Data Protection and Human Rights Components of the Integrated Health Information System (EU-IHIS) Project

- Consultancy Report -

Authors: Solvita Olsena, Dr.iur., MD and Sarah Emami, JD-MPH

Final version – June 2014

Visibility: Public

Target Audience:
EU-IHIS Stakeholders

This document has been produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.
Acknowledgements

The consultants would like to acknowledge the kind support received from the EU-IHIS project staff, the WHO Serbia Country Office, and the WHO European Regional Office. We would especially like to thank those individuals from the following institutions who took the time to meet with us: General Hospital Pirot, the Ministry of Health, Members of the Working Group for Development of the Draft Law on Healthcare Records, the Commissioner for Information of Public Importance and Personal Data Protection, the Serbian Medical Chamber, the National Health Insurance Fund, the Patient Rights Ombudsman’s Office and the Office of the Ombudsman.
# Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHRB</td>
<td>Convention on Human Rights and Biomedicine, CoE</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>DLHR</td>
<td>Draft law on health records</td>
</tr>
<tr>
<td>DPD</td>
<td>Data protection directive 46/95/EC</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EHR</td>
<td>electronic health record</td>
</tr>
<tr>
<td>EMR</td>
<td>electronic medical record</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EU-IHIS</td>
<td>EU funded project on integrated health information system</td>
</tr>
<tr>
<td>GDPR</td>
<td>Draft of the EU General Data Protection Regulation</td>
</tr>
<tr>
<td>HIS</td>
<td>hospital information system</td>
</tr>
<tr>
<td>IHIS</td>
<td>integrated health information system</td>
</tr>
<tr>
<td>LPDP</td>
<td>Law on personal data protection</td>
</tr>
<tr>
<td>PRL</td>
<td>Patients’ rights law</td>
</tr>
<tr>
<td>WHO</td>
<td>World Health Organization</td>
</tr>
</tbody>
</table>
Table of Contents

Summary of consultancy report ....................................................................................................... 6
Conclusions ....................................................................................................................................... 12
Executive Summary .......................................................................................................................... 14
I. Overview of data security and privacy .......................................................................................... 17
   A. Current landscape and challenges in data security and privacy ............................................... 17
   B. Summary of relevant European policy and law ......................................................................... 18
      Council of Europe human rights framework ........................................................................... 18
      EU overview ............................................................................................................................ 22
   C. WHO Policy Framework ......................................................................................................... 25
   D. Serbia legislation on data privacy ............................................................................................ 25
II. Key recommendations .................................................................................................................. 27
    Incorporating key principles ....................................................................................................... 27
    Explicit consent exemption ....................................................................................................... 28
    Opt-in vs opt-out systems for EHR ............................................................................................ 30
    Vital interests exemption .......................................................................................................... 31
    Other exemptions ....................................................................................................................... 31
    Proposed GDPR exemption on processing of health data ......................................................... 32
    Principle of purpose determination and legality principle ...................................................... 34
    Principle of proportionality ........................................................................................................ 34
    Principle of minimization of processing .................................................................................... 35
    Principle of respecting special rights of an individual .............................................................. 36
    Right to access health data ........................................................................................................ 36
    Right to make a copy of health record ....................................................................................... 38
    Right to accurate and up-to-date data ....................................................................................... 38
    Right to “seal and lock” ............................................................................................................. 39
    Principle of limited storage periods of personal data ............................................................... 40
    Principle of providing data security measures .......................................................................... 40
    Patient summaries ..................................................................................................................... 42
    Governance of the eHealth and structure of the EHR ............................................................... 43
    Stakeholder engagement ............................................................................................................ 46
    Training ...................................................................................................................................... 46
    Terminology and usage .............................................................................................................. 47
    Transition from written to electronic records (Article 37) ......................................................... 48
III. Conclusions ............................................................................................................................... 49
Annex One: Key documents and references .................................................................................... 50
Summary of consultancy report

eHealth can be defined as the use of information and communication technologies (ICT) for health. eHealth can benefit citizens, patients, health and care professionals but also health organizations and public authorities. When applied effectively, eHealth delivers more personalized ‘citizen-centric’ healthcare. This approach is targeted, effective and efficient and helps to reduce errors and the length of hospitalization. It also facilitates socio-economic inclusion and equality, quality of life and patient empowerment through greater transparency, access to services and information and the use of social media for health.1

eHealth systems are most effective when they respect patients’ rights and data protection principles. In light of the proposed Serbian draft law on Electronic Health Records, this paper sets out relevant Council of Europe (CoE), European Union (EU) standards and regulations, key Serbian laws and strategies, and the WHO policy frameworks for eHealth. It is crucial to assure strong trust by all into eHealth infrastructures and applications. This requires legal and regulatory certainty, challenges which are among the most demanding aspects of eHealth. Privacy, confidentiality, data protection and liability issues are involved.2

While implementing and operating the eHealth systems, Serbia as a party of the European Convention on Human Rights (ECHR) should provide protection of the right to respect for private and family life stated by the Art. 8 of the Convention. Protection of human rights with regard to the application of medicine is required by the Convention on Human Rights and Biomedicine (CHRB). Art. 1 provides: “Parties to this Convention shall protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine.” As Serbia’s EHR system falls within the scope of this provision, it should be developed and operated in a manner protecting human rights and fundamental freedoms as requested by these conventions.

The CoE has been developing a substantial legal framework with respect to the protection of personal medical data by adopting legally binding treaties within general human rights frameworks, as well as putting strong emphasis on protection of patients’ rights. The human rights framework of the CoE has been further developed by the case law of the European Court of Human Rights (ECtHR). The ECtHR reiterates that the protection of personal data, not least medical data, is of fundamental importance to a person’s enjoyment of the right to respect for his or her private life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve confidence in the medical profession and in the health services in general.3 Consequently, domestic law must therefore afford appropriate

---

2 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. IX
safeguards to prevent any communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention.⁴

Medical data constitute part of one’s private life. The collection of such data by any state institution or other third party constitutes an interference with one’s right to respect for his/her private life. Accordingly, medical data collection, processing and other actions should be classified as an interference with one’s right to respect for private life. It has to be determined whether the interference provided by law or by practice complies with the requirements of the second paragraph of Article 8 of the Convention, i.e. that the processing of health data should be in accordance with the law, the law should state a legitimate aim and that processing should be necessary in a democratic society.

The EU legal framework draws from the ECHR and the constitutional traditions common to member states⁵, as well as the Charter of Fundamental Rights of the European Union⁶. The Charter instrument recognizes both the fundamental right to privacy (Art 7)⁷, and the fundamental right to the protection of personal data (Art 8). Article 8 mandates that data concerning individuals must be processed fairly, for specified purposes, and on the basis of their consent or a legitimate basis laid down by law, that everyone has a right to access and rectify the data collected concerning them, and that compliance with these rules shall be subject to control by an independent authority.

The EU respects the freedom of each Member State (MS) to decide what type of health care it considers appropriate. eHealth and EHR as part of health care is the responsibility of the individual State in all related matters – legislation, financing and governance. It should be emphasized that the deployment of health ICT systems is entirely a national competence.

However, the EU has the competence to regulate cross border health care issues. Directive 2011/24/EU provides rules for facilitating access to safe and high-quality cross-border healthcare and promotes cooperation between MS, taking full account of national competencies in organizing and delivering healthcare.

In 2013, the EU eHealth network adopted Guidelines on minimum/nonexhaustive patient summary datasets for electronic exchange in accordance with the cross-border Directive 2011/24/EU⁸. The primary focus of the guidelines is to support the objective of continuity of care and patient safety across borders. The guidelines focus on emergency or unplanned care in a cross-border context. The secondary focus of the guidelines is for reference use at national level. The aims of implementing the Patient Summary dataset are:

- to ensure access to safe and high-quality healthcare;
- to achieve a high level of trust and security;
- to enhance the continuity of care for individual patients.

---

⁴ Case of L.L. v. France, Application no. 7508/02, § 44 and Z v. Finland, § 95
⁷ “Everyone has the right to respect for his or her private and family life, home and communications”
The WHO Declaration on the Promotion of Patients' Rights in Europe constitutes a common European framework for action and includes general principles. It has played a key role in the development of patients’ rights in Europe. The WHO Declaration and other WHO initiatives on patients’ rights promotion, like training or expert consultancies, has promoted development of patients’ rights legislation in numerous European countries.

Health 2020 is a European health policy framework adopted by the 53 Member States of the Region. It aims to support action across government and society to: “significantly improve the health and well-being of populations, reduce health inequalities, strengthen public health and ensure people-centred health systems that are universal, equitable, sustainable and of high quality”. Serbia is currently developing a national health policy aligned with Health 2020. The EHR under discussion fall into Health 2020’s third priority area, which addresses inter alia people-centred health systems.

Controllers and processors of health data in general and in the context of EHR applications must comply with all **general human rights and data protection principles**, including the following:

- principle of special treatment of health data as sensitive data;
- principle of determination of processing personal data in the law (act or statute) – legality principle;
- principle of minimisation of processing;
- use limitation principle (purpose principle);
- principle of proportionality;
- the data quality principle;
- principle of limited storage periods of personal data;
- principle of respecting special rights of an individual: right to information on processing his/her personal data, right to access her/his own personal data, right to object;
- principle of providing data security measures; and
- principle of the right to an effective remedy.

**Protection of sensitive personal data.** All data contained in medical documentation, in EMR and in EHR systems, should be considered “sensitive personal data”\(^9\). With respect to health data, there is an established double protection system, where general legal requirements for personal data protection and sensitive personal data protection should be applied simultaneously. Additionally, the general human rights and privacy protection framework shall be applied.

The starting point of EU law on health data is Art. 8 (1) of the Data protection directive (DPD), which prohibits the processing of health data: “The Member States shall prohibit [...] the processing of data concerning health or sex life.”. The particular legal framework in order to serve appropriate protection of this special category of data should be developed in Serbia. We recommend improved clarification and definition the scope of personal health data in the Serbian law.

In the health care sector other categories of personal data, for example, data on health care professionals, are often processed. There are processed anonymised data aggregated from personal

---

\(^9\) Working Document on the processing of personal data relating to health 00323/07/EN WP 131 in electronic health records (EHR)
health data as well. Therefore it can be recommended to develop if necessary and to clarify application of definitions related to different sorts of personal and non-personal data used in health care. To secure appropriate treatment of personal health data, development of a separate protection system would be appropriate way to protect this domain of sensitive data. The definitions of different groups of personal data, if appropriate, should be compatible within a national and international legal framework.

Explicit consent. One justification for the processing of sensitive data can be the consent of the data subject (Art. 8 (2) of DPD). An important point is that in order to be valid, consent – whatever the circumstances are in which it is expressed – must be a “freely given, specific and informed indication of the data subject’s wishes. Consent in the case of sensitive personal data and therefore in an EHR must be explicit, and opt-out solutions are not sufficient.\textsuperscript{10}

The current DHRL does not appear to give patients a choice about the creation of an EHR neither allows to “opt-out. This consultancy strongly recommends that requirement to obtain consent of the patient is carefully considered and addressed. There is necessity to discuss relevant factors for implementation of opt-in for EHR. Such approach would be in line with the relevant EU legal framework. In order to choose opt-out model, there should be legal analysis of Serbian human rights, constitutional law and data protection legal framework provided, exploring the legality of the opt-out system introduced.

Vital interests exemption. DPD Art. 8 (2)(c) provides an exception to the prohibition on processing where “processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent”. Here, processing must relate to essential individual interests of the data subject or of another person and it must – in the medical context – be necessary for a life-saving treatment in a situation where the data subject is not able to express his intentions\textsuperscript{11}.

