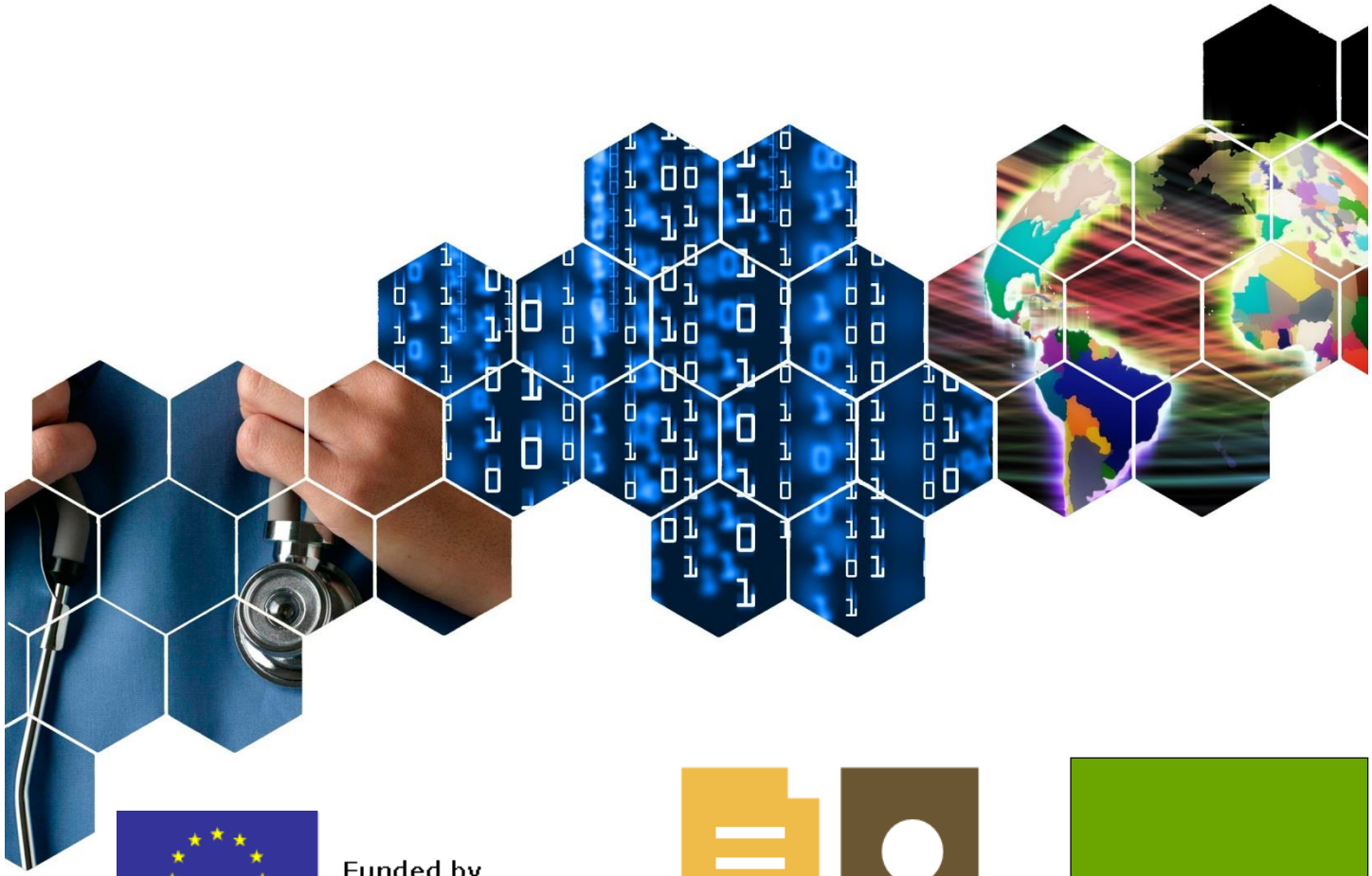
Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services

Final report and recommendations

Contract 2013 63 02



Funded by
the Health Programme
of the European Union

23 July 2014

time.lex

milieu
Law & Policy Consulting

This report was produced and funded under the EU Health Programme (2008-2013) in the frame of a direct service contract with the Consumers, Health and Food Executive Agency (Chafea) acting under the mandate of the European Commission. The content of this report represents the views of the contractor and is its sole responsibility; it can in no way be taken to reflect the views of the European Commission and/or Chafea or any other body of the European Union. The European Commission and/or Chafea do not guarantee the accuracy of the data included in this report, nor do they accept responsibility for any use made by third parties thereof.

Milieu Ltd. (Belgium), rue Blanche 15, B-1050 Brussels, tel: +32 2 506 1000; fax: +32 2 514 3603; florent.pelsy@milieu.be; web address: www.milieu.be
Time.lex cvba/scrl, rue du Congrès 35, B-1000 Brussels, tel. +32 2 229 19 47; fax: +32 2 218 31 41; jos.dumortier@timelex.eu; web address: www.timelex.eu

TABLE OF CONTENTS

TABLE OF TABLES

1 EXECUTIVE SUMMARY

Pursuant to Article 14 of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, the eHealth Network was set up to facilitate the cooperation between the European eHealth systems and to draw up a series of guidelines to facilitate the cross-border transferability of medical data, taking into account the EU data protection rules. In the end of 2012, the Commission adopted a new action plan 2012-2020 proposing a series of measures and expressing its commitment to remove the existing barriers to "a fully mature and interoperable eHealth system in Europe".

The objective of this Study is to provide an overview of the current national laws on electronic health records (EHRs) in the EU Member States and their interaction with the provision of cross-border eHealth services mentioned in Directive 2011/24/EU. This entails first to identify and examine the national laws of the 28 Member States and Norway and identify legal barriers for cross-border transfer data from electronic health records and for the provision of cross-border eHealth services; and second, to make recommendations to the eHealth Network on how the national laws and the European framework must evolve to support cross-border eHealth services.

The first step of this study was the completion of national reports describing the legal requirements applying to EHRs based not only on the existing legislation, but also on planned measures (e.g. draft legal initiatives). As a second step, the information provided in the national reports was used for the purposes of the comparative analysis. Finally the draft recommendations were mainly built upon the findings of the comparative analysis. The following paragraphs summarise the main findings and the recommendations proposed for each of the topics covered under the Study.

EHRs systems and laws: different approaches

The definition of EHR contained in the Commission Recommendation of 2 July 2008 covers different types of electronic health records. EHRs are in use in all countries covered by this Study and there are numerous forms of EHRs at all levels of the healthcare sector of most countries. However, some of these EHRs are not designed for a shared access and therefore not covered by the Study. The Study focuses on the legal requirements applying to nationally organized systems of shared EHRs which can potentially participate in a European-wide sharing system.

There are major disparities between countries on the deployment of EHRs part of an interoperable infrastructure that allows different healthcare providers to access and update health data in order to ensure the continuity of care of the patient. The same can be said about the approach taken to regulate EHRs – some countries have set specific rules for EHRs, others rely on general health records and data protection legislation.

EHRs: content and interoperability aspects

The comparative analysis shows that two broad approaches can be distinguished amongst the countries covered by the Study. While some countries have set detailed requirements as to the content of EHRs, others do not specify what should be this content. The level of details of the legislation on EHR content varies greatly from a simple reference to health data in general to exhaustive and detailed list of categories or data item. In the latter case, however, the detailed rules are often meant to be applicable to specific EHR sharing systems. Anyhow the more or less detailed character of national legislation with regard to the data to be included in EHRs does not seem to constitute an obstacle for interoperability between EHR systems. Regarding this particular aspect, interoperability requires an agreement on which extract of the EHRs will be included in the health data exchange.

While EHR systems in all countries apply standardised terminology and some form of codification to categorise health data, less than half of the countries provide in their legislation the obligation to do so.

According to stakeholders interviewed, EHR systems in the countries covered in this Study are using in practice very different terminology and coding systems, and they consider this semantic diversity as one of the main barriers to the cross-border transfer of health data.

Recommendation at national level: In order to share health information, the EHR systems used by health providers should have a minimum level of interoperability. Such interoperability does not require all systems used to store an identical list of data. Rules or guidelines at the national level should mainly aim at achieving essential requirements with regard to semantic, technical, organisational and legal interoperability. For each of these aspects national and/or regional rules should take into account standards and guidelines agreed on at the European level.

Recommendation at the EU level: An agreement is necessary on general guidelines with regard to the content of EHRs but it does not seem necessary to regulate this in detail. The agreement on the patient summary guidelines by the eHealth Network in November 2013 shows the right way to proceed. Agreements are also needed on a terminological profile for a minimum set of fields included in the patient summary; a technical profile for the cross-border exchange of patient summaries, in particular with regard to the security aspects; a list of the categories of healthcare professionals who can access the patient summary, including a solution for the secure authentication of these professionals and their authorisations, and a roadmap for the implementation of the cross-border exchange of patient summaries between Member States.

EHRs: security aspects

Considering the very sensitive nature of health data and the vulnerability and easy dissemination of information on electronic format, special attention should be paid to the security of data from EHRs. The Study shows, however, that half of the countries covered have not set specific rules for institutions hosting and managing EHRs, relying instead on the general rules setting security requirements for all types of data controllers. In addition, almost all the countries covered have not gone beyond Directive 95/46/EC in what relates to authorisation requirements. The authorisation procedure to host and process EHRs is, in the vast majority of countries, the same as to host and process other data. Also, only a minority of the countries has set specific auditing requirements for institutions hosting and managing EHRs.

Recommendation at national level: It should be left to the Member States themselves to choose the security measures which are most appropriate in the context of their specific situation, possibilities and context. Regarding the use of cloud services for hosting EHRs, Member States should refrain from introducing particular legal rules or even guidelines, codes of conduct or model service legal agreements (SLAs) without taking into account the European perspective. Unilateral initiatives in this field are moreover not in line with Directive 98/48/EC on the provision of information in the field of technical standards

Recommendation at the EU level: A binding European legal framework on basic user and access management that should also include operational rules on other security aspects such as end-to-end encryption (currently not possible because of the lack of a common encryption standard) and audit trails (who will be in charge of recovering data events in case of an incident) should be adopted. Agreement is also recommended on a model service level agreement for cloud services with regard to EHRs. The eHealth Network should closely follow up the progress made in this context and stimulate the development of European model provisions for cloud SLAs dedicated for eHealth services and EHRs in particular

Patient consent

With respect to the issue of patient consent relating to the creation and/or sharing of EHRs most of the countries covered by the Study can be divided into three groups:

- Some countries require explicit consent of the patient for the creation of an EHR (and a fortiori for the inclusion of (data extracted from) this EHR into a sharing system, plus, in addition for the access to the data in the EHR by other healthcare professionals than the one who collected the data);
- Some countries do not require explicit consent for the creation of an EHR but this explicit consent is needed for the inclusion of (data extracted from) this EHR into an EHR sharing system;
- Finally a number of countries do not require explicit consent neither for the creation of an EHR nor for the inclusion of (data extracted from) this EHR into a sharing system, but patient consent is needed for the access to the data in the EHR by other healthcare professionals than the one who collected the data.

For the three groups of countries, the form of the explicit consent varies considerably. For example, in the last group of countries, the patient consent needed for the access to the data in the EHR by other healthcare professionals than the one who collected the data, is deducted from the fact that the patient visits the professional to receive healthcare and hands over, for example, his/her health insurance card so that the EHR system of the professional reads data from this card.

Recommendation at national level: A three stage approach is recommended:
- When a patient visits a healthcare professional in order to receive care, this professional has the duty to keep a record of at least a minimum set of data related to the identity of this patient and related to the care provided; no additional implicit or explicit consent of the patient or even an opt-out possibility is thus needed at this stage.
- When, on the basis of national or regional law, public authorities decide to make available EHRs for exchange among healthcare professionals (e.g. in order to avoid unnecessary public healthcare costs), such EHR sharing systems can be established and include available individual EHRs without additional explicit consent of the patients. Member States are however free to introduce opt-out possibilities for this stage. This viewpoint corresponds to the one expressed by the Working Party in its opinion of 2007.
- When a patient visits a healthcare professional who wishes to receive or access health data collected from this patient by other healthcare providers (by means of the EHR sharing system), such access will require prior explicit consent of the patient concerned. This consent constitutes, at the same time, proof that this patient has engaged into a therapeutic relationship with the healthcare professional.

Recommendation at the EU level: An agreement should be reached by the eHealth Network on the "three-stage" model described in the previous recommendation, promoting this model as a European guideline for all Member States.

Creation access and update

Different categories of access to EHRs

Article 6(1)(c) of Directive 95/46/EC requires that the data processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. This "need-to-know" suggests that access should be role-based and limited to persons needing access. Even though a system that grants the same access rights for different types of health professionals would appear not to be in line with Directive 95/46/EC, the Study shows that this is actually the case in a small number of the countries covered. However, half of the countries do have different categories of access to EHRs for different health professionals. This is done either by defining different rules for different types of health professionals such as doctors, dentists, nurses or pharmacists, by defining different rules depending on the link between the patient and the different health professionals or by assigning to the healthcare providers the task of deciding which health professionals have access to which data.

Recommendation at national level: Member States should, despite the significant financial cost involved, establish certainty on the categories of healthcare professionals who can have access to patient summaries, and trustworthy official registers of those categories of professionals which can be used for authentication purposes and that need to be accessible on-line.

Recommendation at the EU level: An agreement on a list of the categories of healthcare professionals having access to patient summaries (and subsequently for the other priority use cases mentioned before) or a common definition of healthcare professional will most probably not be possible on a short term. An alternative could therefore be to leave it to each Member State to decide who should be considered as a health professional in the context of intra-European EHR exchange.

Patients' rights over the data

Directive 95/46/EC grants data subjects a series of rights over their data. These include right to access data, right to erase and correct data and the right to know who have accessed their data. These are, however, not absolute rights. Thus, there are a series of exemptions listed under Article 13 of Directive 95/46/EC, which if applied by Member States reduce the scope of the various patients' rights. In addition, the right to erase and correct data relates only to data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data. It is, in any case, for the Member States to define what specific measures must be put in place. The Study shows that patients are entitled to all of these rights in all countries covered but that only in some countries the national legislation goes beyond the minimum requirements of Directive 95/46/EC.

In all countries covered patients are entitled to access their EHRs and in half of them this right covers actually all data contained in EHRs. Another right directly connected with the right to access is the right to download data; although only one third of the countries covered by this Study allow the patient to download all or at least some of his/her EHR, in the other countries the patient is entitled to other similar rights.

With regards to the right to erase and correct data, the Study shows that in most countries patients do not have the right to directly erase or modify their data. In fact, no country allows patients to directly modify data that has not been inputted by the patients. Erasure of data not inputted by the patients is only allowed by two countries although other two allow patients to hide some data. Stakeholders from these countries have expressed their concern in this respect indicating their distrust for a system which does not guarantee completeness of information.

The Study also revealed that in the countries which have set specific provisions on the right to know who accessed EHRs, patients have usually access to this information directly online. This also happens in some countries which have not set specific rules in this respect.

Recommendation at national level: Member States should set specific rules allowing the data from EHRs to which the patient already has access, to be downloaded, as well as providing for the availability online of the information about who accessed EHRs. Where countries wish to grant patients the right to erase or hide data that has not been inputted by them, health professionals are at least notified that some data is missing, allowing them to try to convince the patients to disclose such data. It is also recommended that Member States take the necessary measures to implement any guidelines on access to EHRs that may be adopted at EU level.

Recommendation at the EU level: Agreement is recommended on a set of guidelines, e.g. on the possibility for patients to add, modify or erase data from EHRs. Information harmful to the patient should not be directly available to him/her allowing health professionals to decide to hide certain EHR information from the patient for up to six months so that they can personally communicate delicate diagnoses to the patient. The possibility for patients to modify data from EHRs that has not been

inputted by them should be expressly prohibited so as to allow health professionals from other countries to rely on the information available.

Liability

There are currently no detailed rules on the liability of health professionals with regard to health records in the EU. According to the comparative analysis, only a handful of countries have established specific medical liability rules with regard to EHRs, and these rules are mostly reinforcing or highlighting the general liability regime.

Recommendation at national level: It is recommended that Member States ensure that health professionals are informed and trained about their liabilities with regard to EHRs and how the existing rules at national level (either specific or general) apply in this context.

Recommendation at the EU level: The specific practical consequences of the application of the currently existing liability regime for data controllers, laid down in Article 23 of Directive 95/46/EC, on the EHR context should be clarified in order to improve legal certainty on this issue. Such clarification can be carried out in the form of guidelines on how to avoid liability issues, illustrated by typical examples of potential cases of negligence and/or of recommended behaviour.

Secondary use

The secondary use of health data is currently regulated at the EU level through Directive 95/46/EC which requires Member States to lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. The Study shows that more than half of the countries covered have set specific laws on the secondary use of health data while other rely on the general data protection rules. It also underlines that countries do not always have the same legal approach on the secondary use of health data (e.g. purpose assigned, safeguards). On safeguards, the Study reveals that several Member States do not require the anonymisation of health data or do not clearly specify when and how this process should take place (e.g. prior to being transmitted to research institutes). However the Working Party considers that 'whenever feasible and possible, data from EHR systems should be used for other purposes (e.g. statistics or quality evaluation) only in anonymised form or at least with secure pseudonymisation'. Several stakeholders interviewed also stressed the importance of the anonymisation of data and to set specific rules on this point.

Recommendation at national level: It is difficult to give recommendations to the Member States on how they have to fill in the delegation given to them by European legislator in Article 6(1) (b) of Directive 95/46/EC - the first and most urgent task is to develop a European framework (binding or not) in this field.

Recommendation at the EU level: Although the current version of the Draft Data Protection Regulation contains some positive new elements, Article 81(2)(a) should be reconsidered because it will maintain disparities between the Member States in this domain. The conditions for the further processing of health data for research purposes should be regulated at Union level.

Archiving durations

There are no specific rules at the EU level on the archiving of EHRs. However pursuant to Article 6(1)(e) of Directive 95/46/EC, personal data must be kept in a form which permits identification of data subject for no longer than necessary for the purposes for which the data were collected or for which they are further processed. This Study demonstrates that very few countries set specific rules on the maximum archiving duration of EHRs. Most of the countries provide a minimum storage period. The Study does not demonstrate that rules on archiving duration of EHRs are considered as a priority issue.

Recommendation at national level: Rules on minimum archiving duration of EHRs are primarily necessary to avoid destruction of health information that is still relevant. However, it is not necessary to translate this objective in precise archiving duration rules. It is not considered necessary to have specific rules on the archiving duration of EHRs when there are already specific rules on the archiving duration of medical data in general, however, it is recommended that Member States which have set very long periods of archiving, consider revising their approach in light of Article 6(1)(e) of Directive 95/46/EC.

