澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

MASTER THESIS IN EUROPEAN UNION LAW

Patients' right and data protection – use of electronic health records in cross-border healthcare at the European Union

SHA LEQI

MB850044

Supervisor: Vera Lúcia Carapeto RAPOSO

ABSTRACT

With the development of science and technology, the medical field is increasingly benefiting from this trend and continuously deploying e-health. Digital technology is a powerful tool to solve some current medical problems and adapt health systems to future challenges. These digital technologies also help to identify and change patients' treatment methods as early as possible, so as to reduce subsequent complications.

The European Commission wants all EU citizens to have access to their online health records in any Member State by 2020 to boost the digital economy and ensure an accessible health services across the EU. This means that citizens and healthcare providers can securely access and share EHRs. It is believed that in the near future, the EHR will be stored in a centralized supranational central serve, but the privacy threat posed by these networks is a key issue. Cross-border and interoperable EHR systems make confidential data more easily and quickly accessible to the public. Thus, cross-border exchange of EHR increases the risk that personal health data may be accidentally exposed or distributed to unauthorized parties. In addition, the lack of interoperability of EHR has led to the fragmentation of healthcare services and the decline of cross-border medical service quality.

Therefore, the highest standards of security and data protection are essential for the development and exchange of electronic health records. The purpose of this thesis is to analyze how the EU's e-health policy promotes the development of EHR, and how to safeguard these health data of patients in the context of cross-border healthcare to ensure their confidentiality, integrity and availability.

KEYWORDS: European Union (EU); Cross-border healthcare; e-health; Electronic health record (EHR), Data protection; privacy

TABLE

ABSTRACT II

TABLE III

ABBREVIATIONS V

Chapter I Introduction 1

1.1 Background 1

1.1.1 Definition of EHR 3

1.2 Research Questions 6

1.3 Methodology 7

1.4 Chapter layout 7

Chapter II Background of EU cross-border healthcare 9

2.1 The EU role in health sector 9

2.1.1 From Rome to Maastricht: 1957-1992 9

2.1.2 From Maastricht to Lisbon: 1992-2007 12

2.1.3 Post-Lisbon: 2007 to Present 16

2.2 CJEU influence on cross-border healthcare 18

2.3 The EU legislation on patient's rights in cross border healthcare 20

2.4 Roles and responsibilities in cross-border healthcare 23

2.4.1 European Commission 23

2.4.2 Member States 24

2.5 Cooperation in healthcare: e-health 25

Chapter III EU polices in the cross-border medical informatization 29

3.1 Overview of EU medical information development 29

3.2 Relevant planning of EU medical information 29

3.2.1 e-Health Action Plan 2004-2010 29

3.2.2 The European e-health Governance Initiative 2011-2014 31

3.2.3 e-Health Action Plan 2012-2020 37

3.3 Cross-border health project epSOS 41

3.3.1 Content of the project 41

3.3.2 Legal background for epSOS implementation 43

3.3.3 Achievements and influence of epSOS 48

3.4 Other polices 48
Chapter IV: EU privacy and data protection for cross-border healthcare 53
4.1 Council of Europe legal framework 53
4.1.1 Article 8 of the ECHR 53
4.1.2 Convention 108 58
4.1.3 Case law of ECtHR – health data 61
4.2 EU legal framework on privacy and data protection 62
4.2.1 EU Primary Law 63
4.2.1.1 Article 16 TFEU 63
4.2.1.2 EU Charter of Fundamental Rights 65
4.2.2 EU secondary Law – GDPR 71
4.2.3 Soft Law 76
4.3 Exchange of EHRs across the EU 77
4.3.1 EHR in the EU 77
4.3.2 Patient's rights on the EHR 81
4.3.2.1 Information and access 81
4.3.2.2 rectification, erasure and data portability 83
4.3.3 Additional obligations of the controller and processor 86
4.3.4 Health records breach handling 88
4.4 Privacy of cross-border EHR system 90
Chapter V Challenges and Recommendations in EU EHR 94
5.1 Challenges 94
5.1.1 Lack of guarantees of privacy and confidentiality 94
5.1.2 Lack of interoperability and information 97
5.2 Recommendations 97
5.2.1 Guarantee privacy and data protection 97
5.2.2 Requirements on interoperability of EHRs 99
Chapter VI Conclusion 101
Bibliography 103

ABBREVIATIONS

CHAFEA	Consumers, Health and Food Executive Agency
CJEU	Court of Justice of European Union
CPME	Standing Committee of European Doctors
DAE	Digital Agenda for Europe
DG CONNECT	Directorate General for Communications Networks, Content and Technology
DG RTD	Directorate General for Research and Development
DG SANTE	Directorate General for Health and Food Safety
DSM	Digital Single Market
DSS	Decision Support Systems
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEC	European Economic Community
eEHIC	Electronic European Health Insurance Card
EESC	European Economic and Social Commission
EHR	Electronic Health Record
eIDAS Regulation	Regulation on Electronic Identification and Trust Services of Electronic Transactions in the Internal Market
EMR	Electronic Medical Record
ePs	Electronic Prescription System
epSOS	European Patient Smart Open Services
ERNs	European Reference Networks
EU Charter	Charter of Fundamental Rights of the European Union
FAO	Food and Agriculture Organization of the United Nations
FWA	Framework Agreement
GDPR	General Data Protection Regulation
ICTs	Information and Communication Technologies
JRC	Joint Research Council
MDR	Medical Device Regulation
m-health	Mobile Health
NCPs	National Contact Points
NHS	National Health System
NIS Directive	Directive on Security of Network and Information Systems
OECD	The Organization for Economic Cooperation and Development
OMC	Open Method of Coordination
PETs	Privacy Enhancing Technologies
R&D	Research and Development
TLA	Temporary Legal Agreement
WHO	World Health Organization

Chapter I

1.1 Background

The EU's aim is peace and economic development. To some extent, economic development itself can improve health.[1] Because of the improvement of economic level, people will have better quality of life and medical conditions. Specific competencies in healthcare give EU institutions the right to act through "conferred powers" derived from EU treaties but EU must cooperate with Member States in implementation. One of the reasons for cooperative implementation is to comply with the principle of subsidiarity.[2] Article 168 TFEU requires that "a high level of human protection" should be ensured in all EU policies and "shall in particular encourage cooperation between the Member States to improve the complementarity of their health services in cross-border areas.".[3] Also, in order to improve the functioning of the internal market and the free movement of goods, persons and services, Article 114 TFEU is also the appropriate legal basis. Article 114 (3) TFEU explicitly provides that in the process of achieving harmonisation, a high level of protection of human health should be guaranteed, taking into account especially any new developments based on scientific facts.[4]

Cross border patient mobility refers to the possibility of a person receiving healthcare in a Member State rather than their country of residence. Although most patients are more used to receiving treatment near their homes because they can use a language they understand and a procedure they are familiar with,[5] some patients may be willing to receive treatment abroad if there are some advantages. There are many reasons why patients may seek treatment in another EU Member State, including perceived quality of care, the specialized nature of healthcare, or the lack of ability to provide such healthcare in their home country. For instance, patients may have to travel to receive highly specialized healthcare because it is not economically sustainable for a small country, or patients may travel to seek services that are not legal in their home country, such as end-of-life

[1] Greer, S. L., Hervey, T. K., Mackenbach, J. P., & McKee, M. (2013). Health law and policy in the European Union. *The Lancet*, 381(9872), 1135-1144.
[2] Commers, M. J., Van Der Molen, I. N. (2013). Unresolved legal questions in cross-border health care in Europe: liability and data protection. *Public health*, 127(11), 987-993.
[3] Consolidated version of the Treaty on the Functioning of the European Union,2012 O.J. (C326/47). Article 168.
[4] TFEU, 114 (3).
[5] Baeten, R., Busse, R., Glinos, I. A., Legido-Quigley, H., McKee, M. (2012). Analysing arrangements for cross-border mobility of patients in the European Union: A proposal for a framework. *Health policy*, 108(1), 27-36.

assistance or reproductive health services.[6] In EU policy debates, cross-border healthcare usually means short-term and long-term visitors to another EU Member States who find that they must have access to medical care when they are abroad.[7] According to statistics, there are more than 2 million cases recorded each year that citizens residing in one Member State seek healthcare in another Member State.[8] One of the objectives of EU health policy and the principle of internal market is to ensure the right of EU patients to access safe and high quality healthcare, including cross-border healthcare within the EU, as well as the right to receive reimbursement for such healthcare.

In order to promote and regulate the cross-border movement of medical services, EU has enacted Directive 2011/24/EU on patients' rights in cross-border healthcare and it is the first time to lay down the legal framework for e-health.[9] With the rapid development of science and technology, the European Commission enhances the use of digital technology by creating a digital single market and health is one of the sectors included in the agenda.[10] Electronic health records (EHRs) are very meaningful in helping patients in cross-border healthcare. However, the legal issues of personal privacy and data protection arising from the cross-border exchange of EHRs are worth considering. In the context of cross-border healthcare, the need to protect patients' personal data is obvious. Protecting patient's health data means that any patient in cross-border medical care has the right to expect that his/her health data will not be handled by anyone in any way. Patients also have the right to expect that specific bodies and measures can help ensure the effectiveness of data protection.[11] In other words, patients seeking healthcare in another Member State (non-resident country) are entitled to expect the same level of data protection as they would have in their country of residence, and other things should be equal.[12]

[6] Beaten, R., Footman, K., Glonti, K., Knai, C., McKee, M. (2014). Cross-border health care in Europe. World Health Organization. P. 2.
[7] Ibid.
[8] Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format, 2019 O.J. (L39/18).
[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, 2011 O.J. (L88/45).
[10] https://ec.europa.eu/health/ehealth/overview_en
[11] Herveg, J. (2017). Data protection and patient mobility in Europe. *Cross-border health care and European Union Law* (pp. 191-212). s.l.: Erasmus University Press.
[12] Ibid.

While patients' health data are protected by GDPR, they will also face some challenges. Therefore, the purpose of this thesis is to study the data protection and privacy of patients in the context of cross-border healthcare within the EU. More specifically, how to protect the EHR of patients in cross-border exchange, and what challenges will be encountered.

1.1.1 Definition of EHR

An 'Electronic health record' is defined by the Commission Recommendation on cross-border interoperability of electronic health record systems as a comprehensive medical record or similar document that records an individual's past and present physical and mental health information in electronic form, and provides such data on time for medical treatment and other closely related purposes.[13] This can actually be seen as an evolving concept. Such records can be shared among different healthcare settings through an enterprise-wide information system embedded in a network connection. [14] Such records may include a series of comprehensive data, including demographics, medical history, medication and allergies, immunization status, radiology images, laboratory test results, vital signs, personal statistics like age and weight, as well as billing information.[15] As technology advances, EHRs have more flexible functionalities. For example, with artificial intelligence they can help doctors predict acute critical illnesses[16] and make medical decisions. They also have an alarm system[17] to effectively monitor and protect high-risk patients.

The relevant EHR system is the system that EHR uses to record, retrieve and operate health information. EHR system is designed to accurately store data and obtain the health status of

[13] Commission Recommendation of 2 July 2008 on Cross-border interoperability of electronic health records system, 2008 O.J. (L 190/ 37). Available at: http://ec.europa.eu/information_society/newsroom/cf/ itemlongdetail.cfm?item_id1⁄44224.

[14] Gunter, T. D., Terry, N. P. (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. Journal of Medical Internet Research, 7(1). DOI:10.2196/jmir.7.1.e3

[15] Onyejekwe, Egondu R., Rokne, Jon, Hall, Cory L (2019). *Portable Health Records in a Mobile Society*. Springer. P. 213.

[16] Lauritsen, S. M., Olsen, M. V., Larsen M. S., Kristensen, M. Lange, J., et al. (2019). Explainable artificial intelligence model to predict acute critical illness from electronic health records. ArXiv.org; Ithaca, Dec 3, 2019.

[17] Berger, R., Gerard, S., Iriana, S., Krawiec, C., & Levi, B. (2020). What We Can Learn From Failure: An EHR-Based Child Protection Alert System. *Child Maltreatment*, 25(1), 61–69.

patients across times. It solves the tedious problem of tracking patients' previous paper medical records, and helps to ensure the accuracy and clarity of data. Additionally, it can reduce the risk of data being copied and losing paperwork. More than a decade ago, EHR was touted as the key to improving quality of healthcare. Today, healthcare providers are using data from patients' electronic records to improve the quality and efficiency of their patient diagnoses. Combined with a variety of clinical data in the EHR system has helped clinicians identify patients with chronic diseases. Healthcare providers can also use and analyze the data in the patient's EHR to prevent high-risk patients from being hospitalized or die, thereby improving the quality of care.

It is worth noting that EHR and electronic medical record (EMR) are often used interchangeably. However, these terms are different and should not be confused with each other. The EMR is provider centric and contains notes and information collected by clinicians in the office, clinic or hospital about patient's specific encounters.[18] On the contrary, EHR is patient-centered and contains information about patients who have received treatment in all medical institutions.[19] It is a more vertical collection of electronic health information for individuals or populations, and can be shared and interoperable across healthcare environment (inter-institution). The EMR can be regarded as a legitimate patient record created in the hospital environment, and it can be used as the data source of EHR. One of the characteristics of EHR is clinical database repository, which contains healthcare information about patients, computerized input of healthcare professionals, hospitals and pharmacies.[20] These databases allow healthcare professionals and hospitals to electronically exchange health data with entities in the health network. Because digital information can be quickly searchable, EHR is more effective when acquiring medical data to check the development trends of patient's possible disease and predict long-term changes. The widespread adoption of EHRs and EMRs may also facilitate population-based research of health records.

The superiority of EHRs over paper records is outstanding It is obvious that traditional handwritten paper health records may sometimes be illegible, which may lead to medical errors. Traditionally,

[18] Artmann, J., Dumortier, J., Giest, S., Protti, D., Stroetmann, K. A., Stroetmann, V. N., Whitehouse, D. (2011). European Countries on their journey towards national eHealth infrastructures. Luxembourg: Publications Office. P.19.
[19] Ibid.
[20] Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review* 27(5):503-515.

pre-printing forms and writing standardization are encouraged to boost the efficiency and reliability of paper health records. Therefore, the emergence of electronic records can solve this kind of problem, which helps to standardize forms, terms and data input. Higher transparency, portability and accessibility through the use of EHRs may increase the convenience of healthcare professionals accessing these records. Digitalization of health records can help to collect data from epidemiological and clinical studies, and improve the efficiency of diagnosis of health care personnel, so as to reduce costs, complications and mortality of patients. Furthermore, the EHRs can be continuously updated within a legal scope. If the interoperability of exchange records between different EHR systems is improved, it would help to coordinate the healthcare services provided by healthcare providers. Data from the EHR system can also be used anonymously for statistical reports such as infectious disease surveillance and quality improvement.[21] In the recent COVID-19 pandemic, doctors and relevant researchers can analyze the development trend of the epidemic based on the anonymous EHR, and can also develop corresponding vaccines based on these data. In addition, during this pandemic, rural hospitals can use the telehealth system to retain patients (EHR will be used in telehealth), so as to reduce unnecessary transfer to the overburdened tertiary hospitals.[22] This will help the development of rural hospitals to cope with the COVID -19 pandemic crisis. However, EHR is like a double-edged sword with advantages and disadvantages in real life. The use of electronic recording methods has the risk of unscrupulous users stealing EHR of patients by means of technology, such as hackers attacking the system that store health information, which undoubtedly needs to improve the protection of patients' health data. Such concerns about data security will increase resistance to the adoption of these electronic records. At the same time, the requirement for standardization of EHRs will also pose challenges at the national level and EU level, both in terms of technology and law.