It is recommended to consider amending the regulations on health data protection, by incorporating the exception to process health data without consent in the case of vital interests of the data subject or another person where there is no possibility to obtain consent. The drafters should also consider the appropriate use of this exception for the processing data of the EHR in case of medical emergencies.

Other interests exemption. DPD Art. 8 (3) of the Directive provides exception of prohibition and allows health data processing “where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed 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 also subject to an equivalent obligation of secrecy”. As it is possible to observe throughout the text drafted for the DHRL and other relevant documents on eHealth systems, appropriate application in the purpose determination and limitation, proportionality and data minimisation principles is lacking at the present stage of the process. Therefore we could recommend a review of the DHRL and other relevant provision in the light requirements for application of these principles. For the purpose

\textsuperscript{10} WP 131, p.8,9
\textsuperscript{11} WP 131, p. 9, 10
limitation principle, we would recommend using the Article 29 Working party opinion on purpose limitation.

Respecting and protecting the individual patients’ rights. This principle relates to respect for the rights of the individual with respect to processing his/her personal data, accessing his/her personal data, or objecting to the processing of such data. Pursuant to Article 10 of the DPD, data controllers processing information in EHR systems must provide certain information to data subjects, such as information on the identity of the controller, on the purposes of the processing, on the recipients of the data and on the existence of a right of access. Therefore it is recommended to develop and implement a system providing information to data subjects, such as information about the identity of the controller, the purposes of the processing, recipients of the data and the existence of a right of access.

Right to access. DPD Art. 12 establishes the right for individuals to have access to their personal data concerning their health. Serbian legal provisions on health data and patients’ rights place insufficient focus on the individual patient’s rights in respect to access, control and use on of health data. The implementation of patients’ right to access should be addressed as early as possible in the process in order to develop an appropriate legal framework, technical tools and implementation programme. This will secure substantial progress in achieving promotion of patients’ rights through the EHR system.

The right to obtain a copy of medical record is stated in Serbian law. In order to respond to potential requests from patients using eHealth tools, it is recommended to introduce a system capable of providing electronic copies of health data upon request.

Right to accurate and up-to-date data. Article 12 of the DPD provides data subjects with the ability to check on the accuracy of the data and to ensure that the data are kept up to date. These rights fully apply to the collection of personal data in EHR systems. Patients’ rights with respect to amending incorrect health data should be elaborated by the draft law. Additionally, procedural tools to exercise these rights should be provided by law and implemented into practice.

It is suggested that the drafters of the law/planners establish a system capable of controlling accuracy of data and correcting mistakes as soon as they are discovered. This system may include regular quality audits, strong involvement of end-users in identification, correction and improvement, options to submit an inaccuracy reports by users, effective responses to identified problems by IT personnel, necessary technological improvements, and regular training for users where issues related to data accuracy are discussed.

Right to “seal and lock”. There is an established right in many EU countries allowing the patient to restrict access to his medical record in some part. This is done in order to safeguard protection of sensitive data and to enhance patient’s control over his information. The right to “seal and lock” certain aspects for electronic health records should be enshrined in both the Serbian law on medical records and in the EHR system.

Principle of limited storage periods of personal data. This principle requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further

---

12 WP131, p. 12
13 For example, UK or Sweden
processed. Therefore health data should be collected in an EHR and stored for only a limited period of time. Reconsideration of the proposed storage periods for EMR and EHR is suggested, as substantial portions of medical records are outdated in 2, 5, or 10 years and there is little justification for keeping them longer.

**Principle of providing data security measures.** Article 17 of the DPD imposes an obligation upon data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure. The measures can be organizational or technical. It should be determined what measures would be appropriate from Serbian perspective, so that this can be incorporated into the DHRL.

This consultancy recommends the amendment of legal provisions with regard to privacy and security of the EHR in order to ensure minimum quality of the service and to protect patients’ legal interests. The legal requirements included in the GDPR, Art. 30 should be used as a basis for establishing these rules. The law could set out the conditions for accessing EHR, conditions for sharing EHR, obligation to report security breaches and other security-related requirements. It is also recommended to provided data protection impact assessment for the newly developed EHR system; to ensure regular tests, assessments and evaluations of security risks in the EHR; and to develop additional security measures to ensure situational awareness of the risks and the ability to take preventive, corrective and mitigating actions in near real-time against vulnerabilities or incidents detected that could pose a risk to the data.

**Patient summary.** The current draft law on health care records does not address patient summaries per se. Drafters of the law may wish to consider the incorporation of patient summaries, containing basic medical and administrative information about the patient, which will allow health professionals to quickly view relevant information about the patient. This will be in line with recommendations of the current eHealth Network.

**Governance of eHealth and EHR.** The text of the draft law fails to provide complete information on how the governance of eHealth system will be organised. There are missing provisions on how database/es for electronic medical records will be created, which institution will have the legal authority to establish database of electronic medical records and what principles will govern operation of proposed database. There are different ways of addressing this issue across the EU and there will need to be a determination of the best ways to manage this from a Serbian perspective. It should be stressed, that the governance of eHealth system is of crucial importance and should be strengthened by developing, implementing and operating eHealth platform constantly.

Careful planning, organisational setup, and stakeholder involvement are key success factors for eHealth projects. Such bodies in part resolve the challenge of potentially ambiguous or distributed responsibilities for eHealth. Although they are not a sufficient condition for success, it seems they are a necessary ingredient.\(^\text{14}\)

**Training.** “The most important part of eHealth investment that needs expanding is the eHealth skills and knowledge of healthcare staff and ICT suppliers’ staff. An expanded capability is essential to

---

\(^\text{14}\) Ibid, p. X
achieve more success and so help to boost eHealth investment.”\textsuperscript{15} The consultancy would like to recommend the development and implementation of eHealth training programmes for health care practitioners, administrative and IT personal of health care institutions. Training opportunities for patients could also be provided.

**Transition from written to electronic records.** Implementation of eHealth tools to process medical records will take substantial time and there will be need to use paper medical records and electronic medical records parallel for some time. To facilitate implementation of EMR and EHR, the requirement for health care providers to keep the information in paper format should be minimised as much as possible as well as initiatives to use electronic means should be supported. Special regulations for transition period should be enacted in order to secure proper and safe use of two forms of records.

There are number of health databases existing in Serbia already, and furthermore the development of new health databases has been proposed by the draft law and by eHealth implementation tools. In order to have an overview of the integrated health information system in Serbia, a graphic with relevant detailed information about the content of each aspect of the system would be helpful for drafters of the law and those working in the area. This graphic could contain existing databases (like EMR) and proposed databases, such as EHR.

**Terminology and usage.** There is a need for clear terminology and consistent usage of terms throughout the draft law and the eHealth system. It has been noted that there are certain inconsistencies in definitions between the draft law and the Law on Personal Data Protection. Additionally, a number of terms appear in the “definitions” section which do not appear elsewhere in the law. In order to promote consistency throughout the application of this draft law within the Serbian legal system, these differences should be examined and reassessed. This will also assist in the objective of promoting clarity for medical practitioners and patients.

**Conclusions**

eHealth systems are rapidly becoming part of the health care system in Serbia and in other countries, and that the development of these systems is progressing rapidly and dynamically. While they will bring substantial promise in terms of health care improvements, these systems require defined confidentiality policies implemented by law and in practice, and defined security policies which are stated by law, developed by technology and implemented by users. The key elements of trust, transparency, openness towards all stakeholders, security, quality and efficiency should be present in discussions from the outset. Because of the swift implementation of these systems and rapid developments in the area of eHealth, it is difficult to address these issues through lengthy considerations and discussions.

There is already substantial knowledge on some eHealth tools collected by European countries working with EMR and implementing EHR. Wherever possible, these European experiences should be used, adopted and modified according to Serbian needs. Furthermore, numerous academic, policy

and technology related events on eHealth developments are organized by European universities, EU institutions and NGOs. Participation in these may secure knowledge transfer to and from Serbia. Additionally, the EU-IHIS project team has been developing a substantial framework for implementation of eHealth systems. It would be important to secure continuity and to use all relevant preparations for more general development of EHR.

This topic and the scope of the consultancy was broad and complicated. The authors of this report did extensive research into the topic, taking into account Serbian existing legal framework as well as proposed legislation, the existing and proposed legal EU framework, EU-IHIS project documentation, the CoE legal framework as well as articles and other research material. There is a great deal of research which could be carried out in this area, and specific areas of interest might be explored in the future. For instance, two issues which are quite important but which were not addressed given the limited time frame include (1) the protection of children and other vulnerable patient groups and (2) ethical dimensions. However, for this report we did our best to respect the limits set by the consultancy agreement and prepared the report accordingly.
Executive Summary

eHealth can be defined as the use of information and communication technologies (ICT) for health. eHealth can benefit citizens, patients, health and care professionals but also health organizations and public authorities. When applied effectively, eHealth delivers more personalized ‘citizen-centric’ healthcare. This approach is targeted, effective and efficient and helps to reduce errors and the length of hospitalization. It also facilitates socio-economic inclusion and equality, quality of life and patient empowerment through greater transparency, access to services and information and the use of social media for health.¹⁶

eHealth systems are most effective when they respect patients’ rights and data protection principles. In light of the proposed Serbian draft law on health records (DLHR), the initiative to develop an Integrated Health Information System (IHIS) as well as Electronic Health Records (EHR), this paper sets out relevant Council of Europe (CoE), European Union (EU) standards and regulations, key Serbian laws and strategies, and the WHO policy frameworks for eHealth. Key recommendations are set out below:

Key recommendations:

1. The particular legal framework in order to serve appropriate protection of personal health data should be developed in Serbia. We would recommend clarifying and defining the scope of personal health data in the Serbian law, as there are many categories of data as well as processed anonymised data aggregated from personal health data. Therefore it can be recommended to develop if necessary and to clarify application of definitions related to different sorts of personal and non-personal data used in health care. To secure appropriate treatment of personal health data, development of a separate protection system would be an appropriate way to protect this domain of sensitive data. The definitions of different groups of personal data, if appropriate, should be compatible within a national and international legal framework.

2. The current draft law on health records (DLHR) does not appear to give patients a choice about the creation of an EHR, with no “opt-out”, though Article 48 does give a patient the right to inspect the record. This consultancy strongly recommends that requirement to obtain consent of the patient is carefully considered and addressed. There is necessity to discuss relevant factors for implementation of opt-in for EHR. Such approach would be in line with the relevant EU legal framework. In order to choose an opt-out model, a legal analysis of Serbian human rights, constitutional law and the data protection legal framework should be conducted, exploring the legality of the opt-out system introduced.

3. The drafters should consider amending the regulations on health data protection (LPDP), by incorporating the exception to process health data without consent in the case of vital interests of the data subject or another person where there is no possibility to obtain consent. The drafters should also consider the appropriate use of this exception for the processing data of the EHR in case of medical emergencies. This recommendation is suggested for consideration to the Secretary for Personal Data Protection and the relevant ministry (in charge of the implementation and adoption of a law on personal data protection).

4. As it is possible to observe throughout the text drafted for the DLHR and other relevant documents on eHealth systems, appropriate application in the purpose determination and limitation, proportionality and data minimisation principles is lacking at the present stage of the process. Therefore we could recommend a review of the DHRL and other relevant provision in the light requirements for application of these principles. For the purpose limitation principle, we would recommend using the Article 29 Working party opinion on purpose limitation.

5. Planners should develop and implement a system providing information for patients to provide certain information to data subjects, such as information about the identity of the controller, the purposes of the processing, recipients of the data and the existence of a right of access.

6. The implementation of patients’ right to access should be addressed as early as possible in the process in order to develop an appropriate legal framework, technical tools and implementation programme. This will secure substantial progress in achieving promotion of patients’ rights through the EHR system.