Recommendation at the EU level: More precise legal rules on the EU level on this topic do not seem necessary.

EHRs and ePrescriptions

The objective of Directive 2011/24/EC is to improve the access to safe and high-quality cross-border health care and to promote cooperation on health care between Member States. The Directive acknowledges that the mutual recognition of prescriptions is a necessary element of cross-border health care, and envisages that the development of ePrescriptions can facilitate the prescription, dispensation and provision of medicinal products across borders. Yet, the Directive does not lay down any binding provision or common strategy for the coordinated deployment of ePrescriptions across Member States – Art. 11(2)(b) of Directive 2011/24/EC merely empowers the Commission to issue guidelines in this area.

Recommendation at national level: Member States should take into consideration the several positive synergies between EHRs and ePrescriptions. In case the two systems are linked, access to EHRs will be open for additional categories of health professionals (e.g. pharmacists) and therefore it is recommended to adopt a role based approach when setting access requirement.

Recommendation at the EU level: One of the most important current obstacles for the cross-border exchange of ePrescriptions, is the lack of a common data model and a common vocabulary for medicinal products or pharmaceutical products throughout Europe. Efforts to overcome this obstacle are directly useful for the exchange of EHRs because the medication part of the EHRs faces similar terminological challenges. Agreements on standards in this field should therefore simultaneously take into account the needs of cross-border exchange of EHRs, as well as of ePrescriptions.

2 INTRODUCTION TO THE PROJECT

2.1 BACKGROUND

2.1.1 Political context

The first action plan on eHealth was adopted by the European Commission in 2004[1] and set three target areas – address common challenges and create the right framework to support eHealth; launch pilot actions to jump start the delivery of eHealth; and promote the sharing of best practices and measure progress.

At the end of 2012, the European Commission adopted a new action plan "eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century".[2] In this new plan, the European Commission proposes a series of new measures, recognises that the promises of eHealth remain *"largely unfulfilled"* and expresses its commitment to remove the existing barriers to *"a fully mature and interoperable eHealth system in Europe".* These barriers are identified in the action plan and include the lack of confidence in, and the lack of interoperability between, eHealth solutions, for which a strong legal framework can be a solution - e.g. data protection rules can boost confidence in eHealth services, while setting EU-wide standards is clearly a precondition for achieving interoperability.

A recent report by the eHealth Task Force[3] called for the creation of *"a legal framework and space to manage the explosion of health data"*, referring specifically to the need to set principles to ensure the mutual compatibility of data and safeguard measures for security and privacy.

2.1.2 Cross-border eHealth services

Directive 2011/24/EU on the application of patients' rights in cross-border healthcare,[4] reflects the need to balance the deployment of health data and privacy safeguards by making clear that the objectives of eHealth – namely enhancing continuity of care and ensuring access to safe and high-quality healthcare – cannot be pursued in violation of EU data protection rules. The objective of Directive 2011/24/EU is described in its Recital 10 as *"to establish rules for facilitating access to safe and high-quality cross-border healthcare in the Union and to ensure patient mobility in accordance with the principles established by the Court of Justice"*. In accordance with Recital 25, the transfer of health data is essential to ensure continuity of healthcare across borders but at the same time the fundamental rights of the individuals must be assured.

Pursuant to Directive 2011/24/EU, the European Commission must adopt guidelines supporting the Member States in developing the interoperability of ePrescriptions (Article 11.2.b), in order to facilitate the recognition of prescriptions issued in another Member State (Article 11)[5], and set up an eHealth network[6] to draw up a series of guidelines to facilitate the cross-border transferability of

[1] Commission Communication "e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area" (COM (2004) 356 final).
[2] Commission Communication "eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century" (COM (2012) 736 final).
[3] eHealth Task Force Report "Redesigning health in Europe for 2020" (2012), available at http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/redesigning_health-eu-for2020-ehtf-report2012_01.pdf (4 June 2013)
[4] 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.
[5] The Commission has adopted for this purpose the Commission Implementing Directive 2012/52/EU of December 2012 laying down measures to facilitate the recognition of medical prescriptions issued in another Member State.
[6] The Commission adopted the 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. The first meeting of the eHealth Network was held in Copenhagen on 8 May 2012.

medical data (Article 14) [7]. One of the tasks of the eHealth network is, precisely, to make sure that the European eHealth systems attain "*a high level of trust and security"*.[8] However, until more specific EU legislation is adopted, achieving this goal will mainly depend on the regulatory frameworks at national level and on the different ways Member States have implemented Directive 95/46/EC[9].

2.1.3 Privacy of health data

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, is the core instrument of the EU legal framework on data protection and covers also health data. Article 8 of Directive 95/46/EC lists special categories of data of which, as a rule, Member States should prohibit the processing, and includes in such list "data concerning health". Exceptions to the general prohibition include consent from the data subject and cases 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 is processed by a health professional or by another person also subject to an obligation of secrecy. In the 2012 Proposal for a General Data Protection Regulation, reviewing Directive 95/46/EC, the European Commission proposed the inclusion of a definition of "data concerning health" and of a specific provision on "processing of personal data concerning health".[10]

The rights and duties enshrined in Directive 95/46/EC are evidently applicable to health data. Thus, e.g. pursuant to Article 10 of Directive 95/46/EC, a patient from whom data relating to him/her are collected must be aware of, among other information, the purpose of the collection and processing of data and the identity of the recipients or categories of recipients of the data. In addition, under Article 12(a) of Directive 95/46/EC, Member States must ensure that the patient has access to such information, but as the Directive does not refer to specific measures, different solutions are allowed to track who, why and when access to the patient's data. Possibilities to ensure this right can include, for example, having legal provisions on the obligation of notification to patient of access from third parties.

The issue of privacy of health data gained a whole new dimension with the development of eHealth. If traditionally the doctor-patient relationship was fairly simple – physical presence of the patient and personal interaction[11] – and, for example, there was little discussion on the ownership of medical records,[12] the resort to EHR raises a lot of new issues, requiring a much more sophisticated and nuanced approach. The Working Party in its Working Document on the Processing of personal data relating to health in electronic health records[13] also stressed that "*maintaining the legal standard of confidentiality suitable within a traditional paper record environment may be insufficient to protect the privacy interests of a patient once electronic health records are put online"*.

Besides, the European Commission, in order to keep EU law up to date with the new technological

[7] On its 4th meeting, which was held in Brussels on 19 November 2013, the eHealth Network adopted Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange in accordance with the cross-border Directive 2011/24/EU, available at http://ec.europa.eu/health/ehealth/docs/guidelines_patient_summary_en.pdf.
[8] Article 14(2)(a).
[9] 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.
[10] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (2012/0011 (COD). Article 81 of the proposed Regulation sets out the purposes for which the processing of personal data concerning health is allowed, if necessary and as long as suitable and specific measures to safeguard the data subject's legitimate interests are in place.
[11] Van Dooselaere, C., Herve, J., Silber, D. and Wilson, P. (2008) 'Legally eHealth - Putting eHealth in its European Legal Context', p. 6, available at http://www.epsos.eu/uploads/tx_epsosfileshare/Legally-eHealth-Report_01.pdf
[12] Wilson, P (2012), 'Legal frameworks for eHealth', p. 35,
available at http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf
[13] Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR) (00323/07/EN, WP 131), adopted on 15 February 2007.

developments, has proposed a series of new legislation on electronic data and electronic communications which will cover several eHealth related topics. Thus, Directive 1999/93/EC,[14] which established a Community framework for electronic signatures, is being replaced by a new Regulation on electronic identification and trust services.[15] In addition, a proposal for a new Directive on Network and Information Security,[16] tabled by the European Commission in the beginning of 2013, with the aim to ensure a high common level of network and information security, should bring a series of new obligations to public administrations and market operators controlling and using networks and information systems, including eHealth systems.

2.1.4 Objective of the Study

The Study seeks to identify and examine the national laws of the 28 Member States and Norway in order to identify legal barriers for the deployment of shared electronic health records[17] at national level and for their cross-border transfer within the EU. The definition of EHR contained in the Commission Recommendation of 2 July 2008[18] covers different types of electronic health records, some of which are not designed for a shared access; these were not covered by the Study. The Study focuses on the legal requirements applying the nationally organized systems of shared EHRs which can potentially participate in a European-wide sharing system. The ultimate goal of the Study is to make recommendations on how the national laws and the European framework must evolve to support cross-border eHealth services. The final recommendations will be presented to the European Commission and the eHealth Network in November 2014 for their endorsement.

2.2 METHODOLOGY

2.2.1 Completion of national reports

The completion of the national reports was done in two steps. First, legal experts carried out legal desk research to identify how EHRs are regulated in their respective national legislation. This legal research included the identification of the relevant legislation, but also any guidelines that set recommendations on how these requirements must be applied, interpretative case law and, where relevant, opinions from data protection authorities.

After the completion of the legal desk research, the national experts then proceeded with interviews of the relevant stakeholders, for which they used an indicative questionnaire developed by Milieu. They were requested, where relevant, to develop questions specific to the corresponding country. The experts during these interviews had to cross-check whether no information was missing from the desk research and identified potential legal barriers and good legal practices for the development of EHRs and also for the cross-border transfer of eHealth data from EHRs.

National experts had to carry out at least four interviews (i.e. hospital associations, health practitioners' associations, national authorities in charge of the implementation of EHR systems, national data protection supervisory authorities). Prior to the interview, experts had to send a request

[14] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[15] Proposal for a Regulation of the European Parliament and of the Council on Electronic identification and trust services for electronic transactions in the internal market (COM (2012 238 final).
[16] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM (2013) 48 final).
[17] EHRs are defined by the Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems as a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes.
[18] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C ((2008) 3282).

including information about the Study at hand. To secure a high response rate, a letter of introduction from DG SANCO was also prepared to support this request. On the basis of the outcome of the interviews with the relevant stakeholders, the national experts completed the national reports.

2.2.2 Draft comparative analysis

The information provided in the national reports form the basis of the comparative analysis of the legislation applying to EHRs. This analysis is facilitated by the common templates used by the national experts. On the basis of the national reports, we developed comparative tables in order to present, in a synthesised manner, the common or different regulatory approaches of the themes in the countries. These summary tables are mainly a tool to illustrate the analysis of the different and common regulatory approaches in these countries for each specific requirement:

It should be highlighted that the tables do not distinguish between existing and planned measures, so that a positive assessment ("√") is applied both where a measure is already operational and where it is merely planned. More in-depth information on each country can be found in the detailed analysis set out in the country reports.

2.2.3 Draft recommendations

The Draft Recommendations were built upon the findings of the comparative analysis and the section of the national reports on legal barriers and good practices identified by stakeholders. These findings enabled the contractor to make preliminary recommendations on how national laws and the European framework should evolve to allow the deployment of EHRs in the Member States and in Norway and to support cross-border eHealth services.

2.3 MAIN CHALLENGES ENCOUNTERED

- The term EHR is generic and can include many types of patient medical information stored in electronic form. Generally speaking, the data are collected from the individual patients in the context of the provision of care but, once collected, there is a wide variety of EHRs, e.g. with regard to the identification of the patient, the type and format of the data, the place of storage, the use of outsourcing and cloud computing services and more in particular the exchange of the collected data among healthcare practitioners having a therapeutic relationship with the patient.
- Readers of this report should be aware of the fact that the term "creation of an EHR" is ambiguous and take into account that, in some Member States, this concept refers directly to EHRs created to be shared among healthcare professionals. This is typically the case for France (the French report was used as a model for the other country reports).
- Whereas the use of EHR systems at the level of individual healthcare institutions or practitioners is widespread, the exchange among healthcare professionals of data extracted from these EHR systems is in several EU countries still at an early stage of development. As a result, the legal framework tends to evolve rapidly at national level, with new legal developments being proposed as this report was being drafted. This report endeavoured to reflect the latest legal developments in the countries covered even at the stage of proposal or draft laws. The reader should be warned that draft laws, proposed action plans and even adopted legal rules don't necessarily reflect the actual stage of development in the field.
- Several stakeholders mentioned that it was difficult to identify legal barriers or good practices for the deployment of EHRs or for the cross-border transfer since they could not draw conclusions on their national system that was either not implemented or at the pilot phase and/or no EHR legal text was yet adopted.
- In several countries, experts experienced a lack of available information on the policy and legal initiatives developed on EHRs.
- The research focused on one specific aspect of ePrescription systems – their relationship with

EHRs – and therefore it cannot give a complete, final assessment of the state of development of ePrescriptions or the legal barriers and best practices in this field. Moreover, stakeholders surveyed have given only little evidence on the operation of ePrescription systems. This may be because the research concentrated on EHRs, or because stakeholders held stronger views on EHRs than ePrescriptions, or simply because national programmes to roll out ePrescriptions are still relatively recent and practice has not had time to develop yet.

- Finally the Study does not enter into the discussion about the "ownership" of EHRs. The term "ownership" is commonly defined as "a legal title coupled with exclusive legal right to possession". Ownership is therefore closely linked to the notion of "property" ("owner" and "proprietor" are mostly considered as synonyms. Ownership or property can relate to material goods or immaterial goods. In the latter case the term "intellectual property" is mostly used. Data are immaterial goods but they can never be the object of intellectual property *as such*. This does not mean that data can never be the object of rights. For example, a person who makes a substantial investment in the obtaining, verification or presentation of data can have certain rights under the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. This person will, however, not be considered as the "owner" of the data.

3 COMPARATIVE ANALYSIS

The comparative analysis draws on the Country Studies, which can be found in Annex I. The first sub-section summarises the current status of the legal framework and the EHR system implementation in each Member State, while the remaining sub-sections are structured around the main themes listed in the Terms of Reference further refined during the pilot phase and agreed with the Commission:

- Health data to be included in EHRs;
- Requirement placed on the institutions hosting EHRs data;
- Patient consent;
- Creation, access to and updating of EHRs;
- Liability;
- Secondary uses;
- Archiving durations;
- Requirements on interoperability of EHRs;
- Links between EHRs and ePrescriptions.

3.1 OVERVIEW OF LEGAL APPROACHES AND STAGE OF IMPLEMENTATION OF EHR

This section provides an overview of the level of implementation of EHR systems allowing the access and update of EHRs by different health professionals in an interoperable structure. It also includes information on different legal approaches taken by Member States and Norway to regulate EHRs (e.g. specific law on EHRs or reliance on the general law on health in general or guidelines). It finally highlights the disparities of stage of development and legal approaches to regulate EHRs.

Table 1 *Summary table of stage of implementation of shared EHR systems and legal approaches*

Country	Stage of implementation	Legal context
Austria	Deployment phase of shared EHR system since 2012 (ELGA[19])	Specific legal framework for shared EHR system first phase of implementation measures adopted. Reliance on general health record and data protection for non-specific aspects
Belgium	Deployment of shared EHR systems since 2008	Specific legal framework for shared EHR systems at federal and regional level. Reliance on general health record and data protection for non-specific aspects
Bulgaria	Full implementation of a shared EHR system (PIS records)[20] since 2009	No specific legal provision applicable to PIS records General rules on health records, data protection, liability and secondary use apply to PIS records.

[19] Elektronische Gesundheitsakte

[20] The Personalised Information System (PIS) is an electronic record system set in place by the National Health Insurance Fund (NHIF).

Country	Stage of implementation	Legal context
Croatia	Pilot phase of a shared EHR system (CEZIH)[21] since 2006	Specific rules concerning EHRs Reliance on general health data legislation and data protection legislation for certain aspect of EHRs Legal initiative underway (e.g. requirement on patient access)
Cyprus	Deployment phase of shared EHR system (early stage) since 2012	No specific legal framework that regulates EHRs and ePrescriptions Reliance on general health and data protection law
Czech Republic	No shared EHR systems. Several policy initiative underway since 2013	No specific legislation on EHRs reliance on general health record legislation and data protection rules
Denmark	Full implementation of shared EHR systems since 2003	No specific and comprehensive legislation on EHRs Reliance on general legislation on patients' rights and health care professional's duties. Certain provisions of this legislation contain few specific rules targeting EHRs.
Estonia	Full implementation of shared EHR systems (ENHIS)[22] since 2008	Specific and comprehensive legislation on EHR systems
Finland	Deployment phase of a data transmission and archiving service (Kanta) [23] that ensure interoperability of regional EHR systems since 2007	Specific legislation on EHR system Reliance on general health law and data protection law for non-specific aspects Legal initiatives are in place (interoperability, information security, data protection and functionality)
France	Deployment phase of shared EHR system since 2006 (DMP[24])	Specific legislation on EHR system Reliance on general data protection and health legislation for non-specific aspects of EHRs
Germany	No shared EHR systems. Several policy initiative underway	General provision setting the general framework for the development of EHR system Reliance on general data protection and health record legislation
Greece	Pilot phase of a shared EHR system since 2014	Only general legislation on EHRs (requiring further regulation) Reliance on general health records legislation and data protection rules

[21] Central Information Health System of the Republic of Croatia
[22] Estonian National Health Information System
[23] Kanta-palvelut
[24] Personal Health Record (*dossier médical personnel*)

Country	Stage of implementation	Legal context
Hungary	Shared EHR system in place (health information registry where patient can access certain health information). Policy initiative to develop further shared EHR system	Reliance on general health records legislation and data protection rules
Ireland	No shared EHR system, but some policy initiatives underway	No specific legislation on EHRs but a proposal is under discussion Reliance on general data protection rules
Italy	Deployment phase of EHR system at regions and autonomous provinces	Legal obligation for region and autonomous provinces to develop EHRs Draft law specific on EHR
Latvia	Pilot phase of a shared EHR system since 2014	Only few legal provisions specific on EHRs but a proposal is under discussion Reliance on general health records legislation and data protection rules
Lithuania	Final phase of a shared EHR system to be completed in 2015	Specific legislation on EHRs Reliance on general health record legislation and data protection rules for certain aspects of EHRs
Luxembourg	Deployment phase of shared EHR system (RSC)[25] since 2012	Adoption of several provisions in general healthcare legislation setting the legal framework for the EHR system Implementing measures on the EHR system to be adopted Reliance on data protection law for non-specific aspects of EHRs
Malta	Shared EHR system (myHealth) since 2012	No specific legislation on EHRs Reliance on general health record legislation and data protection rules
Netherlands	Several shared EHR systems being deployed. Deployment of a shared EHR system (LSP)[26] since 2011 that has the potential of being a nationwide system.	No specific legislation on EHRs but a proposal is under discussion Reliance on general health records legislation and data protection rules
Norway	Pilot phase of a shared EHR system (Nasjonal Kjernejournal)[27] since 2013	Specific legislation on shared EHR system Reliance on general health record legislation and data protection rules for non-specific

[25] Records of Shared Care (Dossiers de Soins Partagé)
[26] The LSP (National Switch Point) makes exchange of medical data between the healthcare providers possible.
[27] The Nasjonal Kjernejournal is a central and inter-institutional health data filing system currently being introduced and tested in a few counties in Norway.