With the development of electronic health, privacy and protection issues related to health data has risen to a new dimension. In fact, traditionally, the doctor-patient relationship is relatively simple,

[21] Anonymous. (2003). New Events Pepper the Show.(Healthcare Information and Management System Society's 2003 Annual Conference & Exhibition)(Brief Article). Health Data Management, 11(1), 24.
[22] Gutierrez, J., Kaboli, P. J., Kuperman, E. (2020). Using Telehealth as a Tool for Rural Hospitals in the COVID-19 Pandemic Response. *The Journal of rural health*, p. 1.

which is mainly the physical presence of patients and personal interaction,[23] while there is little discussion on the ownership of health records.[24] Nowadays, using EHR will cause many new issues, which need more complex and detailed methods to deal with. The Article 29 Data Protection Working Party in its Working Document on the Processing of personal data relating to health in EHR also emphasized that maintaining the confidentiality legal standards applicable to traditional paper recording environment may not be enough to guarantee the privacy interests of patients after EHRs are online.[25] As a consequence, the data protection framework is very important to the EHR, and at the same time, it also needs to comply with the relevant rules on electronic data and electronic communication.

1.2 Research Questions

The author of this thesis mainly studies the following five groups of research questions.

First, the health sector is becoming increasingly important in the EU. It is not only related to the citizen's health, but also related to the economic development of the EU. Therefore, what role does the EU play in healthcare? In other words, how does EU intervention in the health sector evolve over time? Does the CJEU's decision on the right of citizens to seek healthcare across borders have a significant impact on the broader discussion of legal clarify of cross-border healthcare rights and provisions?

Second, Directive 2011/24/EU emphasizes the cooperation in healthcare domain, so what are the positive and negative aspects of e-health? What policies or initiatives has the EU adopted in the field of e-health in cross-border healthcare? What legal issues are involved in some policies or initiatives?

[23] Van Dooselaere, C., Herve, J., Silber, D. and Wilson, P. (2008*), Legally eHealth - Putting eHealth in its European Legal Context*, p. 6.
[24] Wilson, P (2012), *Legal frameworks for eHealth*, p. 35.
[25] Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records 2 (Working Paper No. 131, 2007). Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp 131_en.pdf.

Third, what is the legal framework for data protection in Europe? What EU policies promote the development of the EHR? What rights do patients have to protect their EHRs? Does GDPR effectively protect patients' personal health data when they cross borders for healthcare treatment?

Finally, what challenges do EU citizens face in obtaining their own EHR across borders?

1.3 Methodology

Firstly, the thesis will use the method of literature collection and simple historical review to analyze how the intervention of the EU in the field of health has evolved over time. Meanwhile, the development of some health-related policies in the EU can also be studied.

Secondly, the method of case law will be adopted in this research. This method can help authors to analyze the development of health in the EU, and the positive impact on the promotion of EU cross-border healthcare by CJEU. In addition, the development of personal privacy and data protection in Europe can be explored through case law.

In addition, the materials of this thesis are mainly collected from Library of University of Macau, legal database such as HeinOnline, Westlaw and LexisNexis as well as other books. Furthermore, the white paper, the official website of the European Commission and EUR-Le also provide much worthy information for the thesis.

1.4 Chapter layout

Chapter I is a brief introduction of the whole thesis, including the reasons for choosing the topic, the research feasibility of this topic and the situation of cross-border healthcare in EU, as well as the definition of EHR.

Chapter II briefly describes the development of the health sector in the EU, briefly analyzes the Directive 2011/24/EU, especially in the field of e-health. And the author also lists the positive and

negative aspects of e-health, in order to explore the legal issues that e-health will face in more depth.

Chapter III includes some EU initiatives in the field of e-health, including project epSOS, e-health action plan 2004-2010 and e-health action plan 2012-2020, as well as other initiatives. Among them, the epSOS project is analyzed in detail, because the content of the first phase of this project can be used as a significant reference for cross-border exchange of EHR. And the legal problems encountered in the project can also be used for reference in the future.

Chapter IV analyzes the legal framework of EU on privacy and data protection. After that, the author answers the development of EHR in the EU. Then the author discusses the rights of patients to their own health records, including the right to access, right to be forgotten and right to rectification. Furthermore, the author also briefly analyzes how to deal with the data breach according to the provisions of GDPR.

Chapter V includes the possible challenges in cross-border exchange of EHR, which is mainly summarized as the lack of guarantee of privacy and confidentiality, as well as the lack of information and interoperability. In addition, the author also put forward the suggestions.

Chapter VI is the summary of the whole thesis.

Chapter II Background of EU cross-border healthcare

2.1 The EU role in health sector

The legal order of the EU is unique. It is not only different from the national legal system of its Member States, but also different from traditional international law. Its purpose is to "integrate" the market, the economy and the relevant policies of Member States. In fact, “integration” refers to the various mechanisms of EU to achieve its integration goals, rather than simple centralization of power or legal coordination.[26] EU law has a profound impact on health issues in EU countries. How does EU intervention in health evolved over time? To what extent and in what ways does EU law affect health laws and policies? According to the process of EU treaty reform, I will divide the development of EU health law into three parts in chronological order: from Rome to Maastricht; from Maastricht to Lisbon; post-Lisbon.

2.1.1 From Rome to Maastricht: 1957-1992

The purpose of establishing the European Economic Community (EEC) was to promote peace and stability in Europe through cooperative economic growth and development, and to continuously improve people's living and employment conditions.[27] The Community's initial aim was to achieve economic integration, including a customs union and common market (now called ‘internal market’). At the time, health was not an explicit EU competence in the 1957 Rome Treaty, but concerned about the free movement of services, goods, capital and people across borders led to more legislative actions on health issues.

Regarding the question of when the EU health law started, this is actually a controversial topic. As early as the 1960s, people began to pay attention to the safety of food, because food is an important disease vector. The EU insists on protecting human health by regulating food safety. Hence the first EU legislation on health is about food safety - the Directive on colorants in foodstuffs was

[26] Historical, legal and institutional contexts. (2004). In J. V. McHale & T. K. Hervey (Eds.), *Health Law and the European Union*. Cambridge: Cambridge University Press. P. 31.
[27] Treaty establishing the European Community，2002 O.J. (C 325/33). Article 2.

adopted in 1962.[28] This view is based on the fact that we trace EU health laws back to food or agricultural production. However, in terms of internal market law, EU health law can also be traced back to legislation on pharmaceuticals. Pharmaceuticals have been regulated at the EU level since 1965. [29] For pharmaceuticals, a set of legislation regulating pharmaceutical patents, price transparency and market access is necessary. In principle, pharmaceuticals can only be put on the market with marketing authorization approved by the competent authorities. Since the 1960s, a lot of legislation has been made around this principle, which has gradually harmonized the requirements of marketing authorization in the whole European Economic Area. In terms of controlling their prices, the intervention of the EU is to regulate the prices of medicinal products for human use through its Directive 89/105/EEC on transparency.[30] Furthermore, in terms of paying attention to patients and the health care system, the rules on workers' social security coordination guarantee the right of migrant workers and their dependents to health care system in the host country. Thus, this legislation belongs to the scope of EU health law on patients' rights and health care system. As a matter of fact, the branch of EU law and policy is also related to workers and it was introduced an EU competence to legislate on this issue in Article 118a EC. The relevant EU legislation affecting health is the Working Time Directive, which stipulates the maximum working hours and provides paid holidays and rest time.[31] This Directive was established in accordance with the Article 118a EC at that time to ensure "health and safety at work". The UK government has challenged this Directive, arguing that Article 118a EC was the wrong legal basis for this measure.[32] The Court of Justice of European Union (CJEU) clearly drew on the WHO's definition of health as "state of complete physical, mental and social well-being

[28] Council Directive on the approximation of the laws of the Member States concerning the colouring matters authorised for use in foodstuffs intended for human consumption, 1962 O.J. (Spec Ed 279).
[29] Council Directive 65/65/EEC of 26 January 1965 on the approximation of provisions laid down by law, regulation or administrative action relating to medicinal products, 1965 O.J. (L22/369).
[30] Council Directive 89/105/EEC of 21 December 1988 relating to the transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of national health insurance systems, 1989 O. (L40/8). See Joined Cases C-352/07 to C-356/07, C-365/07 to C-367/07 and C-400/07, ECLI:EU:C:2009:217.
[31] Council Directive 93/104/EC of 23 November 1993 concerning certain aspects of the organization of working time, 1993 O.J. (L 307/18).
[32] Historical, legal and institutional contexts. (2004). In J. V. McHale & T. K. Hervey (Eds.), *Health Law and the European Union*. Cambridge: Cambridge University Press. P. 41.

that does not consist only in the absence of illness or infirmity".[33] Therefore, working time belonged to the concept of health and safety and Working Time Directive was valid.

The origin of EU health law is not only legislation but also case law. In this basic stage of EU, CJEU established several key principles of EU law, which laid a foundation for the future development of EU health law. In mid-1980s, the European Commission proposed a "new approach" to promote free movement for the internal market, which is based on the 1979 Cassis de Dijon case law of the CJEU.[34] In addition, products complying with EU-level standards can ensure their entry into the entire internal market. This is to a large extent the EU's approach to the regulation of medical devices. Since the early 1990s, medical devices have been regulated at the EU level, as part of the internal market drive to promote free movement through "new approach". Medical device regulation attaches importance to the guarantee of health and safety, and combines it with market access. The most prominent point is that medical devices that have passed the EU's manufacturing and design standards must be certified with the CE mark. In the 1990s, EU adopted three directives in the field of medical devices, including the general Directive on medical devices,[35] the Directive on implantable devices[36] and the Directive on in vitro diagnostic devices.[37] At present, the three medical device directives have been merged into two regulations and will come into force in 2020 and 2022 respectively. In addition, the CJEU's case law applicable to professionals and health care institutions on the free movement of services have far-reaching implications. In the following decades, case law has been widely used in this context.[38]

[33] Case C-84/94 *United Kingdom v Council (Working Time)*, ECLI:EU:C:1996:431.
[34] Commission Practice Note on Import Prohibitions, 'Communication from the Commission concerning the consequences of the judgment given by the Court of Justice on 20 February 1979 in Case 120/78 ('Cassis de Dijon')', 1980 O.J. (C 256/2).
[35] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, 1993 O.J. (L169/1).
[36] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices, 1990 O.J. (L 189/17).
[37] European Parliament and Council Directive 98/79 EC of 27 October 1998 on vitro diagnostic medical devices, 1998 O.J. (L331/1).
[38] What is European Union health law? (2015). In J. V. McHale & T. K. Hervey (Eds.), *European Union Health Law: Themes and Implications*. Cambridge: Cambridge University Press. P. 38.

The CJEU held that restricting access to health care professions on the grounds of de facto discrimination based on nationality is also considered a violation of EU law.[39]

2.1.2 From Maastricht to Lisbon: 1992-2007

In order to promote European integration, the 1992 Maastricht Treaty had profound significance during this period. The treaty led to the creation of an economic and monetary union, a common foreign and security policy as well as the expansion of the powers of the European Parliament. However, the European integration process was deadlocked in 2005 because France and Dutch rejected the Constitutional Treaty in referendums in May and June 2005 respectively. Following a period of reflection, the Treaty of Lisbon was created to replace the Constitutional Treaty.

During this period, the CJEU continued to develop case law on the free movement of services. In the case of Kohll and Decker regarding the restitution-based insurance system, for example, the CJEU required home member states to reimburse cross-border treatment costs.[40] In a series of cases involving medical treatment within the scope of 'social insurance' health care systems and other aspects,[41] the CJEU held that medical services should be regarded as 'services' in internal market law.[42]

For years, EU was expected to take action on issues of concern to citizens, such as health. However, most governments do not want union intervention because health policy is high on the national political agenda.[43] Until this period, the scope of the right to health was greatly expanded. The mandate given to health issues in the 1992 Maastricht Treaty of the EU was to "encouraging cooperation between member states" and "if necessary, lending support to their actions" in public

[39] see Case C-96/85 *Commission of the European Communities v French Republic (Doctors and Dentists),* ECLI:EU:C:1986:189.
[40] Case C-158/96 *Raymond Kohll v Union des caisses de maladie*, ECLI:EU:C:1998:171.
[41] The Treaty provision covers the right to provide and obtain cross-border services, see: Case C-186/87 *Ian William Cowan v Trésor public,* ECLI:EU:C:1989:47.
[42] What is European Union health law? (2015). In J. V. McHale & T. K. Hervey (Eds.), *European Union Health Law: Themes and Implications*. Cambridge: Cambridge University Press. P. 37.
[43] Duncan, B. (2002). Health policy in the European Union: how it's made and how to influence it. *British Medical Journal,* 324(7344), 1027.

health.[44] EU had authority to spend funds on health projects at European level but was banned from passing laws and regulations to harmonize public health measures in the Member States.[45]

The mandate was considerably strengthened after the Treaty of Amsterdam of 1997 amended the EU's power over health policy. The EU was required in Article 152(1) of the EC Treaty (now Article 168 TFEU) to ensure "a high level of human health protection" in the "definition and implementation of all Community policies and activities". Obviously, the EU's public health competence has developed to into a mainstreaming element,[46] encouraging cooperation not only between the EU and Member States[47] to "improve public health, prevent human illness and diseases and obviate source of danger to physical and mental health",[48] but also with third countries and the competent international organizations.[49] In addition, Article 168 emphasizes that the EU should respect the responsibilities of member states in providing health services and health care and the health policies of Member States.[50]

In order to find a proper balance between respecting the diversity of Member States and realizing the unity of EU governance, EU has developed a new governance model called the "Open Method of Coordination" (OMC). The OMC was originally coined by the Maastricht Treaty as an instrument for coordinating national economic policies. Since then, this governance model has been gradually promoted. This open approach relies on the soft law mechanisms such as indicators and guideline, performance assessment and benchmarking, which purpose is to share the best practices and achieve convergence towards EU objectives in these policy areas that fall into the competence of Member States.[51]As Member States face more and more common concerns in the

[44] Maastricht Treaty, Article 129(1).
[45] Maastricht Treaty, Article 129(4).
[46] Guy, M., & Sauter, W. (2017). "The history and scope of EU health law and policy". In Research Handbook on EU Health Law and Policy. Cheltenham, UK: Edward Elgar Publishing. Available at: https://doi.org/10.4337/9781785364723.00012
[47] TFEU, Article 168(2).
[48] TFEU, Article 168(1).
[49] TFEU, Article 168(3).
[50] TFEU, Article 168(7).
[51] European Parliament (2014). The OMC Method of Coordination. At a glance October. Available at: https://www.europarl.europa.eu/EPRS/EPRS-AaG-542142-Open-Method-of-Coordination-FINAL.pdf?

realm of healthcare, the application of the OMC in this field has also been discussed. In 2004, the European Commission proposed to use OMC in healthcare and long-term care to protect a "European social model".[52] The Member states can seek to use the OMC procedures to address common problems in their healthcare systems. Therefore, the OMC provides a potential for the future development of EU health policy. However, there are difficulties and problems in applying OMC process to health policy, especially in trying to measure the performance of health systems. It is difficult to compare the national health systems of each Member States because they develop independently in a specific historical, cultural and institutional context.[53] The Commission identified three principles of the "healthcare" OMC to make the system as efficient as possible: high-quality care; accessibility of care based on equity and solidarity; long-term financial sustainability.