7. In order to respond to potential requests from patients, introduce a system capable of providing electronic copies of health data upon request.

8. Patients’ rights with respect to amending incorrect health data should be elaborated by the draft law. Additionally, procedural tools to exercise these rights should be provided by law and implemented into practice.

9. It is suggested that the drafters of the law/planners establish a system capable of controlling accuracy of data and correcting mistakes as soon as they are discovered. This system may include regular quality audits, strong involvement of end-users in identification, correction and improvement, options to submit an inaccuracy report by users, effective responses to identified problems by IT personnel, necessary technological improvements, and regular training for users where issues related to data accuracy are discussed.

10. The right to “seal and lock” certain aspects for electronic health records should be enshrined in both the draft law and in the EHR system.

11. Reconsideration of the proposed storage periods for EMR and EHR is suggested, as substantial portions of medical records are outdated in 2, 5, or 10 years and there is little justification for keeping them longer.

12. This consultancy recommends the amendment of legal provisions with regard to privacy and security of the EHR in order to ensure minimum quality of the service and to protect patients’ legal interests. The legal requirements included in the GDPR, Art. 30 should be used as a basis for establishing these rules. The law could set out the conditions for accessing EHR, conditions for sharing EHR, obligation to report security breaches and other security-related requirements. It is also recommended to provide data protection impact assessment for the newly developed EHR system; to ensure regular tests, assessments and evaluations of security risks in the EHR; and to develop additional security measures to ensure situational awareness of the risks and the ability to take preventive, corrective and mitigating actions in near real-time against vulnerabilities or incidents detected that could pose a risk to the data.

13. The current draft law on health care records does not address patient summaries per se, though contents of the patient information are spelled out in Articles 13 and 14. Drafters of the law may wish to consider the incorporation of patient summaries, containing basic medical and
administrative information about the patient, which will allow health professionals to quickly view relevant information about the patient. This will be in line with recommendations of the current eHealth Network (which developed the guidelines on minimum dataset) and the EPSOS project patient summaries.

14. The text of the draft law fails to provide complete information on how the governance of eHealth system will be organised. There are missing provisions on how database/es for electronic medical records will be created, which institution will have the legal authority to establish database of electronic medical records and what principles will govern operation of proposed database. There are different ways of addressing this issue across the EU and there will need to be a determination of the best ways to manage this from a Serbian perspective. It should be stressed, that the governance of eHealth system is of crucial importance and should be strengthened by developing, implementing and operating eHealth platform constantly.

15. The consultancy would like to recommend the development and implementation of eHealth training programmes for health care practitioners, administrative and IT personal of health care institutions. Training opportunities for patients could also be provided.

16. Implementation of eHealth tools to process medical records will take substantial time and there will be need to use paper medical records and electronic medical records parallel for some time. To facilitate implementation of EMR and EHR, the requirement for health care providers to keep the information in paper format should be minimised as much as possible as well as initiatives to use electronic means should be supported. Special regulations for transition period should be enacted in order to secure proper and safe use of two forms of records.

17. There are number of health databases existing in Serbia already, and furthermore the development of new health databases has been proposed by the draft law and by eHealth implementation tools. In order to have an overview of the integrated health information system in Serbia, a graphic with relevant detailed information about the content of each aspect of the system would be helpful for drafters of the law and those working in the area. This graphic could contain existing databases (like EMR) and proposed databases, such as EHR.
I. Overview of data security and privacy

A. Current landscape and challenges in data security and privacy

eHealth can be defined as the use of information and communication technologies (ICT) for health. eHealth can benefit citizens, patients, health and care professionals but also health organizations and public authorities. When applied effectively, eHealth delivers more personalized ‘citizen-centric’ healthcare. This approach is targeted, effective and efficient and helps to reduce errors and the length of hospitalization. It also facilitates socio-economic inclusion and equality, quality of life and patient empowerment through greater transparency, access to services and information and the use of social media for health.

eHealth systems are most effective when they respect patients’ rights and data protection principles. In light of the proposed Serbian draft law on Electronic Health Records, this paper sets out relevant CoE, EU standards and regulations, key Serbian laws and strategies, and the WHO policy frameworks for eHealth.

Closely related and complementary is the need to assure strong trust by all into eHealth infrastructures and applications. This requires legal and regulatory certainty, challenges which are among the most demanding aspects of eHealth. Privacy, confidentiality, data protection and liability issues are involved.

There are several important issues which are beyond the scope of this report. This includes telemedicine and electronic medical devices which convey patient data, ePrescribing, the use of medical data for research purposes and the application of mHealth technologies. The use of EHR for the purpose of public health protection and re-use of anonymised health data is touched upon in this report, but detailed analysis of this topic would require much broader scope of research in Serbian law and practice and is not analysed in detail here.

The implementation of EHR might be considered from a number of different perspectives, each with its own key issues:

<table>
<thead>
<tr>
<th>Perspective</th>
<th>Key Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual</td>
<td>Protection of privacy, use of medical data, need for information, right to be informed, right to decide on interventions, control of your personal information, right to be compensated for wrongful actions</td>
</tr>
<tr>
<td>State</td>
<td>Protection of individual rights; protection of public health and wellbeing; duties of medical practitioners; requirement to safeguard equitable access to health</td>
</tr>
</tbody>
</table>

18 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. IX
B. Summary of relevant European policy and law

Under the terms of reference of this consultancy, the authors were requested to provide recommendations on patients’ rights and human rights, within the framework of the European Union and under the principles of the Council of Europe. Accordingly, a brief summary of these policies is presented below.

Council of Europe human rights framework

In 1950, the Council of Europe (CoE) Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) was adopted. While implementing and operating the eHealth systems, State parties of the ECHR should provide protection of the right to respect for private and family life (Art. 8): Everyone has the right to respect for his private and family life, his home and his correspondence.

ECHR Art. 8 (2) generally prohibits public authority interference into an individual’s private life, stating certain exceptions when interference may be legitimate:

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

With technological advances and more complex privacy concerns, the protection of personal data was later guaranteed in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)\(^\text{20}\), which was adopted by the Council of Europe in 1981. At the same time, the Organization for Economic Co-operation and Development (OECD) issued guidelines to its members, urging the introduction of measures to protect personal information.

\(^{19}\) Convention on Human Rights and Biomedicine, Article 3

With respect to the protection of human rights with regard to the application of medicine, in 1997 CoE adopted the Convention on Human Rights and Biomedicine (CHRB). The overall purpose of patients’ rights protection system is stated in Art. 1 “Parties to this Convention shall protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine.” As Serbia’s EHR system falls within the scope of this provision, it should be developed and operated in a manner protecting human rights and fundamental freedoms as requested by the Convention.

The primacy of the human being is stated in the Art. 2 of the Convention - “The interests and welfare of the human being shall prevail over the sole interest of society or science”. Priority is given to the former, which must in principle take precedence over the latter in the event of a conflict between them.  

CHRB Art. 10 addresses the right to private life and right to information regarding health:

1. Everyone has the right to respect for private life in relation to information about his or her health.
2. Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.
3. In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient.

The first paragraph establishes the right to privacy of information in the health field, thereby reaffirming the principle introduced in Art. 8 of the ECHR and reiterated in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Under Article 6 of the latter Convention, personal data concerning health constitute a special category of data and are as such subject to special rules.

The second paragraph establishes that individuals are entitled to know any information collected about their health, if they wish to know. This right is of fundamental importance in itself but also conditions the effective exercise of other rights such as the right of consent set forth in Article 5 of the CHRB. A person's "right to know" encompasses all information collected about his or her health, whether it be a diagnosis, prognosis or any other relevant fact. The "right to know" goes hand in hand with the "right not to know", which is provided for in the second sentence of the second paragraph.

The final paragraph states that in exceptional cases domestic law may restrict on the right to know or not to know in the interests of the patient's health. In some cases, the doctor's duty to provide information, also covered under Article 4, conflicts with the interests of the patient's health. It is for domestic law, taking account of the social and cultural background, to solve this conflict. Where

---

22 Ibid, para 63
23 Ibid, para 66, 67
appropriate under judicial control, domestic law may justify the doctor sometimes withholding part of the information or, at all events, disclosing it with circumspection ("therapeutic necessity").\textsuperscript{24}

The right to privacy stated in the Art. 10 of the CHRB may be restricted as provided by Article 26 (1): *No restrictions shall be placed on the exercise of the rights and protective provisions contained in this Convention other than as are prescribed by law and are necessary in a democratic society in the interest of public safety, for the prevention of crime, for the protection of public health or for the protection of the rights and freedoms of others.*

Certain restrictions on the exercise of the right to privacy are possible for one of the reasons and under the conditions provided for in under Article 26.1. For example, a judicial authority may order that a test be carried out in order to identify the author of a crime (exception based on the prevention of a crime) or to determine the filiation link (exception based on the protection of the rights of others).\textsuperscript{25}

The Council of Europe has been developing a substantial legal framework with respect to the protection of personal medical data by adopting legally binding treaties within general human rights frameworks, as well as putting strong emphasis on protection of patients’ rights. The human rights framework of the CoE has been further developed by the case law of the European Court of Human Rights (ECtHR).

The ECtHR reiterates that the protection of personal data, not least medical data, is of fundamental importance to a person’s enjoyment of the right to respect for his or her private life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve confidence in the medical profession and in the health services in general.\textsuperscript{26} Consequently, domestic law must therefore afford appropriate safeguards to prevent any communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention.\textsuperscript{27}

Medical data constitute part of one’s private life. The collection of such data by any state institution or other third party constitutes an interference with ones right to respect for his/her private life. Therefore medical data collection, processing and other actions should be classified as an interference with one’s right to respect for private life. It has to be determined whether the interference provided by law or by practice complies with the requirements of the second paragraph of Article 8 of the Convention, i.e. that the processing of health data should be in accordance with the law, the law should state a legitimate aim and that processing should be necessary in a democratic society.

Medical data processing should be in accordance with the law. It is well established in the ECtHR case law that the wording “in accordance with the law” requires the impugned measure both to have

\textsuperscript{24} Ibid, para 69
\textsuperscript{25} Ibid, para 69
\textsuperscript{27} Case of L.H. v. Latvia, Application no. 52019/07, § 56, Z v. Finland, cited above, § 95, and Varapnickaitė-Mažyliénė v. Lithuania, no. 20376/05, § 44, 17 January 2012
\textsuperscript{27} Case of L.L. v. France, Application no. 7508/02, § 44 and Z v. Finland, § 95
some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.\(^\text{28}\)

In the case that the law restricts rights, the domestic law must afford adequate legal protection against arbitrariness. Accordingly the domestic law must indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.\(^\text{29}\)

When considering the application of the Art. 8 (2) in the case of interference with private life by retention of fingerprints and cellular samples and DNA profiles (individual personal information) after the criminal proceedings had ended with an acquittal or had been discontinued, the ECtHR stressed: “is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness”.\(^\text{30}\)

The ECtHR stressed the requirement for the state to state a legitimate aim for the interference with private life. When providing any third party with a right to receive medical data, the law should explicitly state the legitimate purpose for the collection of data, for the processing of data and, if applicable, for the storage of data.