Country	Stage of implementation	Legal context
		aspects of EHRs
Poland	Shared EHR system under development foreseen by 2017	Specific legislation on shared EHR system Reliance on general health record legislation, patients' rights and data protection rules
Portugal	Deployment phase of a shared EHR system (RCU2)[28] since 2012	No specific legislation on EHRs (but for a ministerial order on content of EHRs) Reliance on general health records' legislation and data protection rules
Romania	Pilot phase of a shared EHR system (DES)[29] since 2013	No specific legislation on EHRs but several legal initiatives under discussion Reliance on general health legislation and data protection rules
Slovakia	Deployment phase of a shared EHR system since 2013(NHIS)[30]	Specific legislation on EHRs Reliance on general health record legislation and data protection and medical rules for non-specific aspects of EHRs
Slovenia	No shared EHR system, but some policy initiatives underway	No specific legislation on EHRs Reliance on general health record legislation and data protection rules
Spain	Shared EHR systems developed at regional level (at different stages of development) Interoperability system in deployment at state level (cross-regional e-patient summary system) since 2006	Specific legislation on shared e-patient summary at state level (a minima requirements possibility for regions to implement further measures) Reliance on general health record legislation and data protection rules (a minima requirements possibility for regions to implement further measures)
Sweden	Full implementation of a shared EHR system (NPO) since 2012[31]	Specific legislation on shared EHR system Reliance on general health record legislation for non-specific aspects of EHRs
UK[32]	Full implementation of a shared EHR system in the UK countries - England (SCR in 2008)[33], Scotland (ECS[34] in 2006, ePCS in 2009[35], KIS in 2013[36]),	Only few legal provisions specific on EHRs Reliance on an information governance

[28] Portuguese Patient Summary (RCU2 - Resumo Clinico Unico do Utente).
[29] Dosarul Electronic de Sanatate (DES).
[30] National Health Information System (NHIS).
[31] National Patient Summary (Nationell patientöversikt – NPÖ).
[32]The United Kingdom (UK) consists of four countries namely England, Scotland, Wales and Northern Ireland, each having separate national health systems. The major emphasis of the UK report was on England with references made to national summary records in the other UK countries when necessary.
[33] SCR _ Summary Care Record
[34] ECS - Emergency Care Summary
[35] ePCS - electronic Palliative Care Summary
[36] KIS - Key Information Summary

Country	Stage of implementation	Legal context
	Wales (IHR in 2005[37]) and Northern Ireland (ECS in 2008[38],NIECR in 2013[39])	framework which includes - general health record legislation, data protection legislation and medical rules Institutional guidelines on EHRs

3.1.1 Disparities of stage of development in countries

EHRs are in use in all countries covered by this Study. However there are major disparities between countries on the deployment of electronic health records part of an interoperable infrastructure that allows different healthcare providers to access and update health data in order to ensure the continuity of care of the patient. Czech Republic Germany, Ireland, Slovenia are only at the stage of policy initiatives to develop shared EHR systems. Croatia, Greece, Latvia, Norway, and Romania are testing shared EHR systems at the pilot phase. Austria, Belgium, Cyprus, France, Italy, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Slovakia are in the process of deploying EHR systems. Finally EHR systems are fully implemented in Bulgaria, Denmark, Hungary, Estonia, Finland, Malta, Netherlands, Sweden and UK.

3.1.2 Disparities of legal approaches

Table 1 highlights wide disparities of legal approaches to regulate EHRs in the countries covered. Austria, Belgium, Croatia, Estonia, Luxembourg, Lithuania Finland, France, Portugal, Poland, Norway, Slovakia, Spain (e-patient summary), Sweden have set specific legal requirements on shared EHRs. It should be noted that in all these countries several aspects of EHRs (e.g. archiving, secondary use) are regulated by general health records and data protection legislation. Countries that have developed EHR systems, such as Bulgaria, Denmark, and Hungary however, rely on general health records and data protection legislation to regulate all aspects of EHRs. Finally, a number of countries that are only at the stage of a policy initiative for the development of an EHR system have not adopted specific rules on EHRs.

3.1.3 Legal initiatives underway

Croatia, Italy, Luxembourg, Latvia, Ireland and Romania are preparing legal texts to specifically regulate EHRs.

3.2 HEALTH DATA TO BE INCLUDED IN EHRs

Determining what information should be included in EHRs requires balancing competing interests. On the one hand, comprehensive EHRs provide a better overview of the patient's health. They allow health professionals to provide more informed diagnosis and medical responses to patients. On the other hand, medical information in EHRs which can be more easily been accessed and replicated than information on paper-records can be particularly sensitive (e.g. information on sexual transmitted diseases, mental disorder, addictions to drugs or alcohol). This aspect finds explicit attention under EU law. The Charter of Fundamental Rights recognises every person's right to the protection of privacy and of personal data, and Directive 95/46/EC afford special protection to health data. The general principle in this Directive that data collected must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed' is particularly relevant for defining which data should be inserted into EHRs. Furthermore it is also important to analyse how EU

[37] IHR - Individual Health Record
[38] Emergency Care Summary (NIECR)
[39] Northern Ireland Electronic Care Record

Member States and Norway have regulated the sharing of information included in EHRs since different approaches may limit the interoperability between national systems (e.g. use of different terminology or categories of health data) and the cross-border transfer of health data.

This section provides an overview of the choices Member States have made to regulate information to be included in EHRs in general (shared or non-shared). It looks at whether countries have adopted legislation or not, on the following aspects:

- Whether the countries have adopted specific rules on the content of EHRs or not;
- Whether the countries provide a legal definition of EHRs or not;
- The different legal approaches on the content of EHRs, depending on the existence of detailed requirements on the content of EHRs;
- Whether the national legislation requires that EHRs include information beyond health data, and, if so, which type of information;
- Whether the national legislation refers to common terminology or code of systems or not.

3.2.1 Rules on the content of EHRs

As shown in the table below, many countries have specifically regulated the content of EHRs. This legislation however, is often specifically applicable to shared EHR systems. For example, the French law determines the content of the DMP or the Finnish law establishes which information participating healthcare professionals should transfer into the KANTA system. The table identifies countries where specific legal rules on EHR content are already adopted or on the point of being adopted.

Table 2 *Setting of specific rules on the content of EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific rules on EHR content	√					√	√	√	√	√	√	√	√			√	√	√	√					√	√		√	√	

The majority of countries (15) have adopted specific rules on the content of EHRs and Italy and Latvia are about to adopt such specific rules. Many of these countries, however, have general rules on the content of health records and do not distinguish in this respect between electronic and paper-based health records. Besides these general rules, these countries often adopt specific rules on the items of information to be included in the shared EHR systems they are setting up. Bulgaria, Belgium, Cyprus, Czech Republic, Hungary, Ireland, Malta, Poland, Norway and Slovenia and UK rely on general rules on health records to define the content of EHRs for both situations. For example, in Cyprus rules regarding the content of 'medical files' apply to shared or not-shared EHRs. Note that Romania is discussing the opportunity to prepare specific rules on the content of EHRs but no legal initiative has started yet. In Netherlands EHRs are regulated both by general rules on health records and electronic information systems.

3.2.2 Legal definition of EHRs

EHRs are defined by the Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems as a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes[40].
Table3 singles out those 15 countries which provide a legal definition of EHR or patient's summary.

[40] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C ((2008) 3282).

Table 3 *Countries with legal definition of EHRs or patient's summary*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Legal definition of EHR	√			√		√			√	√			√			√	√				√	√	√	√			√	√	

Around half of the countries (15) provide definitions of EHRs in legislative texts. It is again noteworthy that several legal definitions of EHRs include a reference to the sharing of health data between health institutions. For example in Germany EHR is defined as an application that supports the collection, processing and utilisation of data concerning medical findings, diagnoses, therapy measures, treatment reports and vaccinations for a comprehensive documentation of various medical cases [of one patient] between different medical institutions. Lithuania defines health records as the patient's electronic health items[41] collected from all health institutions operating in the system.

Greece, Spain, and UK (England) (in non-binding guidelines) provide a definition of patient summary. The definition of patient summary pursuant to the Greek legislation is in line with the definition of the epSOS project[42]. In the Spanish legislation, the 'summary clinical history' is defined as an electronic document, automatically generated and updated on the basis of data that healthcare professionals include in the full clinical history of the patient. Swedish legislation provides that the coordinated patient summary is an electronic system that allows a healthcare provider to give or receive direct access to personal data stored at another healthcare provider. Finally, in the UK (England) the Summary Care Record means the system for the automated uploading, storing and displaying of patient data relating to medications, allergies, adverse reactions and, where agreed with the contractor and subject to the patient's consent, any other data taken from the patient's electronic record.

3.2.3 Different legal approaches on the content of EHRs

Two broad approaches can be distinguished amongst the countries covered by the Study. While some countries, as identified in the table below, have set detailed requirements as to the content of EHRs, others do not specify what this content should be. In addition, in some countries with a decentralised system, the legislation defines a common set of health data categories which applies to all regions.

Table 4 *Existence of detailed requirements on the content of EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Detailed requirement on EHR content	√	√						√	√	√	√		√			√		√	√			√		√			√	√	√

- *Exhaustive list of health data*

Around half of the countries (15) set detailed requirements on the content of EHRs, but in most of these countries these detailed requirements are applicable to the specific shared EHR system established or planned in those countries. The degree of detail varies between countries. For example, the legal texts in Spain, Estonia and Slovakia contain several annexes that set detailed categories of

[41] Electronic health item is electronic data on the patient's physical or mental health status and records on the activities of healthcare institutions

[42] "The epSOS Patient Summary is a standardised set of basic medical data that includes the most important clinical facts required to ensure safe and secure healthcare.

health data that must be included in EHRs. While other countries, such as Luxembourg and Portugal, refer to general categories of data.

For example, pursuant to Luxembourg legislation, [shared EHR] must include information about the patient relevant and useful in order to promote safety, continuity of care, coordination of care as well as an efficient use of healthcare services. It must contain:

- Medical data in the form of medical reports, test results, reports of diagnostic investigations, medical prescriptions, medical imaging or any document related to the health or therapeutic treatment of a patient;
- Prescriptions made in the field of bio-medical analysis, medical imaging and possibly the related results;
- The history and records of the care of certain health care services;
- Information or declarations made by the patient him/herself.

- *Non-exhaustive list of health data*

On the other hand, the rest of the countries (14) do not define in detail the content of EHRs, either because they do not have shared EHR systems created or planned, or because they do not distinguish between electronic and paper-based health records, shared or not. For example, France limits itself to requiring that personal health data updated on EHRs is necessary for the coordination of health-related care given to the care recipient or be 'key elements of the stay' in a health institution[43]. Another example is the German legislation, which provides that medical findings, diagnoses, therapy measures, treatment reports and immunisations must be included in the EHR.

- *Common data categories in decentralised systems*

Both Italy (at a draft law level though) and Spain set minimum common health data categories that must be used in regions/Autonomous Communities as an 'a minima' requirement. For example, the draft implementing Decree in Italy distinguishes between a minimum content of data and documents and additional content. The minimum content is common to all EHRs regardless of the region or autonomous province in which they are issued, and it consists of identification data, health reports, emergency treatment reports, discharge letters, synthetic health profile, pharmaceutical dossier and consent to the donation of organs and tissues. The scope of additional content – an exemplary list of data and documents which may be included is set out in the draft law – must be defined by the regions and autonomous provinces.

Of particular interest is the Spanish approach to define, in a very detailed manner, the set of health data to be included in the summary of the clinical history [patient summary][44] . The minimum content of the Spanish summary clinical history includes an administrative part that covers the data on the institution emitting the document, data on the patient, including the Code NHS and European[45] or the clinical history number and address and, on the other side, the health data including the data in the protocol of clinical investigation, resolved, closed or inactive problems, problems and active episodes, treatment, nurses diagnostics, nursing results and interventions or subjective observations of professional staff.

[43] Note that the French law sets an obligation for the adoption of an implementing decree that should define in more details the content of the EHRs.
[44]This clinical history is an electronic document created automatically and updated from data introduced by health professionals and allows the continuity of care of a patient in the different Autonomous Communities (health professionals in one Autonomous Community can access the summary of clinical history of a patient affiliated to the healthcare system of another Autonomous Community).
[45] This category was created in case of adoption of a European Code for the identification of patients.

3.2.4 EHR restricted to health data

With regard to the type of data to be included in EHRs as described in the table below, the great majority of the countries require EHR to cover health data only

Table 5 *Countries which restrict EHRs to health data*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
EHR restricted to health data	√	√	√	√	√	√					√				√		√		√	√	√		√	√	√		√		√

More than half of the countries (17), apart from general administrative information on the patient (e.g. name, gender, date of birth, national insurance number), require that only health data is included in EHRs. Bulgaria Luxembourg, France and Italy allow that information can be added on EHRs about patient donation of organs.

On the other hand, in several countries EHRs are not only restricted to health data (12). The additional data which should be included in EHRs are very diverse. This information covers various personal data ranging from profession to health habits or criminal offences.

In Croatia, the EHRs must also include information on insured person's work and profession related data, but also specific habits (smoking, alcohol drinking and addiction to drugs). In Denmark, the name of patients' relatives must be specified. In Estonia, the EHRs must include the patient's employer and profession, description of work conditions, educational institution, the family situation, health habits, psychosocial background and development, mental background and development. In France, the EHRs include a section on prevention which will cover medico-social information. In Greece, the medical records must also contain the father's name and the occupation of the patient. In Hungary, the occupation of the patient must also be included. In Italy, the EHRs contain, in addition to health data, 'socio-health' data. However, no clear definition of what this covers is provided. In Luxembourg, the law allows the patient to complete a section of the EHR where he/she can provide additional information or declarations. In Slovenia, the marital status, the education and the profession of a patient must be included in EHRs. In Spain, the occupation of a patient must be indicated. Sweden allows information to be included about criminal offences of a patient, only if there is an absolute necessity to do so. Romania is discussing the possibility of adding in the EHRs information on religion, occupation, lifestyle/behaviour, family history. There is however no legal initiative for the moment and the current EHRs are restricted to health data.

3.2.5 Common terminology and clinical coding systems mentioned in law

While all countries apply in practice terminology and clinical coding systems (e.g. SNOMED Clinical Terms, NOMESCO[46], ICD-10 International Classification of Diseases), as indicated in the table below, less than half of the countries provide in their legislation, references to the use of the common terminology and clinical coding of systems related to health data. Furthermore, the terminology and coding systems to define and categorise health information differ from one country to another.

Table 6 *Countries with rules on common terminology or code of systems*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Rules on	√		√				√		√	√	√					√	√					√	√	√		√	√	√	√

[46] The Nordic Medico-Statistical Committee classification

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
termino-logy or code																													

Fourteen countries have set a legal requirement to use common health terminology or specific clinical coding systems. In such cases, the legislation refers to national, regional or international nomenclatures and codes, showing a wide variety of different approaches to define and categorise health information across the countries covered

For example, the legislation in Austria provides that health terminology must be defined by the Minister of Health and published on their website, and the use of this terminology is obligatory. The Bulgarian legislation mentions that the health data system must use established national codes and nomenclatures for registration and reporting activities in healthcare. In Italy, the draft implementing decree provides that EHR information shall be codified and classified in such a way as to ensure interoperability at regional, national and European level. An annex to the draft implementing decree sets out the applicable codification and classification rules. The draft law in Latvia states that for the entries regarding surgeries, NOMESCO classification should be used and for Surgical Procedures Classification NCSP+ should be used. For diseases, disorders and disability ICD-10 International Classification of Diseases Latvian adapted version (SSK-10) should be used. The Portuguese legal text refers to international coding systems and standards (i.e. International Classification for Nursing Practice, International Classification of Diseases) and national coding systems (i.e. National list of medicines and health products of the National Authority of Medicines and Health Products, National list of support products of the National Institute of Rehabilitation). In Poland the legislation provides that the International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, is used for names and statistical numbers of diseases diagnosed.

In Slovakia, the law provides that in the patient summary, diseases should be identified according to the codes of diseases defined in the International Classification of Diseases with its detailed specification for the diseases of the patient in the past six months. The UK (England) uses common terminology and code systems based on the SNOMED Clinical Terms.

3.3 REQUIREMENTS ON INSTITUTIONS HOSTING AND MANAGING EHRs

Article 17 (1) of Directive 95/46/EC requires Member States to provide that the data controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, taking into account the state of the art and the cost of their implementation. The sensitive nature of health data would always require that institutions hosting and processing EHRs should ensure a high level of security, but it is for the Member States to define what specific measures must be put in place.

This section provides an overview of the choices the countries covered have made in this respect, showing, in particular, whether they have established specific rules on hosting and management of EHRs, required a specific authorisation to host and process EHRs (i.e. that goes beyond the notification procedure provided for in Article 18 of Directive 95/46/EC), set any kind of legal obligation to have the data encrypted or set specific auditing requirements for the institutions hosting and managing EHRs.

3.3.1 Specific rules on hosting and processing of EHRs

The table below identifies the countries which have set (or are about to set) specific rules on the hosting and processing of EHRs.

Table 7 *Countries with specific rules on the hosting and processing of EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific rules	√				√			√	√	√	√	√	√				√		√			√	√				√	√	√

While all the countries covered by the Study have data protection rules that would apply to institutions hosting and processing EHRs, only half of them (15) have set specific rules. In most countries, these rules were set by the laws that established the respective EHRs systems, or in subsequent regulations; this is the case for Austria, Estonia or Slovakia. In France, the rules are set in the Public Health Code, which was amended by the law setting the French EHR system. In the Czech Republic, it is the Act on Health Service that sets the requirements for health data to be kept in an electronic form.

It should be noted that in Latvia the rules applying to institutions hosting and processing EHRs are contained in legislation that was still not adopted. In the UK (England), the rules stem from contractual obligations placed on healthcare providers and information governance requirements including good practice guidelines issued by the government.

3.3.2 Specific authorisation

Pursuant to Article 18 of Directive 95/46/EC, Member States must provide that the data controller must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. Article 19 defines the minimum requirements of such notification.