With the challenges of market governance within the EU and the need for closer cooperation between Member States, EU policy makers are increasingly turning to executive or regulatory agencies outside the Commission structure. These agencies are mandated to carry out a wide range of tasks from simple information collection and dissemination to the adoption of decisions that are binding on all Member States. As the EU's competences in social affairs continues to develop, the Commission's use of agencies has expanded further into health-related areas.[54] The main agencies involved in the field of health such as the European Medicines Agency (1993), the European Agency for Safety and Health at Work (1994), the European Monitoring Centre for Drugs and Drug Addiction (1995), the European Food Safety Authority (2002), the European Centre for Disease Prevention and control (2004). These agencies thus play an active role in exercising executive powers at the EU level. They exercise different powers within different terms of reference, but most of them use technical and scientific expertise to achieve the protection of EU

[52] European Commission, 'Modernizing social protection for the development of high quality, accessible and sustainable health care and long-term care: support for the national strategies using the "open method of coordination"'(Communication) COM (2004) 304 final.
[53] Conclusions and future prospects. (2004). In J. V. McHale & T. K. Hervey (Eds.), *Health Law and the European Union*. Cambridge: Cambridge University Press. P. 414.
[54] Permanand, G., & Vos, E. (2010). EU regulatory agencies and health protection. In E. Mossialos, G. Permanand, R. Baeten, & T. K. Hervey (Eds.), *Health Systems Governance in Europe*: The Role of European Union Law and Policy. Cambridge: Cambridge University Press. P. 134.

citizens' health, so as to achieve the goal of the internal market.[55] Moving this coordination to the European level will benefit European innovation and competitiveness while protecting human health.

It can be seen that the EU has become more involved in health care laws and policies. At the same time, it is also increasingly concerned with fundamental human rights. The Charter of Fundamental Rights of the EU (EU Charter) was adopted in 2000, it protects a series of civil rights which can promote a rights-based approach to EU health law. The EU Charter's chapters on dignity, freedom, equality and solidarity are closely linked to the health rights. For instance, the EU Charter sets out that 'everyone has the right of access to preventive health care and the right to benefit from medical treatment' in accordance with national conditions,[56] and states the principle of equality[57]and non-discrimination.[58] The EU Charter also stipulates that "everyone has the right to respect for his or her physical and mental integrity".[59] Furthermore, the EU Charter provides special protection for members of vulnerable groups,[60] which means that their rights require particular concern in the context of health law.[61] In terms of the rights to health, from the perspective of the jurisprudence of the CJEU, we can see that human rights issues are increasingly being considered in EU litigation.[62] For example, the 'right to health care' in the EU Charter was cited more frequently by the CJEU.[63] However, with the incorporation of the EU Charter into EU Law, if a citizen wants to cross border to another member state for euthanasia or abortion, could a Member State more easily refuse to approve cross-border medical treatment that may be interpreted as a violation of the right to life? [64] Such questions can only be solved gradually through future litigation. In addition, the

[55] Ibid.
[56] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326/391). Article 35.
[57] EU Charter, Article 20.
[58] EU Charter, Article 21.
[59] EU Charter, Article 3.
[60] Children, the elderly and persons with disabilities, Article 24-26 of EU Charter.
[61] What is health law? (2015). In J. V. McHale & T. K. Hervey (Eds.), *European Union Health Law: Themes and Implications* (pp. 10-29). Cambridge: Cambridge University Press.
[62] Rights: health rights as human rights. (2015). In J. V. McHale & T. K. Hervey (Eds.), *European Union Health Law: Themes and Implications* (pp. 156-183). Cambridge: Cambridge University Press.
[63] See Case C-544/10 *Deutsches Weintor eG v Land Rheinland-Pfalz,* ECLI:EU:C:2012:526; C-84/11, *Marja-Liisa Susisalo and Others,* ECLI:EU:C:2012:374.
[64] Rights: health rights as human rights. (2015). In J. V. McHale & T. K. Hervey (Eds.), *European Union Health Law: Themes and Implications*. Cambridge: Cambridge University Press. P. 166.

EU has also enacted legislation related to the health rights in 2000s. For instance, EU legislation on drugs for pediatric use and orphan medicinal products guarantees equal access to medical treatment as well as healthcare for children and patients suffering from rare diseases.

2.1.3 Post-Lisbon: 2007 to Present

During this time, human rights still permeate different aspects of EU health legislation. For example, the Patients' Rights Directive is EU legislation on the entitlements of free movement of patients seeking medical services in other Member States. Relevant specific legislation also includes the EU's General Data Protection Regulation (superseding the Data Protection Directive 95/46/EC), which involves the right to privacy and makes special provisions on health.[65] The CJEU increasingly rely on moral reasoning and human rights in health law cases.[66]

There is a growing recognition that health is also a factor in the productive economy, not just a matter of rights or social welfare. Although the CJEU has repeatedly invoked citizens' right to health and the main status of public health over economic considerations,[67] economic issues also have a place in EU case law.[68] For example, in Duphar, CJEU accepted that the Dutch refused to reimburse medicines with extremely high costs.[69] Such a decision indicates that the Court has upheld the national money-saving measures. The prices of some drugs are now prohibitively high, making it difficult for patients and national health services to pay for these pharmaceuticals. Therefore, economic factors completely prevent the selection of authorized drugs, allowing the use of a cheaper alternative drug.[70] The premise is that it can provide similar security and efficiency guarantees. This was also affirmed in the case of the Novartis Farma SpA by the CJEU,[71]

[65] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016 O. J. (L 119/1).
[66] Case C-84/11 Marja-Liisa Susisalo and Others, 21 June 2012; Case C-101/01 *Criminal proceedings against Bodil Lindqvist*, ECLI:EU:C:2003:596.
[67] Raposo, V. L. (2020) The CJEU's ruling in the Novartis Farma case - Money, Health and Medicines", *Maastricht Journal of European and Comparative Law*. See Case C-180/96 *United Kingdom of Great Britain and Northern Ireland v. Commission of the European Communities*, ECLI:EU:C:1998:192; Case T-392/02 *Solvay Pharmaceuticals BV v. Council of the European Union,* ECLI:EU:T:2003:277.
[68] Ibid.
[69] Case C-238/82 *Duphar BV and others v. The Netherlands State*, ECLI:EU:C:1984:45.
[70] Raposo, V. L. (2020) The CJEU's ruling in the Novartis Farma case - Money, Health and Medicines", *Maastricht Journal of European and Comparative Law*. P. 195.
[71] Case C-29/17, *Novartis Farma SpA v Agenzia Italiana del Farmaco (AIFA) and Others*, ECLI:EU:C:2018:931.

and some off-label prescription for economic reasons should be authorized. Besides, it is also recognized that health as a "service of universal economic significance" occupies a special place in EU competition law[72], and the CJEU has explicitly acknowledged that the health system does not operate entirely in the general market.[73] For example, the amended EU Tobacco Directive is now closely related to the EU's health laws and policy agenda, and are no longer closely related to the EU's internal market forces. Similarly, legislation on EU medical devices takes into account a variety of interests, not just treating relevant laws as part of internal market legislation.

Besides, the EU' s strategy and programmes also has a certain impact on the development of health. In the Lisbon Strategy, the EU set itself the goal of being the most competitive knowledge-based economy in the world by 2010. However, the failure to achieve this target was mainly caused by the economic crisis and recession. As a result, the EU has relaunched its "Europe 2020" strategy which aims to make the EU a smart, sustainable and inclusive economy promoting growth for all. The premise of this strategy is health.[74] "Europe 2020" strategy follows the Lisbon strategy 2000-2010, and "healthcare" OMC continues to be adopted.[75] In addition, health is a factor in a productive economy, related to the "Europe 2020" and internal market. EU's action in the health sector has developed a Third Health Programme, which is legally based on Regulation No.282/2014(EU) and is integrated in the "Europe 2020" strategy.[76] This Health Programme supports actions that are necessary or helpful for the implementation of EU legislation in cross-border healthcare.[77] Other co-funded instruments involve the Horizon 2020 research programme to support projects in areas such as biotechnology and medical technology, the European Fund for Strategic Investment as well as the EU cohesion policy.[78] Therefore, the basic idea of health as a

[72] See further, Prosser, T. (2005). The limits of competition law: markets and public services. Oxford; New York: Oxford University Press.
[73] See Judgment of the Court of 24 July 2003, *Altmark Trans GmbH and Regierungspräsidium Magdeburg v Nahverkehrsgesellschaft*, Case C-280/00, ECLI:EU:C:2003:415.
[74] European Commission-EU health programme. Available at: https://ec.europa.eu/health/funding/programme_en
[75] Vanhercke, B., Zeitlin, J. (2014). Socializing the European Semester? Economic governance and social policy coordination in Europe 2020. Stockholm: Swedish Institute for European Policy Studies. P. 9.
[76] European Commission, 'Towards Social Investment for Growth and Cohesion including implementing the European Social Fund 2014-2020' COM (2013) 83 final.
[77] Regulation (EU) No 282/2014 of the European Parliament and of the Council of 11 March 2014 on the establishment of a third Programme for the Union's action in the field of health (2014-2020) and repealing Decision No 1350/2007/EC, 2014 O.J. (L 86/1).
[78] European Commission - EU health policy. Available at: https://ec.europa.eu/health/policies/overview_en

factor of production helps to strengthen the cohesion of EU health law and improve the sustainability of future health systems.

Finally, the EU competence in Article 168 TFEU has been strengthened and the fundamental right to health care in the EU Charter, so the EU's external role in term of health has been reinforced.[79] The Commission considers that a more comprehensive method is needed to respond to the explicit competence to 'foster cooperation with third countries and the competent international organizations in the sphere of public health'.[80] In 2010, the European Commission indicated that the EU's leading role in international trade and global environmental governance, as well as its performance in equitable quality healthcare give EU strong legitimacy to take action on global health.[81] The EU is always active in global institutions such as the UN's Food and Agriculture Organization (FAO) and the World Health Organization (WHO). Thus, In the context of globalization and external health threats (like AIDS, malaria, tuberculosis SARS and H1N1), the importance of international cooperation has become increasingly prominent.

2.2 CJEU influence on cross-border healthcare

The judgements of CJEU on the right of citizens to seek healthcare in Member States outside their own countries have had a significant impact on the broader discussion of legal clarify of cross-border healthcare rights and provisions. Moving social policy issues to the specific role of the Courts in healthcare, the CJEU's rulings in the Kohll and Decker cases can be regard as a turning point in the development of EU health policy. In fact, before that, from the perspective of EU internal market law, the application of internal market rules to health services had been recognized.[82]

Regulation 1408/71/EEC, on the application of social security schemes to employed persons and their families moving within the EU had already allowed for the healthcare to be provided in other

[79] EU external health law. (2015). In J. V. McHale & T. K. Hervey, European Union Health Law: Themes and Implications (pp. 433-532). Cambridge: Cambridge University Press.
[80] TFEU, Article 168 (3).
[81] Commission, 'The EU Role in Global Health' (Communication) COM (2010) 128 final.
[82] Joined Cases 286/82 and 26/83, *Luisi and Carbone v Ministero del Tesoro*, ECLI:EU:C:1984:35.

Member States under specific circumstances,[83] and the Court also reiterated this Regulation in the Kohll and Decker cases. Additionally, the CJEU had applied the principles of internal market law in the realm of healthcare. In the Luisi and Carbone case of 1984, the Court declared that patients could travel to another member state as "recipients of services".[84] Therefore, the economic factors of free flow have been considered to include health services and fall within Article 60 EEC (now Article 56 TFEU). As a matter of fact, it can be said that the Court is actually interpreting and applying existing hard laws to fill the gaps found in legal challenge.[85] These interpretations tend to be precedents for application in all similar circumstances, so the role of interpretation of EU law in filling these gaps in specific circumstances has attracted people's attention.[86]

Certain 'public' provisions of welfare services (including healthcare service) are not exempt from the free movement of Treaty.[87] Member States are able to organize their own health care systems in ways they think fit, but they must comply with EU laws.[88] In most cases, if patients are receiving medical treatment in another Member States, the CJEU required the home country to reimburse patients for cross-border treatment costs. In this way, a precedent was set for increasing patient choice and mobility to conform EU internal market goals. The case law on the restitution-based insurance systems was extended to taxation-based national health services. In the British Watts case, there are also problems from the perspective of the national health system based on taxation.[89]As the budget allocated by the government to the NHS is not enough to allow for the swift provision of treatment to all patients, the NHS uses existing resources by setting priorities regardless of the urgency, which results in some quite lengthy waiting list for less urgent treatment.[90] Whether there was an "undue delay" that entitled Mrs. Watts to get reimbursement for

[83] Regulation 1408/71/EEC of the Council of 14 June 1971 on the application of social security schemes to employed persons and their families moving within the Community, 1971, O.J. (L149/2).
[84] Joined Cases 286/82 and 26/83, *Luisi and Carbone v Ministero del Tesoro*, ECLI:EU:C:1984:35.
[85] Mossialos, E., Permanand, G., Baeten, R., & Hervey, T. (2010). Health systems governance in Europe: the role of European Union law and policy. Cambridge: Cambridge University Press. P. 29.
[86] Ibid.
[87] Ibid.
[88] Damjanovic, D., & De Witte, B. (2008). Welfare Integration through EU Law: The Overall Picture in the Light of the Lisbon Treaty. *IDEAS Working Paper Series from RePEc*. P. 13.
[89] Case C-372/04, *Yvonne Watts v Bedford Primary Care Trust and Secretary of State for Health,* ECLI:EU:C:2006:325.
[90] Ibid., para 13.

her hip surgery in France, the Court held that in assessing the extent of the "undue delay", all the circumstances of the case, including patient's medical condition and, where appropriate, of the degree of pain or the nature of the patient's disability, must be taken into consideration.[91] After the incident, the case was resolved and national regulations changed. The National Health Service used the idle capacity of the private sector to treat patients who had been waiting for a long time for surgery.[92] There has been no situation of a worrisome mass of patients going to other EU Member States for medical treatment.