The restriction of private life by processing of health data may well be necessary in a democratic society. An interference will be considered “necessary in a democratic society” for a legitimate aim if it answers a “pressing social need” and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are “relevant and sufficient”. While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention.\(^\text{31}\)

The ECtHR, in the judgment of case where collection of medical data by the state institution without consent of the patient was questioned, has looked for evidence on how “potentially decisive” the data could be for achievement of purposed aim. The ECtHR found a violation of Art. 8 due to an indiscriminate collection of medical data. The Court noted “that the MADEKKI – a Latvian Health inspectorate, appears to have collected the applicant’s medical data indiscriminately, without any prior assessment of whether the data collected would be “potentially decisive”, “relevant” or “of importance” for achieving whatever aim might have been pursued by the MADEKKI’s inquiry.”\(^\text{32}\)

When the data controller is considering data disclosure and a state institution requires personal

\(^{28}\) Case of S. and Marper v. the UK, Applications no. 30562/04 and 30566/04, §99

\(^{29}\) Case of L.H. v. Latvia Application no. 52019/07, § 47

\(^{30}\) Case of S. and Marper v. the UK, Applications nos. 30562/04 and 30566/04, § 99

\(^{31}\) Ibid, § 101

\(^{32}\) Case of L.H. v. Latvia, Application no. 52019/07, § 58
health data, the ECtHR decisions emphasize the need to evaluate “whether the contested measure was therefore subject to important limitations and was accompanied by effective and adequate safeguards against abuse”\textsuperscript{33}.

To clarify protection of personal health data, the CoE has issued the Recommendation No.R (97) 5 of the Committee of Ministers to Member States on the protection of medical data \textit{(Adopted by the Committee of Ministers on 13 February 1997)}\textsuperscript{34}, which has to be applied in the development of eHealth systems.

**EU overview**

The EU legal framework draws from the European Convention of Human Rights (ECHR) and the constitutional traditions common to member states\textsuperscript{35}, as well as the Charter of Fundamental Rights of the European Union\textsuperscript{36}. The Charter instrument recognizes both the fundamental right to privacy (Art 7)\textsuperscript{37}, and the fundamental right to the protection of personal data (Art 8). Article 8 mandates that data concerning individuals must be processed fairly, for specified purposes, and on the basis of their consent or a legitimate basis laid down by law, that everyone has a right to access and rectify the data collected concerning them, and that compliance with these rules shall be subject to control by an independent authority.

Electronic Health Records (EHR) have been present on the EU policy and law agenda since 2000. In 2004, the first eHealth action plan was published\textsuperscript{38} and implemented through policy initiatives, research projects and legislation. The eHealth Action Plan 2012-2020 “Innovative healthcare for the 21st century” provides a roadmap to empower patients and healthcare workers, to link devices and technologies, and to invest in research towards the personalized medicine of the future. \textsuperscript{39} The Action Plan emphasizes cross-border activities, but it should be noted that work at the EU level has a strong effect at the national level and vice versa. Therefore, the Action Plan encourages national and regional authorities, healthcare and social care professionals, industry, patients, service providers, researchers and EU Institutions to work together closely. \textsuperscript{40}

As set out in Article 168 (7) of the Treaty on the Functioning of the European Union (TFEU), Member States retain responsibility for providing safe, high quality, efficient and quantitatively adequate healthcare to citizens on their territory. The EU respects the freedom of each Member State to

\textsuperscript{33} Case of M.S. v. Sweden, Application No. 74/1996/693/885, § 43

\textsuperscript{34} Recommendation No.R (97) 5 of the Committee of Ministers to Member States on the protection of medical data

\url{https://wcd.coe.int/ViewDoc.jsp?id=571075&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=E1B021&BackColorLogged=F5D383} and Explanatory Memorandum

\url{http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/EM_R%2897%295_EN.pdf}


\textsuperscript{36} Charter of Fundamental Rights of the European Union, OJ C 83 30 March 2010.

\textsuperscript{37} “Everyone has the right to respect for his or her private and family life, home and communications”

\textsuperscript{38} \url{http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF}


\textsuperscript{40} Ibid.
decide what type of health care it considers appropriate. eHealth and EHR as part of health care is the responsibility of the individual State in all related matters – legislation, financing and governance. It should be emphasized that the deployment of health ICT systems is entirely a national competence.

However, the European Union has the competence to regulate cross border health care issues. Under Article 168(1) of the Treaty on the Functioning of the European Union (TFEU), a high level of human health protection is to be ensured in the definition and implementation of all Union policies and activities, as well as when the Union acts under other Treaty provisions. Article 114 TFEU is the legal basis aimed to improve the functioning of the internal market and the free movement of goods, persons and services; Article 114(3) TFEU explicitly requires that, in achieving harmonization, a high level of protection of human health is to be guaranteed taking account in particular of any new development based on scientific facts.41

Based on TFEU Articles 114 and 168, the Union adopted 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. Directive 2011/24/EU provides rules for facilitating access to safe and high-quality cross-border healthcare and promotes cooperation between Member States, taking full account of national competencies in organizing and delivering healthcare.

Article 14 states:

1. The Union shall support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States.

2. The objectives of the eHealth network shall be to:

(a) work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare;

(b) draw up guidelines on:

   (i) a non-exhaustive list of data that are to be included in patients’ summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders; and

   (ii) effective methods for enabling the use of medical information for public health and research;

(c) support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.42

Accordingly, the eHealth Network was established in 201143 and since then has been working to implement tasks provided by the Directive. In 2013 the eHealth network adopted Guidelines on

---

41 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
42 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
minimum/nonexhaustive patient summary datasets for electronic exchange in accordance with the cross-border Directive 2011/24/EU. The primary focus of the guidelines is to support the objective of continuity of care and patient safety across borders, as stated in Article 14 (2) (b) (i) of the Directive. The guidelines focus on emergency or unplanned care in a cross-border context. The secondary focus of the guidelines is for reference use at national level. More advanced and elaborate Patient Summaries exist in some Member States (MS), but the eHealth Network agreed that the guidelines could serve as a common baseline for Patient Summaries at national level. The aims of implementing the Patient Summary dataset are:

- to ensure access to safe and high-quality healthcare;
- to achieve a high level of trust and security;
- to enhance the continuity of care for individual patients.

The measures proposed are not legally binding and shall take full account of the responsibilities of the Member States for the organization and delivery of health services and medical care.

The provisions of Directive 95/46/EC on the protection of personal data and free movement of such data are the legal basis for using personal health data. According to Article 8 of the Directive, the legal foundations for using personal data will be the explicit consent to the processing of data (Article 8 (2) (a)), vital interests (Article 8 (2) c, i.e. medical emergencies (Article 8 (2) (c)) or the necessity for healthcare purposes (Article 8 (3) (b)). The present legal framework will be amended in due time when the proposed General Data Protection Regulation (GDPR) is adopted by EU legislative bodies, and so at this point, we are in a transition period of data protection system within the EU. With respect to health data, the proposed GDPR will provide more harmonized conditions for the processing of health data in EU Member States and across borders.

In the Working Document on the processing of personal data relating to health in electronic health records (EHR), the Article 29 Working Party provides guidance on the interpretation of the applicable data protection legal framework for EHR systems and explains some of the general principles. The Working Document also gives indications on the data protection requirements for setting up EHR systems, as well as the applicable safeguards. The authors of this report will use this document as an authoritative source for interpretation of EU data protection law in application of EHR. A detailed description of this framework is given under the related key recommendations.

---

43 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
44 Guidelines on minimum/nonexhaustive patient summary dataset for electronic exchange in accordance with the cross-border Directive 2011/24/EU
45 Ibid. p.3
46 Ibid. p. 5
47 At the writing this report the Draft of Data protection regulation legislation is not likely to be passed before 2015, followed by a two-year period of preparation for enactment.
discussed later in this paper. With respect to the purpose limitation requirement, the Article 29 Working party issue opinion⁴⁹ is also used as authoritative source for this report.

C. WHO Policy Framework

The WHO declaration of patients’ rights was developed at a 1994 European Consultation on the Rights of Patients under the auspices of the WHO Regional Office for Europe (WHO/EURO). The purpose was to define principles and strategies for promoting the rights of patients, within the context of the health care reform process underway in most countries.

The Declaration on the Promotion of Patients’ Rights in Europe constitutes a common European framework for action and includes those principles, as endorsed by the Amsterdam Consultation. It has played a key role in the development of patients’ rights in Europe. The WHO Declaration and other WHO initiatives on patients’ rights promotion, like training or expert consultancies, has promoted development of patients’ rights legislation in numerous European countries. Today, principles stated by the Declaration form key aspects of patients’ rights protection systems all over Europe. However, implementation of patients’ rights protection is still a challenging task in many contexts.

Health 2020 is a European health policy framework adopted by the 53 Member States of the Region during the sixty-second session of the WHO Regional Committee for Europe in September 2012. It aims to support action across government and society to: “significantly improve the health and well-being of populations, reduce health inequalities, strengthen public health and ensure people-centred health systems that are universal, equitable, sustainable and of high quality”. Serbia is currently developing a national health policy aligned with Health 2020. The electronic health records under discussion fall into Health 2020’s third priority area, which addresses inter alia people-centred health systems.

When completed in 2016, the Framework for Action towards Coordinated/Integrated Health Service Delivery will provide a roadmap for implementing one of the Health 2020 priority policy areas relating to people-centred health systems. Launched in October 2013, the Framework aims to support countries with policy options and recommendations that target key areas for strengthening the coordination/integration of health services. These changes are in line with the vision of Health 2020 and the values of universal health coverage. Potential benefits of more coordinated and integrated services can reduce adverse outcomes associated with fragmented care; improved access coordinated transfer and use of information by providers; and empowerment of patients⁵⁰.

D. Serbia legislation on data privacy

Existing Serbian legislation and policy providing the legal framework and environment regarding the further development of the integrated health information system (IHIS) and eHealth includes:

---

- Serbian Constitution
- Law on Health Care
- Law on Personal Data Protection\(^{51}\)
- Law on Patients’ Rights;
- Strategy for Information Society Development in the Republic of Serbia until 2020;
- Government decree about the Program of work, development and organization of an integrated health information system - "e-Health";
- The *Strategy for the Prevention and Control of Chronic Non-Communicable Diseases of Serbia*\(^{52}\) provides that in order to control chronic diseases, the strengthening of information and knowledge includes, among other things, the development of a national health information system and the adoption of legislation in order to ensure privacy, confidentiality and security of information.
- The *Integrated Health Information System (EU-IHIS)* is a 2.5 million Euro project funded through European Union (EU) Pre-accession assistance (IPA). The project foresees implementation of hospital information systems (HIS) in 19 selected hospitals throughout Serbia as well as development of electronic health record (EHR). The purpose of the EU-IHIS is also the improvement of information and communications technologies used in the health system of the Republic of Serbia. Based on the functions and mandate of the health institutions, the project will address issues like data entry, flow and sharing, data security, patients rights and privacy.

During their consultancy visit in Belgrade, the authors of this report met with a number of national institutions and organisations involved in the protection of patient’s rights, responsible for health care policy, human rights and data protection - namely the Ministry of Health, Members of the Working Group for Development of the Draft Law on Healthcare Records, the Commissioner for Information of Public Importance and Personal Data Protection, the National Health Insurance Fund, the Patient Rights Ombudsman’s Office in Belgrade and the Office of the Ombudsman. Valuable insight with respect to implementation of hospital electronic medical records was provided by health care and IT professionals in Pirot hospital. A meeting with Serbian Medical Chamber provided view of professionals on EHR development in Serbia. These meetings provided important information on implementation of patient’s rights principles in Serbian health care system and secured fruitful discussion on eHealth development and challenges, and the authors are extremely grateful that authorities from those office found time in their busy schedules to support this project. The authors throughout the consultancy have also been supported by EU-IHIS project staff, the WHO Serbia Country Office, and the WHO European Regional Office.

---

\(^{51}\) Law on Personal Data Protection (Official gazette of the Republic of Serbia, Nos. 97/2008 and 104/2009) - (*original language version: Zakon o zaštiti podataka o ličnosti*).