Most of the countries covered do not go beyond the provisions of Directive 95/46/EC, but a small group has set specific authorisation requirements for hosting and processing of EHRs. The table below identifies the countries which require a specific authorisation for the hosting and processing of EHRs.

Table 8 *Countries requiring a specific authorisation for the hosting and processing of EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific authorisation						√					√	√							√								√		√

France has adopted very detailed requirements applicable to the institutions hosting EHRs data: applicants must provide extensive information demonstrating that their hosting system is secure and sophisticated enough to ensure that the rules on EHRs (e.g. consent, access, confidentiality) are fulfilled and that health data is well protected, especially considering the risk. In Slovakia, the current legislation provides only general principles and the legal basis for implementing legislation to define standards for medical IT information systems (yet to be adopted).

In Finland, the data systems of institutions hosting and processing data must comply with essential interoperability requirements and obtain a certificate of conformity issued by the information security inspection body. In Latvia, the draft legislation requires institutions to obtain prior authorisation by concluding a written agreement with the National Health Service and showing compliance with security, connectivity and confidentiality requirements of the internal systems.

In the UK (England), a standard services contract is required to be signed by a contractor providing medical services to the National Health Service and contains provisions for keeping computerised records. In addition, institutions need to adhere to specific information governance requirements.

3.3.3 Legal requirement for encrypted data

Encryption of data is one of the most common ways to ensure data security. Data is translated into a secret code i.e. encrypted; in order to decrypt these data, a password or key will be needed. In practice, in almost all of the countries covered, data from EHRs is encrypted in some form or at least in certain circumstances. In several cases this results from the advice of the data protection authorities on data protection like in Denmark, Greece or Portugal. In other cases, like Bulgaria, this obligation results from general data protection rules that are applicable to EHRs.

Only a very small group of countries established a legal obligation specific for the encryption of data from EHRs, the table below identifies these countries.

Table 9 *Countries establishing a legal obligation to encrypt data from EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Legal obligation to encrypt data	√															√						√	√						

In Austria, although there is not a general obligation to store the information in encrypted form, health data must be encrypted when stored in cloud computing storage environments; the transfer of health data is only allowed on closed networks or in encrypted form. In Italy, encryption is required by the proposed legislation still to be adopted. In Norway, health data that directly identifies a person must be encrypted, however this does not apply to the national database for electronic prescriptions. In Poland, healthcare providers must also ensure that data are encrypted.

3.3.4 Specific auditing requirements

Even though all the countries covered have general auditing requirements that are applicable to institutions' hosting and processing of EHRs, only a few of them have set auditing requirements specific to EHRs.

Table 10 *Countries with specific auditing requirements for institutions' hosting and processing of EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific auditing requirements								√			√	√				√						√						√	√

In Estonia, security systems are independently audited every two years. In France, once the licence for hosting EHRs expires, the hosting institution can ask for renewal, which will include, inter alia, an external audit attesting the implementation of privacy and security policy. Swedish healthcare providers are responsible to implement measures to keep logs[47] on the access to patients' records; the

[47] Logs or audit trails register the system threads of access or changes and are useful to know who and when had access to the patient's records.

verification of logs should be done regularly and systematically and be documented and the logs should be stored for at least 10 years.

In Norway, the specific legislation adopted in 2013 sets a series of rules on internal control institutions hosting and processing of EHRs. The standard services contract that contractors are required to sign in the UK (England) in order to be able to provide medical services to the National Health Service mandates that the auditing functions of the computerised system must be enabled. In Finland, it is required the external auditing of the data systems of institutions hosting and processing of EHRs as well as the continuing self-auditing for users of the data systems (health care providers and pharmacies). Italy is also planning to set specific requirements on operators tracking and audit.

3.4 PATIENT CONSENT

The concept of informed consent is directly related to the principle of the autonomy of the patient and therefore it is understandable that most legislation on EHRs "includes the requirement to seek a patient's consent before collecting, processing, or sharing health related information" to ensure that the right to privacy of health data is respected.[48] Consent is, under Article 8(2)(a) of Directive 95/46/EC, one of the exceptions to the general rule of prohibition of the processing of special categories of data, including data concerning health; in accordance with the definition of the same Directive, the consent must be freely given, specific and informed.[49] As with the content of the patient's summary, the options taken by the legislator on the consent of the data subject will have influence on the whole eHealth system and on the interoperability with other systems. A general "opt-in" solution, where the patient would have to give his/her consent every time data were added to his/her EHR, would certainly be coherent with the data protection requirements of Directive 95/46/EC, but may hamper an effective eHealth system. While a general "opt-out" solution may appear to some not to be in line with the requirement of having specific consent. The Working Party favoured an intermediate solution which could *"guarantee the necessary amount of protection on the one hand and the necessary practicability and flexibility on the other hand"*.[50] The Working Party is of the opinion that the exemption of Article 8 (3), to process personal data without the explicit consent of the data subject, could only pertain to the processing of medical data strictly for those medical and healthcare purposes mentioned there, and strictly under the conditions that processing is "required" and done by a health professional or by another person subject to an obligation of professional or equivalent secrecy. In the context of EHR, the Article 29 Working Party notes that the arguments for introducing EHR systems may, however, establish "substantial public interest" (Art. 8 (4) of Directive 95/46/EC). It argues that in some Member States a 'right to health protection' is enshrined in the constitution which would underline the importance attributed to all appropriate means to achieve a high level of "health protection". An EHR system in such legal environments would, according to the Working Party, certainly be founded on "substantial public interest" as it is an "instrument fundamentally intended to guarantee adequate medical assistance to patients"[51].

According to the Working Party, Article 8(4) of the Directive could, therefore, serve as a legal basis for EHR systems, provided that all the conditions mentioned therein are fulfilled. In particular, suitable safeguards for the protection of personal data in an EHR system must be provided for. The patient's self-determination concerning when and how his/her data are used should have a significant role as a major safeguard. The Working Party introduces at this point the distinction between "consent" and "agreement". "The functionality of "agreeing" in the context of suitable safeguards is different from "consent" under Article 8 (2) of the Directive and therefore needs not to meet with all requirements of Article 8 (2): e.g. whereas consent as a legal basis for processing health data would

[48] Wilson, P (2012), 'Legal frameworks for eHealth', p. 19 (June 2013).
[49] Article 2(h) Directive 95/46/EC.
[50] Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR) (00323/07/EN, WP 131), adopted on 15 February 2007
[51] ibid., p.13

always have to be "explicit" according to Article 8 (2), agreement as a safeguard need not necessarily be given in form of an opt-in – the possibility to express self-determination could – depending on the situation – also be offered in form of an opt-out/ a right to refuse."[52].

The view that the concept of consent is in fact not the most adequate basis for processing data in eHealth applications is also shared by literature[53]. Van Dooselaere and others stress that the European Commission should *"co-ordinate the adoption of specific rules for the processing of health information to allow for proper balancing of patients' and public health interests, without recourse to the concept of consent".*[54] Although Article 8 of Directive 95/46/EC gives several exemptions[55] (other than patient consent) to the prohibition on processing medical data, in some Member States, patient consent is needed for the creation of an EHR and also for access to an EHR (unless the patient is unable to give it, e.g. due to being temporarily incapacitated by medication). Arguably, there may be valid public health reasons for making EHRs mandatory for every patient[56] and for giving healthcare professionals lawful authority to access an EHR even when a patient wilfully withholds his/her consent[57].

This section provides an overview on the stances taken by the countries covered by this Study. In particular, it investigates which legal or practical solutions have been chosen with respect to the following aspects:

- Whether there is specific legislation on patient consent as regards EHRs or not;
- For what consent is required – creation and/or sharing of EHRs;
- Whether opting-in or opting-out are foreseen by the relevant legislation or not;
- Whether there are legal information requirements prior to the creation of EHRS or not;
- Whether consent must be given in writing or not;
- Whether consent is required for cross-border access or not.

3.4.1 Specific rules on patient's consent

Only few countries have specific legal rules regulating the patient's consent in relation to EHRs in place. As shown in the table below, less than half of the countries covered by this Study (13) have legal rules on patient consent in relation to EHRs in place.

Table 11 *Countries with legal rules on patient consent*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific legal rules on consent	√	√				√	√			√	√	√	√			√		√	√									√	√

The fact that a country has specific rules on consent in relation to EHRs in place does not necessarily imply that the patient's consent is required for the establishment of an EHR. For example, Belgium

[52] Ibid. as note 46, p. 13-14

[53] Van Dooselaere, C., Herve, J., Silber, D. and Wilson, P. "Legally eHealth, Deliverable 5 – Final Recommendations on Legal Issues in eHealth" (2007), p.22 -23, available at http://www.ehma.org/files/Legally_eHealth-Del_05-Recommendations2.pdf

[54] Van Dooselaere, C., Herve, J., Silber, D. and Wilson, P. "Legally eHealth, Deliverable 5 – Final Recommendations on Legal Issues in eHealth" (2007), p.22 -23, available at http://www.ehma.org/files/Legally_eHealth-Del_05-Recommendations2.pdf

[55] E.g. Article 8(3) of Directive 95/46/EC gives an exemption to the prohibition of processing health data where such 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 […]".*

[56] E.g. to facilitate epidemiological studies.

[57] E.g. to investigate public health emergencies.

has legislation on EHRs in place but does not require the consent of the patient for the setting up of the EHR (but sometimes for the sharing); the same applies to Denmark, Estonia, Finland Spain and Sweden. Draft legislation in Italy, on the other hand, stipulates that the patient's free and informed consent is necessary for information to be included in the EHR. It further clarifies that failure to consent access to EHR data does not prejudice the patient's right to health services.

In all of the countries, general rules on data protection and often also general rules on health data apply. Among these countries, the requirements are not uniform either. In most of the countries, like for instance, in Cyprus, Ireland, Lithuania, Portugal, Romania, Slovakia and Slovenia, general rules apply but no consent is required for the setting up of EHRs. It may, however, be required for the sharing of data, for example in Cyprus and Ireland. Greece and Bulgaria do not have specific rules on EHRs in place and the general legislation on data protection applies. In contrast to Greece, Bulgaria does have an EHR system in place. The EHR is, however, set up automatically for every insured person covered by the Health Insurance Law.

3.4.2 Rules on patient's consent to create EHRs

Rules on the requirement of the patient's consent to create EHRs have been identified in only the seven countries set out in the table below.

Table 12 *Countries requiring consent to create EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Consent required for creation	√					√						√	√			√		√										√	√

It should be noted that in the case of Austria, Luxembourg, Norway, Sweden and the UK (England)[58], the consent is implied, and patients have the choice to opt-out(see below the section on opt-out). The extent to which the consent is voluntary in Croatia is questionable. Here, the use of services of 'primary healthcare doctors', such as GPs and dentists, is conditioned by the patients giving their consent to the creation of an EHR. It should also be noted that, under Norwegian legislation, no consent is required for the processing of non-anonymised health data where this is necessary 'to achieve the purpose of the register'. Relevant registers are, not only the System of Notification of Infectious Diseases but also, for example, the Cancer Registry and the Norwegian Register of Patient Records. In practice, consent will therefore not be required in many cases.

A relatively large number of countries apply general data protection laws and do not require the patient's consent to process health data. For example, Belgium has transposed Article 8(3) of the Directive 95/46/EC literally. It thus states that the prohibition to process personal data concerning health must not apply 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 to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. This approach has been taken, in the same or similar forms, by Lithuania, Portugal, Romania, Slovakia and Slovenia.

The table below identifies the (four) countries that have chosen an opt-in approach for the creation of EHRs and those (three) countries that have chosen an opt-out approach.

[58] Note that in the UK consent is not required for a GP or hospital to create an EHR, however for the summary record (e.g. SCR in England) consent is implied but patients can opt-out

Table 13 *Approach to the creation of EHRs: opt-in versus opt-out*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Opt-in option						√						√	√			√													
Opt-out option	√																	√										√	√

The countries that require the patient's consent for the creation of EHRs can be split in two groups: Those countries where the patient must actively give their consent to the EHR to be created (opts-in) and those countries where the patient's EHRs are created by default, unless the patient objects (or 'opts out'). The first group covers Croatia, France, Germany and Italy. The second group consists of Austria, Luxembourg and the UK (England). In the UK (England), for example, a Summary Care Record (SCR) is created with the (implicit) consent of a patient. A SCR by default only contains a patient's medications, adverse reactions and allergies (core information). Additional information can be added to the SCR with the consent of the patient. All patients (16 years and over) are sent information packs containing a letter from their Clinical Commissioning Group, a Patient Summary leaflet and a Freepost opt-out form. Patients are given a period of time (about 12 weeks) to decide whether they wish to have an SCR created for them. They can seek further advice via various sign-posted information sources. If they wish to have an SCR they are not required to take any action and one will be created for them. If they do not wish to have an SCR they are required to complete the opt-out form and return it to their GP practice.

3.4.3 Rules on patient's consent to share the health data

The table below identifies only those nine countries in which legislation requires, under certain circumstances, the patient's consent for his/her EHR to be shared.

Table 14 *Countries requiring consent to share EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Consent required for sharing	√						√	√			√	√	√					√		√	√	√						√	√

The countries in which legislation requires the patient's consent for his/her EHR to be shared can be divided into two groups.

The first group is the group of countries where an explicit consent is required for EHRs to be shared but often this explicit consent is not necessary for sharing data among healthcare providers having a therapeutic relationship with the data subject. This group consists of Croatia, Denmark, Estonia, Finland, France, Germany, Luxembourg, the Netherlands, Norway, Sweden, and (to a certain extent) the UK (England). For example, under Danish legislation certain situations do not require an explicit consent. These situations are listed in the relevant Act. For these cases the legislator assumes 'implied acceptance' by the patient. In addition, the treatment of the patient must require that his/her data are shared. A similar policy applies in Finland where the legislation also provides for certain exemptions from the requirement of informed consent. In the Netherlands, the rule is that explicit consent is required for sharing data by healthcare practitioners with third parties, unless there is a 'treatment relation' with the third party in case of 'push traffic'[59]. In Hungary, the explicit consent is not required,

[59] The Code of Conduct on Electronic Data Exchange in Healthcare makes a distinction between 'pull traffic' and 'push traffic'. The term 'pull traffic' is used if a healthcare provider discloses data from his medical file to a group of healthcare

except if data regarding previous treatments is to be shared. In Sweden an explicit consent of the patient is not needed to include the health information of that patient into the national EHR sharing system (NPÖ) but this consent is needed before an individual professional is allowed to access the data. The particular situation in the UK (England) is described in greater detail below (opt-in for sharing).

The second group are those countries where consent is always implied. These are Austria, Estonia and France. The situation in Austria is described in greater detail below (opt-out). In France, the patient's explicit consent is mandatory for the creation of the DMP. Once a DMP is created, no additional explicit consent is required for the sharing. For the sharing, consent is implied. A similar approach is taken by Estonia, where initial patient consent to share data for the purpose of providing healthcare services is not required.

Two countries (Malta and Ireland) require the patient's consent to share their EHRs under the general data protection laws but these laws are of course transpositions of the European Directive 95/46 and sharing EHR information will therefore also possible on the basis of the (other) exemptions provided for by Article 8 of this Directive. The other countries do not require the patient's consent to sharing their EHRs, at least not as long as the data are used for medical purposes concerning the respective patient.

In the table below, countries are identified which have chosen to apply an opt-in or opt-out option as regards the sharing of EHRs.

Table 15 *Approach the sharing of EHRs: opt-in versus opt-out*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Opt-in option						√												√									√		√
Opt-out option	√						√	√				√		√								√						√	

In the category of 'opt-in', only those countries are included that require an explicit consent each time EHRs are shared. This is the case in only three countries: Germany, Luxembourg and with respect to sharing data with specialised physicians, Slovakia. As explained in the introduction to this report, Luxembourg does not have any legislation in place yet containing a requirement on patient consent. Luxembourg, however, decided to adopt an opt-out approach for the creation of its EHR-system and the processing of related health data. During the pilot phase, the consent from patients is needed to create an EHR. After the pilot phase, an RSC will be created for all patients and patients will have the opportunity to opt-out. The patient will be entitled to decide which health professionals can have access to the RSC. Furthermore each time patients visit a health professional, they must consent on the access by the health professional to their EHR by giving a 'presence password' that documents that the patient is physically present at the health professional's premises and accepts the access. The patient has, hence, to opt-in each time they visit a healthcare professional. A similar approach is taken in the UK (England) as regards SCRs (Summary Care Records). Patient consent is required each time an SCR needs to be viewed. If the patient is unable to consent at the specific time (e.g. due to being unconscious) and it is in the best interests of the patient to view their SCR, then the SCR will be accessed without the patient's permission, but this access will be noted on the patient's SCR. As mentioned before, this is also the approach followed in Sweden.

In Slovakia, there are opt-in rules for patient consent but only in relation to granting access to

providers who need to take the initiative to consult the data. Push traffic' involves the sending of personal data to the healthcare provider who has a treatment relationship with the person in question, who will receive the data without having to take the initiative or without having to undertake any additional action.

specialised physicians. If the patients would like a specialised physician to have full access to their EHR, they must give their consent.

The group of countries which have chosen an opt-out approach are those which provide patients an option to object to sharing their EHRs partially or totally. Austria, for example, is currently implementing a new legislation according to which all insured patients have EHRs by default. However, the patient may exclude all data or certain data to be shared and can also exclude certain healthcare providers from being granted access to their EHRs. This flexibility is also allowed under Estonian, French, Hungarian and Spanish legislation. Spanish legislation seems to restrict the opt-out, however, to historical health data. In addition, under Spanish legislation, the healthcare provider that would have been excluded from the access would be notified of this fact. The Danish law differs in that an opt-out is only granted in those cases where explicit consent is not required.

3.4.4 Patient's right to be informed before the creation of EHRs

Whether a country requires the information of the patient prior to the creation of EHRs can be seen in the table below. However, this table only shows which countries have introduced *specific* legal rules with regard to the information to be provided before the creation of EHRs. In all other countries the duty to inform the patient is based on the general European and national data protection legislation. It should thus be clear that there is no country where EHRs can be created without informing the patient in one way or another.