This is actually the Court's "intervention" in national health policy. When any national court of Member States raises questions, the CJEU has the power to make authoritative rulings on the validity and interpretation of the EU law (reference for preliminary ruling). Due to the supremacy of EU law, the result of these authoritative interpretations is that any national rules that conflict with the regulations of the CJEU are not applicable.[93] National courts respect the power of the CJEU to make a clear interpretation of EU law and therefore delegate its power to the decision of the Court. This is so even when the rulings of the CJEU are startling, especially when the CJEU uses approaches of interpretation that goes beyond literal meaning.[94] Consequently, in practice, it is hard for Member States to reverse the CJEU progress that are based on the Treaty.[95] EU law can protect individual rights from decisions of national administrations.

2.3 The EU legislation on patient's rights in cross border healthcare

In 2012, president of the Standing Committee of European Doctor (CPME) pointed out that healthcare is a very professional and personalized service, and patients will face risks if it is reduced to market-oriented technology simplification and standardization. Every patient has the right to receive the best care for his or her personal condition.

[91] Ibid, para 62.
[92] What is European Union health law? (2015). In J. V. McHale & T. K. Hervey, European Union Health Law: Themes and Implications. Cambridge: Cambridge University Press. P. 57.
[93] See Case 6/64 *Flaminio Costa v E.N.E.L*, ECLI:EU:C:1964:66.
[94] What is European Union health law? (2015). In J. V. McHale & T. K. Hervey, European Union Health Law: Themes and Implications. Cambridge: Cambridge University Press. P. 56.
[95] Ibid.

In order to promote the cooperation of EU member states in medical services and strengthen the coordinated operation of different social security systems, the Directive on the application of patients' rights in cross-border healthcare (Directive 2011/24/EU) came into force in 2013. Thirteen years after the well-known Kohll and Decker case law, the Directive provides a legal framework for cross-border healthcare, which creates the rights of patients, establishes rules for cooperation in the medical field (e.g. e-health, cooperation health technology assessment, etc.) to promote the quality and safety of healthcare. The Directive firmly establishes the right of EU citizens to seek health care in other member states.

This Directive is based on Article 114 TFEU as the legal basis, and its purpose is to promote the internal operation of the market and the free movement of goods, patients and healthcare professionals, as well as healthcare services. The Directive 2011/24/EU covers both the internal market (Article 114 TFEU), and the provision on public health governed by EU Member States (Article 168 TFEU). It clearly requires Member States to use the same scales of fees and hospitals cannot charge foreign patients higher than the normal price.[96] The European Union seems to use its economies of scale to improve healthcare for all European patients.[97]

In the Directive 2011/24/EU, the rule of reimbursement is the codification of the Kohll-Decker case law. According to the rules identified in the Kohll-Decker case law, the Member States of affiliation shall ensure that reimbursement of the costs incurred by an insured person if cross-border healthcare is among the rights to which the insured person is entitled.[98] In the exceptional circumstances, the insured person may be subject to the prior authorization for reimbursement of cross-border health care costs.[99]

Another important part of the Directive 2011/24/EU is the clarification of obligations concerning Member States. On the one hand, the obligations of the Member States of treatment include

[96] Directive 2011/24/EU, Article 4 (4).
[97] Peeters, M. (2012). Free Movement of Patients: Directive 2011/24 on the Application of Patients' Rights in Cross-Border Healthcare, *European Journal of Health Law*, *19*(1), p. 29.
[98] Directive 2011/24/EU, Article 7 (1).
[99] Marian, B. (2018). Considerations regarding Directive 2011/24/EU on the application of patients' rights in cross-border healthcare in EU Member States. *Juridical Tribune Journal*, 8(3), 681-689.

legislation,[100] information accessibility related to cross-border medical services,[101] the remedies in the event of medical damage,[102] privacy of personal data processing,[103] and the right of informed consent as well as medical service fees[104], and other aspects of fair and transparent. On the other hand, the obligations of the Member States of affiliation include the reimbursement of cross-border healthcare costs,[105] remote access or replicate patients' medical records,[106] and ensuring medical continuity.[107]

It also sets up a framework for cooperation in medical services among Member States, and promotes cross-border medical cooperation between member states by recognizing prescriptions from other Member States, digital health (e-health), rare diseases and medical technology assessment of other Member States, so as to protect the interests of European citizens. All of these are designed to provide high-quality cross-border healthcare, as well as the insured person can obtain the optimal care for patients' health conditions.[108] These collaborations are extremely important in cross-border healthcare, especially in the area of e-health. Reading the patient's medical history in the electronic health records (EHRs) allows doctors in Member States of treatment to continue medical treatment without repeating various expensive diagnostic tests and treatment methods, thereby ensuring continuity of healthcare and improving efficiency.[109] Thus, promoting cross-border access to EHRs by treating physicians and patients is a key factor in achieving cross-border care. However, the privacy of the patient's health data involved will be a big challenge. The fundamental rights to privacy in the processing of personal data in cross-border health care is protected by national measures implementing the EU provisions on personal data protection, in particular the Privacy and Electronic Communications Directive and General Data

[100] Directive 2011/24/EU, Article 1.
[101] Directive 2011/24/EU, Article 2 (a).
[102] Directive 2011/24/EU, Article 2 (c)
[103] Directive 2011/24/EU, Article 2 (e).
[104] Directive 2011/24/EU, Article 4.
[105] Directive 2011/24/EU, Article 5 (b).
[106] Directive 2011/24/EU, Article 5 (d).
[107] Directive 2011/24/EU, Article 5 (c).
[108] Marian, B. (2018). Considerations regarding Directive 2011/24/EU on the application of patients' rights in cross-border healthcare in EU Member States. *Juridical Tribune Journal*, 8(3), 681-689.
[109] Den Exter, A. (2017). eHealth Challenges under EU law. *Cross-border health care and European Union Law* (pp. 101-116). Erasmus University Press.

Protection Regulation (GDPR). This is also what I intend to focus on discussion and analysis in this thesis.

2.4 Roles and responsibilities in cross-border healthcare

2.4.1 European Commission

Within the Commission, responsibility for the implementation of the Directive 2011/24/EU rests primarily with the Directorate General for health and Food Safety (DG SANTE), which is supports the efforts of EU countries to protect and improve the health of their citizens. DG SANTE is responsible for strategic planning, monitoring and evaluation of Health Programme, as well as ensures the accessibility, effectiveness and resilience of EU countries' health systems.[110] Moreover, DG SANTE supports Member countries in developing National Contact Points (NCPs) for cross-border medical and promotes the recognition of cross-border prescriptions. It also supports the development of European Reference Networks (ERNs) to facilitate the sharing of patient data and improve collaboration on complex and rare diseases with a highly specialized knowledge.

The European Commission also works with other DGs and executive agencies. The Consumers, Health and Food Executive Agency (CHAFEA) implements various projects based on the Health Programme. In the field of research, DG SANTE also regularly engage with the Joint Research Council (JRC), and with the Directorate General for Research and Development (DG RTD) on relevant funding opportunities.

Together with other European Commission services, according to an administrative agreement with DG SANTE, the JRC has been developing the European Platform on Rare Diseases Registration to provide a central access point for information on rare disease, improve access to patient registries, harmonize data and promote interoperability between registries.[111] The other relevant department within the Commission is the Directorate General for communications

[110] European Commission -EU health policy. Available at: https://ec.europa.eu/health/funding/programme_en
[111] https://ec.europa.eu/jrc/en/research-topic/public-health

networks, content and technology (DG CONNECT). This Directorate General is responsible for e-health under its Digital Single Market (DSM) strategy.

2.4.2 Member States

EU countries have primary responsibility for organizing and providing health services and medical care. In cross-border health care, Member State of treatment is responsible for providing the health services requested by the patients, and Member State of affiliation ensure that related costs are reimbursed. The national healthcare services of Member States are responsible for setting criteria for citizens to receive health care in another Member State including pre-approval procedures, eligible treatment checklists and reimbursement arrangements. Each Member State is represented on the e-health network and on the Board of Member States for ERNs, overseeing the implementation of EU policies and helping to promote significant voluntary cooperation on digital health and ERNs. [112]

In order to enable patients to make use of their entitlements relation to cross-border healthcare, all Member States must have one or more NCPs to provide citizens with information about their rights to cross-border healthcare and concerning providers of healthcare.[113] NCPs provides information about healthcare providers to patients in other Member States, including on a specific provider's right to provide services or any restrictions on its practice.[114] They also provide information on patients' rights, complaints procedures and mechanisms for seeking remedies under the legislation of that Member State.[115] Besides, it also includes legal and administrative options available to settle disputes, involving in the case of damage caused by cross-border healthcare.[116]

[112] European Court of Auditors (2018). Cross-border healthcare in the EU. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BP_CBH/BP_Cross-border_healthcare_EN.pdf
[113] Directive 2011/24/EU, Article 6 (1).
[114] Directive 2011/24/EU, Article 6 (3).
[115] Ibid.
[116] Ibid.

2.5 Cooperation in healthcare: e-health

With the increase of cross-border health activities, compared with the past, the number of patients receiving treatment in other Member States are also increasing.[117] Hospitals and healthcare professionals are increasingly using information and communication technologies (ICTs) applications to communicate health data for treatment. There are also many healthcare participants who consider it necessary to exchange medical data between Member States for treatment and other purposes. In addition, patients may obtain electronic prescriptions (e-prescriptions) from other Member States or order medicines from pharmacies in other Member States through the network. It can be seen that many of these developments are related to e-health.[118] The cross-border provisions of the Directive 2011/24/EU deploy e-health and telemedicine applications, including the remote monitoring and diagnosis, remote consultation, electronic health records (EHRs), e-prescriptions and e-referrals.

According to the European Commission definition of e-health: "the use of information and communication technologies in health products, services and processes, combined with organizational change in health systems and new skills".[119] This definition emphasizes the interaction between patients and health professionals. It is common to use electronic decision support systems (DSS) to help doctors make clinical decisions based on a patient's medical history. Another initiative is the electronic prescription system (ePs), which enables doctors to transfer prescriptions electronically to pharmacies. Using this system can increase the safety and efficiency of the prescription process. Ultimately, these applications will be integrated into the patients' electronic health records (EHRs).[120] So for cross-border healthcare, medical data portability is vital. When it comes to e-health, mobile health (m-health) is often mentioned. The m-health is regarded as a subset of e-health, which often refers to the use of mobile communication devices

[117] Beaten, R., Footman, K., Glonti, K., Knai, C., McKee, M. (2014). Cross-border health care in Europe. World Health Organization, p.1.
[118] Callens, S. (2010). The EU legal framework on e-health. In E. Mossialos, G. Permanand, R. Baeten, & T. K. Hervey (Eds.), Health Systems Governance in Europe: The Role of European Union Law and Policy. Cambridge: Cambridge University Press. P. 561.
[119] European Commission, 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century' COM (2012) 736 final.
[120] Den Exter, A. (2017). eHealth Challenges under EU law. *Cross-border health care and European Union Law* (pp. 101-116). Erasmus University Press.

(such as tablet computers and mobile phone) as well as wearable devices, for health data collection and healthcare services.[121] The m-health can be extended to many applications, including the use of mobile devices to collect clinical medical data, providing health information to patients and researchers, monitoring patients' vital signs in real time, and even providing direct healthcare (through mobile telemedicine).

The positive aspect of e-health and m-health are obvious. They can improve healthcare quality, from the digital medical equipment to high-level information and knowledge sharing. Information sharing between healthcare institutions facilitates patient referral and make continuous healthcare possible. In addition, e-health can innovate the healthcare services model. Through telemedicine, patients can obtain the diagnosis and treatment of multiple experts without having to be transferred to the hospital.

Nevertheless, this may pose certain risks to citizens. First is that the cross-border transmission of health data may increase the inaccuracy of data processing. Technological developments in the provision of health care across national borders through the use of ICTs may lead to uncertainty in the exercise of supervisory responsibilities by Member States, thus may constitute an obstacle to cross-border healthcare and potentially pose additional risks to health protection. The reason is that there are wide differences and incompatibilities in the formats and standards for using ICTs to provide healthcare within the EU.[122] Therefore, the EU should support and promote cooperation and exchange of information among Member States working within a voluntary network designated by Member States to connect with national authorities responsible for e-health.[123] This e-health network, as the main decision-making body on e-health at EU level, sets a common vision and strategy for e-health in Europe. It was established in accordance with Article 14 of Directive 2011/24 /EU, which defines the role of the network 'foster cooperation between Member States to ensure EU wide interoperability of electronic health systems and wider use of e-health'. Specifically, providing sustainable economic and social benefits and interoperability for e-health

[121] Gleason, A. M. (2015). mHealth - Opportunities for Transforming Global Health Care and Barriers to Adoption. *Journal of Electronic Resources in Medical Libraries*, 12(2), 114-125.
[122] Directive 2011/24/EU, Preamble, consideration (56).
[123] Directive 2011/24/EU, Article 14 (1).

system services in Europe, and supporting Member States to develop common identification and authentication measures to promote the transmission of cross-border healthcare data are the objectives of the transparent operation of such e-health network.[124]

Secondly, cross-border exchange of health data may increase the risk of illegitimate data processing. Because any form of cross-border healthcare, including e-health and m-health, involves the exchange of patient data, protecting personal health data in the field of cross-border healthcare has been a challenge. The European Data Protection Supervisor (EDPS) also specifically pointed out the inevitable link between the closely related areas of privacy in EU legislation on organ donation and transplantation, telemedicine and electronic health records. The Commission's legal framework on cross-border interoperability of EHRs emphasizes the right of patients to self-determination in the storage and disclosure of health-related personal data.[125] Patients have the right to access, request rectification and erasure of data in cross-border healthcare. At the same time, from the perspective of patients' entitlements to informational privacy, it is possible for patients to indicate a refusal to secondary use their personal health data, especially for research purposes.[126] This should also be added to the list of entitlements related to patients' personal data for cross-border healthcare in e-health networks.[127]

There is no doubt that e-health and some related applications may provide unprecedented possibilities for clinical and other purposes, but at the same time, they will also raise a series of legal and regulatory issues at the national and EU levels, such as liability, equal access, privacy, reimbursement, jurisdiction, etc.[128] Some European instruments such as the Medical Device Regulation (MDR) that will be enforced in May 2020, the GDPR and the Electronic Commerce

[124] Directive 2011/24/EU, Article 14 (2).
[125] Commission Recommendation of 2 July 2008 on Cross-border interoperability of electronic health records system, 2008 O.J. (L 190/ 37).
[126] GDPR, Recital 33.
[127] Roscam Abbing, H.C. (2015). EU Cross-border Healthcare and Health Law, *European Journal of Health Law*, *22*(1), 1-12.
[128] Den Exter, A. (2017). eHealth Challenges under EU law. *Cross-border health care and European Union Law* (pp. 101-116). Erasmus University Press.