\(^{52}\) "Official Gazzette of the RS", n. 22/2009
II. Key recommendations

This consultancy has reviewed relevant EU-IHIS Project technical documentation, with the view of providing recommendations for further developments and improvements. It has reviewed proposed technical solutions focusing on data security and privacy, enabling for the data to be available to relevant health providers in accordance with patients’ needs for health services and treatment.

Below are set out key recommendations for further steps regarding the data protection and human rights aspects in the development of health information systems at all levels and eHealth in Serbia.

Incorporating key principles

Often, legislation includes principles to guide its interpretation and implementation. These may be explicit – i.e. a specific section in the law which sets out relevant principles – or more implicit, and reflected in the content of the law. This consultancy would recommend that there be consideration of incorporating key principles which are set out below into the draft law.

Controllers collecting data in the context of EHR applications must therefore comply with all general human rights and data protection principles, including the following:

- principle of special treatment of health data as sensitive data.
- principle of determination of processing personal data in the law (act or statute) – legality principle;
- principle of minimisation of processing;
- use limitation principle (purpose principle);
- principle of proportionality;
- the data quality principle;
- principle of limited storage periods of personal data;
- principle of respecting special rights of an individual: right to information on processing his/her personal data, right to access her/his own personal data, right to object;
- principle of providing data security measures; and
- principle of the right to an effective remedy.

All data contained in medical documentation, in EMR and in EHR systems, should be considered “sensitive personal data”. With respect to health data, there is an established double protection system, where general legal requirements for personal data protection and sensitive personal data protection should be applied simultaneously. Additionally, the general human rights and privacy protection framework shall be applied.

The starting point of EU law on health data is Art. 8 (1) of the DPD, which prohibits the processing of health data: “The Member States shall prohibit […] the processing of data concerning health or sex life.”. The draft of GDPR proposes a general prohibition of health data processing: “The processing of
personal data, revealing race or ethnic origin, [...] the processing of genetic or biometric data or data concerning health or sex life, [...] shall be prohibited\textsuperscript{54}.

The GDPR provides detail about the scope of personal health data:

“Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test\textsuperscript{55}.

Recommendation No.1:

The particular legal framework in order to serve appropriate protection of this special category of data should be developed in Serbia. We recommend improved clarification and definition the scope of personal health data in the Serbian law.

In the health care sector other categories of personal data, for example, data on health care professionals, are often processed. There are processed anonymised data aggregated from personal health data as well. Therefore it can be recommended to develop if necessary and to clarify application of definitions related to different sorts of personal and non-personal data used in health care. To secure appropriate treatment of personal health data, development of a separate protection system would be appropriate way to protect this domain of sensitive data. The definitions of different groups of personal data, if appropriate, should be compatible within a national and international legal framework.

In order to serve important individual and societal legal interests, the DPD provides for mandatory derogations laid down in Article 8(2) and (3), and an optional exemption in Article 8(4) lifting prohibition to process health data. All of these are limited, exhaustive and should be construed in a narrow fashion\textsuperscript{56}.

Explicit consent exemption

One justification for the processing of sensitive data can be the consent of the data subject (Art. 8 (2) of DPD). An important point is that in order to be valid, consent – whatever the circumstances are in which it is expressed – must be a “freely given, specific and informed indication of the data subject’s

\textsuperscript{54} Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

\textsuperscript{55} Para 26, Explanatory of Data protection regulation

\textsuperscript{56} WP 131, p.8
wishes. Consent in the case of sensitive personal data and therefore in an EHR must be explicit, and opt-out solutions are not sufficient.\textsuperscript{57} This requirement is echoed in the draft GDPR (Art. 9(2)(a)), allowing processing where “the data subject has given consent to the processing of those personal data for one or more specified purposes”.

The processing of personal health data should be analyzed in a broader context of patient’s rights. Informed consent for medical intervention is a general legal requirement stated by Art. 3 (2) of the Charter of Fundamental Rights of the EU\textsuperscript{58} and other relevant international\textsuperscript{59} and national norms. The right of an individual to decide whether to allow medical intervention forms a cornerstone of patient’s rights law. Processing of health data obtained in the context of medical intervention should be considered as part of a medical intervention requiring informed consent of the patient as general legal requirement. The WHO Declaration on the Promotion of Patients’ Rights provides a legal requirement to obtain consent for disclosure (processing may mean disclosure as well) stating: “\textit{Confidential information can only be disclosed if the patient gives explicit consent or if the law expressly provides for this.}\textsuperscript{60}” In the case that information is provided and processed in direct relationship with health care providers involved in care of the patient, “[c]onsent may be presumed where disclosure is to other health care providers involved in that patient’s treatment”\textsuperscript{61}. However, the patient has a right to restrict disclosure of some information even to the health care provider involved, especially where particular information is irrelevant for the intervention in question. Requiring informed consent of a patient in the case an institution is considering/planning processing of health data for any secondary purpose is also an obligation according to the DPD.

The preamble of the draft GDPR provides general description of the consent for data protection purposes: “Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject’s wishes, either by a statement or by a clear affirmative action that is the result of choice by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data. Clear affirmative action could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of their personal data. Silence, mere use of a service or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject’s consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.”\textsuperscript{62}

\textsuperscript{57} WP 131, p.8,9
\textsuperscript{58} Charter of Fundamental Rights of the European Union (2000/C 364/01), 18.12.2000 Official Journal of the European Communities, C 364/1
\textsuperscript{59} Convention of Biomedicine Art. 5, Law on Patient Rights in Serbia Art. 15
\textsuperscript{60} A Declaration on the promotion of patients’ rights in EuropeDECLARATION ON THE PROMOTION OF PATIENTS’ RIGHTS IN EUROPE, http://www.who.int/genomics/public/eu_declaration1994.pdf (accesed on 22/05/2014), 4.2.
\textsuperscript{61} Ibid.
\textsuperscript{62} GDPR, preamble, Para 25,
Opt-in vs opt-out systems for EHR

In all countries, trust in eHealth systems by both citizens and professionals has been identified as a key challenge; privacy is recognized as the most sensitive aspect of electronic health record systems. The question as to whether the creation of a shareable/national electronic record for a specific patient should be opt-in (the citizen has to explicitly agree to its creation) or opt-out (the record will be established unless the patient explicitly refuses) is the most controversial issue being addressed around the world and not only in Europe. Many countries are still debating the type of option to introduce.

Different options are in use throughout Europe. Countries like Belgium, France, Italy, Spain, Iceland and Switzerland require the patient to consent explicitly orally or in writing before an electronic health record may be created for her/him. In Spain, the requirement for explicit consent follows from the Health Law enacted in conjunction with the Data Protection Legislation. In Iceland, the Health Sector Database Act, enacted in 2002, was heavily criticized for the fact that citizens were identifiable in the national opt-out 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 (Commission nationale de l’informatique et des libertés) did however point out that by linking reimbursement rates to the use of the DMP (Dossier Medical Personnel), the right to consent is at risk of being compromised.

Other countries have chosen an opt-out system. Examples include Estonia, Poland, Scotland, Slovak Republic and Sweden. In Estonia, the Amendment Act (Amending the Health Services Organisation 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 regard to the creation of a health record. The dominant view in Scotland is that although the UK Data Protection Act (which is in force in Scotland) does require explicit consent, this does not preclude obtaining consent on an opt-out basis. In the Slovak Republic, 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. There, the maintenance of medical records which “is an integral part of the health care provision” is found in a (heavily) state-sponsored mandatory health system (not patient sponsored) which is a similar context to Serbia.

Recommendation No.2:

The current DHRL does not appear to give patients a choice about the creation of an EHR, with no “opt-out”, though Article 48 does give a patient the right to inspect the record. This consultancy strongly recommends that requirement to obtain consent of the patient is carefully considered and

63 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. 23/24
64 Ibid. eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. 23/24
addressed. There is necessity to discuss relevant factors for implementation of opt-in for EHR. Such approach would be in line with the relevant EU legal framework. In order to choose opt-out model, there should be legal analysis of Serbian human rights, constitutional law and data protection legal framework provided, exploring the legality of the opt-out system introduced.

The present regulation of health data processing provided by the PRL, the Art. 21 is stating the right to confidentiality of data on the patient’s health. Art. 21 (2) provides obligation to safeguard health data. However, this provision permits data processing by such thirds parties as higher health education institutions and not listed other legal entities or private insurance companies. The PRL does not provide regulation on data disclosures to any third parties. The PRL, Art. 22 provides requirement to obtain written consent of the patient for the release of health care professionals from the duty of confidentiality.

Due to limited scope of this consultancy, the authors of this report are not able to analyse legal framework of health data disclosure to third parties in an extensive manner. However, it seems that legal provisions of PRL and other legal acts in respect to health data protection do not sufficiently address the requirement to obtain consent for health data disclosure to the third parties.

**Vital interests exemption**

DPD Art. 8 (2)(c) provides an exception to the prohibition on processing where “processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent”. Here, processing must relate to essential individual interests of the data subject or of another person and it must – in the medical context – be necessary for a life-saving treatment in a situation where the data subject is not able to express his intentions.65

The similar exception is provided by the LPDP, Art. 12.

Accordingly, this exception could be applied only to a small number of cases of treatment and could not be used to justify processing personal medical data for purposes other than treatment of the data subject such as, for example, to carry out general medical research that will not yield results until some time in the future.66

**Recommendation No.3:**

The drafters should consider amending the regulations on health data protection, by incorporating the exception to process health data without consent in the case of vital interests of the data subject or another person where there is no possibility to obtain consent. The drafters should also consider the appropriate use of this exception for the processing data of the EHR in case of medical emergencies.

**Other exemptions**

DPD Art. 8 (3) of the Directive provides exception of prohibition and allows health data processing “where processing of the data is required for the purposes of preventive medicine, medical diagnosis,
the provision of care or treatment or the management of health-care services, and where those data are processed 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 also subject to an equivalent obligation of secrecy”. There are stated three cumulative conditions for health data processing:

1. the processing must be “required”;
2. the purpose of processing is one or more of listed in the norm: preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services; this does not cover further processing such as medical research, the subsequent reimbursement of costs by a sickness insurance scheme or the pursuit of pecuniary claims.
3. the data “are processed 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 also subject to an equivalent obligation of secrecy”\(^{67}\) (processing of sensitive personal data must be performed by medical or other staff subject to professional (medical) secrecy or an equivalent obligation to secrecy.)

**Proposed GDPR exemption on processing of health data**

In the draft of GDPR Art. 9 (2) (h), the prohibition of health data processing has a broader scope of exception than in the DPD. The draft law states that the prohibition should not be applied in the case “processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81”.

At this stage of legislative process, the Article 81 on processing of personal data concerning health states:

1. In accordance with the rules set out in this Regulation, in particular with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable, consistent, and specific measures to safeguard the data subject's interests and fundamental rights, to the extent that these are necessary and proportionate, and of which the effects shall be foreseeable by the data subject, for:

   (a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where those data are processed by a health professionals subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or

   (b) reasons of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices, and if the processing is carried out by a person bound by a confidentiality obligation; or

\(^{67}\) WP 131, 10
(c) Other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost effectiveness of the procedures used for settling claims for benefits and services in the health insurance system and the provision of health services. Such processing of personal data concerning health for reasons of public interest shall not result in data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.

The new regulation will allow the processing of health data only where such action is based on Union law or a law of Member State. Legitimate purposes for health data processing are stated in the Art. 81 (1) (a) (b) (c). In order to achieve permission to process health data, the Union or a Member State should have a particular legal provision on health data processing for the purposes allowed by the regulation. At the same time, this law should provide suitable, consistent, and specific measures to safeguard the data subject’s interests and fundamental rights.

Processing of health data for the provision of treatment will be allowed only by a health professionals or another person who is subject to the obligation of confidentiality under Member State law. The same confidentiality obligation established by law is required when health data are processed for public interest in the area of public health (Art. 81 (1) (b)).