Table 16 *Specific right to be informed prior to EHR creation*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Information requirements prior to EHR creation						√					√	√				√						√		√				√	√

Only few countries covered by this Study have established a specific legal requirement to inform the patient of the content of the EHR and their rights before the EHR is put in place. The ways to do this vary. In Finland, a healthcare service provider, which has joined the national data system services, must inform the patient of these services and other relevant information, such as the rights of the patient, at the latest in connection with the first service. Under French legislation, the patient must be provided with an information paper leaflet in an accessible manner for all patients Also, under German legislation, the patient must be informed; the form is however, not specified. In addition, it is not certain that this requirement which currently applies with respect to the use of the eHealth Card (before its first use) will be applicable also to EHRs. The draft Italian decree stipulates that information must include, among other things, the advantages of EHR, the clarification that the patient's refusal does not in any way affect their right to health care services, and the indication of the category of persons who will have access to the EHR. Similar provisions are in place in Norway. In the UK (England), before the creation of an SCR, information about purposes of an SCR is sent to the patients and they are also directed to additional sources of information about the SCR. Also an opt-out form is sent to the patients in case that they do not want an SCR to be created. It should be noted that Austria does not have an information requirement in place although patients must actively opt-out if they do not want their health data to be recorded in an EHR.

3.4.5 Written consent

The below table identifies the countries that require the patient's written consent for the creation and/or sharing of an EHR.

Table 17 *Countries requiring written consent*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Consent in writing											√		√																

Only Croatia and Finland require that the patient must submit his/her consent in writing to be effective. For Finland however this written consent specifically applies to the KANTA archiving system. There is, of course, not an obligation to collect a written consent before creating or sharing EHRs in general. In Norway, the Patients' Rights Act provides that the relevant Ministry may issue regulations regarding a requirement of written consent. In Germany (which does not require written consent), the consent is 'documented' on the E-Health-Card.

3.4.6 Consent to cross-border access

No country covered by this Study requires patient consent for cross-border access. Generally cross border access to EHRs is not operational.

3.5 CREATION, ACCESS AND UPDATE OF EHRS

Health professionals

The general obligation to prohibit the processing of health data implies that only very few individuals or institutions should have access to such information and the possibility to erase it or somehow change that information. Therefore, it is important to know how Member States determine who can create EHRs, who can access their information and who can update the data. The "need-to-know principle", a derivation from Article 6(1) of Directive 95/46/EC would advise that access is role-based and limited to those needing access. Since the main purpose of EHRs is medical treatment and other related purposes, in principle health professionals should have access to their content. In order for an EHR access management system to take this principle into account, it must be backed up by reliable "identification and authentication" of the health professionals.

The question of access to EHRs by health professionals is quite complex. It may happen that not all health professionals have the same rights (both access and creation/updating rights) making it possible, for example, that a specialist may have access to more information than a general practitioner, who in turn will be able to access more data than a nurse or a pharmacist. In addition, some professions which work also in the health sector can actually have access denied due to possible conflicts of interests (e.g. occupational physicians). On the contrary, in cases of emergency, the access requirements will not be so strict. It is also important to know whether Member States have determined not only rights, but also duties for health professionals.

This section provides an overview of the choices Member States have made to regulate the identification and authentication of health professionals, as well as who exactly can create and access EHRs – including also who has been explicitly excluded from having access and who only has access in exceptional circumstances – or whether there is a legal obligation to update EHRs in place.

3.5.1 Rules for the identification and authentication of health professionals

The table below indicates whether or not the countries have set specific rules on the identification and authentication of health professionals. If they have, the table distinguishes between those that set rules requiring the use of e-signature or smartcards.

Table 18 *Setting of rules on the identification and authentication of health professionals*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
e-signature / smart-cards	√		√			√	√			√	√	√	√	√			√			√					√		√	√	√
Other		√		√				√								√							√	√					
No specific rules					√				√						√			√	√		√	√				√			

About half of the countries covered by this Study have clear rules for the authentication and identification of health professionals; in most of these cases, the rules result from internal procedures or practical guides and are not established by law. The remaining half has either, not defined any rules, or just set general principles stressing the need for a proper identification of health professionals accessing data from EHRs.

Among the countries which have defined rules, the use of electronic cards, whether alone or accompanied by a personal password or an e-signature, is clearly the preferred option for the authentication and identification of health professionals. Normally, the electronic card used to identify health professionals is specific for health purposes, but for example in Malta the personal national e-ID is used.

Other approaches include the use of a username and password; this is the case for Cyprus. In Belgium, the eHealth-platform has a strict user and access management system and checks in authentic sources whether or not a health professional is registered. Additionally the healthcare professional has to provide evidence of a therapeutic relationship with the patient from whom he requests to access health-related data; the evidence of the therapeutic relationship can be provided by various means. In Italy, the draft legislation lays down provisions on the profiling and authentication of persons who can access EHRs but does not refer expressly to a specific method .In Poland, users are identified either with a qualified certificate or the so-called "trusted profile" provided by the Electronic Platform of Public Administration Services. In Portugal, the access is made through the local applications of the healthcare providers, in accordance with their own internal rules for authentication and identification (in Portugal these applications connect directly with the centralised Platform for Health Data).

3.5.2 Creation of EHRs

The section summarises whether or not the countries have set specific rules on the creation of EHRs and, when this is the case, whether it falls under the responsibility of health professionals or other individuals or organisations.

About half of the countries (14) covered by this Study have either no specific rules on who can create EHRs or rely on general rules for the creation of medical records or general data protection rules (which would apply independently of the format of such records). When there are no specific rules on the creation of EHRs, the norm is that this task will fall on health professionals; likewise, in the vast majority of the countries where there are specific rules, it is for the health professionals to create EHRs.

The type of health professionals able to create EHRs is seldom specified. In Greece, Spain and Slovakia, EHRs are created by the family doctor or general practitioner. In Poland, doctors, nurses and midwives are authorised to create EHRs. In France and in Latvia, although it is not specified which

health professionals can create EHRs, the law requires that the health professional is face-to-face with the patient when inputting the information.

When the law does not recognise the competence to create EHRs to health professionals, the approaches vary. Under Austrian law, some data can be entered by 'hospitals' and some by 'pharmacies', there is no express reference to health professionals. In Bulgaria, the National Health Fund automatically creates EHRs (i.e. Personalised Information System Records) based on the electronic reports its partners are legally required to send. In Luxembourg, EHRs will be created for all citizens of Luxembourg by the eHealth agency of Luxembourg. In Sweden, once a public authority or private organisation or company are allowed to provide healthcare, there are no particular additional requirements.

When there are shared EHRs systems in place, EHRs are normally created automatically or by public authorities, based on the information of the more detailed EHRs of healthcare providers. This is for example the case in Portugal, Spain, Luxembourg and the UK (England); however, in France it is the health professional who creates the EHR directly.

3.5.3 Different categories of access for different health professionals

The table below identifies which countries have established different categories of access for different health professionals.

Table 19 *Countries with access rights differentiated per type of health professionals*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Different categories of access	√			√			√			√	√	√	√	√		√		√	√	√		√					√	√	√

About half of the countries covered (16) have set different categories of access to EHRs for different health professionals. These rules stem from existing and planned legislation or established practices and reflect the "need to know" principle derived from Article 6(1) of Directive 95/46/EC. Among the other half of countries, only some have clear rules setting the same access rights for different types of health professionals. This is the case of Bulgaria, where once access is granted no type of data can be hidden, and Estonia, which grants access to all persons who are healthcare professionals under Estonian law.

When countries define different categories of access for different professionals, the approaches vary. Some countries like Austria or Hungary defined different rules for different types of health professionals such as doctors, dentists, nurses or pharmacists. Other countries differentiate between the patient's GP and other health professionals, giving full access to the former but not to the latter; this is the case for France, Luxembourg or Slovakia. Another group of countries, including Sweden and the UK (England), attributed the task of deciding which health professionals have access to which data to the healthcare providers (the data controllers).

Another approach is to give the patient the power to choose which health professionals will have access to data, and to which data. In this case, the decisive element is the relationship between the health professional and the patients. For example in Croatia, the future EHR system is envisaged in a way to give the patient the power to grant access only to the patient's selected doctor (primary health care); to all doctors within the primary healthcare and other users with the additional approval; to all the users; or to no user at all.

3.5.4 Explicit prohibitions

The table below identifies those countries which have set explicit occupational prohibitions in relation to access to data from EHRs.

Table 20 *Countries with explicit occupational prohibitions*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Explicit prohibitions	√	√										√				√					√	√							

Only a small minority of the countries covered (6) has set clear and explicit occupational prohibitions to access data from EHRs. However, in practically all of the remaining countries, even though there is no explicit occupational prohibition, insurance companies, occupational physicians, and others are a priori excluded from accessing data from EHRs. It results in some cases from the fact that the law lists the categories of professionals who can access the data (and occupational physicians or employees from insurance companies are not included) and in other cases from the structure of the systems in place, which only allow access to health professionals authenticated in health care institutions or otherwise duly certified.

The countries that have set explicit occupational prohibitions have chosen different approaches. In Austria, the law prohibits the access of occupational physicians, employers, human resource consultants and insurance companies. In Belgium, insurance companies are also not allowed to have access to or to receive a copy of the EHR. Under the French Public Health Code, occupational physicians are denied access to the EHR, which also cannot be used to conclude insurance contracts or any other contracts (e.g. loan) that require a health assessment. In the Netherlands, a proposal Patient's Rights law provides for the prohibition of access of healthcare insurance companies, company medical doctors, insurance companies' medical advisors and medical examiners. In Norway, it is forbidden to disclose information of some EHRs to the employer, insurance company or the public prosecutor even if the data subject consents. Italy is also planning to exclude certain professionals from accessing EHRs.

3.5.5 Exception to access requirements in emergency situations

About a third of the countries covered have set exceptions to the access requirements to EHRs. However, it should be noted that in the remaining countries exceptions for emergency situations would generally also be allowed under more general rules of data protection and/or health data.

Exceptions to the general access requirements are particularly relevant for the countries which require the consent of the patient to access EHRs. Thus, for example in Finland, EHRs may be shared only on the basis of the consent of the patient, except if a legal provision provides that the consent is not necessary, for example if the patient is unconscious. Also in France, if the person is unable to express his will and if circumstances require, an emergency physician may decide, in the interest of the patient, to access the EHR without obtaining prior consent.

In Italy, a draft implementing decree widens the scope of the exception to situations which do not specifically regard the patient, such as public health emergencies. The approach in Spain is different, but it is still related to consent: the patient may decide to hide part of the information but the GP has access to the fact that the patient decided to hide data and due to emergency vital reasons the GP may overrule this decision.

3.5.6 Legal obligation for health professionals to update EHRs

The table below indicates which countries specifically require health professionals to update EHRs.

Table 21 *Countries requiring health professionals to update EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Legal obligation	√		√					√				√	√						√				√	√	√		√	√	

Only a minority of the countries covered by this Study have a specific obligation for health professionals to update EHRs established by law: Austria, Bulgaria, Croatia, Estonia, France, Latvia, Poland, Portugal, Romania, Slovakia and Sweden. In Austria and in Bulgaria, the timeframe for the update of EHRs is also set by law; in Poland and Slovakia, EHRs need to be updated "immediately" after the provision of health care. In Portugal, a ministerial order was adopted specifically with the purpose of improving the quality and quantity of the information from EHRs, setting the minimum requirements for the discharge letters and requiring these to be in electronic format. In France the legislation requires that each health professional must report diagnostic and therapeutic elements in the DMP during each act or consultation. In addition during the stay of a patient in a health establishment, health professionals must report in the DMP, the summaries of the key elements of the stay.

It should be noted, however, that in the remaining countries this obligation also exists in practice, based on the more general rules on data protection, health data or even medical ethics.

Patients: the rights on their data?

Under Directive 95/46/EC, patients are empowered with a number of rights in relation to the data included in their EHRs, most of which are directly related to the patient's consent. Thus, pursuant to Article 12(a), Member States must ensure that the patient has access to the data that was processed as well as to the purpose of the processing of data and the identity of the recipients or categories of recipients of the data.

The rights to the erasure and correction of data, provided for in 12(b) of Directive 95/46/EC are also related to the patient's consent. In particular the right to the erasure of EHR is not without controversy, probably due to the fact that in several systems health records are still seen as property of the doctor or of the health system, although much less in Europe. It is important to know in the different forms in which these and other connected rights (e.g. the right to download EHRs) have been reflected in the national laws of the Member States. It is also worth identifying the different ways patients are identified and authenticated for EHR purposes, in order to assess if a patient's right to privacy and the access to his/her own data are ensured.

This section provides an overview of the choices Member States have made to regulate the identification and authentication of patients, their access rights in relation to the information included in EHRs – including whether they can know who had access to their EHRs - as well as a patient's right to download, modify or erase that information.

3.5.7 Rules on patient specific identification number for eHealth purposes

The table below distinguishes the different systems used by the countries to identify patients depending on whether they rely on specific identification number for eHealth purposes or use ID card or health insurance number.

Table 22 *National systems for patient identification number for eHealth purposes*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific eHealth number																													
ID card		√	√	√			√	√			√						√		√	√	√	√	√				√	√	
Health insurance number	√					√			√	√		√	√	√	√	√		√						√	√				√

There are a lot of disparities between countries on the rules to identify patients. None of the countries currently apply a specific identification number for eHealth purposes except for UK (Scotland) where the Community Health Index (CHI) database created to hold patient demographics and some clinical information has an associated CHI number used to uniquely identified patients (for eHealth purposes).

All countries rely either on the ID card number or the health insurance number for the identification of patients. However some of the countries have set in place measures to ensure confidentiality of data. For example, in France, patients are allocated a number generated automatically which does not allow for identification of the person. This number is the INS which is an identifier assigned to each beneficiary of the national healthcare through the patient's Healthcare Card.

In the Czech Republic and in Slovenia there are still no EHRs systems in place or rules on the identification of patients for eHealth purposes. In Cyprus, Germany and Ireland, although there are no EHRs systems yet in place there are already rules on the identification of patients for eHealth purposes in place or envisaged.

It is important to note that in Spain, in a decentralised system where Autonomous Communities have set in place their own EHR system, all health cards have to incorporate a common set of basic data and will be linked to the unique personal identification code for every citizen in the National Health System. This harmonisation aims to provide standard data for each person regardless of the health administration issuing the card. The basic data on the health card include the personal identification code assigned by the regional health administration issuing the card (CIP-AUT), the name of the card holder and the unique personal identification code of the National Health System (CIP-SNS).

3.5.8 Right to access information

While all countries covered by the Study provide to patients the access to their EHRs, only some of them grant full access to these data, without providing for exemptions and/or restrictions. The following table identifies those countries where full access is granted, without exemptions or restrictions.

Table 23 *Countries granting patients with full access to their EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Full Access	√		√		√	√			√	√			√			√	√	√			√		√		√		√		

In all countries covered, patients are entitled to access their EHRs[60]. In some cases, like Austria or Slovakia, this right to access is established in legislation specific to EHRs; however in the vast

[60]Note that at the time of writing such right to full access to EHRs content is not in force in Netherlands but it is planned under a draft law.

majority of the cases, the patient's right to access his EHRs is guaranteed by the general data protection rules, transposing Directive 95/46/EC. About half of the countries covered extended this right to all the data included in the patient's EHR, not making use of the possibility to apply exemptions and restrictions in this context, as possible pursuant to Article 13 of Directive 95/46/EC. Among the countries which do not allow patients to access all the content of their EHRs, the typical exception is where access could cause harm to the patient. Other grounds for not providing full access include, for example, genetic information where access could also cause serious harm to the relatives of the patients (Cyprus) or access to results of medical examinations (in Hungary).

There are different approaches to condition the patient's access to more sensitive data. Thus, in Estonia, patients can have access to all of their EHRs, but in order to protect a patient's life or health the healthcare provider may set a time limit of up to 6 months upon forwarding data to the Estonian National Health Information System in the course of which the patient can only first examine his or her personal data only through a health professional. Under Slovakian law, the patient has no direct access to the result of the examinations of diagnostic and treatment components; however, these can be made available to the patient by the health professional who requested the medical examination or the treatment. Under French law, patient has as a principle full access to his/her EHR; however in certain situations that could cause harm to the patient the information needs to be first disclosed to the patient in a meeting before being accessible on the DMP.

3.5.9 Right to download

The following table indicates which countries have provided for the patient's right to download part of all his/her EHR content.

Table 24 *Countries with right to download patient's data*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Right to down-load	√						√			√	√	√				√	√	√			√	√	√		√		√		

More than one third of the countries covered by this Study allow the patient to download all or at least some of his/her EHR content, even though in most cases this is not detailed in legislation. In the remaining countries, however, the patient is normally allowed to request paper and/or digital copies of the information included in the EHRs. In some cases, like in Bulgaria, although the patient cannot download the content, s/he can still copy-paste the information from the screen, which will have the same effect. The norm is that when patients have access to their EHRs, they will, by one means or another, be able to have copies of that information.

3.5.10 Right to know who accessed EHRs

The patients' right to know who accessed their EHRs is in principle guaranteed by the general rules of data protection law transposing Article 12(a) of Directive 95/46/EC. The table below identifies those countries which have enacted specific provisions granting such a right in relation to EHRs.

Table 25 *Countries where patients can know who accessed their EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific right to know who	√					√	√	√			√					√	√				√	√					√	√	

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
accessed																													

Therefore, about two thirds of the countries covered do not have specific provisions for EHRs. In some of the countries that have established a specific right for the patients to know who accessed their EHRs, the information is usually directly available on online platforms - this is the case for example for Estonia or Lithuania. In Italy, draft legislation will also allow that possibility. Note that in Sweden, patients can know who accessed their EHRs but upon request to the health care providers. It should be noted, however, that in practice this happens also in several countries which have not set a specific right to know who accessed EHRs, including for example France, Latvia or Portugal.

3.5.11 Right to modify and/or erase data from EHRs

Article 12(b) of Directive 95/46/EC grants data subjects the right to erasure and correction of data that concerns them. This provision applies to data, the processing of which does not comply with the provisions of Directive 95/46/EC, in particular because of the incomplete or inaccurate nature of the data. Thus, in principle the mere transposition of Directive 95/46/EC would not give the patients the right to erase or modify all data of their EHRs for reasons other than the non-compliance with the provisions of the Directive.

Table 26 *Patient's right to erase/modify EHRs data*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Erase data inputted by another person	√											√									√								
Hide data																√		√											
Modify/erase data inputted by the patient			√			√	√	√								√								√	√		√		

Most of the countries covered do not go beyond the provision of Directive 95/46/EC, not allowing patients to directly erase or modify any data from EHRs. Austria appears to be the only country where patients have the right to directly erase all data from their EHRs. They cannot, however, update or modify any data. In France, erasure of documents may take place in common agreement with a health professional. In case the patient decides so, users of the DMP will not be aware that some data has been deleted or that a file is incomplete apart from the author of the document and the family doctor. Furthermore the IT system keeps track of these actions. Two countries allow the patients to hide some of the data in their EHRs. In Italy, draft legislation will allow the patient to decide to hide certain EHR data, which would thus remain visible only to him and to the person(s) who generated them. This seems that it will also be the case for Luxembourg once the EHR system is in place.