Directive[129] all play significant roles in the healthcare system through the use of e-health applications. The GDPR replaces the previous Data Protection Directive, which provides more detailed provisions on the protection of personal health data in order to fully respect Article 8 of the Charter of Fundamental Rights of the EU. Under the legal framework of EU data protection, patients' rights and interests can be better protected It is foreseeable that in the near future, the emergence of new e-health startups such as remote and multidisciplinary consulting will bring flexible contract virtual doctors, enabling patients to get immediate healthcare services. However, this model may trigger new e-health controversy, which complicates the legal debate.[130]

[129]Callens, S. (2010). The EU legal framework on e-health. In E. Mossialos, G. Permanand, R. Baeten, & T. K. Hervey (Eds.), *Health Systems Governance in Europe: The Role of European Union Law and Policy*. Cambridge: Cambridge University Press. P. 566.

[130] Den Exter, A. (2017). eHealth Challenges under EU law. *Cross-border health care and European Union Law* (pp. 101-116). Erasmus University Press.

Chapter III EU polices in the cross-border medical informatization

3.1 Overview of EU medical information development

Within the EU, all activities that use ICT to assist in disease prevention, diagnosis, treatment, monitoring fall within the scope of e-health. The EU has put forward two rounds of e-health action plans as a program for carrying out the work. At the legal level, Directive 2011/24/EU is one of the most important regulations. Under the guidance of this Directive, the EU has established the e-health network, which plays a key role in solving the problem of information interaction in the electronic health system. Many contents of the Directive have been tested in practice through the epSOS project, and the problems exposed have also been corrected in the follow-up work of Member States.

In general, the EU started the layout of e-health in the early stage, standardized the system and problems in the e-health process through a series of administrative orders and regulations, and established a strict regulatory system. However, the EU is a community composed of Member States with different languages, cultural backgrounds and economic strengths. Therefore, EU also spends a lot of resources to solve the problems of information sharing and medical resource docking.

3.2 Relevant planning of EU medical information

3.2.1 e-Health Action Plan 2004-2010

Since the late 1990s, the European Commission has been initiating and funding Research and Development (R&D) activities related to ICT for health, which covered priority themes such as national, regional and local health networks, electronic health records in primary healthcare, as well as the deployment of health (smart) cards.[131] On this basis, the European Commission began to play a leading role in coordinating e-health policy formulation and application deployment. The purpose of this action is to accelerate the transformation of Europe into a knowledge-based

[131] Lymberis, A., Olsson, S., Whitehouse, D. (2004). European Commission activities in eHealth. *International Journal of Circumpolar Health*, 63(4), 310-316.

economy, achieve higher potential benefits, and provide more employments and better opportunities for all EU citizens to enjoy healthcare services in the era of electronic information.[132] Meanwhile, EU Member States have particularly supported EU action in the area of e-health. The EU's emphasis on the health sector has promoted the emergence and development of this emerging industry in Europe. However, different national laws and regulations pushed up the cost of development and customization, which would hinder the e-health industry's large investment in e-health solutions. Although there were certain competitive advantages, it still needed to develop a better business environment. Based on this background, the EU launched the Action Plan 2004–2010 to promote the wide adoption of electronic health technology in the EU.[133]

The EU estimates that by 2051, the EU population over 65 years old will account for about 40% of the total population.[134] The EU citizens desire for better medical service mainly includes the following aspects. First, EU citizens' demand for equity in healthcare. The second is the need for medical institutions to increase the mobility of patients and medical professionals. Thirdly, the need for public health to reduce chronic diseases and address the risks of new diseases. The last is the demand for the management and interconnection of EU citizens' health information. In response to these needs, a series of solutions have been mentioned in the Action Plan. For example, it was necessary to implement infrastructure in the field of e-health, such as the construction of healthcare database including patient identifiers and electronic health records. Using information technology to carry out health education and disease prevention was also part of the Action Plan. In addition, it was necessary to jointly discover and build demonstration cases in the field of e-health, and also needed to summarize and disseminate them. The ultimate objective of this action plan was for e-health to be a norm for the citizens, patients and healthcare profession by the end of this century. However, in the initiative of the action plan, a number of major challenges for wider implementation have also been raised, such as interoperability of e-health systems, lack of

[132] Cipriani G. (2014) EU Support to eHealth and Cost-Benefits. In: Gaddi A., Capello F., Manca M. (eds) *eHealth, Care and Quality of Life*. Springer, Milano. P. 94.
[133] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - e-Health - making healthcare better for European citizens: an action plan for a European e-Health Area {SEC(2004)539} COM(2004)0356 final.
[134] Braun, A., Constantelou, A., Karounou, V., Ligtoet, A., Burgelman, J.C. (2003). Prospecting ehealth in the context of a European Ageing Society: Quantifying and qualifying needs. Final report. November 2003.

regulation and fragmentation of the e-health market in Europe, confidentiality and security issues as well as access to e-health care for all.

A few years later, the 2006 Aho Report "Creating an Innovative Europe" identified the development of ICT infrastructure and clinical information systems as a domain of action for EU to address specific healthcare challenges and promote innovative markets.[135] The e-health Action Plan 2004–2010 preliminarily realized the digitization of healthcare information and sharing within the EU, and strengthened the cooperation between the Member States in e-health.[136] The EU issued the Directive on the application of patients' rights in cross-border healthcare and initiated the set up the e-health network.[137] This indicated that the EU aimed to promote further formal cooperation between Member States and stakeholders through the implementation and interconnection of e-health system, so as to maximize social and economic benefits.

3.2.2 The European e-health Governance Initiative 2011-2014

Having a shared vision and identifying the main measures needed to make progress is the best solution to the potential challenges that currently stand in the way of deploying interoperable e-health in Europe. With this goal in mind, EU member states are willing to actively develop closer cooperation. The European Commission and Member States held three meetings to discuss the challenges of deploying e-health in their countries. They agreed that cooperation could be a good opportunity to promote development e-health deployments. The outcome of the meeting resulted in a proposal to support the e-health Governance Initiative, which is composed of Joint Action (co-funded by DG SANCO) and a Thematic Network (funded by DG INFSO).[138] Cooperation between the Member States goes far beyond solving cross-border problems. The European e-health

[135] Aho E. (2006) Creating an innovative Europe: Report of the independent expert group on R&D and innovation, European communities, Luxembourg. P. 11.
[136] See also Giorgio, F.（2013). A New Way Forward. In *European eHealth Governance Initiative*. Springer. P. 373,
[137] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, 2011 O.J. (L88/45).
[138] European Commission. e-health Governance Initiate: Joint Action EHGov & SEHGovIA Thematic Network. Available at: http://www.ehgi.eu/Download/eHGI%20Documentation%20eHealth%20Governance%20Initiative%20Factsheet(7-November-2011).pdf

Governance Initiative is a cooperative mechanism established between EU Member States and stakeholders to support Member States in deploying e-health care and achieving its interoperability.

The EU promoted e-health Governance Initiative of Member States is a political and strategic commitment, which is designed to address e-health care goals and priorities, including improving the patients' safety and quality of health care, removing barriers to the deployment of e-health, and supporting the continuity of cross-border care as well as and ensuring better use of health care resources. The e-health Governance Initiative also provides a platform for Member States to strengthen and support technical and political cooperation in e-health in European countries (based on successful e-health practices), so as to design future e-health strategies and infrastructure in Europe and contribute to the single European e-health area. In addition, the interoperability roadmap is a specific strategy for establishing e-health networks in Member States and Europe, and it is one of the main health policy tools for establishing the de facto basis for decision-making in the field of e-health.

The e-health Governance Initiative involve a range of legal issues, which are important and need to be considered. Although e-health has developed rapidly in recent decades, it is still a relatively new field in the legal sense. So far, there is no specific law on e-health at the EU level. Initially, some legal provisions were not intended to cover e-health systems at the time of formulation, but now they will often apply to e-health systems. For instance, electronic signature is often used in e-health projects. It is a key tool to ensure the confidentiality, integrity and authenticity of health data transmission between electronic sources.[139] At that time, the EU's Directive on Electronic Signatures (replaced by eIDAS Regulation in 2016) provided that electronic signature was regarded as equivalent to handwritten signature, which could provide guarantee for remote implementation of electronic signature by healthcare providers or patients.[140] Another example, the Directive 2000/31/EC on certain legal aspects of information society services in the internal market (known as e-commerce Directive) was introduced to address issues related to e-commerce

[139] Callens, S. (2010). The EU legal framework on e-health. In E. Mossialos, G. Permanand, R. Baeten, & T. K. Hervey (Eds.), *Health Systems Governance in Europe: The Role of European Union Law and Policy* (pp. 561-588). Cambridge: Cambridge University Press.

[140] European Parliament and Council Directive 1999/93 on a Community framework for electronic signatures, 2000 O.J. (L 13/12).

for goods and certain types of services. [141] In a way, it can be said that e-health applications can be regarded as an item of information society services, such as services for transmitting information through communication networks or online drug procurement.[142] Every healthcare service provided at distance for a fee falls within the scope of the e-commerce Directive.[143] Therefore, e-health is subject to e-commerce Directives to a certain extent. For example, Article 3 establishes that service providers must comply with the legal requirements of the country where the commercial establishment is located, rather than the legal order of the place where the services are received.[144] Article 8 of the e-commerce Directive deals with regulated professions, that is, healthcare professionals are required to respect their relevant professional rules when providing information society services.[145] It is also recommended that Member States should encourage healthcare professional associations to develop guidelines for conduct at the EU level 'in order to determine the types of information that can be given for the purpose of commercial communication'.[146] These norms are particularly significant for telemedicine. However, when looking at interoperability at the EU level, the main legal challenges remain. For example, in the cross-border transmission of patient data, although the Data Protection Directive in force at that time provided certain guarantees for sensitive data such as patient data in some aspects, each Member States had different requirements for security and privacy protection. This still leads to legal uncertainty, which is confirmed by epSOS. The e-health Governance Initiative built on the results of the epSOS and reviewed policy developments at the time, such as the adoption of Directive on patient rights in cross-border healthcare.[147] By identifying these issues, the EU/ national level can propose viable ways forward and implement them in the next phase of the policy framework.

[141] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') 2000 O.J.(L 178/1).
[142] Callens, S. (2010). The EU legal framework on e-health. In E. Mossialos, G. Permanand, R. Baeten, & T. K. Hervey (Eds.), *Health Systems Governance in Europe: The Role of European Union Law and Policy*. Cambridge: Cambridge University Press. P. 567.
[143] Raposo, V. L. (2016). Telemedicine: The legal framework (or the lack of it) in Europe. *GMS Health Technology Assessment*, 12, Doc03.
[144] Directive 2000/31/EC, Article 3(1).
[145] Directive 2000/31/EC, Article 8(1).
[146] Directive 2000/31/EC, Article 8(2).
[147] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, 2011 O.J. (L88/45).

In addition to these legal issues that need to be explored, there are other issues that are also the focus of the work plan of the Initiative. Identification and authentication are the main obstacles to e-health security deployment. It is very important to ensure that users (including patients and health professionals) are determined with full respect for their privacy rights. Meanwhile, such identification should ensure that the person concerned has access to specific types of data (including patients' health data if necessary). The ability to identify security across borders is also covered by technical solutions. In addition, the acceptance and trust of health professionals and patients in e-health system is also an important issue that must be regarded as technology-related and challenging, which also hinder the deployment of e-health. These mentioned issues are only part of the work of the initiative. In fact, it can be found that many of these issues are closely linked. For instance, trust by users can be associated with technical solutions for accessing services that must meet specific legal provisions. Hence, the work plan of the Initiative is to integrate all these issues while ensuring the necessary links between them.

Since the design and implementation of e-health Governance Initiative, there have been new developments in Europe.[148] The European Commission continues to carry out its policy activities to fulfil its obligations under the Treaty, in particular Articles 26 (the internal market) and Article 168 (public health). There are three Commission level policy and action developments that are particularly relevant to the e-health Governance Initiative. The following is a brief analysis of how the e-health Governance Initiative relate to these policies and actions.

Initiative-related policy one - Digital Agenda for Europe

One of the most significant area of economic policy in the EU is its Single Market policy, which aims to remove barriers to the cross-border movement of goods, services, capital and labor between EU Member States. In today's digital era, the notion of DSM is a priority policy in the Digital Agenda for Europe (DAE) by the European Commission.[149] It is a market where individuals and enterprises can access and participate in online activities seamlessly under the conditions of fair competition and personal data protection, regardless of nationality and place of

[148] See also Giorgio, F.（2013）.A New Way Forward. In *European eHealth Governance Initiative*. Springer.

[149] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe COM(2010)245 final http://ec.europa.eu/information_society/digital-agenda/documents/digital- agenda-communication-en.pdf.

residence. DAE outlines a strategy supported by more than 100 actions designed to help Europe become digital. The ultimate goal is to implement the digital internal market so that citizens, enterprises and public administration can fully benefit from the digital society. Given the potential benefits of digital services for citizens and businesses in this area, health is one of the sectors on this Agenda. The Agenda identified specific actions on e-health, one of which is to enhancing patient empowerment and telemedicine, and the other two were to achieve continuity of cross-border healthcare and to strengthen standardization activities at the EU level. The Agenda also deals with more horizontal issues, such as the need to strengthen e-government services, enhance interoperability and trust in digital services, which are relevant to e-health.[150]

Initiative-related policy two – Directive 2011/24/EU (eHealth network)

E-health Governance Initiative has promoted the development of other relevant actions, among which the adoption of the Directive on the application of patient rights in cross-border health care is one of the relevant developments of e-health Governance Initiative. The Directive 2011/24/EU includes provisions on e-health (Article 14), which advocates closer cooperation among Member States in the e-health domain and identifies areas in which such collaboration should be initiated. According to the development of e-health and part of the e-health Governance Initiative agenda, these areas can mainly include three aspects. The first is the interoperability of patient summaries, which needs to follow the agreement reached in the European Patients' Smart Open Services. The second aspect is to make medical information available for public health and research, because these medical information data are very important for the development of public health. For medical experts and researchers, the information of some patients is also of great significance to the development of medical and science. Thirdly, it is also very important to develop common identification and authentication measures to protect the data security of patients and promote the transmission of cross-border healthcare data. In addition, the Article 14 of the Directive establishes a network of Member States representatives. It serves as a mechanism to enable enhanced cooperation among Member States and to address identified areas of action. It can be imagined that the establishment of such a network is a big step forward in the field of healthcare, because it

[150] See also Giorgio, F.（2013）.A New Way Forward. In *European eHealth Governance Initiative*. Springer. P. 381.

is the first time that cooperation between EU Member States in the field of e-health has been formalized under the protection of a legal framework.