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. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.

The new GDPR will require proof of necessity to process personal health data instead of non-personal data. A professional who processes personal data concerning health should receive, if possible, anonymised or pseudonymised data, leaving the knowledge of the identity only to the General Practitioner or to the Specialist who has requested such data processing.

Art. 81 (1b) will provide:

1b. Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or more specific and similar researches. However, the data subject may withdraw the consent at any time.

1c. For the purpose of consenting to the participation in scientific research activities in clinical

---

68 Preamble, 123
69 1a. When the purposes referred to in points (a) to (c) of paragraph 1 can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent to of the data subject or Member State law.
70 Preamble, 112a
Directive, Art. 8 (4) allows the Member States to derogate further from the prohibition of processing sensitive categories of data: “Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority”.

Consequently, should a Member State intend to make use of this possibility, the exemption must be contained in a legal provision or a decision of the supervisory authority (special legal basis). Such processing of sensitive personal data must be justified by reasons of substantial public interest. The substantial public interest must be presented by the Member State for each case in the entire scope of the processing exempted, and the processing must be necessary in the light of that substantial public interest. Any such measure must be proportionate, i.e. there must not be other less infringing measures available.\(^\text{71}\)

**Principle of purpose determination and legality principle**

As it was described above, in certain cases, the general rule on prohibition to process health data should be lifted in order to secure justified public interests. In order to secure legality principle, the national law should define one or more specified purposes for health data processing. These norms should be written in a clear and appropriate manner. The law should provide the authority to designated institutions and/or persons to process health data for this defined purpose. Furthermore, the law should define the individual dataset for reaching each defined purpose. Data processing which is incompatible with the purpose(s) of the collection, or carried out by unauthorized authorities, should be prohibited.

**Principle of proportionality**

The European Court of Human Rights has acknowledged that State Parties enjoy some discretion in restricting guaranteed rights, but monitors the relevance and the proportionality of the reasons and the means of the interference undertaken by national authorities. It leaves the States a wide margin of appreciation where there are diverse traditions or concepts of law in the national legal orders.\(^\text{72}\)

The principle of proportionality requires consideration whether there are less restrictive measures available for reaching the purpose, and should always be considered by all parties involved in processing data of individuals. The principles of relevance and proportionality of data collection, mandate that every compilation of data must be limited to those data which are relevant and not excessive for the defined purpose of the processing.\(^\text{73}\)

---

\(^{71}\) WP 131, p. 12  
\(^{72}\) EuroSOCAP project recommendations, p. 8  
\(^{73}\) WP 131, p. 18
**Principle of minimization of processing**

In order to apply the principle of minimization of personal health data processing, there must be a decision about the minimum content of specific datasets required for reaching the stated purpose. Only adequate, relevant and not excessive personal information should be entered or processed into the EMR or EHR systems for the purpose stated by law. Different purposes will require different datasets. Accordingly, the law providing permission to process certain sets of health data should regulate the content of particular datasets.

One of the most difficult questions when establishing an EHR system will be therefore to decide which categories of medical information should be collected in an EHR and stored for which period of time. Whereas this question has foremost to be answered by medical experts, it also has a data protection dimension. The legitimacy of EHR systems will therefore also depend on an adequate solution of choosing the ‘right’ categories of data and the ‘right’ length of time for storing information in an EHR.74

Concerning the presentation of data within the EHR, the fact that different categories of health data requiring quite different degrees of confidentiality suggests that it might be generally useful to create data modules within an EHR system with specific access requirements. For example, a “vaccination data module” should be accessible at any time for the data subject and could also be accessible for a rather broad range of personnel within the health-care services; a “medication data module” could be supplied with special access to pharmacists if the patient agrees; an “emergency data module” could have special technical means for access, etc. 75

Particularly sensitive data could also be better protected by storage in separate modules with especially strict conditions for access. Examples would include data on psychiatric treatment or on HIV or abortion. Instead of excluding such data from an EHR – which might be detrimental for future successful medical treatment – special restrictions for access to such EHR-data should be built into the system including explicit consent of the patient and special technical barriers (e.g. “sealed envelopes”). 76

In summary, the principle of minimization requires lawmakers to decide when there is a need to process personal data and when the designated purpose can be achieved by making data pseudonymous or anonymous.

**Recommendation No.4:**

As it is possible to observe throughout the text drafted for the DHRL and other relevant documents on eHealth systems, appropriate application in the purpose determination and limitation, proportionality and data minimisation principles is lacking at the present stage of the process. Therefore we could recommend a review of the DHRL and other relevant provision in the light requirements for application of these principles. For the purpose limitation principle, we would recommend using the Article 29 Working party opinion on purpose limitation.

---

74 WP 131, p. 18
75 Ibid., p. 18
76 WP 131, p.
Principle of respecting special rights of an individual

This principle relates to respect for the rights of the individual with respect to processing his/her personal data, accessing his/her personal data, or objecting to the processing of such data. Pursuant to Article 10 of the Directive, data controllers processing information in EHR systems must provide certain information to data subjects, such as information on the identity of the controller, on the purposes of the processing, on the recipients of the data and on the existence of a right of access. The Patient Information Notice must be sufficient to enable the patient to give explicit consent to the processing of data in accordance with the requirements of DPD and PRD.

Patient empowerment requires providing legal rights, facilitating effective implementation tools for the realization of rights and to allow active use of the patient’s medical record. The principles allowing the patient to control and use his records are stated in the WHO Declaration on promotion of patients’ rights: “Patients have the right of access to their medical files and technical records and to any other files and records pertaining to their diagnosis, treatment and care and to receive a copy of their own files and records or parts thereof.”

Recommendation No.5:

Planners should develop and implement a system providing information to data subjects, such as information about the identity of the controller, the purposes of the processing, recipients of the data and the existence of a right of access.

Right to access health data

DPD Art. 12 establishes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. Those provisions should also apply in the context of cross-border healthcare covered by this Directive.

It is important to secure the right of the individual patient to access his/her health data, to control processing of health data and to use his/her health data for any purpose he/she may wish. At present, the right to access, control and use of health data are regulated in the PR Law, will be regulated by the DHRL law and in general is regulated by the LPDP.

Serbian legal provisions on health data and patients’ rights place insufficient focus on the individual patient’s rights in respect to access, control and use of health data. It can be observed that the

77 WP131, p. 12
78 See more detailed in the epSOS project paper “Legal and Regulatory Requirements at EU level”, http://www epsos eu uploads/tx epsosfileshare/O2.1.1_legal requ_final_01.pdf
80 Art 20,
81 Art 48
82 Art. 20. The analysis on Serbian LPDP in respect to patients’ rights is provided in the paper “Towards the Launch of Electronic Health Records in Serbia - Legal Gap Analysis” Aleksandar Zavišić, Legal Expert, EU-IHIS project, p. 14 - 18
proposed development of the EMR and/or EHR system is not designed in a way to promote and strengthen patient’s right to access, control and use his own data from the very beginning of the EHR development. It is proposed that “initially, patients will be able to get insight into their personal EHR through EPR systems with chosen doctor(s) acting as mediator(s). Patients’ online access to their EHR data will become available at a later stage of EHR implementation, after majority of healthcare facilities are integrated into the system and a simple solution for highly reliable patient authentication becomes available.”

It is not sufficient to require a medical doctor to act as mediator for exercising one’s rights or to provide implementation of patients’ rights at a later or last stage of the whole process. It is not appropriate to limit patients’ rights allowing just inspecting his record, as it is proposed in the draft law Art. 48 “A patient shall have the right to inspect data kept in an electronic medical record.” The following norm in the draft law, Art. 48 (3) stating “patient may exercise the right to access via the Internet if technical requirements and protective measures adopted pursuant to this Act and the Personal Data Protection Act have been met” would require clarification as to whether the right to access his health records can be limited due to unmet technical and protective measures by undefined entity.

Whether direct (electronic) reading access to their EHR should be granted to patients is a matter of medical feasibility. The data protection right of access e.g. under Article 12 of Directive 95/46/EC need not necessarily always mean direct access. Direct access might, however, contribute considerably to trust into an EHR system. From a data protection point of view a precondition for granting direct access would be secure electronic identification and authentication in order to prevent access by unauthorized persons. Free of charge, easy to use but safe access points for data subjects to check on the content and on disclosure of their EHR record might also be a valuable contribution to transparency and thereby trust in the system.

An EHR system must ensure that the data subject is able to exercise his access rights without undue difficulties. In principle, it is the data controller who is obliged to give access. EHR systems are, however, information pool systems with many different data controllers. In such systems with a large number of participating data controllers, a single special institution must be made responsible towards the data subjects for the proper handling of access requests. In view of the foreseeable complexity of a fully developed EHR and the necessity of building trust with patients in the system, it seems essential that patients whose data are processed in an EHR system know how to reach a responsible partner with whom they could discuss possible shortcomings of the EHR system. Special regulations to this end will have to be included in any regulation on EHR systems.

The right to access is not absolute. Health care providers can refuse access to medical records in the case that providing access to the information would cause serious harm to a patient or another person. Furthermore, the data subject has a right to object to data processing and to prevent

---

83 For example, the individual patient is not listed as a user of EHR  
84 Paper EHR Security and Privacy  
85 Draft of Medical Record law, art 48  
86 WP 131, p. 17  
87 WP 131, p. 20  
88 WP 131, p. 21
processing of data, especially when such processing might be stressful or damaging for the individual. A patient should also have the right to see the log and know who used or saw his/her medical data.

**Recommendation No. 6:**

The implementation of patients’ right to access should be addressed as early as possible in the process in order to develop an appropriate legal framework, technical tools and implementation programme. This will secure substantial progress in achieving promotion of patients’ rights through the EHR system.

**Right to make a copy of health record**

The WHO Declaration on promotion of patients’ rights states the right to receive a copy of medical record: “Patients have the right […] to receive a copy of their own files and records or parts thereof.” The right to receive a copy of one’s own medical file is provided by the Serbian LPDP Art. 21., LPR Art. 23. By implementing EMR and EHR, the right to request and receive a copy should be provided using IT tools developed for EMR and EHR. It should be provided, that individual may request and receive a copy electronically.

**Recommendation No.7:**

In order to respond to potential requests from patients, introduce a system capable of providing electronic copies of health data upon request.

**Right to accurate and up-to-date data**

WHO Declaration on Patients’ Rights states: “Patients have the right to require the correction, completion, deletion, clarification and/or updating of personal and medical data concerning them which are inaccurate, incomplete, ambiguous or outdated, or which are not relevant to the purposes of diagnosis, treatment and care.” Article 12 of the DPD provides data subjects with the ability to check on the accuracy of the data and to ensure that the data are kept up to date. These rights fully apply to the collection of personal data in EHR systems.

Serbian LPDP, Article 22 provides: “Data subject has the right to request from the controller correction, amendment, updating, and erasure of data as well as termination and temporary recess of processing”. Personal data in general and health data in particular may be incomplete, inaccurate, and ambiguous or outdated; therefore the patient may request a correction, completion, deletion, clarification and/or updating. In order to have a complete, quality and updated health record, the patient’s input may be highly relevant. For the EHR system in Serbia, it is proposed: “Potentially, patients may have ability to submit a request for change of the incorrect data. These changes are subject to approval by the chosen doctor or authorized professionals.” Besides general data protection framework, there are no legal provisions with respect to patients’ right to require correction of data in Serbia and these are not proposed in the draft law on MR.

---

90 WHO Declaration, Art. 4.5.
91 Paper EHR Security and Privacy, p.20
Recommendation No.8:

Patients’ rights with respect to amending incorrect health data should be elaborated by the draft law. Additionally, procedural tools to exercise these rights should be provided by law and implemented into practice.