In about a third of the countries covered patients are entitled to directly modify and erase the data included in their EHRs that they themselves have inputted and which is stored separately from the rest. It should be noted that no country allows patients to directly modify data that has not been registered by the patients. In Germany, patients will be able to input some data in some of the application of their EHRs, which they can also delete later. Also in Portugal the patients can, at any time, update, modify and erase the information that they have registered themselves (including e.g. height, weight, blood glucose, blood pressure, cholesterol).

In Slovenia, under the general patient's right legislation, patients would have the right to make a request to the healthcare provider that their comments are added to the records in their medical files, which would include EHRs. A similar system, a system called "la carpeta de salud del paciente" is currently being developed in the Basque Country to enable the patient to add specific comments in the EHRs, in relation to the treatment followed.

3.6 LIABILITY OF HEALTH PROFESSIONALS WITH REGARD TO EHRS

While EHRs may allow the correction of medical errors (e.g. no more handwriting errors, better traceability of data), the liability of health professionals may be enhanced by EHRs (e.g. omission to check EHRs resulting in a misdiagnosis that led to serious harm, omission to enter relevant health data in EHRs leading to mistreatment by other health professionals, potential personal data violations). However almost all of the countries covered have chosen to rely on their existing medical liability rules for health professionals with regard to EHRs.

With regard to those countries which have adopted specific liability rules, Croatia, Finland and Sweden have adopted specific medical liability rules with regard to data errors and erasing EHRs' data. In some countries, liability for erasing EHRs' data may simply not be possible: for instance, the Austrian EHR system does not allow health professionals to erase data.

In Croatia, health professionals are responsible for the completeness and accuracy of the data entered into the EHR under the Croatian EHR legislation[61]. Moreover, they are also forbidden to damage, alter, erase, destroy or make unusable data and programmes contained in the EHRs system.

Under the Finnish EHR legislation[62], healthcare service providers are considered 'controller of EHRs' and as such are responsible for the content and accuracy of EHRs stored in the national data repository. Moreover, the person that enters the data in the patient data management system is also responsible, and a draft law proposes to extend this liability to include the correction of faulty data.

In Sweden, the EHR legislation[63] stipulates that the person taking care of a patient's journal is also responsible for the information in this EHR, and that patients' records may not be erased or made incomprehensible. However, the legislation refers to the Swedish Personal Data Act with regard to liability for damages.

These specific liability rules are mostly reinforcing or highlighting the general liability regime. As such, apart from a degree of legal certainty provided by the expressed mention in the specific national EHR legislation, these specific rules do not add any new element to the national liability regimes (e.g. exemptions whether general or related to different medical professions or circumstances).

3.6.1 Accompanying measures on liability with regard to EHRs

Three of the countries covered (Bulgaria, Italy, United Kingdom) are implementing accompanying measures on liability with regard to EHRs, such as the development of a set of guidelines or awareness raising activities including training delivery. These measures are only legally foreseen in one country, albeit at the moment in draft legislation (Italy).

The very nature of the Bulgarian EHR system, whereby EHRs are automatically updated from information provided by health professionals under a reporting system in order to obtain remuneration,

[61] Ordinance on the Method of Keeping of Personal Health Record in the Electronic Form (*Pravilnik o načinu vođenja osobnog zdravstvenog kartona u elektroničkom obliku*) ("O.G.", No. 82/10).
[62] Act on Electronic Processing of Client Data in Social and Health Care (*Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä*, 159/2007).
[63] Patient Data Act (*Patientdatalag 2008:355*).

means that measures aimed at limiting responsibility of health professionals with regard to EHR are mostly indirect. For instance, input errors into EHRs would stem from input errors in the reporting system. As such, guidelines and trainings are provided with regard to the reporting system which indirectly result in limiting the liability risks posed by EHRs to health professionals. In particular, the Bulgarian National Health Insurance Fund publishes guidelines on its official website to ensure the correct use of its software and in particular its reporting system. Moreover, in the event of an update to the fund's system, the fund publishes new instructions at least a month prior to the launch of the updated system. Finally, the Bulgarian Medical Association also organises regular trainings for health practitioners regarding the correct use of the reporting system.

A draft decree in Italy foresees the delivery of training in order to inform users of risks affecting personal data, of access and processing of data, and of relevant security measures.

In the United Kingdom, general practitioners' guidelines include guidance on the development, deployment and use of IT systems. Moreover, the Information Commissioner's Office website contains various types of information dedicated to the healthcare sector[64] including on data protection obligations, awareness toolkit on data protection, incidents reporting toolkits, information on audits and advisory visits.

3.7 SECONDARY USE OF HEALTH DATA

The Commission Action Plan on eHealth has as one of its main objectives to support research, development and innovation; an 'additional focus' will be placed on ways to analyse large amounts of data for the benefit of citizens, researchers, practitioners, businesses and decision makers[65]. Accordingly, Article 14(2)(b)(ii) Directive 2011/24/EU sets as one of the objectives of the eHealth network to draw up guidelines on *'effective methods for enabling the use of medical information for public health and research'.* The enormous potential of using of eHealth data for scientific research is widely acknowledged by medical researchers and has been addressed by legislators, which have been usually focusing on whether the data is identifiable or not[66]. Article 8(4) Directive 95/46/EC refers to reasons of substantial public interest, subject to suitable safeguards and laid down by law, as a valid basis for exceptions to the general rule prohibiting the processing of sensitive data. The Working Party considers that the exception set by Article 8(4) opens the door for the use of EHR data for medical scientific research and government statistics but considers that whenever feasible and possible, data from EHR systems should be used for other purposes (e.g. statistics or quality evaluation) only in anonymised form or at least with secure pseudonymisation[67]. According to the American Medical Informatics' Association, secondary use of medical health data applies personal health information for uses outside of direct healthcare delivery. It includes such activities as analysis, research, quality and safety measurement, public health, payment, provider certification or accreditation, marketing, and other business applications, including strictly commercial activities[68].

This section analyses the approaches adopted in the countries covered by this Study on the secondary use of health data. It identifies in the countries covered whether there is a specific legal text on the secondary use of health data, what are the secondary uses foreseen in law and the safeguards to control and secure the secondary use of health data.

[64] ICO guidance for the health care sector, http://ico.org.uk/for_organisations/sector_guides/health (last access April 2014).
[65] Commission Communication "eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century" (COM (2012) 736 final).
[66] Wilson, P (2012), 'Legal frameworks for eHealth', p. 54, available at: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf
[67] Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR) (00323/07/EN, WP 131), adopted on 15 February 2007.
[68] Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper, American Medical Informatics Association 2006 available at: http://jamia.bmj.com/content/14/1/1.full

3.7.1 Specific law on secondary use of health data or rules from the data protection legislation

The table below highlights the countries that have decided to regulate the secondary use of health data compared to the ones that rely on general data protection law.

Table 27 *Specific law on secondary use of health data or rules from the data protection legislation*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific law on secondary use of health data					√			√		√	√	√	√	√		√		√	√		√	√	√	√		√	√	√	√
General data protection legislation	√	√	√	√		√	√		√						√		√			√					√				

More than half of the countries (18) have set specific laws on the secondary use of health data. For example the legislation in Italy provides that EHRs are established, inter alia, for the purposes of medical and epidemiological research, as well as health service planning and evaluation. The draft Latvian law on EHRs specifies that health data kept in EHRs may be used for a secondary purpose under certain conditions. The legislation of Luxembourg provides that anonymised information for statistical or epidemiological purposes from the shared EHR system can be exchanged between different competent authorities (e.g. the eHealth Agency, the Health Ministry, the National Health Laboratory) using automatic procedures or not. The French law requires that health data for research purposes is subject to authorisation by the data protection body and consultation by a committee composed of relevant persons in the field of health, epidemiology, genetics and biostatistics. This committee delivers an opinion on the research methodology, the need for use of personal data and the relevance of these in relation to the objective of the research.

The other countries rely on the personal data protection legislation to regulate the secondary use of personal data. For example Germany allows the collection of special categories of personal data 'when required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where these data are processed by health professionals subject to the obligation of professional secrecy or by other persons also subject to an equivalent obligation of secrecy', but does not regulate in further details the secondary use of health data.

3.7.2 Secondary use foreseen in law

The table below highlights what the secondary uses of health data foreseen in the countries covered are (i.e. general research/scientific purpose, epidemiology, statistics, other uses).

Table 28 *Secondary uses foreseen in law*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
General research/ scientific purpose	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√		√	√
Epide-				√						√	√			√		√		√	√							√			√

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
miology																													
Statistics	√	√	√	√	√		√	√	√	√	√		√	√	√		√	√	√	√	√				√	√	√	√	√
Other uses		√	√	√						√	√	√				√			√						√			√	√

All countries covered specify in the law the secondary uses of health data (for which purposes?), with the exception of Germany. They almost all (with four exceptions) mention in their legislation that secondary uses will serve the purpose of scientific and statistical studies. Some specifically state in the law that health data can be used for epidemiological purposes.

Several legal texts refer to other uses. For example Cyprus, Bulgaria, Belgium and Romania refer to the use of data for historical purpose. The Italian law specifies that EHRs are established also for the purposes of medical and epidemiological research, as well as health service planning and evaluation. The Latvian law states that health data can be used by State institutions and courts when it is necessary to protect other interests protected by law. Spanish legislation mentions that access to the clinical history is possible for judicial, epidemiological, public health, research or education but within the framework of the data protection and the General Health legislation. The Swedish law provides that health data can be used to systematically and regularly develop and safeguard the quality of health care, administration, planning, follow-up, evaluation and supervision of health care, and to create statistics.

It is interesting to note that the Danish legislation explicitly prohibits secondary uses other than scientific and statistical ones.

3.7.3 Safeguards

Several measures exist to secure the secondary use of data. This sub-section identifies what measures are taken by the countries covered to protect personal health data in case of secondary use. It focuses on:

- Whether there are requirements to anonymise health data for secondary use;
- Whether the patient consent is taken into account for secondary use.

Table 29 *Requirements on anonymisation*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Anony-mised data	√	√	√		√		√	√		√	√	√		√		√	√	√	√		√	√	√	√	√	√	√		√

In almost all countries covered, the national legislation provides that, as a principle, health data must be anonymised for secondary use with the exception of Cyprus, Croatia, Greece, Ireland, Malta, and Sweden[69]. In the countries that set rules on anonymisation, some provide exceptions to this obligation of anonymisation of data under very specific circumstances and safeguards such as a prior authorisation from the data protection body and/or the prior consent of the patient. For example, in Belgium, if the secondary use of health data is not possible without the identification of patients, an authorisation is needed from the Sector Committee for Social Security and Health. In any case, such secondary use will only be possible after prior informed consent of the patient. In Estonia the processing of non-anonymised EHR data is only permitted if, after removal of the data enabling

[69] In general no, but in certain cases, data has to be anonymised, which depends on the specific register.

identification, the goals of data processing would not be achievable or it would be unreasonably difficult. There must be predominant public interest for such processing and the obligations of the data subject must not be changed as a result of the processing and the rights of the data subject must not be excessively damaged in any other manner. The patient is notified that his/her health data is being processed. The aforementioned requirements apply only if secondary use of health data takes place without the consent of the patient. If the patient consents to secondary use, the requirements do not apply, however, the processing of health data must still be registered with the data protection body.

Table 30 *Patient consent related to secondary use*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Patient consent		√						√				√					√					√						√	√

Very few countries set requirements on patient consent for secondary use of health data (7). As already mentioned Belgium and Estonia request the consent of the patient in case health data are not anonymised or it is not possible to anonymise data. Lithuanian legislation provides that personal data may be processed for the purposes of scientific research on condition that the data subject has given his consent. Without the data subject's consent, personal data may be processed for the purposes of scientific research only upon notifying the State Data Protection Inspectorate. In this case, the State Data Protection Inspectorate must carry out a prior control. Under the Data Protection Act in the UK, a patient can withdraw consent to the processing of personal information for secondary care purposes. A withdrawal form can be downloaded from the relevant competent authority website[70]. In Sweden the law provides opt-out consent if the secondary use is for research.

3.8 ARCHIVING

Archiving duration of EHRs in the context of this project refers to the period of time during which health data is stored in an electronic health record system. There are no specific rules at the EU level on the archiving of EHRs. However, pursuant to Article 6(1)(e) of Directive 95/46/EC, personal data must be kept in a form which permits identification of data subject for no longer than necessary for the purposes for which the data were collected or for which they are further processed.

This section will provide an overview of the rules that apply to the archiving of EHRs. It identifies whether the countries have adopted specific rules for the archiving duration of EHRs or whether they rely on the general rules on health records and data protection.

Specific rules for the archiving of EHRs

The table outlines which countries covered have set specific rules on archiving duration of EHRs and the ones that rely on the general archiving rules on health records.

Table 31 *specific rules for the archiving duration of EHRs*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific rules	√							√				√						√				√							
General		√	√		√	√	√		√	√	√		√	√		√			√		√		√		√	√	√	√	√

[70] In the case of UK the Health and Social Care Information Centre (HSCIC)

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
rules on health records																													

Very few countries (5) set specific rules on the archiving duration of EHRs. Austria, Estonia, Lithuania set specific archiving rules with respect to the shared EHRs they have set in place. In Austria shared EHRs must be stored for ten years and then must be deleted. In Estonia, the legislation requires that the data from shared EHRs must be archived indefinitely. Lithuanian legislation requires that shared EHRs are kept in the data base throughout the life of the patient and for three years after his/her death. This is not yet decided, but Luxembourg is planning to set a ten years' archiving duration from the closure of the shared EHR. France requires that shared EHRs must be kept for a period of ten years after their closure. The Norwegian legislation provides that data in shared EHRs must be deleted when they are no longer necessary for the purpose of processing.

In contrast, the majority of the countries (19) rely on the general archiving rules on health records. Four countries rely on the general data protection rules to regulate the archiving of EHRs. It is important to flag that the archiving duration rules from general health records diverge significantly between countries.

3.9 INTEROPERABILITY

The European Commission has renewed in 2012 its commitment to '*a fully mature and interoperable eHealth system in Europe*'[71]. Interoperability in this context means the ability of two or more electronic health record systems to exchange both computer interpretable data and human interpretable information and knowledge[72].

Interoperability issues arise not only at the cross-border level, but also for instance between health institutions, health practitioners, and different geographical areas in a single Member State. In the national development of eHealth, the countries covered may therefore already have experienced different obstacles linked to the issue of interoperability of EHRs and developed various solutions to address those. This section therefore assesses how the interoperability of EHRs is regulated and achieved in the countries covered, including with other eHealth solutions. It should also be noted that five of the countries covered (Cyprus, Czech Republic, Germany, Ireland, Slovenia) have not started the development of EHRs and therefore are not identified as possessing either a national system or regional schemes.

3.9.1 Interoperability of national EHRs schemes

– National systems

A small majority of the countries covered have elected to implement EHRs through a national system, and a vast majority of these countries have complemented their national scheme with a centralised database (e.g. France, Luxembourg). In some countries, the national EHR scheme has not been launched or deployed but it is planned to be national (Latvia, Poland, Romania). In Croatia, the national scheme will be integrated with an existing national system used for other eHealth solutions (ePrescription and eReferral).

[71] Commission Communication 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century' (COM (2012) 736 final).
[72] WHO Glossary of globalisation, trade and health terms, available at: http://www.who.int/trade/glossary/story021/en/.

In cases where a centralised database has not complemented a national system, the national scheme relies on regional schemes or local data stores by providing an interface between them. For instance, in Austria the national system is a mere redirection system with links to the decentralised databases maintained by the numerous actors involved (hospitals, health professionals, etc.). A similar system is used in Spain where the centralised database consists of an exchange platform redirecting to the different data stores implemented in the autonomous communities (regional database, regional health centres, etc.).

In Belgium, since 2008, the eHealth-platform provides a series of so-called 'basic services' which can be used by all actors in the healthcare sector and which can be integrated into the various eHealth solutions offered by information and communications technology providers. The Belgium eHealth-platform consists essentially of two layers: a Metahub and a Hub. The Metahub consists of a first layer of information available on the level of the eHealth-platform itself which refers to the regional or local network (the "hub") where further data for a given patient can be found. The Hub is a second layer of information where one is referred to the actual location of the data, for example the local hospital.

- Regional schemes

A minority of the countries covered have decided to implement EHRs through a regional scheme. All of these regional schemes are complemented by regional databases. In certain countries, such as Italy and Spain, implementation of EHRs regional schemes and databases is ongoing and/or at different level of deployment.

Less than half of the countries vested with regional schemes provide for interoperability of these schemes among themselves and a small number provide for interoperability with other eHealth solutions.

- Interoperability between national systems and regional schemes

To note that a small number of the countries covered possess both a national system or database and regional schemes. For instance, in Belgium, a national eHealth platform is developing as both a tool providing certain services and a referral tool integrating different databases and networks that function at the regional level.

In Finland, the national interface, Kanta, functions as a data transmission and archiving service whereby regional schemes that join in the national infrastructure are required to be interoperable with Kanta. Since Kanta also provides for other eHealth solutions such as ePrescription, interoperability with these systems is ensured through this national interface.

- Interoperability of EHRs systems with other eHealth solutions

More than a third of the countries with a national system have legal provisions relating to the interoperability of their national system with other eHealth solutions (e.g. ePrescription). National studies however reveal that this does not mean that interoperability is effective at the moment. For instance, in France the law provides for interoperability of the EHRs with the national ePrescriptions scheme, yet these two eHealth initiatives function under different schemes and databases. In Romania, the EHR system is currently at the technical stage and, whilst different eHealth solutions will be directly integrated in the national infrastructure along with EHRs, the law also provides for interoperability of any other information system used.

While a majority of countries with a national system do not have legal provisions relating to the interoperability of their national system or database with other eHealth systems, this situation could not be a hurdle in certain countries and with regard to certain eHealth solutions (Croatia, Latvia, Romania) where the national system will not only be dedicated to EHRs but will also integrate other

eHealth solutions. This is also the situation in Luxembourg, but at this stage only with regard to ePrescriptions. However, coexistence in the same platform does not necessarily include interoperability in every sense of the term.

In Germany, while there is no specific EHR scheme in place, telematics infrastructures are legally required to be 'interoperable and compatible' and therefore any future development of EHRs, whether at the federal or regional level, should be interoperable.

3.9.2 Specific rules and standards on EHR interoperability

As shown in the table below, less than half the countries covered by the Study implemented specific rules and standards on interoperability.

