisms are considered through three segments: (1) Network segment and system architecture; (2) application security; (3) specific data access functionalities. Considering security risks, it is crucial to point-out that the implementation allows only reading of the data, and not one functionality offers the option of data altering in the database. The only data recorded are the ones related to the administrative part of the HER application, with two main functionalities: (1) Patient consent management; (2) EHR access log management. Access to this part of the system has the patient, in order to have full control and overview of the consent-related decisions, as shown in Table 1, as well as who and when has accessed the data. Due to the possible emergency situations, which would require access to the data without the possibility for a patient to explicitly render his/her consent, a system will provide for „break the glass" mechanisms. This way of accessing the data will be clearly marked and „use in life threatening situations only" and those situations will be carefully logged.

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

Table 1. Authentication levels for access to patients' EHR

Auth. level	*Access granularity*	*Description*
1	Patient does not allow any access to the data	Practitioners can search for the patient in the database, view the basic identification data and are informed that the patient has refused to give them permission to access his/her medical data
2	Patient has gave only the limited access to the data only for the chosen practitioners in primary healthcare level	Other users can only view the basic identification data and are informed that the patient has refused to give them permission to access his/her medical data
3	Patient gives full access with prior consent	Primary level practitioners can view all of the patient's data, and the other users can view basic identification data and the information that a written consent is needed from the patient to access other data. This can be issued for the period of 1, 15 or 30 days
4	Patient gives full access to the data	Access to the data have all authorised users with no need for a specific consent

Medical practitioner is responsible for the medical documentation about its patients. That documentation, according to the aforementioned legislation, upon request can be given to the institutions such as Ministry of health, Croatian Medical Chamber or judicial authorities. This request will also be logged in the system, with a note of the name of the person who have made the request. Patient can also request to view all of his/hers medical documentation, and the practitioner is obliged to fulfil the patient's request.

5 Discussion and Conclusion

Main issues regulated in the proposal are right to erasure, data access and correction. The proposal contains meaningful balance between freedom of expression and freedom of information in line with the protection of personal data as confirmed in the recent Court of Justice of the EU judgement. Due to the fact that consent wasn't clearly enough defined within the national laws of MS and applied, informed consent is a cornerstone of this proposal. According to the EU Parliament there must be more rights to information and transparency. The information must be understandable for the users. Strong sanctions are also proposed for the companies up to two percent of global annual turnover. The idea is to discourage companies from data protection violations regarding the personal data which forms one of the fundamental rights.

Important efforts are being made in harmonised enforcement of the rules which must be ensured by the European data protection Board. This centralized approach, with only one data protection authority on EU level like in EU competition law is still discussed

S. Loshkovska, S. Koceski (Editors): ICT Innovations 2015, Web Proceedings, ISSN 1857-7288

by the MSs. Maybe the proposed EU General Data Protection Regulation will help to regulate issues bearing in mind direct effect of regulation as a regulatory tool and trying to regulate issue on supranational level? But question remains are the legal actions fast enough to ensure flow of personal data.

Regarding the eHealth data protection efforts in Croatia, CHIF has been working recently on establishing a security assessment framework for eHealth in Croatia, allowing country-level practices and perspectives on cyber defence, information security and data protection in e-health to be considered in a holistic manner. The framework covers assessment criteria on different levels: from national security and critical infrastructures to personal data protection and user and information privacy, as well as dealing with various cyber security aspects in government-to-government, government-to-citizen and government-to-business categories of e-government ecosystem. Security assessment criteria are grouped into and analysed through four interoperability aspects: legal, technical, semantic and organizational.

Acknowledgement

This work was supported by TD COST Action TD1405 – "European Network for the Joint Evaluation of Connected Health Technologies" (ENJECT).