This principle in the Directive requires data to be accurate and kept up-to-date. Data should be erased when not necessary for the purpose for which they have been required and processed. There are not a lot of data on accuracy of EHR, however a study on malpractice claims in US revealed: Computer systems that don’t “talk” to each other, test results that aren’t routed properly, and mistakes caused by faulty data entry or copying and pasting were among the EHR related problems found in the claims, which represented $61 million in direct payments and legal expenses. Incorrect information in the EHR was a factor in 20% of the 147 medical error cases reviewed. Such errors might include: faulty data entry, unexpected conversion of data, data entered in wrong file or field, repeated errors. In order to avoid inaccuracies and to secure up-to-date personal records, there is a need to design the system considering various risks of data accuracy. Training and regular IT support services would help health professionals to minimize human errors while working with documents, and regular quality audits may reveal inaccuracies in design and will help to improve the software. Control of documents by patients and easy reporting system for inaccuracies for patients would help as well to secure accuracy of data.

Recommendation No.9:

It is suggested that the drafters of the law/planners establish a system capable of controlling accuracy of data and correcting mistakes as soon as they are discovered. This system may include regular quality audits, strong involvement of end-users in identification, correction and improvement, options to submit an inaccuracy reports by users, effective responses to identified problems by IT personnel, necessary technological improvements, and regular training for users where issues related to data accuracy are discussed.

Right to “seal and lock”

There is an established right in many EU countries allowing the patient to restrict access to his medical record in some part. This is done in order to safeguard protection of sensitive data and to enhance patient’s control over his information. Such approach is supported by the Art. 29 Working Party’s opinion on EHR: “Particularly sensitive data could also be better protected by storage in separate modules with especially strict conditions for access. Examples would be data on psychiatric treatment or on HIV or abortion. Instead of excluding such data from an EHR – which might be detrimental for future successful medical treatment – special restrictions for access to such EHR-data

---

93 For example, UK or Sweden
should be built into the system including explicit consent of the patient and special technical barriers (as e.g. “sealed envelopes”).”

As WHO publications have noted, this method for granting greater autonomy to the patient can have two detrimental effects. First, the existence of a sealed record may inadvertently create privacy issues, since the mere fact that the record flags that some information is not accessible indicates that highly sensitive information exists for that patient, which is a piece of personal data in itself. Second, in giving a patient the right to conceal certain information, not all health care professionals have access to the complete record, which could compromise the health of the patient who has concealed information and could also impact negatively on the health of others.

In Serbia, there is no such option to realize such a right to control under the draft law. This issue is highlighted in the project document, which suggests: “Patients may be allowed to specify visibility of some sensitive health data within their own health record. However, this should only be allowed in relation to predetermined data groups and not for individual data items.”

Recommendation No.10:

The right to “seal and lock” certain aspects for electronic health records should be enshrined in both the Serbian law on medical records and in the EHR system.

**Principle of limited storage periods of personal data**

This principle requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further processed. Therefore health data should be collected in an EHR and stored for only a limited period of time. By stating the time period for electronic medical records, various individual and public interests should be considered. Proposed storage time for various medical records by the DLHR seems being too extensive. It is not appropriate to require storage of electronic records permanently.

Recommendation No.11:

Reconsideration of the proposed storage periods for EMR and EHR is suggested, as substantial portions of medical records are outdated in 2, 5, or 10 years and there is little justification for keeping them longer.

**Principle of providing data security measures**

Article 17 of the DPD imposes an obligation upon data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure. The measures can be organizational or technical. It should be determined what measures would be appropriate from Serbian perspective, so that this can be incorporated into the DHRL.

---

94 WP 131, p.18
95 WHO, Legal frameworks for eHealth: based on the findings of the second global survey on eHealth. ([Global Observatory for eHealth Series, v. 5), p. 60]
The acceptability of a system of data processing with an exceptional risk potential is dependent on an adequately high level of data security for the complete performance of the system. Access by unauthorised persons must be virtually impossible and prevented, if the system is to be acceptable from a data protection point of view. However, availability of the system for authorized professionals must be virtually unlimited where there is a genuine need to know, if the system is to result in the promised advantages for the medical treatment of patients.\textsuperscript{96}

The legal framework for setting up an EHR system would have to foresee the requirement of implementing a series of measures of a technical and organisational nature appropriate for avoiding loss or unauthorized alteration, processing and access of data in the EHR system. Integrity of the system must be guaranteed by making use of the knowledge and instruments representing the present state of the art in computer science and information technology.\textsuperscript{97}

An effective tool to control security breaches involves mandatory reports to authorities and to the data subject. The European Data Protection Supervisor (EDPS) emphasises that an obligation to report security breaches could empower the data subject. The EDPS argues that such a security breach notification will make individuals on the one hand more aware of the risks they face when their personal data are compromised. On the other hand, it could incentivize data controllers to implement stronger security measures and prevent breaches. A similar obligation was recently integrated in US regulations.\textsuperscript{98}

With the new GDPR general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.\textsuperscript{99}

In the proposed GDPR, Art. 30 places a strong emphasis on data security:

\begin{table}[h]
\centering
\begin{tabular}{|c|}
\hline
\textbf{Security of processing (Art 30)} \\
\hline
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, taking into account the results of a data protection impact assessment pursuant to Article 33, having regard to the state of the art and the costs of their implementation. \\
1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include: \\
\hspace{1cm} (a) the ability to ensure that the integrity of the personal data is validated; \\
\hline
\end{tabular}
\end{table}

\textsuperscript{96} WP 131, p. 19  
\textsuperscript{97} WP 131, p. 19  
\textsuperscript{98} Dumortier J., Verhenneman G. Legal regulation of electronic health records: A comparative Analysis of Europe, p. 47 in book:  
\textsuperscript{99} GDPR, Recital 70
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;

(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;

(d) in the case of sensitive personal data processing according to Articles 8 and 9, additional security measures to ensure situational awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data;

(e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.

2. The measures referred to in paragraph 1 shall at least:

(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;

(b) protect personal data stored or transmitted against accidental or unlawful destruction, or accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and

(c) ensure the implementation of a security policy with respect to the processing of personal data.

In DHRL Art. 45 and 46, data security issues are addressed. There is provided delegation to the minister to prescribe detailed requirements in respect to security of the EMR and EHR. However, we could recommend to revise these provisions and to amend them in a way that minimum set of security requirements are stated by the law.

Recommendation No.12:

This consultancy recommends the amendment of legal provisions with regard to privacy and security of the EHR in order to ensure minimum quality of the service and to protect patients’ legal interests. The legal requirements included in the GDPR, Art. 30 should be used as a basis for establishing these rules. The law could set out the conditions for accessing EHR, conditions for sharing EHR, obligation to report security breaches and other security-related requirements. It is also recommended to provided data protection impact assessment for the newly developed EHR system; to ensure regular tests, assessments and evaluations of security risks in the EHR; and to develop additional security measures to ensure situational awareness of the risks and the ability to take preventive, corrective and mitigating actions in near real-time against vulnerabilities or incidents detected that could pose a risk to the data.

Patient summaries

Patient summaries contain basic medical and administrative data which allow health professionals to more effectively treat a patient across health care institutions, on visits to other EU countries, or in the case of unexpected or unscheduled medical situations. In the current draft law on health care records, these are not considered, though contents of the patient information are spelled out in
Articles 13 and 14. As described below, there are clear European pieces of guidance and templates in relation to patient summaries.

In November 2013, EU member states adopted new guidelines on minimum/nonexhaustive patient summary datasets in order to facilitate sharing of basic health information across EU borders. These guidelines allow patients to explicitly request the availability of the summary electronic health record when visiting another EU country, containing relevant medical information such as allergies, vaccinations and recent surgical procedures. The summary would also contain basic administrative data such as details of the healthcare provider in the home country or insurance information. As member states develop their own electronic health records, this provides an important reference for consistency in basic procedures and content.

Additionally, European Patients’ Smart Open Services (EPSOS) has developed a patient summary, a standardized set of basic medical data that includes the most important clinical facts required to ensure safe and secure healthcare, which helps health professionals especially in the event of an unexpected medical situation and in moves between institutions or countries.

**EPSOS patient summaries contain the following data:**

- General information about the patient (e.g. name, birth date, gender).
- A medical summary consisting of the most important clinical patient data
- A list of current medication including all prescribed medicines
- Information about the Patient Summary itself, including when generated and updated (used for security and protocol reasons)

**Recommendation No.13:**

The current draft law on health care records does not address patient summaries per se, though contents of the patient information are spelled out in Articles 13 and 14. Drafters of the law may wish to consider the incorporation of patient summaries, containing basic medical and administrative information about the patient, which will allow health professionals to quickly view relevant information about the patient. This will be in line with recommendations of the current eHealth Network (which developed the guidelines on minimum dataset) and the EPSOS project patient summaries.

**Governance of the eHealth and structure of the EHR**

There are three approaches to EHR within Europe: the decentralized approach, the centralized model and a patient-centred design. A decentralized approach to shared EHR consists of keeping individual health record stored in the IT system of every (connected) health care provider and health care institution; these are connected through a repository. A second model for organizing EHR involves

---


101 This model is introduced in Belgium.
the creation of a central register\textsuperscript{102}. The third option is a patient–centred approach, where the patient chooses a service provider to host his electronic health record and requests his healthcare provider to update it\textsuperscript{103,104}. A shift can be observed towards a hybrid centralized and decentralized storage approach, based on regional networks and one national central connection\textsuperscript{105}.

As observed during the consultancy visit in Serbia, institutional (individual hospital) databases containing individual EMR are being developed within the framework of EU IHIS project. The primary focus of these decentralized databases is on clinical use within individual healthcare institutions, and at this stage the existing institutional databases are not connected. At the same time, one central database of health records has been established and is used by the National Health Insurance Fund to secure financial management of state provided healthcare services\textsuperscript{106}.

Within the framework of the EU IHIS project, the establishment of Serbian EHR system is proposed. The project sets out the requirements for access and management of EHR, which are developed and described in the document “EHR Security and Privacy”. However, the document does not describe legal regulations relating to the establishment and governance of the EHR system as such. During the consultancy visit to Serbia, the question of legal status of the governing body and other issues in respect to governance of the EHR system has been raised. At the moment, there is no clear vision about the placement and role of the institution which will have the legal competence to establish, develop and operate the EHR system.

The documents prepared within the EU-IHIS project describe the centralized system where one entity holds and operates the EHR database. However, a different approach is taken in the Draft Law on Health Records (DLHR)\textsuperscript{107}. The law stipulates the establishment the Integrated Health Information System of the Republic of Serbia. Part III contains provisions on this system, which will contain “health and statistical system, information system of health insurance organisations and information systems of health care facilities, private practice and other legal entities\textsuperscript{108}.”

The draft law Article 46 provides for the regulation of electronic medical records under a separate entity\textsuperscript{109}:

\begin{quote}
An electronic medical record shall mean a data extract from basic medical records kept electronically for one patient which contains all medical data relevant for patient’s long-term health and which are, if necessary, available in providing health care, to make treatment of a patient more successful.
\end{quote}

\textsuperscript{102} This model is developed in Scandinavian countries and Estonia.

\textsuperscript{103} This model is introduced in France

\textsuperscript{104} Dumontier J, Verhenneman G, Legal regulations of Electronic Health Records: A Comparative Analysis of Europe and the US. In book: \textit{...}, p 37 - 40

\textsuperscript{105} Dumontier J, Verhenneman G, Legal regulations of Electronic Health Records: A Comparative Analysis of Europe and the US. In book: \textit{...}, p. 51

\textsuperscript{106} Amendments proposed to the Health Insurance act, Art 124, 3 »(3)The Republic Fund keeps special evidence (database) for insured persons from articles 22 and 23, which consists of the data on (…) and the same categories of personal data as provided by the articles 115 – 123

\textsuperscript{107} The authors of this report are using unofficial translation of the Draft low done in October, 2013 and provided by EU IHIS project for consultants to use solely for ...