Initiative-related policy three - European Innovation Partnership on Active and Health Ageing

Another policy relevant to the European e-health Initiative is the European Innovation Partnership on Active and Health Ageing. In October 2010, the European Commission adopted a Communication on the Innovation Union,[151] which is also one of the projects of the Europe 2020 Strategy.[152] The aim of the innovation Union is to improve the conditions and financing channels for research and innovation in Europe and to ensure that such innovative ideas can be translated into products and services that generate growth and employment. One of the tools that can achieve this vision is the European Innovation Partnership, which aims to address any weaknesses in the European research and innovation system that hinder innovation from entering the market. In February 2011, the European Commission launched its proposal for the first partnership focused on Active and Healthy Ageing. There are three principles goals of the Active and Healthy Ageing. The first is to pursue a healthy, active life for EU citizens before they reach old age. The second is to boost the sustainability and efficiency of the healthcare system, which is directly related to improving the quality of life of citizens. Last but not least, it is to develop EU markets for these innovative products and services, create new opportunities for enterprises, and thus improve the employment rate of society.[153] This partnership will help to mobilize and share expertise and resources in Europe, establish mechanisms for cooperation between the EU and Member States and provide corresponding support, so that innovation that promote the smooth and rapid access of active and healthy aging to the market. Therefore, there is no doubt that the implementation of the partnership is closely linked to the European e-health Governance Initiative, because the use of new technologies will be very common and play a crucial role. It can be seen that the purpose of the e-health initiative in Europe is related to the implementation partnership to introduce

[151] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Europe 2020 Flagship Initiative Innovation Union COM (2010) 546 final. Available at: http://ec.europa.eu/research/innovation-union/pdf/innovation-unioncommunication_en.pdf#view1⁄4fit&pagemode1⁄4none.

[152] Communication from the Commission Europe 2020 a strategy for smart, sustainable and inclusive growth – com (2010) 2020 final.

[153] See also Giorgio, F.（2013). A New Way Forward. In *European eHealth Governance Initiative*. Springer. P. 383.

innovation into the healthcare system through the deployment of more and more efficient e-health services and instruments. Since 2013, the Commission has also discussed the legal issues affecting e-health in the two themes of the e-health Network and the European Innovation Partnership on Active and Healthy Ageing, and carried out cross-sectoral legal work to integrate e-health with other ICT-led innovation. Strengthening the coordination of e-health processes can make society better adapt to the challenges of an aging society and the personal needs of citizens, patients and medical professionals.

Through the implementation of these policies, the urgency of action to achieve e-health and create broader innovation can be recognized. One of the challenges facing the e-health governance initiative is to ensure that this commitment is not only effective throughout its implementation time, but also sustainable. It can be seen that cooperation at the European level is not easy, and the deployment of e-health at the national level is challenging, but it is stimulating for the development of the EU and will reflect a major commitment to the future of Europe. In the development of the e-health Governance Initiative, it is clear that Member States are working together to improve the non-expandable or non-interoperable situation of e-health care, so that patients' healthcare can reach continuity and thus contribute to the continued fragmentation of the market. The establishment of an e-health network under the Directive 2011/24/EU offers significant opportunities to advance this agenda, but at the same time it also brings new challenges. It is not always easy for Member States to reach consensus on the topics they have identified.[154] At the national and EU levels, new approaches are being developed to identify and implement e-health strategies.

3.2.3 e-Health Action Plan 2012-2020

Aware of the importance of e-health, EU has launched a new plan - the e-health Action Plan 2012-2020.[155] Like the 2004 Action Plan,[156] it is a Communication from the European Commission (a

[154] Ibid.
[155] European Commission, 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century'. COM (2012) 736 final.
[156] European Commission, 'e-Health - making healthcare better for European citizens: an action plan for a European e-Health Area' {SEC(2004)539} COM(2004)0356 final.

policy document adopted by the Commission but not legally binding). According to the objectives of the Europe 2020 strategy and Digital Agenda for Europe, it clarifies the policy areas and outlines the vision of European e-health. The EU believes that e-health is an important innovation field, which plays a key role in economic development and employment. The main target of the action plan is to accelerate the deployment of e-health on the basis of achievements and to propose specific measures for progress.

Promoting e-health is one of the specific actions to facilitate the free movement of EU citizens in the EU. Despite the e-health has the opportunity and benefit of development, especially through the open and effective exchange of health data, there are some obstacles that will prevent it from being widely used in healthcare. Actually, it can be found that the e-health Action Plan 2012-2020 largely reflects the four aspects of the e-health Governance Initiative activities, even if not fully. For instance, users' acceptance of e-health, various technical problems related to interoperability and legal challenges have been listed as the theme of the action plan. In response to these issues, the EU has proposed four major work priorities in the action plan. The first is to increase the publicity of e-health, improve people's awareness of the benefits and opportunities brought by e-health, and give citizens, patients and healthcare professionals more power to use e-health care system and services. Secondly, efforts should be made to reduce barriers to collaboration in the field of e-health. The third action is to establish a sound legal framework to ensure the development of e-health, which is also the key to secure the health records of patients. The last point is to support research and development in the field of e-health to promote the establishment of a competitive Europe, as well as boost dialogue and international cooperation in e-health policies at the global level.

Digital technologies (such as mobile applications) will enable the market for high-quality living to grow rapidly. The convergence between healthcare equipment and wireless communication technology as well as between health and social care is constantly creating new business possibilities.[157] This can improve the market economy of the EU and enable patients to get more efficient healthcare services, but from a legal point of view, the e-health Action Plan 2012-2020

[157] European Commission, 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century'. COM (2012) 736 final.

also faces new legal challenges. These legal issues are also likely to impede the smooth operation of e-health. For example, there is a lack of legal clarity on health-related mobile applications and a lack of transparency on the data collected using such applications. If the problem of inadequate health data exchange is to be addressed, it must be addressed by dealing with a fragmented legal framework, a lack of legal clarity and systematic interoperability. Therefore, reducing legal barriers is essential for deploying e-health in EU. The Directive 2011/24/EU will help to achieve this target, as it clarifies the right of patients to receive cross-border healthcare, including telemedicine. The Commission Staff Working Paper on the applicability of the existing EU legal framework to telemedicine services specifically lists the EU legislation applicable to issues such as licensing, data protection, reimbursement and liability that may occur when telemedicine is provided across borders. [158]

In terms of protecting patients' health data, effective data protection is critical to building trust in e-health and is a key driver of successful cross-border deployments. In the cross-border deployment of e-health, it is very important to coordinate the rules of cross-border exchange of health data, so it is necessary to establish safeguard measures. Both the report of the e-health Task Force and the responses to the public consultation[159] on the e-health Action Plan indicated that there is a strong interest in discussing the concept of data control. They also provided a clearer explanation of the conditions for accessing and re-using health data and the flow of such data across the healthcare system. Taking into account the privacy of patients and the conditions for the legal processing of health data, relevant EU legislation includes:

- Article 8 of the European Convention on Human Rights, Article 8 of the EU Charter of Fundamental Rights and Article 16 (1) TFEU.
- Directive 2011/24/EU on the application of patients' rights in cross-border healthcare.
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

[158] Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services accompanying the document - eHealth Action Plan 2012-2020 – innovative healthcare for the 21st century SWD (2012) 414 final. Available at: https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:52012SC0414
[159] http://ec.europa.eu/information_society/activities/health/ehealth_ap_consultation/index_en.htm

- Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Additionally, a series of data protection problems need to be solved in terms of health data processing using cloud computing infrastructure and services. The wellbeing ICT initiatives and e-health should comply with the principle privacy by design and enhance the use of Privacy Enhancing Technologies (PETs)[160] in accordance with the Data Protection Regulations. This requires the controller to carry out data protection impact assessment[161] and comply with enhanced security requirements.

In addition, the growth of mobile health and welfare market is accompanied by the rapid growth of corresponding software applications. For example, some patients with chronic diseases can use these applications to obtain information, diagnostic tools, and possibly achieve new models of care. Therefore, the legal framework applicable to this particular area needs to be further clarified. For instance, the applicability of the current legal framework, the use of data collected by individuals and healthcare professionals through the applications, as well as how to integrate them into healthcare systems. In 2014, the European Commission published the Green Paper on mobile health, which aimed to develop the use of mobile devices (including applications) to enhance the health of EU citizens.[162] In the Green Paper, the legal issues and other issues involved in mobile health were clarified more clearly.

From here we see that improving the legal and market conditions for the development of e-health products and services is very important. In order to carry out e-health Action Plan 2012-2020 smoothly, it needs not only sufficient legal framework to support, but also the joint efforts of Member States. The previously implemented epSOS pilot project (see section 3.3 for details) has defined how Member States can collaborate and integrate their processes to deploy e-health

[160] London Economics. (2010). Study on the economic benefits of privacy- enhancing technologies (PETs). Final Report to the European Commission, DG Justice, Freedom and Security.
[161] GDPR, Article 35.
[162] The European Commission. Green Paper on mobile Health ("mHealth") COM (2014) 219 final. Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-219-EN-F1-1.Pdf

services across Europe. The experience from the epSOS project has shown that Member States gathered together to establish and deploy interoperable infrastructures and information structure at the EU level, which also helps to deploy at the national, regional and local levels. Furthermore, the e-health Action Plan 2012-2020 emphasizes cross-border activities in healthcare. It is worth noting that the work done at the EU level has a strong impact at the national level, and the impacts at the EU and national levels are mutual. Thus, the Action Plan encourages close collaboration among EU institutions, national and regional authorities, healthcare professionals, patients, researchers as well as industry. Through the development of e-health, cross-border healthcare, health security and universality can be promoted in the EU. At the same time, it is important to foster innovation and a clear legal framework for e-health in Europe, ensuring that EU citizens have access to higher quality and safer healthcare, greater transparency and empowerment, more efficient and sustainable healthcare systems, as well as a more competitive European economy. The most pressing health and health system challenges of the first half of the 21st century can only be addressed through the joint efforts of all sectors.

3.3 Cross-border health project epSOS

3.3.1 Content of the project

With the deepening of the integration of EU countries, cross-border people flow more and more frequently within the EU. The European Union then began to pay attention to whether citizens can easily access high-quality medical services abroad, and how to smoothly transfer medical information among different countries As the EU is a union composed of many sovereign countries, different languages, different health care systems and different information infrastructure of different Member States hinder the establishment of a unified medical information system in the European Union, which will hinder the access of EU citizens to habitual and comfortable medical services anytime and anywhere. Even though EU Member States had their own medical data storage methods or systems, there was no attempt to make these systems connected. This would result in European lives being at risk when medical authorities are unable to obtain their health records. In September 2008, ten EU Member States signed a new initiative aimed at revolutionizing the way Europeans can access health records electronically. The European Patient

Smart Open Services project (epSOS), known as a Large-Scale Pilot, is a bold attempt to break the barriers to providing seamless medical services to EU citizens who are sick outside their home countries. When patients receive medical care across borders, both patients and doctors will face a series of problems.

These problems include prescribing appropriate medicine when healthcare providers have little knowledge of patients' medical history, or patients informing foreign language doctors about their medical conditions. Therefore, the epSOS project is seen as helping to eliminate language management and technical barriers and make it easier for people to get medical assistance based on their own medical history, even if they are not at home. It is more like a bridge to span the gap between Member States' health systems. The epSOS project has done a lot of research and practice in the standardization and privacy transmission of patient electronic health data, which has laid a solid technical foundation for the EU to promote medical informatization in a wider range.

The six-year (2008-2014) epSOS project aimed to develop, pilot and evaluate cross-border e-health services and develop recommendations for future work.[163] It focused on providing safe, reliable and high-quality services for the exchange of electronic prescriptions and patient summary data between EU Member States. Such large-Scale Pilot deployment projects required national administrations to jointly develop, test as well as validate interoperable ICT solutions. This is the benefit of achieving economies of scale and moving towards market fragmentation, and e-health is regarded as a domain where such a method can bring significant benefits to society and the market. [164]

The epSOS project was divided into two phases.[165] The first phase focused on cross-border access to patient health summary and cross-border use of e-prescription. The second stage was to test the use of the European Emergency Number 112 and the electronic European Health Insurance Card (eEHIC), as well as the patient's access to personal medical data. This was the first time that patients in pilot countries and regions had access to cross-border medical insurance services. In

[163] European Commission – Cross-border health project epSOS: what has it achieved? Available at: https://ec.europa.eu/digital-single-market/en/news/cross-border-health-project-epsos-what-has-it-achieved.
[164] Giorgio, F.（2013). A New Way Forward. In *European eHealth Governance Initiative*. Springer. P. 384
[165] Ibid.

the first phase, the infrastructure was mainly built in the Participating Nations to explore and test the cross-border exchange and visit of interoperable patient summary and e-prescription. In the case of unexpected and unplanned medical treatment (such as an accident or emergency), the doctor can access the patient's minimum health data set (patient summary) in their native language on their operating system due to the epSOS service, so they can understand the patient's health status and basic information. In addition, it can also be used as a reference in referral, general health care and other planned treatment. The e-prescription means that doctors of medical service institutions send patients' prescriptions to the regional or national electronic prescription database in electronic format. After patients arrive at the drugstore to collect medicine, the drugstore reports to the database system that medicine have been sent to patients and can feed back the whole process to doctors. Besides, the second phase of epSOS project aimed to achieve cross-border e-health services in the future by building modules in pilot member countries and conducting cross-border e-health services testing. Therefore, in order to achieve these goals, epSOS must address interoperability at all levels, from legal to semantic and technical.[166]

3.3.2 Legal background for epSOS implementation

In fact, the epSOS project faced a wide range of challenges such as the identification and authentication of service users, semantic challenges (such as codes used to translate patient diagnosis), the definition of technical infrastructure and legal framework for providing such services. The project must ensure the safety of health data processing. Therefore, the confidentiality, availability and integrity of data must be guaranteed through appropriate security requirements. To be more precisely, the security requirements of epSOS must be able to guarantee the following contents: provide identity certificate, conduct authentication, use authority control, data confidentiality, data availability, and system security operations for records. In the first few years of operation, epSOS gradually found solutions to these challenges. It set the technical, semantic and legal framework for the pilot work.

[166] Commission Recommendation of 2 July 2008 on Cross-border interoperability of electronic health records system, 2008 O.J. (L 190/ 37), page 9. Available at: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id1⁄44224.

From the legal and regulatory perspective, it should be noted that epSOS services were provided on a 'pilot' basis. It followed the existing EU regulatory framework at that time, so there was no need for Member States to amend their national legislation on the provision of healthcare services. As a pilot, the epSOS project promoted the close cooperation between national data protection authorities of various countries, as well as between Member States and EU data protection authority. As far as the project itself was concerned, epSOS transformed the experience processing collected from the pilot activities into the practice guide to solve the outstanding problems of regulatory supervision, so as to promote the process of the project from pilot to comprehensive application.

A major challenge for the project was to pursue the synergy between the project implementation plan and the existing policies at that time, so as to ensure the consistency of concepts and development. The Data Protection Directive and its supporting guidance documents were an important supplement to the regulatory work of epSOS project.[167] On the contrary, working experience gained from epSOS could also contribute to the revision of the Data Protection Directive.[168] Therefore, compared with the Data Protection Directive, there are some new definitions and provisions on health data in the General Data Protection Regulation. It is reasonable to believe that these new definitions or provisions are largely related to the implementation of the epSOS project.