References

1. B.M. Caulfield, S.C. Donnelly: What is Connected Health and why will it change your practice? QJM Monthly Journal of the Association of Physicians, No. 106, pp. 703-707. (2013)
2. Directive 95/46/EC of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of European Communities 281/131 (1995)
3. Charter of Fundamental Rights of the European Union (2000/C 364/1)
4. European Commission: eHealth Action Plan 2012-2020: Innovative care for the 21st century, COM(2012) 736 (2012)
5. Z. Kolitsi, V. Stroetmann, M. Thonnet: EU eHealth Interoperability Roadmap; Calliope Network, European Commission (2010)
6. eHealth Network, URL: http://ec.europa.eu/health/ehealth/policy/network/index_en.htm [accessed: 01/06/2015]
7. The Directive on the Application of Patient's Rights in Cross Border Health care 2011/124/EU, Official Journal of European Communities 88, pp. 45 (2011)
8. Key documents on eHealth of the European Commission, URL: http://ec.europa.eu/health/ehealth/key_documents/index_en.htm [accessed: 01/06/2015]
9. H. Horak, N. Bodiroga Vukobrat, K. Dumančić: Utjecaj Direktive 24/2011/EU o pravima pacijenata i implementacija u pravo Republike Hrvatske, zbornik radova s konferencije „Suvremeni pravni izazovi EU-Mađarska-Hrvatska", Pravni fakultet Sveučilišta u Pečuhu i Pravni fakutet Sveučilišta J.J. Strossmayera, Osijek, 2012, ISBN 978-963-642-473-2, 978-953-6072-68-2, pp. 533-553 (2012) (in Croatian)
10. Treaty of Lisbon amending the Treaty on the European Union and the Treaty Establishing the European Community, Official Journal of European Communities 306/17 (2007)

11. Overview of the national laws on electronic health records in the EU MSs and their interaction with the provision of cross-border eHealth services Final report and recommendations, URL: http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf [accessed: 01/06/2015]
12. Commission Implementing Decision of 22 December 2011 providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on eHealth (2011/890/EU). URL: http://ec.europa.eu/health/ehealth/docs/decision_ehealth_network_en.pdf [accessed: 01/06/2015]
13. Commission recommendation on cross-border interoperability of electronic health record systems, C(2008) 3282, pp. 56 (2008)
14. E. Rynning: Public Trust and Privacy in Shared Electronic Health Record, European Journal of Health Law, Vol.14, No.2 2007, pp. 107 (2007)
15. M. Hartlev: Striking the Right Balance: Patient's Rights and Opposing Interests with Regard to health Information, European Journal of Health Law 14, pp. 167 (2007)
16. Regulation (EC) No 45/2001 of the European Parliament and of The Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJL 8 (2001)
17. N. Bodiroga-Vukobrat, H. Horak, H., A. Martinović: Temeljne gospodarske slobode u Europskoj uniji (Croatian), Inženjerski biro, ISBN 978-953-262-057-3, Zagreb, Croatia (2011)
18. Directive 2012/52/EU of 20 December 2012 laying down measures to facilitate the validation of medical prescriptions issued in another Member State, URL: http://ec.europa.eu/health/cross_border_care/docs/impl_directive_presciptions_2012_en.pdf [accessed: 01/06/2015]
19. K. Dulčić, N. Bodiroga-Vukobrat: Protection of Patient's Personal Data in European and Croatian Law, Conference Proceedings, University of Rijeka, Croatia, pp. 1-42 (2008)
20. T.L. Beauchamp, J.F. Childress: Principles of Biomedical Ethics, 5th edition, Oxford University Press, New York, pp. 340 (2011)
21. S. Hoffman, A. Podgurski: eHealth Hazards.Provider Liability and Electronic Health Record Systems, Case research paper series in legal studies - working paper 09-25, pp. 1527 (2009)
22. Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations, Contract 2013 63 02, Health Programme of the European Union, July 23, 2014. URL: http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf
23. De PaulJ.Health Carestr.22 article Information technology meets…
24. S. Rodin, T. Ćapeta: Osnove prava Europske unije, Gradivo za cjeloživotno obrazovanje pravnika, Zagreb, Croatia (2009) (in Croatian)
25. H. Horak, K. Dumančić, J. Pecotić Kaufman: Uvod u europsko pravo društava, Školska knjiga, Zagreb, Croatia (2010) (in Croatian)
26. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council 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), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)
27. Declaration on eHealth, Academy of Medical Sciences of Croatia, Zagreb, URL: http://www.amzh.hr/news%20and%20events.html (2011) [accessed: 01/06/2015]