\textsuperscript{108} Art. 44 (2)

\textsuperscript{109} Systemic legal analysis of the norms allows to draw conclusion that is not proposed to collect personal medical records in the part of the system named “health system”.

The electronic medical record referred to in paragraph 1 of this Article shall obtain data from basic medical records kept in a health care facility, private practice and other legal entity as well as data kept in the health and statistical system and information systems of health insurance organisations.

The minister shall prescribe more detailed contents of the data kept in an electronic medical record, the manner and procedure for obtaining data as well as other issues relevant for creating and using data upon obtaining an opinion from the institute of public health established for the territory of the Republic of Serbia.

These norms would establish a repository of individual electronic medical records kept separately by the relevant institution or by an outside health care institution.

Article 49 of the draft law provides: “A developed integrated health information system shall serve as a basis for the introduction of an electronic medical record in accordance with uniform methodological principles and standards.” This provision suggests that the “developed integrated health information system” will serve as a basis for the introductory phase of electronic medical records.

Furthermore, it should be taken into consideration that the draft law provides that the Minister will elaborate further rules regarding the above-mentioned systems. At the moment, it is unclear this process will take place, as there is no indication relating to the content of an opinion from the Institute of Public Health. Accordingly, detailed analysis in this respect cannot be provided.

The allocation of responsibility for eHealth strategy development and their implementation is not uniform across EU Member States. More than a dozen countries have established legal entities as specific consultative bodies or competent authorities under ministerial supervision in order to develop, oversee and monitor the country’s strategic goals, and/or implement and manage eHealth infrastructure and application projects.

**National competence centres:** Another indication of the strong political commitment at the national policy level is the growing establishment of permanent administrative support structures. National competence centres such as gematik (Society for Telematics Applications of the Health Card) in Germany, ASIP - Agence des Systèmes d’ Information de Santé Partagés in France, or THL National Institute for Health and Welfare in Finland are increasingly being created or expanded to also cover eHealth infrastructure requirements.

On specific aspects of electronic health record (EHR) systems, the recent EC Recommendation on cross-border interoperability of electronic health record systems notes under “Monitoring and Evaluation”, that “in order to ensure monitoring and evaluation of cross-border interoperability of electronic health record systems, Member States should: consider the possibilities for setting up a monitoring observatory for interoperability of electronic health record systems in the Community to

---

110 Some clarification is needed in respect to what kind of data will be included from the health and statistical system and information systems of health insurance organisations, Art. 46 (2)
111 As part of its individual health information system as provided in the Art. 45
112 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p.9
113 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. VII
monitor, benchmark and assess progress on technical and semantic interoperability for successful implementation of electronic health record systems.”

**Recommendation No.14:**

The text of the draft law fails to provide complete information on how the governance of eHealth system will be organised. There are missing provisions on how database/es for electronic medical records will be created, which institution will have the legal authority to establish database of electronic medical records and what principles will govern operation of proposed database. There are different ways of addressing this issue across the EU and there will need to be a determination of the best ways to manage this from a Serbian perspective. It should be stressed, that the governance of eHealth system is of crucial importance and should be strengthened by developing, implementing and operating eHealth platform constantly.

**Stakeholder engagement**

In line with the requirement of a “common understanding and concerted efforts by all stakeholders” (eH-AP), many countries have by now established advisory bodies involving e.g. professional associations, patient representatives, third party payers or care providers as part of their eHealth governance structures. Careful planning, organisational setup, and stakeholder involvement are key success factors for eHealth (infrastructure) projects. Such bodies in part resolve the challenge of potentially ambiguous or distributed responsibilities for eHealth. Although they are not a sufficient condition for success, it seems they are a necessary ingredient.

Representatives of the eHealth industry and other stakeholder groups would be keen to see an approach which assures for co-shaping in developing and implementing eHealth strategies. A governance process should be initiated where, e.g., companies and patients are encouraged to examine the availability and analysis of personal data for the common good and not purely out of self-interest.

**Training**

Qualified human resources are another key ingredient for success. Education, training and continuous professional development for all, including for those citizens and patients which are capable and motivated to become engaged in their own care, must be strongly promoted. “The most important part of eHealth investment that needs expanding is the eHealth skills and knowledge of

---

115 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. VIII
116 Ibid, p. X
117 Ibid, p. XI
healthcare staff and ICT suppliers’ staff. An expanded capability is essential to achieve more success and so help to boost eHealth investment.”

There is a strong need to improve eHealth training and education for professionals, but also to focus on reducing the asymmetry in capabilities, information and knowledge between health professionals and patients, and thereby strengthen stakeholder engagement.

**Recommendation No.15:**

The consultancy would like to recommend the development and implementation of eHealth training programmes for health care practitioners, administrative and IT personal of health care institutions. Training opportunities for patients could also be provided.

**Terminology and usage**

There is a need for clear terminology and consistent usage of terms throughout the draft law and the eHealth system. It has been noted that there are certain inconsistencies in definitions between the draft law and the Law on Personal Data Protection. Additionally, a number of terms appear in the “definitions” section which do not appear elsewhere in the law. In order to promote consistency throughout the application of this draft law within the Serbian legal system, these differences should be examined and reassessed. This will also assist in the objective of promoting clarity for medical practitioners and patients. Key definitions are set out below.

The epSOS55 project’s definition of *patient summary* is “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)”. Patient summaries, also referred to as core minimum datasets, are usually generated and maintained by general practitioners.

The term *EHR* is less clear, but the following distinctions can be made (these are taken from the eHealth strategies report):

- Electronic Medical Record (EMR) – the electronic record of an individual in a physician’s office or clinic, which is typically in one setting and is provider-centric
- Electronic Patient Record (EPR) – the electronic record of an individual in a hospital or health care facility, which is typically in one ‘organisation’ and is facility-centric
- Electronic Health Record (EHR) – the longitudinal electronic record of an individual that contains or virtually interlinks data in multiple EMRs and EPRs, which is to be shared and/or interoperable across healthcare settings (interinstitutional) and is patient-centric.

---

119 Ibid, p. XI
120 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. 19, 20
The eHealth Strategies Report defined a patient’s electronic health record (EHR) as 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 many cases, an EHR is understood to contain a patient summary as one of its core elements or artefacts.”

**Transition from written to electronic records (Article 37)**

Article 37 of the draft law addresses a period of transition from written to electronic records. With regard to the regulation of electronic health records it can be noted that nearly all European countries legally enforce a duty to keep a carefully updated and safely stored health record, but most keep the option open of storing the health record on paper or electronically. If they have an electronic form, additional requirements concerning content, access and security often apply. It is however expected that the obligation to store the records electronically will arise in more and more countries, if only because many are currently planning to roll out electronic health record-like systems that will become mandatory unless patients opt-out.

The storage of paper records should be organised according to the existing law, but for transition period from paper to digitalised records appropriate rules should be enacted. It is not advisable to require to produce paper and electronic record in the same time. Such an approach would not facilitate development of eHealth systems. However, planning and regulation of transition period which could be quite long in some case, e.g. where long-term care of a patient will require usage of older paper records and more recent electronic ones, should secure smooth development of electronic records environment.

**Recommendation No.16:**

Implementation of eHealth tools to process medical records will take substantial time and there will be need to use paper medical records and electronic medical records parallel for some time. To facilitate implementation of EMR and EHR, the requirement for health care providers to keep the information in paper format should be minimised as much as possible as well as initiatives to use electronic means should be supported. Special regulations for transition period should be enacted in order to secure proper and safe use of two forms of records.

**Recommendation No.17:**

There are number of health databases existing in Serbia already, and furthermore the development of new health databases has been proposed by the draft law and by eHealth implementation tools. In order to have an overview of the integrated health information system in Serbia, a graphic with relevant detailed information about the content of each aspect of the system would be helpful for

---

121 Ibid.
122 eHealth Strategies Report January 2011, European countries on their journey towards national eHealth infrastructures, p. 13
drafters of the law and those working in the area. This graphic could contain existing databases (like EMR) and proposed databases, such as EHR.

### III. Conclusions

eHealth systems are rapidly becoming part of the health care system in Serbia and in other countries, and that the development of these systems is progressing rapidly and dynamically. While they will bring substantial promise in terms of health care improvements, these systems require defined confidentiality policies implemented by law and in practice, and defined security policies which are stated by law, developed by technology and implemented by users. The key elements of trust, transparency, openness towards all stakeholders, security, quality and efficiency should be present in discussions from the outset. Because of the swift implementation of these systems and rapid developments in the area of eHealth, it is difficult to address these issues through lengthy considerations and discussions.

There is already substantial knowledge on some eHealth tools collected by European countries working with EMR and implementing EHR. Wherever possible, these European experiences should be used, adopted and modified according to Serbian needs. Furthermore, numerous academic, policy and technology related events on eHealth developments are organized by European universities, EU institutions and NGOs. Participation in these may secure knowledge transfer to and from Serbia. Additionally, the EU-IHIS project team has been developing a substantial framework for implementation of eHealth systems. It would be important to secure continuity and to use all relevant preparations for more general development of EHR.

This topic and the scope of the consultancy was broad and complicated. The authors of this report did extensive research into the topic, taking into account Serbian existing legal framework as well as proposed legislation, the existing and proposed legal EU framework, EU-IHIS project documentation, the CoE legal framework as well as articles and other research material. There is a great deal of research which could be carried out in this area, and specific areas of interest might be explored in the future. For instance, two issues which are quite important but which were not addressed given the limited time frame include (1) the protection of children and other vulnerable patient groups and (2) ethical dimensions. However, for this report we did our best to respect the limits set by consultancy agreement and prepared the report accordingly.
Annex One: Key documents and references

Serbian laws and related documents:
- Aleksandar Zavišić. Towards the Launch of Electronic Health Records in Serbia: Legal Gap Analysis
- Law on Patient Rights (4 March 2013)
- Draft Law on HEALTH RECORDS AND STATUTORY RECORDS IN THE FIELD OF HEALTH CARE
- REPUBLIC OF SERBIA, Ministry of Justice LAW ON PERSONAL DATA PROTECTION (2008)
- EU-IHIS, Core Patient Dataset for Serbian EHR
- EU-IHIS, EHR Security and Privacy
- Patient dataset in Electronic Health Record (EHR)
- Law on Health Care – Analysis
- Law on Health Care – proposed amendments
- Law on Health Insurance - analysis
- Law on Health Insurance – proposed amendments

Key European Instruments:
- The Charter of Fundamental Rights of the European Union[123]
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[125]

Reports and articles:


• Dr. Juergen Hohmann, Stefan Benzschawel Dr. rer.nat. *Data Protection in eHealth Platforms IN:* Legal and Forensic Medicine 2013, pp 1633-1655 Print ISBN 9783642323379


• Syed Naqvi, Gautier Dallons, Arnaud Michot, Christophe Ponsard. *Assuring Privacy of Medical Records in an Open Collaborative Environment - A Case Study of Walloon Region’s eHealth Platform IN:* Privacy and Identity Management for Life IFIP Advances in Information and Communication TechnologyVolume 320, 2010, pp 146-159 Online ISBN 978-3-642-14282-6/ Print 978-3-642-14281-9


• EPSONS: Smart Open Services for European Patients - Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription

• Legally eHealth: Putting eHealth in its European Legal Context


• consolidated text of the regulation at http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf


**Key WHO resources:**


• http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf?ua=1

• http://apps.who.int/iris/bitstream/10665/76794/1/9789241504645_eng.pdf?ua=1