The regulatory issues involved in epSOS can be divided into four categories: data protection and confidentiality, legal issues related to the health care system, liability-healthcare professionals and social dimension, work protocols, audit and traceability.[169] The epSOS project provided a detailed analysis of these four areas to enable them to be used in the necessary regulation design of safety and security.

[167] The data protection legislation that was applicable in the EU at that time was the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, which was replaced by General Data Protection Regulations in 2018.

[168] ICTPSP. epSOS – legal and regulatory perspectoves. Available at: https://www.promisalute.it/servizi/gestionedocumentale/visualizzadocumento.aspx?ID=2461

[169] Ibid.

The institutional basis of implementing epSOS included the NCP and Framework Agreement (FWA). Each EU Member State participated in the project through its NCP. The NCP is authorized by the relevant government authority of each Member State according to law and act as two-way technical, organizational and legal interface between the existing different national functions and infrastructures. At the legal level, NCP had the right to cooperate with other organizations to provide necessary services, which are necessary to meet epSOS use cases,[170] and played the role of communicator and communication channel of regulatory affairs. In addition, FWA was embedded in the framework of the project, which was also a necessary condition for Member States to join the pilot project. It established epSOS Trusted Domain between NCPs. Using this general FWA as a guide for communication among EU Member States was conducive to establishing a trust system between project participants, so that patients could also enjoy seamless healthcare services when moving between Member States participating in epSOS Large Scale Pilot. The health data exchange cooperation model based on FWA can also be used as a document reference for multi-party data exchange credit in the future.[171] It also improves the transparency of patients' cross-border healthcare in maintaining the right to privacy of personal health data.

The epSOS also issued a Legal Sustainability Recommendation for long-term operational cross-border e-health services at the end of the pilot, which included necessary actions for national as well as EU level supervisory authorities.[172] In this Recommendation, the legal and regulatory sustainability of epSOS was proposed. It noted that in the past few years, the EU legislative has made significant progress in creating a clear and basic governance framework to support cross-border electronic services. First of all, the Directive 2011/24/EU creates conditions for the legal certainty of patients' rights to reimbursable cross-border healthcare, and provides clear guidance on how to resolve major legal obstacles (such as the recognition of e-prescriptions). In addition, during the life cycle of epSOS, the EU has also initiated other important policy and legislative development, laying the foundation for the formulation of long-term operational recommendations for epSOS services. For example, GDPR are designed to ensure a consistent level of data

[170] The ‘use cases’ means real patients who participated in the epSOS project in real life.
[171] ICTPSP. epSOS – legal and regulatory perspectoves. Available at: https://www.promisalute.it/servizi/gestionedocumentale/visualizzadocumento.aspx?ID=2461
[172] D2.2.7 Legal Sustainability Recommendations. 06 June 2014. Available at: file:///Users/shaleqi/Downloads/D2.2.7%20Recommendations_v1.5.pdf

protection and privacy rights for all individuals in the EU. The Regulation on electronic identification and trust services of electronic transactions in the internal market (eIDAS Regulation)[173] and the European Standardization Regulation[174] which mainly affects the adoption of ICT technical specifications also promote the development of e-health and provide security. These EU legal interventions have created conditions to coordinate aspects of the operation of cross-border e-health services that are essential. To a certain extent, they also complement Directive 2011/24/EU that regulates these services.

National and EU laws provide the legal basis for interoperability at the organizational and legal levels, including the ability of technical interoperability through the use of common semantic and the technical standards, as well as legal requirements and governance rules for interoperability.[175] EU and national legislation on e-health (especially cross-border access to EHRs and e-prescriptions) clarifies the level of legal interoperability. Despite the lack of legal interoperability, by supporting the implementation of epSOS, the foundation can be laid for stronger legal interoperability in the future. This also includes intervention through other EU legislations. The EU and national legal frameworks also define the conditions for sharing health data and provide the relevant safeguards to be implemented. The implementation of safeguard measures is a prerequisite for the deployment and sustainability of cross-border e-health services. In addition to making laws, it also creates conditions for the interoperability of organizations. This was successfully achieved in epSOS and was also documented in FWA. From the perspective of law and regulation, the issues that need to be clear include data protection and confidentiality, patient consent, legal issues related to health systems, liability as well as security.[176] At the same time, in order to solve a series of issues such as the safety of patient health data, epSOS safeguards have reached an agreement on its content, implementation, evaluation and monitoring.[177]

[173] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014 O.J. (L 257/73).
[174] Regulation (EU) no 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardization, 2012 O.J. (L 316/12).
[175] D2.2.7 Legal Sustainability Recommendations, 06 June 2014. file:///Users/shaleqi/Downloads/D2.2.7%20Recommendations_v1.5.pdf
[176] Ibid.
[177] Ibid.

Based on the experience of the epSOS pilot, it is also recommended that the European Commission and the e-health network ensure that follow-up EU level initiatives are built on the experience of broad cooperation among EU Member States. With regard to e-health governance in the EU, it is recommended to provide cross-border healthcare services for patients in a sustainable trust environment, as well as monitoring the agreements of all active parties in data sharing. Before the new EU legal framework on cross-border e-health is fully in place, the deployment of e-health services should have a common legally binding framework of Member States, which should be based on agreements applicable within the EU. For such agreements, it is recommended that they can only be modified during the conversion to local legal and organizational frameworks and guidelines for compliance with local laws or customs. This is to create as much conditions as possible for legal and organizational interoperability. In addition, the European Commission and Member States should strengthen cooperation and actively collect and publish information on cross-border e-health services, so that e-health services can be better developed. In terms of data protection and confidentiality, since all data contained in medical documents and EHRs are "sensitive personal data", healthcare data processing must have a clear legal basis and should comply with the provisions of GDPR It is worth noting that the processing of personal health data must be strictly limited to the minimum necessary to perform any explicit and legal cross-border e-health services. Furthermore, it is recommended that privacy and confidentiality be included in the design of all e-health cross-border services, such as mandatory components for patient consent, encryption between NCPs, and access in case of emergency.[178]

In September 2014, Henrique Martins, chairman of e-health Network Sub-group for upkeep e-health cross-border services announced the introduction of a Temporary Legal Agreement (TLA) to maintain cross-border e-health services developed by epSOS, aiming to provide legal basis for relevant countries. The TLA is closely consistent with the epSOS Legal Sustainability Recommendations. It provides a simplified but secure way to achieve the legal interoperability baseline required for Member States to operate cross-border e-health services.

[178] Ibid.

3.3.3 Achievements and influence of epSOS

European e-health interoperability has a strong momentum, and it is exciting to see it happen at the EU level. The e-health network has set up a group of Member States dedicated to continuing the epSOS services.

Although the project had been completed, the results, components and well- structured infrastructure delivered by epSOS project will be further used in projects and initiatives such as EXPAND, STORK2.0, health record sharing between patients in the EU and the United States, and in addition to the construction of e-health network. From the perspective of sustainable development, these existing and future initiatives will continue to maintain and manage the work of former epSOS participants, and the projects built in member countries will also be supported. The results of epSOS are bound to be relevant to future initiatives.

The epSOS made a great contribution to supporting the public health system and cross-border health data exchange within and even beyond Europe. In terms of Legal and Regulatory, epSOS project introduced a regulatory constraint (epSOS FWA), in which experimental electronic medical information exchange could be achieved. When similar operations are needed outside the project, a more appropriate regulatory framework is needed to deliver patient health data across borders. To some extent, the epSOS project has completed the latter framework, which is expected to support the process leading to the application of the sustainable regulatory framework. The epSOS project also provides the patient summary data set for the e-health network. It also worked in the field of e-prescription and supported the convergent development of the medical informatization process through various forms of cooperation. It promotes the process of health care sharing within the EU.

3.4 Other polices

In addition to the above-mentioned policies on e-health, there are a number of other initiatives in the EU aimed at encouraging patients and healthcare providers to use digital health. For instance,

the Action plan for a European e-health Area,[179] the Commission Communication on telemedicine for the benefit of patients, healthcare systems and society,[180] as well as the Commission Recommendation on cross-border interoperability of electronic health record systems.

The mid-term review on the implementation of the DSM strategy in May 2017 underlined a strong willingness to access and share health data for research and treatment purposes, as well as to encourage patients to provide feedback on the quality of healthcare services.[181] In accordance with the Commission's DSM strategy, the European Commission has also published a Communication on Digital Transformation of Health and Care in the DSM to empower citizens and build a healthier society on 25 April 2018. This policy document provides guidance for the EU's activities in e-health in the coming years.[182] It is clear that e-health aims to empower EU citizens to better control their medical data and records. This is also the significance of the European e-health policy. The Communication identified three priorities:

- Secure cross-border access and sharing of health data by citizens;
- Collecting better data to promote research, disease prevention, and personalized healthcare;
- Strengthening citizen empowerment and person-centered healthcare services through digital tools.

In order to facilitate wider cross-border healthcare access, the European Commission is gradually establishing the e-health Digital Services Infrastructure. This will allow and facilitate the exchange of patient summaries and e-prescriptions between healthcare providers. The first cross-border exchanges began in 2019, and most EU Member States should be able to achieve this by 2021.[183] However, more needs to be done to enable all citizens can access and transmit their complete EHRs in full privacy and confidentiality when they receive healthcare in another Member States. The

[179] The Action plan for a European e-Health Area {SEC(2004)539} COM(2004) 0356 final.
[180] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society COM (2008) 0689 final.
[181] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:228:FIN
[182] Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society SWD (2018) 126 final.
[183] https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_ga.

Commission is also developing a European EHR exchange format for use by all EU citizens. The European Economic and Social Commission (EESC) has adopted a positive opinion on this Communication.[184] With regard to the first priority of Communication (secure access to citizens' own health data throughout the EU), the EESC endorsed the European Commission's efforts to support the development and adoption of the EHR exchange format, as well as further emphasized that citizens should have the right to access their health data and decide whether and when to share their data.[185]

Digital technology can effectively improve people's health and address the challenges facing the healthcare system. Through advanced data infrastructure and efficient data analysis, high-performance computing can play a powerful role in health with big data. However, data protection rules must be fully respected when developing such tools. Under the framework of GDPR, individuals' fundamental rights to the protection of health data can be guaranteed to the greatest extent in the digital era. Health data processed with the explicit consent of patients or other legal basis permitted by GDPR can accelerate research with high quality under appropriate safeguards.[186] Using digital technology in the field of health can not only effectively detect infectious diseases in the early stage, but also stimulate innovative healthcare solutions, such as telemedicine.[187] Furthermore, the proposal of the revised e-Privacy Regulation[188] will supplement the GDPR and ensure consistency with the relevant rules of the GDPR. This will further improve legal certainty and protect users' online privacy, and will also increase the commercial use of communication data based on user consent. Adopting e-Privacy Regulations allows consumers and businesses to benefit from a complete digital privacy framework, which is as effective for

[184] Draft Opinion-Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society. COM (2018).
[185] Ibid.
[186] Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All. COM (2017) 228 final.
[187] Ibid.
[188] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD).

patients as for healthcare providers. This enables citizens' health data to be transmitted in a more secure environment.

In addition, eIDAS plays an important role in the digital transformation of healthcare. It is the EU's Regulation on electronic identification and trust services for electronic transactions in the European Single Market and the result of the European Commission's attention to the European Digital Agenda. The eIDAS Regulation aims to strengthen trust in electronic transactions among EU citizens, businesses and the public sector by providing a common legal framework for cross-border identification of electronic identities. All organizations providing public digital services in EU Member States must recognize the electronic identity of all EU Member States. It also provides various aspects of safeguards for the digital transformation of health care. Firstly, such initiatives could change the way medical data are recorded and shared, providing citizens with a secure way to have seamless cross-border access to their medical and health-related data from all EU countries. Any delay in obtaining medical records in an emergency is unacceptable. The GDPR will control the use of individual data including health data. Meanwhile, the instrument provided by eIDAS is also important here. It requires that health records must be matched with individual citizens and must not be tampered with or misused.

Secondly, creating a framework for pan-European healthcare data sharing infrastructure to improve the efficiency of data usage is an important part of e-health initiative. In fact, a shared Research and Development infrastructure for European health data accounts for a large part of the expenditure of many medical institutions. Thus, efforts need to be made to improve efficiency as much as possible, because such research and development is crucial to promote the development of disciplines. Researchers can save a lot of extra costs by sharing data, expertise, and other resources. eIDAS can play a key role in protecting data from abuse by providing authentication and trust services. Finally, in order to improve the quality of health care and ultimately citizens' health and well-being, it is necessary to establish a patient-feedback mechanism. An ideal feedback loop is to continuously obtain input from end users and then transform it into an operational point for medical service providers. Empowering citizens to use this tool is another focus of this initiatives to achieve the digital transformation of healthcare. Only the full deployment of this new model of care will make it possible to improve the efficiency of health and health systems and to

provide better health services to all segments of the population equally and inclusively. Nevertheless, this requires ensuring that the right people provide feedback on the treatment or services they received to prevent abuse of the system. From this perspective, the authentication infrastructure enabled by eIDAS can guarantees this.

High quality healthcare services have gradually become one of the important needs in modern life. Human beings are now in an era in which most services have been digitized, so health care also has to follow the pace into this digital era. Initiatives such as those related to e-health can ensure that patient's health records, research tools and personalized drugs can be used more securely by EU citizens and healthcare providers, supported by eIDAS Regulation and the legal framework for privacy and data protection.

Chapter IV EU privacy and data protection for cross-border healthcare

4.1 Council of Europe legal framework

The legal instruments adopted by the Council of Europe are particularly important for the legal purposes of the EU. They also define the obligations of EU Member States on privacy and protection of personal data. In addition to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which is essential for interpreting the rights guaranteed by the EU Charter, it is also extremely important for EU law. We can see the provisions in Article 6 (2) of TEU that 'the Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms'.[189] Additionally, the fundamental rights guaranteed by the ECHR, as well as the those resulting from the constitutional traditions common to the Member States, should constitute general principles of the EU law.[190] All EU Member States are members of the Council of Europe and are bound by the ECHR. The instrument most relevant to data protection in the context of the Council of Europe is Article 8 of the ECHR, which protects the right to privacy and personal data and additionally guarantees the right to respect for private and family life, homes and correspondence. Another important binding instrument is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal data, known as Convention 108, and its Additional Protocol.[191] In fact, the legal instruments related to data protection adopted by the Council of Europe also include the 1987 Recommendation on the Use of Personal Data in the Police Sector, but this will not be analyzed in detail in this paper.