Table 32 *Countries with specific rules on interoperability*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Specific rules on interoperability	√	√					√			√	√					√	√		√			√	√	√			√	√	

A dozen countries covered have set up specific rules and standards on interoperability.

However, nearly half of these countries can be considered as having only partially adopted such rules and standards (Denmark, Finland, Lithuania, Latvia, Poland, and Portugal). Different reasons explain this classification. Firstly, EHR legal requirements in some of these countries are only in draft legislation and regulations, or not yet implemented. Secondly, these requirements may only cover certain specific elements of EHRs or certain schemes.

In Sweden, two standards have been developed based on European or International standards: the National Information Structure (NI) and the National Interdisciplinary Terminology for Health and Social Care (the latter is partly based on the SNOMED Clinical Terminology (CT SNOMED)).

Belgium has developed and uses a standard for the exchange of minimal medical transaction information, called SumEHR. The SumEHR standard was introduced in 2005 and an EHR software package used by a physician should be capable of exporting a SumEHR message for any given patient. Currently more than 80% of all GPs across Belgium use certified EHR systems with this capability. In Slovakia, health care providers are required to use certified information systems which comply with connectivity and security standards, as well as with rules on identification and authentication of health professionals. In Italy, the draft implementing decree and an annex thereto lay down specific provisions on interoperability.

Although limited by the stage of implementation of its national EHR system, Poland has adopted a detailed set of rules and standards. In Poland, EHRs should be exchanged as Extensible Markup Language (XML) files or multimedia files, with their logical structure further determined by the administrator of the EHR system. The exchange of data should be compliant with the XML or XML Scheme (XSD) format and the Digital imaging and communications in medicine (DICOM) format. Moreover, the same instrument details the steps and security requirements related to access to EHRs.

The absence of rules and standards does not therefore mean that interoperability requirements are not being implemented, and therefore national experts informed that certain standards are being applied (e.g. Greece, France, Luxembourg) and developed (e.g. France, Ireland) in practice. For instance in Luxembourg, while no rules or standards have been adopted, the State is providing support to health professionals to update their software to be interoperable with the national system which is tantamount

to ensuring the harmonised application of certain rules or standards. In France, the National Health Agency is involved in international negotiations for the establishment of health-related semantics. In that perspective, the French EHR initiative is foreseen to make use of the development of international norms developed for instance under the Integrating the Healthcare Enterprise (IHE) initiative which uses ISO recognised standards (Health Level 7 (HL7), including 'Clinical Document Architecture' (CDA), and Digital imaging and communications in medicine (DICOM) standards) based on the Logical Observation Identifiers Names and Codes (LOINC) database and universal standard. In Greece, compliance with the HL7 standard for exchanging information between health applications is a practical requirement. On this basis, HL7 Hellas is promoting a Memorandum of Understanding for compliance with this standard.

Out of the standards and rules identified by the national experts, most standards seem to be based on Extensible Markup Language (XML) which derives from Standard Generalised Markup Language (SGML; ISO 8879:1986). Bulgaria currently uses XML codes and in Poland EHRs should be, inter alia, exchanged as XML files, whilst Health Level 7 (HL7) standards that use the XML codes are used or envisaged in Greece, France, and Lithuania, including in their latest standard 'HL7 v3' and 'Clinical Document Architecture' (CDA) (ISO/HL7 27932:2009). Other standards identified include:

- Digital imaging and communications in medicine (DICOM; ISO 12052:2006)[73];
- International Classification of Health Interventions (ICHI) developed by the WHO, such as ICD-10;
- Logical Observation Identifiers Names and Codes (LOINC) universal standards;
- Nordic Medico-Statistical Committee (NOMESCO) classifications, including for instance the SNOMED Clinical Terms codes;
- NCSP+ (Nordic Casemix);
- SSK10 klasifikators.

3.10 LINKS BETWEEN EHRs AND ePRESCRIPTIONS

EPrescriptions are prescriptions for a medicinal product issued by a member of a regulated health profession who is legally entitled to do so. Unlike traditional prescriptions, ePrescriptions are issued and transmitted electronically[74].

The prescription, dispensation and provision of medicinal products constitute a central element of healthcare[75]. One of the ways by which Directive 2011/24/EC seeks to enhance safety and continuity of cross-border healthcare is by ensuring that prescriptions issued in any Member State are, as a rule, recognised in all other Member States[76]. The development of ePrescriptions and their interoperability can help achieve this objective.

EPrescription may or may not be connected to EHRs. EHRs may include data on medicinal products prescribed to the patient, offering doctors a record of previous or current medical treatments and allowing them to evaluate interactions of different medicines. Pharmacists may be able to visualise and/or insert data into EHRs, thereby improving continuity of care between different health professionals. EHRs may also be used as a tool accessible to doctors and pharmacists to receive and submit ePrescriptions.

The following table provides an overview of the status of implementation of ePrescriptions in the countries covered. The table shows that in 20 countries, ePrescriptions are already operational.

[73] ISO standard 12052:2006 'Health informatics -- Digital imaging and communication in medicine (DICOM) including workflow and data management'.
[74] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C (2008) 3282), §3(f), read in conjunction with Article 3(k) of Directive 2011/24/EC.
[75] Article 3(a), Directive 2011/24/EC.
[76] Article 11, Directive 2011/24/EC.

However, this might not equate to full implementation. For example, in ePrescriptions are mainly used in hospitals in Belgium and Cyprus, but not in local medical centres. Another five countries, namely Bulgaria, Hungary, Luxembourg, Latvia and Poland, are planning to develop ePrescription systems in the future.

Table 33 *Countries that have implemented, or are taking steps to implement, ePrescriptions*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Implementation of ePrescriptions		√	√ [77]	√	√	√	√	√	√	√	√		√	√ [78]		√	√	√ [79]	√ [80]		√	√	√ [81]	√	√	√	√	√	√

The countries reviewed have taken different approaches in regulating the relationship between ePrescriptions and EHRs.

In eight countries, no ePrescription system is yet in place. These are Austria, Bulgaria, France, Ireland, Latvia, Luxembourg, Malta and Poland. However, Bulgaria, Hungary, Latvia, Luxembourg and Poland do plan to develop ePrescriptions systems in the future. In other four countries, ePrescriptions exist, but no EHR system is yet in place. These are Croatia, Czech Republic, Greece and Slovenia. In relation to all the countries listed above, the question of the relationship between ePrescriptions and EHRs is therefore not applicable, because either one or the other system is not yet operational.

In Hungary, however, draft legislation suggests that the existence of EHRs will become a precondition for ePrescriptions in the future. Similarly, in Luxembourg, there are clear indications from stakeholders and publicly available information that EHRs and ePrescriptions will be integrated into one system and the existence of an EHR will become a precondition for ePrescriptions.

In the remaining 16 countries, both ePrescription and EHR systems exist, albeit they may be at different stages of development. It is possible, for example, that ePrescriptions are used in (all or some) hospitals, but not in local clinics, as appears to be the case in Belgium and Cyprus.

In any case, as the table below shows, out of the 16 countries in which both ePrescription and EHR systems exist, only four have made or are planning to make the existence of an EHR a necessary precondition for issuing ePrescriptions. These are Hungary, Luxembourg, Norway and Slovakia. In all other 12 countries, ePrescriptions can be issued regardless of whether an EHR has already been created.

Table 34 *Countries in which an EHR is or will be required for an ePrescription to be issued*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
EHR required for ePrescription														√				√				√					√		

[77] At planning stage
[78] At planning stage
[79] At planning stage
[80] At planning stage
[81] At planning stage

This study thus indicates that, at present, in most countries, ePrescriptions and EHRs constitute two parallel systems which are not being integrated.

4 CROSS-BORDER TRANSFER OF EHRS

4.1 LEGAL PROVISIONS FOR CROSS-BORDER INTEROPERABILITY OF EHRs

In the absence of specific EU legislation only a few Member States have set legal provisions for cross-border interoperability of EHRs.

The Table below identifies which countries have adopted legal provisions relating to the interoperability of EHRs in cross-border situations.

Table 35 *Countries regulating cross-border interoperability*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SI	SK	SE	UK
Provisions on cross-border interope-rability				√						√						√	√	√							√				

A large majority of the countries covered (24) do not have provisions relating to the cross-border interoperability of EHRs.

Out of the countries (6) that do have such have provisions, legal situations are very different and largely depend on the development stage of EHRs in the country. In most cases, cross-border interoperability is either only required to be taken into account or considered but is not a legal requirement in the development of EHR laws and policies or implementation of EHR systems. For instance, in Luxembourg, the Law on the reform of the health system provides that an implementing regulation on her system (RSC) should set up conditions for the cooperation and cross-border transfer of data to the relevant authorities in other Member States of the EU or part of the EEA, but this Regulation has not yet been adopted. In other cases, such as Romania, the draft Health Law provides that the Health Ministry supports the development of European networks by connecting medical services suppliers within the national territory, and encouraging national stakeholders to participate in them. The draft law in Italy provides that the implementing ministerial decree(s) must establish criteria for the interoperability of EHRs at regional, national and European level and the draft law in Lithuania provides that exchange of patient data, medical images and ePrescriptions with other European Union Member States shall be implemented by using epSOS and guidance and experience of other projects as well as statutory requirements of the EU law, including specific standards.

Several stakeholders interviewed flagged that there were few legal and policy initiatives on cross-border transfer of health data at national level because Member States were mainly focusing their efforts on the deployment of their EHR system internally. They underlined that competent authorities did not consider the cross-border transfer of EHR as a main priority and that it should be dealt with at the EU level. It was also mentioned that competent authorities did not want to develop cross-border systems (e.g. through regional and bilateral agreements) that could potentially be in contradiction with the future action of the EU.

5 RECOMMENDATIONS

5.1 CONTEXT

The recommendations in this chapter are built upon the findings of the comparative analysis and the section of the national reports on legal barriers and good practices identified by stakeholders, taking also into account the conclusions presented by the different working groups during the expert workshop that took place on 18 June 2014, in Brussels. They focus on how Member States' laws and the European legal framework should evolve to allow the deployment of EHRs in the EU and to support cross-border exchange of health data. The recommendations are addressed to competent national authorities (the eHealth Network) and the European Commission

Recommendations on possible legal/regulatory initiatives will need to balance different interests at stake, the patient's rights, the health professional obligations, and the request for efficiency of healthcare systems.

Moreover, recommendations on legal action in this field should take into account national and European initiatives related to non-legal aspects of EHRs. In its 2008 Recommendation on cross-border interoperability of electronic health record systems, the European Commission already recognised that, in order to achieve the objectives of the European eHealth Action Plan, legal initiatives should go hand in hand with financial measures, agreement on an organisational framework, promotion of the use of technical standards and architectures, the establishment of common interoperability platforms, coordination at the semantic level and, finally, education mechanisms and awareness raising.[82]

Recommendations on legal action with regard to EHRs need to take into account the wider legal issues with regard to eHealth and in particular with regard to the delivery of cross-border eHealth services. In the Calliope Roadmap, these wider legal issues are illustrated by the following example: "when an eHealth solution is the primary vehicle for delivery of [cross border] care, for example a second opinion delivered by video conferencing with simultaneous capture and transfer of bio-data, then the legal and ethical issues are wide and will arise not only in terms of the data sharing, but also in terms of identity certification, professional accreditation, liability for shared care and other issues yet to be identified. The legal and regulatory issues include also administrative regulations such as those of reimbursement, and – in the context of cross border care - the mutual recognition of professional qualifications and the complex issue of entitlement to care".[83]

With regard to EHR interoperability, considerable efforts have been made by the eHealth European Interoperability Framework (eEIF) and by many other initiatives (eHGI, epSOS, HITCH, ISA, semantic Healthnet, Antilope, eSens, Expand, STORK 2.0, etc.).[84] One of the results of these initiatives is a better understanding of the interoperability needs and of the layers on which interoperability needs to be achieved (using a distinction between technical, semantic, organisational and legal interoperability). These layers will now be populated with standards, specifications, use cases, workflows, subset of terminologies, interoperability agreements, guidelines developed by specialised organisations, fora, consortia or EU funded projects after they have been identified or endorsed by the relevant EU governance bodies (eHealth Network, ICT Standards Multistakeholders platform and later the Connecting Europe Facility – CEF- governance).[85]

[82] Commission recommendation on cross-border interoperability of electronic health record systems (C(2008) 3282), 2008, http://ec.europa.eu/health/ehealth/key_documents/index_en.htm

[83] http://www.calliope-network.eu/Portals/11/Roadmap.pdf

[84] http://ec.europa.eu/digital-agenda/en/news/ehealth-interoperability-framework-study; for an overview of the various European projects on eHealth interoperability, reference is made to the eHealth Stakeholder Group report on " Perspectives and Recommendations on Interoperability, March 2014.

[85] See more in detail: http://ec.europa.eu/digital-agenda/en/pillar-vii-ict-enabled-benefits-eu-society/action-77-foster-eu-wide-standards-interoperability

More in particular with regard to technical and semantical interoperability, some tangible progress has been made in the recent past. The eHealth Stakeholder Group estimates that "the maturity of the concept of an eHealth European Interoperability Framework appears more advanced on technical and semantic levels". The eEIF builds further on technical specifications from the epSOS project and from international eHealth consortia such as Integrating the Healthcare Enterprise (IHE)[86] and Continua Health Alliance[87]. The patient summary guidelines adopted by the eHealth Network in November 2013 have been largely inspired by the patient summary and the interoperability framework developed by the epSOS project.[88]

The results of the eEIF report are currently (May 2014) used by the ANTILOPE Thematic Network that has been tasked with a validation of refinements to the eEIF across Europe, setting up quality control for interoperability testing and proposing various alternatives for certification or quality labelling of solutions.[89] Further progress could position the eEIF for the deployment of cross-border eHealth services in the frame of the CEF, but they will also potentially be used for national, regional or project based deployments.[90]

Finally, all efforts in the field of semantical interoperability have to take into account the wider international perspective. The European Commission therefore strengthened cooperation with organisations such as IHTSDO and WHO. A specific objective to study SNOMED CT has been included in H2020 work plan 2014-2015. The Commission also agreed on, and published, a roadmap supporting the objectives of the EU-US Memorandum of Understanding on eHealth interoperability standards and specifications.[91]

More challenging still are the organisational and legal obstacles to achieve EHR interoperability. Organisational interoperability - also called process or co-operability interoperability - refers to the broader environment of policies, procedures and bilateral cooperation needed to allow the seamless exchange of information between different organisations, regions and countries. Although Article 6 of Directive 2011/24/EU requests Member States to designate one or more national contact points for cross-border healthcare,[92] there is a need to further implement this network at the operational level. Financial support via the CEF will be crucial in this perspective.

Legal interoperability refers to the existing legal framework at EU and national levels that support and allow the exchange of data both within countries and across borders. With regard to the legal aspects, the most obvious obstacle is the diversity between Member States in transposing the Directive 95/46/EC on Data Protection. According to the eHealth Stakeholder Group "the dedicated effort to reach closure on the definition of a legal environment that allows the exchange of information across care settings, and across borders, should be concluded and extended with a harmonised data protection legal framework in the EU, where a single and uniform set of rules applies to all 28 Member States."

Besides the legislative initiative to replace the Directive 95/46/EC by a Data Protection Regulation, the European Commission announced a number of other initiatives with regard to the legal aspects of the eEIF. One of them is the development of an appropriate legal framework for an eHealth Interoperability Framework in view of the deployment of cross border eHealth services under the CEF. Another one is the establishment of a legal framework for the deployment of an eHealth testing

[86] IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. More information on http://www.ihe.net.
[87] Continua Health Alliance is a non-profit, open industry organization of healthcare and technology companies joining together in collaboration to improve the quality of personal healthcare. More information on http://www.continuaalliance.org
[88] http://www.epsos.eu/epsos-services/patient-summary.html
[89] http://www.antilope-project.eu/
[90] http://ec.europa.eu/digital-agenda/en/connecting-europe-facility
[91] http://ec.europa.eu/digital-agenda/en/news/transatlantic-ehealthhealth-it-cooperation-roadmap
[92] http://europa.eu/youreurope/citizens/health/contact/index_en.htm

and certification system at the European level.[93]

The underlying Study provides a clearer view on the current status and planned development of EHRs in the EU Member States and Norway. On the basis of the information collected in the countries covered and of the comparative analysis in the previous chapters, a series of recommendations can now be formulated for possible legal action in order to promote the development and the sharing of EHRs.

5.2 HEALTH DATA TO BE INCLUDED IN EHRs

Recommendation 1 at national level:
It is unthinkable today of a modern public national or regional healthcare system without the possibility of sharing health information among healthcare providers involved in the provision of care to the patient concerned. In order to share health information, the EHR systems used by these providers should have a minimum level of interoperability. Such interoperability does not require all systems used to store an identical list of data. Data should however, as much as possible, be available in those systems in a form which allows them to be exchangeable with the other systems used, whether such exchange is being organised via a central node or not. In some countries procedures have been installed to submit EHR software systems to a voluntary certification in order to test whether or not they allow extracting a standardized patient summary. This does not imply that the data included in the various EHR systems have an identical content, syntax or format. Consequently the recommendation is to make sure that the necessary information – necessary, for example, to generate a standardized patient summary – can be extracted from all EHR systems that are used by a relevant number of healthcare providers or institutions. As far as the data to be included in EHRs is concerned, it is also important to make sure that the data collected by healthcare providers and relevant to be shared with other providers, actually enter into a sharing network. Evidently it is very difficult to ensure that this actually happens if every healthcare provider is free to participate in the sharing network. It is also recommended that Member States take the necessary measures to implement any guidelines that may be adopted at EU level.

In more and more countries and/or regions in the EU, healthcare professionals are therefore requested by **mandatory legal rules** to share health data in EHR systems created by national or regional authorities. Participation in the national or regional EHR network is, in other words, no longer voluntary but is becoming mandatory for every healthcare professional. Mandatory participation of healthcare professionals in EHR sharing systems can, of course, only be introduced if all major obstacles for such participation have first been removed. In practice this means that it does not make sense to force healthcare providers to connect to a sharing system that does not function properly. As an alternative for mandatory participation healthcare professionals can be stimulated via various kinds of incentives (e.g. subsidies to health professionals to install relevant IT systems).

Recommendation 2 at EU level:
At the EU level agreement is necessary on general guidelines with regard to the content of EHRs but it does not seem necessary to regulate this in detail. The agreement on the patient summary guidelines by the eHealth Network shows the right way to proceed. The guidelines are, in our view, clear enough to enable next steps to achieve cross-border interoperability (see further recommendations 17 and 18). It will be crucial for the ultimate success of the guidelines to actively monitor its implementation by the Member States. Therefore the guidelines need to be complemented by agreements on technical and organisational aspects. Technical aspects include, for example, exchange formats, protocols and end-to-end security. Organisational aspects relate, for example, to the question via which intermediaries or nodes a healthcare provider in one Member State will actually get access to the summary information of a patient in another Member State. A lot of these aspects have been examined in the context of the

[93] http://ec.europa.eu/digital-agenda/en/pillar-vii-ict-enabled-benefits-eu-society/action-77-foster-eu-wide-standards-interoperability

EPSOS project and solutions have been tested. It is time now to proceed to their actual implementation in practice.

5.3 REQUIREMENT PLACED ON THE INSTITUTIONS HOSTING EHR DATA

Recommendation 3 at national level:
Institutions hosting EHR data, play a crucial role in countries such as France[94] where "personal health record" schemes have been introduced.. Applicants must provide extensive information demonstrating that their hosting system is secure and sophisticated enough to ensure that the rules on EHRs (*e.g. consent, access, confidentiality*) are fulfilled and that health data is well protected, especially considering the risk. Different commissions and committees are required to give their opinion on the application, and the authorisation is eventually granted by the Minister of health. This kind of legislation does not exist in the large majority of other countries covered in the Study. It is evident that, in most of these countries, EHRs can be hosted by external service providers, acting for example as processors on behalf of healthcare professionals, healthcare institutions or specific eHealth agencies established by public authorities. In any case, specific and more stringent rules for institutions hosting and managing EHRs, which take into account the specificities of EHRs (both in terms of content and format) as required by Article 17(1) of Directive 95/46/EC, should be adopted. These rules would not necessarily need to include an obligation to have data from EHRs encrypted as the lack of a legal obligation does not seem to have inhibited countries from having data encrypted anyway. It should be left to the Member States themselves to choose the security measures which are most appropriate in the context of their specific situation, possibilities and context. However, in view of cross-border exchange of EHRs it is absolutely necessary to take as much as possible European security standards into account in this domain.

The most frequently asked legal questions in this domain relate to the risks of using cloud services for hosting EHRs. For the time being, Member States should refrain from introducing particular legal rules or even guidelines, codes of conduct or model service legal agreements (SLAs) without taking into account the European perspective. Unilateral initiatives in this field are moreover not in line with Directive 98/48/EC on the provision of information in the field of technical standards.

Recommendation 4 at EU level:
The main recommendation at EU level concerns hosting institutions but covers also other security-related issues. Again the necessary European standards for securely exchanging EHRs are currently missing and therefore Member States are nowadays forced to invent bilateral solutions themselves. One important aspect in this context relates to basic user and access management. Many stakeholders interviewed in the course of the Study are convinced that there should be a binding European legal framework covering this issue. This framework should ideally also include operational rules on other security aspects such as end-to-end encryption (currently not possible because of the lack of a common encryption standard), audit trails, recovery disaster procedures, etc.

At European level, agreement is also recommended on a model service level agreement for cloud services with regard to EHRs. The European Commission is currently working on the development of such model SLAs in the context of the European Cloud Strategy. Healthcare is one of the sectors receiving particular attention in these activities. The eHealth Network should closely follow up the progress made in this context and stimulate the development of European model provisions for cloud SLAs dedicated for eHealth services and EHRs in particular. The recommendation is consequently to, as much as possible, synchronise with progress made in the context of the EU Cloud Strategy and not to develop something in parallel.

[94] France is the only country that has adopted a very detailed authorisation procedure for institutions hosting personal health data through electronic means.

5.4 PATIENT CONSENT

Recommendation 5 at national level:
Some Member States have adopted a three stage approach in relation to consent:

- When a patient visits a healthcare professional in order to receive care, this professional has the duty to keep a record of at least a minimum set of data related to the identity of this patient and related to the care provided; no additional implicit or explicit consent of the patient or even an opt-out possibility is thus needed at this stage.
- When, on the basis of national or regional law, public authorities decide to make available EHRs for exchange among healthcare professionals (e.g. in order to avoid unnecessary public healthcare costs), such EHR sharing systems can be established and include available individual EHRs without additional explicit consent of the patients. Member States are however free to introduce opt-out possibilities for this stage. This viewpoint corresponds to the one expressed by the Working Party in its opinion of 2007.
- When a patient visits a healthcare professional who wishes to receive or access health data collected from this patient by other healthcare providers (by means of the EHR sharing system), such access will require prior explicit consent of the patient concerned. This consent constitutes, at the same time, proof that this patient has engaged into a therapeutic relationship with the healthcare professional.

This approach has proven to be successful for the deployment of the EHRs systems in some countries and it is, at the same time, in line with the 2007 Opinion of the Article 29 Working Party. Therefore, this could be seen as good practice and its replication by other countries should be considered.

As flagged by workshop participants informing the patient about the consequence and the functioning of shared EHRs prior to the consent is highly recommended as a prerequisite for the public acceptance of the shared EHR system. It is therefore important that Member States set awareness and communication campaigns (e.g. leaflets, websites).

Recommendation 6 at EU level:
With regard to the protection of privacy of EHRs, Member States are not allowed to maintain for the patients on their territory a higher level of protection than the one provided for by the Directive 95/46/EC. Therefore, the issue whether or not the creation and/or sharing of health data requires the consent of the patient and, if so, which type of consent would be needed, is an issue that can only be decided at EU level. The disparities between Member States on this issue, as demonstrated again in the underlying Study, should be eliminated as soon as possible bearing in mind the objective of achieving free flow of data across the EU. Of course this is precisely one of the main objectives of the draft Data Protection Regulation which is currently under discussion in the Council and the European Parliament. Although the current text as proposed by the Commission and amended by the Parliament – in particular Article 81 – does not really clarify the issue discussed here, the current version (May 2014) of the draft Regulation contains a small opening for regulating the question more specifically by way of a secondary European legislation via a delegated act issued by the European Commission.[95] However, following this path will most probably take many years and one can argue that a much more urgent intervention at European level is necessary in this domain. Therefore, it would be more appropriate to obtain, on a much shorter term, an agreement by the eHealth Network on the "three-stages" model described in the previous recommendation, promoting this model as a European

[95] See Article 81.3: "The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying public interest in the area of public health as referred to in point (b) of paragraph 1 and high public interest in the area of research as referred to in paragraph 2a." This provision gives the Commission the possibility to confirm in a delegated act that the establishment of EHR schemes are legally grounded on "public interest" (and are therefore possible to set up without explicit consent of the patient).

guideline for all Member States.

5.5 CREATION, ACCESS TO AND UPDATE OF EHRs

Identification and authentication of health professionals, access of health professionals to EHRs

Recommendation 7 at national level:
In its 2013 report on patient access to the EHR, the eHealth Stakeholder Group states: "The electronic health record poses challenges in ensuring that only authorised health professionals gain access to information for legitimate purposes related to the patient. The possibility of abuse is significant and the risk increases when systems become more interconnected. As a consequence most of the stakeholder group members consider that there is still lack trust in the security of the system and are reluctant to use it. Among stakeholders, there remains in general uncertainty over the "who and how" can access and modify data and who is responsible for it."[96] The underlying Study has moreover demonstrated the disparities between countries, and even between regions, with regard to the professions included in their lists (when they exist) of health professionals with access to EHRs. Finally it has shown that not all the countries covered have trustworthy registers of (all categories of) healthcare professionals.

The most urgent tasks for all Member States in this field are, despite significant financial cost involved: 1) to establish certainty on the categories of healthcare professionals who can have access to patient summaries, and 2) to establish trustworthy official registers of those categories of professionals which can be used for authentication purposes and that need to be accessible on-line.

Recommendation 8 at EU level:
At Union level there should ideally be an agreed list of the categories of healthcare professionals having access to patient summaries (and subsequently for the other priority use cases mentioned before) or a commonly agreed definition of healthcare professional. Such an agreement will however most probably not be reached on a short term. An alternative could therefore be to leave it to each Member State to decide who should be considered as a health professional in the context of intra-European EHR exchange. Moreover, the eHealth Network should agree on a limited number of basic principles. Some of these principles have already been put forward by the eHealth Stakeholder Group: "Certain categories of personal health data such as genetic information must be subject to especially strict access controls. A system of data modules or sealed envelopes could help establish a different level of confidentiality and restrict access to some information to some health professionals only. Moreover access to patients‟ health records should only be permitted to the health professionals on a "need to know basis."[97]

Patients' rights to access, right to erasure and correction and right to know who accessed EHRs

Recommendation 9 at national level:
The eHealth Stakeholder Group already recommended to grant patients' rights relating to EHRs as follows: "Patients should be in charge of their own medical file, they should be able to „log in‟ and inspect it", and "Patients should be given the possibility to know who accessed their EHR and restrict access if they wish so and are informed about the risks of doing so".[98]

As shown in this Study some Member States adopted specific rules allowing the data from EHRs to which the patient already has access, to be downloaded, as well as providing for the availability online of the information about who accessed EHR. This is an effective way by which patients would be entitled to those data "without constraint at reasonable intervals and without excessive delay or

[96] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5169, p. 4
[97] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5169, p. 14
[98] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5169, ibidem

expense", as required by Article 12 of Directive 95/46/EC. However, it is important to bear in mind that if the patient is entitled to download information his/her information will then be less protected than if it will be kept under a secure EHR system.

It is also recommended that where countries wish to grant patients the right to erase or hide data that has not been inputted by them, health professionals are at least notified that some data is missing, allowing them to try to convince the patients to disclose such data. Such an approach would help to ensure the accuracy of data, as required by Article 6(1)(d) of Directive 95/46/EC. Finally, it is also recommended that Member States take the necessary measures to implement any guidelines that may be adopted at EU level.

Recommendation 10 at EU level:
In the context of cross-border transfers of EHRs, agreement is recommended on a set of guidelines, e.g. on the possibility for patients to add, modify or erase data from EHRs. One example of such a guideline could be to take into account the protection of the data subject or the rights and freedoms of others when allowing access to EHRs in order to guarantee, for example, that information that is harmful to the patient is not directly available to him/her; and fostering the replication of approaches like the one taken by Estonia, where health professionals may decide to hide certain EHR information from the patient for up to six months, allowing them to personally communicate delicate diagnoses to the patient. It is also recommended to adopt a provision expressly prohibiting the possibility for patients to modify data from EHRs that has not been inputted by them so as to allow health professionals from other countries to rely on the information available. For the same reason, it is also recommended that where patients have the right to erase or hide data that has not been inputted by them, health professionals are at least notified that some data is missing.

5.6 LIABILITY

Recommendation 11 at national level:
The Study did not discover many dedicated rules on the liability of health professionals with regard to EHRs in the countries covered. According to the comparative analysis, only a handful of countries have established specific medical liability rules with regard to EHRs, and these rules are mostly reinforcing or highlighting the general liability regime. Many stakeholders interviewed pointed out that application of general rules on medical liability led to reluctance of health professionals to use and develop EHR.

At national level there is primarily a need to inform and educate health professionals about their liabilities with regard to EHRs and how the existing rules at national level (either specific or general) apply in this context. Introducing dedicated rules on this issue does not seem necessary.

Recommendation 12 at EU level:
The specific practical consequences of the application of the currently existing liability regime for data controllers, laid down in Article 23 of Directive 95/46/EC, on the EHR context should be clarified in order to improve legal certainty on this issue. Such clarification can be carried out in the form of guidelines on how to avoid liability issues, illustrated by typical examples of potential cases of negligence and/or of recommended behaviour. In particular, with a view on cross-border sharing of EHRs it is also recommended to include the basic principles of private international law with regard to liability, illustrated by typical examples. The primary objective of commonly agreed guidelines on liability with regard to EHRs would be to reduce the reluctance of healthcare professionals to adhere to EHR schemes by removing some of the uncertainties in this area.

5.7 SECONDARY USE

Recommendation 13 at national level:
Under the, secondary use of health data is legally permitted if 1) the secondary use is not incompatible with the purposes for which the data have been collected, or 2) the secondary use is for historical, statistical or scientific purposes.[99] For the latter hypothesis, the Member States are requested to provide "appropriate safeguards" in their national legislation. This broad concept has been interpreted and implemented in different ways as shown by our Study (e.g. different approaches to anonymisation/ pseudonymisation / consent/ control by data protection authorities)

It is therefore difficult to give recommendations to the Member States on how they have to fill in the delegation given to them by European legislator in Article 6(1)(b) of Directive 95/46/EC. The first and most urgent task is to develop a European framework on secondary use of health data, binding or not.

Recommendation 14 at EU level:
A European legal framework for the secondary use of health data, in particular for research purposes, is currently missing. The proposal for a Data Protection Regulation contains some positive new elements. If adopted, it will, for example, eliminate possible contradictions between the application of the national data protection legislation and the European Clinical Trials Directive.[100] It will, however, not eliminate the disparities between the Member States with regard to the secondary use of health data for research purposes. Article 81(2)(a) in the version adopted by the European Parliament (May 2014) stipulates: "Member States law may provide for exceptions to the requirement of consent for research, as referred to in paragraph 2, with regard to research that serves a high public interest, if that research cannot possibly be carried out otherwise. The data in question shall be anonymised, or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent unwarranted re-identification of the data subjects. However, the data subject shall have the right to object at any time in accordance with Article 19."[101]
In the perspective of a European research market for health data this far-going delegation to the Member States should be reconsidered because it will maintain disparities between the Member States in this domain. The conditions for the further processing of health data for research purposes should be regulated at Union level.

5.8 ARCHIVING DURATIONS

Recommendation 15 at national level:
Most of the countries covered by this Study have introduced rules on the ***minimum*** archiving duration of health records. Other studies have shown that, in practice, health professionals keep their records much longer than the mandatory minimum period. Health records can contain information collected when the patient was a child and this information can remain relevant during the patient's entire lifetime. Rules on minimum archiving duration of EHRs are primarily necessary to avoid destruction of health information that is still relevant. In our view, however, it is not necessary to translate this objective in precise archiving duration rules.

On the other hand, Article 6(1)(e) of Directive 95/46/EC requests Member States to ensure that personal data, which permits identification of the data subject, are kept for no longer than necessary. This rule relates, in other words, to the ***maximum*** archiving duration. Again it is extremely difficult to formulate precise rules in this domain because the relevance of health data depends very much on the type of data and on other circumstances. Probably not all data collected by healthcare professionals will be relevant for very long periods. As in other domains, healthcare professionals, as data

[99] Art. 6.1 (b) of Directive 95/46/EC.
[100] Article 81.1c is currently (May 2014) worded as follows: "For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Directive 2001/20/EC shall apply."
[101] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (

controllers, have a legal obligation to manage the data they process in line with the proportionality principle. It is not considered necessary to have specific rules on the archiving duration of EHRs when there are already specific rules on the archiving duration of medical data in general (the format in which data is stored does not seem to play a very important role in this context). However, it is recommended that Member States which have set very long periods of archiving, consider revising their approach in light of Article 6(1)(e) of Directive 95/46/EC.

Recommendation 16 at EU level:
Our recommendation for the EU level is more or less identical as at national level. EHR content should be kept as long as necessary and it is the responsibility of every data controller to keep an eye on this legal objective. More precise legal rules on the EU level on this topic do not seem necessary.

5.9 REQUIREMENTS ON INTEROPERABILITY OF EHRs

Recommendation 17 at national level:
In order to share health information the EHR systems used by these providers should have a minimum level of interoperability. This does not necessarily mean that legal rules have to impose uniformity in EHR systems. Multiple technical solutions can perfectly co-exist. Rules or guidelines at the national level should mainly aim at achieving essential requirements with regard to semantic, technical, organisational and legal interoperability. For each of these aspects national and/or regional rules should take into account standards and guidelines agreed on at the European level.

Recommendation 18 at EU level:
Commonly agreed rules at European level with regard to terminological, technical, legal and organisational interoperability of EHRs are currently largely missing. Member States, wishing to exchange health records in a cross-border context –today mainly done between entities located close to national territorial borders – are nowadays forced to develop their own bilateral solutions. The lack of European rules in this domain is also the most important obstacle hindering the breakthrough of a European eHealth industry. ICT solution providers in the domain of EHRs are still facing an extremely fragmented European market and therefore experience a serious disadvantage when competing with the US eHealth industry.

It is true that some efforts to develop European rules for EHRs have already been made, not only in the context of European projects, but also in the form of "soft law". One example is the agreement on the patient summary guidelines by the eHealth Network. A second one is the Commission Implementing Directive on medical prescriptions.

With regard to the organisational aspect, the agreement between the Council and the European Parliament on the draft Regulation concerning electronic identification and trusted services is a step forward. Much more is however needed to implement the selected use cases, in particular for secure cross-border authentication of healthcare professionals.

The conclusion is therefore that, after having reached the agreement on the content of a patient summary, agreements are now needed on a) a terminological profile for a minimum set of fields included in the patient summary, b) a technical profile for the cross-border exchange of patient summaries, in particular with regard to the security aspects, c) a list of the categories of healthcare professionals who can access the patient summary, including a solution for the secure authentication of these professionals and their authorisations, and d) a roadmap for the implementation of the cross-border exchange of patient summaries between Member States.

5.10 LINKS BETWEEN EHRs AND ePRESCRIPTIONS

Recommendation 19 at national level:
The obvious link between EHRs and ePrescriptions is the fact that the medication information is part of the EHR. The medication summary is even part of the patient summary dataset agreed on in the Guidelines on the minimum/non-exhaustive patient summary dataset adopted by the eHealth Network. Part of the medication summary relates to the prescribed medicines (dispensed or not). It is therefore surprising that very few countries have set, or are planning to set, links between EHRs and ePrescriptions. However, integrated EHR and ePrescription systems have proved to have many advantages (e.g. some stakeholders have highlighted, that it would allow doctors to understand the patient's consumption of medicines). Member States should take into consideration these synergies between these two systems. ePrescription data can be used as direct input for EHRs. In case the two systems are linked, access to EHRs will be open for additional categories of health professionals (e.g. pharmacists) and therefore it is recommended to adopt a role based approach when setting access requirements (see recommendations 7 and 8).

Recommendation 20 at EU level:
One of the most important current obstacles for the cross-border exchange of ePrescriptions, is the lack of a common data model and a common vocabulary for medicinal products or pharmaceutical products throughout Europe. Efforts to overcome this obstacle are directly useful for the exchange of EHRs because the medication part of the EHRs faces similar terminological challenges. Agreements on standards in this field should therefore simultaneously take into account the needs of cross-border exchange of EHRs, as well as of ePrescriptions.