4.1.1 Article 8 of the ECHR

The ECHR was drafted by the Council of Europe in 1950 and entered into force in 1953. It soon became the most important human rights instrument in European history. All member states of the Council of Europe, including all EU Member States, are party to the Convention. The ECHR

[189] Treaty on European Union (TEU), Article 6(2)
[190] TEU, Article 6(3)
[191] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14. Council of Europe. Rome, 4. XI.1950.

established the ECtHR, which is why it is considered to be the most effective in protecting individuals against human rights violations in Europe. Judgments finding violations are binding on the States concerned and they are obliged to enforce them. It is applicable at the national level and has been incorporated into the legislation of States Party, so all domestic courts must apply it. The interpretations by the ECtHR on the provisions of ECHR are very important, because through these interpretations the protection of human rights and freedom has been developed and strengthened.

In April 1967, the Consultative Assembly of the Council of Europe referred a resolution on human rights and the development of modern science and technology in general to its legal Committee.[192] The Council of Europe's Legal Committee suggested it was necessary to study 'the question whether Article 8 of the Convention on Human Rights as well as national legislation in the Member States adequately protect the right to privacy against violations which may be committed by the use of modern scientific and technical methods'.[193] Following this intervention, the Parliamentary Assembly of the Council of Europe adopted a Recommendation 509 (1968) on Human Rights modern Scientific and Technological Developments to the governments of its member states.[194] This Recommendation, which was influential, declared that 'modern scientific and technical methods'[195] were 'a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8' of the ECHR,[196] and called for a study of this issue.[197] As a result, by the early 1970s, the Council of Europe had changed its initial interest in protecting individuals in the face of technological developments, understood the issue of individual protection as an information privacy problem, and generally believed that the use of computers needed to be regulated first. It also used the term "privacy" to refer to the content of Article 8 of the ECHR.[198]

[192] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing. . 83.
[193] Council of Europe's Consultative Assembly 1968, p. 754.
[194] Council of Europe, Recommendation 509 (1968) on Human Rights and modern Scientific and Technological Developments, adopted by the Assembly on 31st January 1968 (16th Sitting).
[195] Recommendation 509 (1968), para. 8(i).
[196] Ibid.
[197] Ibid, para. 8(ii).
[198] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing, p. 84.

Article 8 (1) ECHR explicitly provides a right to respect for private life and family life, as well as the inviolability of the home and the confidentiality of correspondence. Its scope is broad,[199] however, the protection afforded by Article 8 of the ECHR is limited, as the rights protected by paragraph 1 may be impeded by the requirements set out in paragraph 2 [200]. The ECtHR has not yet defined precisely the concept of "private life", noting that "private life" is a broad term and cannot be defined in detail. Nevertheless, in recent decades, the ECtHR has been elaborating on the scope of Article 8 of the ECHR and the necessary conditions for considering interference as legitimate and lawful. This is in line with the nature of the Court as a living instrument, as it must take into account changing legal, social or technical conditions in order to be practical and effective.[201]

However, Article 8 (2) provides some limitations. According to Article 8 (2), there are three circumstances in which public authorities can legally interfere with the rights provided for in Article 8(1). Firstly, the interferences must be in accordance with the law. In Taylor-Sabori v. the United Kingdom, the applicant's communications had been accessed through a 'clone' of the applicant's pager, after which he was arrested and charged with conspiracy to provide controlled drugs.[202] The application complains that, under Article 8 of the ECHR, the interception of his pager messages by the police constitutes an unjustified interference with his private life and correspondence which was not 'in accordance with the law'. Since there was no provision for such interception in British law at that time, the ECtHR held that the intervention was not being 'in accordance with law'. The requirement of being 'in accordance with the law' requires certain qualities of domestic legal provisions. Similarly, in Liberty and others v. the United Kingdom, it was noted that the term "in accordance with the law" under Article 8 (2) required that the alleged measure should have some basis in domestic law, but that such basis should be consistent with the

[199] Greer, S. (1997). The exceptions to Articles 8 to 11 of the European Convention on Human Rights, Council of Europe, Printed at the Council of Europe.
[200] Article 8 (2) of ECHR states: there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
[201] ECtHR, Tyrer v. the United Kingdom, App. No. 5856/72, 25 April 1978.
[202] ECtHR, Taylor-Sabori v. the United Kingdom, App. No. 47114/99, 22 October 2002.

rule of law, and the consequences can be foreseen.[203] The ECtHR stressed that 'the national law must be clear, foreseeable, and adequately accessible'.[204] Therefore, any State's intervention in privacy rights in the context of enforcement must be firmly rooted in legislation that meets the following three criteria: first, the practice must be based on domestic law; second, the law must be accessible and sufficient clarity and accuracy with respect to individuals in order to understand the conditions and circumstances under which authorities are empowered to resort to any interference with an individual's right to private and family life, home and correspondence; third, the consequences need to be foreseeable.

Secondly, these limitations must pursue legitimate objectives. Article 8(2) provides a limited list of legitimate purposes for violating the rights protected in the first paragraph. Last but not least, the limitations must be "necessary in a democratic society". It seems clear that the rights protected by Article 8(1) are not absolute, and the ECtHR has been examining whether the above conditions apply. For instance, The S. and Marper case involved two individuals who were not convicted and wanted to remove their records from the DNA database used for criminal identification in the United Kingdom, in particular their fingerprints, cellular samples and DNA profiles.[205] In its judgment, the Strasbourg court held that the indefinite storage of such personal information relating to innocent persons in a database of this nature violated the requirements of Article 8 of the ECHR. ECtHR declared that the indiscriminate practice by the British authorities constituted the interference with the applicants' right to respect their private life, which was not considered 'necessary in a democratic society' and therefore violated Article 8 of ECHR.[206] In order to determine whether these interventions are 'necessary in a democratic society', it is crucial to provide relevant and sufficient reasons for the legitimacy of these interventions, and these interventions are proportionate with the legitimate objectives pursued.[207]

[203] ECtHR, Liberty and others v. the United Kingdom, App. No. 58243/001, July 2008. para. 59.
[204] Silver and others v. the United Kingdom, App No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983.
[205] ECtHR, S and Marper v. United Kingdom, App. No 30562/04 and 30566/04, 4 December 2008.
[206] Ibid. S and Marper v. United Kingdom Judgment, para 125. Available at: https://rm.coe.int/168067d216
[207] Z v. Finland, App. No. 22009/93, 25 February 1997.

The principle purpose of Article 8 may involve taking measures designed to ensure respect for private life. The CJEU, based in Luxembourg explicitly affirmed that there was a strong link between EU personal data protection law and the right to privacy as recognized by Article 8 the ECHR. For decades, the ECtHR, based in Strasbourg, had also in fact been dealing with the issue of data relating to individuals from the perspective of Article 8 of the ECHR and continues to do so.[208]

The ECtHR interpreted the scope of Article 8 of the ECHR as including the compilation of personal data by public authorities.[209] In different rulings, the ECtHR held that the collection, registration or use of personal information may infringe the right to private life.[210] In determining whether the personal information held by the authorities relates to any aspect of private life, the Court will give due consideration to how these data are used and processed, the nature of the records, and the results that can be obtained.[211] The ECtHR declared that the protection of personal data is 'of fundamental importance' for the enjoyment of the right to respect for private life guaranteed by Article 8 ECHR. Domestic law must provide appropriate safeguards against the use of personal data that may be inconsistent with its guarantees.[212] The ECtHR also stressed that the need for such safeguards 'is all the greater where the protection of personal data undergoing automatic processing is concerned'. It examined a variety of situations related to the storage of personal data by public authorities. Therefore, when it comes to personal data protection, the scope of Article 8 of the ECHR also needs to be interpreted in accordance with the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. With regard to the protection of personal data, Strasbourg's case law can be summarized as providing some protection against the processing of information about individuals by establishing Article 8 of the ECHR. Even though the scope of such protection may not be entirely consistent with the scope of application

[208] Fuster, G. G., & Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. International Review of Law, *Computers & Technology*, 26(1), p. 73-82.
[209] See, ECtHR, Uzun v Germany, App. No. 35623/05, 2 September 2010.
[210] see E. Brouwer (2008), Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System, Martinus Nijhoff Publishers, p.155-176.
[211] Carrera, S., Fuster, G. G., Guild, E., & Mitsilegas, V. (2015). Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights. Brussel: CEPS, p. 25.
[212] See ECtHR, S. and Marper v. the United Kingdom, App. Nos. 30562/04 and 30566/04, 4 December 2008, para 103.

of the Convention 108, from another perspective, according to these two legal instruments, the general principles of Directive 95/46/EC could be asserted to constitute the general principles of European Community law even before the adoption of the Directive in 1995.

4.1.2 Convention 108

The Council of the Organization for Economic Cooperation and Development (OECD) issued its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980 OECD Guidelines).[213] The 1980 OECD Guidelines put the concept of personal data at the forefront and emphasized the need to ensure the free flow of data by OECD Member countries in the face of environmental changes caused by new technologies.[214] However, this free flow was threatened by growing concern about privacy and the emerging privacy and data protection laws at that time.[215] At least, the 1980 OECD Guidelines were a globally influential instrument, but not legally binding. The Council of Europe was preparing to finalize a legally binding instrument to play a greater role in Europe. Soon thereafter, the Council of Europe adopted Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) in 1980.[216] This Convention is the first legally binding international instrument in the field of data protection and formally links data protection to general guarantees of 'rights and fundamental freedoms'. The Convention 108 obliged Members States of the Council of Europe to enact legislation implementing the declared principles and was intended to coordinate the existing but fragmented legislation on data protection at that time.[217] The purpose of the Convention 108 is to ensure that all individuals within the territory of States parties to the Convention respect their rights and fundamental freedoms, in particular their right to privacy, in the automatic processing of personal data related to them, which corresponds to the substantive concept of data

[213] Council of the OECD, Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal data, 23 September 1980.
[214] Kindt, E. J. (2013). Privacy and Data Protection Issues of Biometric Applications A Comparative Legal Analysis: Springer, p. 90.
[215] Ibid, p. 91.
[216] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No. 108.
[217] See Miller, A. P. (1986). Teleinformatics, transborder data flows and the emerging struggle for information: an introduction to the arrival of the new information age. Columbia Journal of Law and Social Problems, 20(1), 89-144.

protection.[218] Thus, it is reasonable to believe that in terms of the Convention 108, something called "data protection" is implemented to protect what is designated as "privacy".[219]

The Convention 108 protects the processing of personal data against infringement and seeks to regulate the transborder movement of such data. It is contrary to the goals pursued in the 1980 OECD guidelines. The Convention is really concerned about privacy, and tries to reconcile the relationship between privacy and personal data transmission. Nevertheless, the free flow of data is still considered important, and Convention 108 is also directly concerned with the protection of this aspect. The Convention sets out various provisions on "transborder data flows"[220] and generally prohibits any restriction on the movement of personal data into the territory of another Party for sole the purpose of protecting privacy.[221]

The scope of application of this Convention includes 'automated personal data files and automatic processing of personal data in the public and private sectors'.[222] The definition of personal data in Convention 108 is the same as in the 1980 OCED guidelines, that is 'any information relating to an identified or identifiable individual (data subject)'.[223] In the chapter entitled 'Basic principles of data protection', there are provisions mainly concerning the concept of data quality, special categories of data, data security and additional safeguards for the data subjects as well as remedies. Convention states that disclosure of personal data on racial origin, political views or religious, as well as the processing of personal data relating to health, sexual life or criminal conventions should be prohibited if national laws do not provide appropriate safeguards.[224] This type of data should be classified as 'sensitive data', especially health data should be specially protected. In addition, a series of safeguards are established for the data subject. It enshrines data subject the right to know

[218] Convention 108, Article 1.
[219] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing. P. 89.
[220] Convention 108, Chapter III.
[221] Convention 108, Article 12(2); see also Articles 12(1) and 12(3).
[222] Convention 108, Article 3(1).
[223] Ibid. Article 2(a).
[224] Ibid. Article 6.

the information on his or her personal data files,[225] the right to access data stored,[226] and the right to correct or erase the data if unduly processed.[227] Moreover, in the case of non-compliance, the data subject has the right to claim remedy.[228] However, Convention 108 does not take into account whether the consent of the data subject is a legitimate ground for processing.

Convention 108 aroused the strong interest of the EC Commission, which had facilitated the ratification of the Convention by EU Member States and had expressed its intention to accede to the Convention. In the fourteenth year following its entry into force in 1985, the Convention 108 was amended and the European Community was allowed to accede to the instrument.[229] In 2001, an Additional Protocol was adopted and introduced supplementary provisions on the mandatory established of national data protection supervisory authorities, and on the flow of data across borders, in order to bring Convention closer to the EC system already established at the time. The Additional protocol had set out the requirements of an independent data protection authority a significant element in the implementation of data protection and improved the methods of restricting the requirements for the export of personal data.[230]

It has been proposed that the opening provision of the future convention should define its purpose as the protection of personal data rights for the security of each individual, thereby ensuring respect for their own rights and fundamental freedoms, in particular the right to privacy in the handling of personal data.[231] In order to justify the reference to the right to the protection of personal data in future instruments, it has been argued that this right has gained a meaning of autonomy over the past few decades, whether through the EU Charter of fundamental rights the case law of the ECtHR. At present, the Convention is undergoing a process of modernization. This process began in 2010

[225] Ibid. Article 5(a).
[226] Ibid. Article 5(b).
[227] Ibid. Article 5(c).
[228] Ibid. Article 5(d).
[229] Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of ministers, in Strasbourg, 15.6.1999.
[230] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing, p. 91.
[231] Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012.

with the Council of Europe's regulators trying to ensure that the modernized Convention are compliance and compatible with the GDPR.[232] The modernization of the Convention addresses the challenges to privacy posed by the use of new information and communication technologies, and therefore requires strengthening the Convention's mechanisms to ensure its effective implementation. In 2018, a Protocol amending Convention 108 was adopted and it will entry into force in 2023.[233] Some of the innovations added to the protocol, such as expanding the types of sensitive data (genetic and biometric data, trade union membership and ethnic origin are newly added),[234] improving the transparency of data processing,[235] strengthening the responsibility of data controllers[236] and establishing a clear regime for transborder data flows.[237] Additionally, the new rights for the person in an algorithmic decision making context are added in this Protocol, which are particularly relevant to the development of artificial intelligence.[238] This Protocol provides a strong and flexible multilateral legal framework to facilitate cross-border data flows while providing effective safeguards when using personal data. It serves as a bridge between different regions of the world and different regulatory frameworks, including the EU's GDPR and which refers to Convention 108 in the context of transborder data flows.

4.1.3 Case law of ECtHR – health data

The ECtHR undoubtedly describes health-related data as a type of data worthy of protection under article 8 of the ECHR. In terms of health data, ECtHR often emphasizes the importance "data protection" and Convention No. 108. For example, the case of Z v. Finland in 1997 involved the disclosure of the medical condition of an applicant with HIV in a sexual assault proceeding.[239] The ECtHR emphasized in its judgment that 'the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private

[232] EU Agency for Fundamental Rights and Council of Europe, Council of Europe. (2018). *Handbook on European data protection law* 2018 edition, Luxembourg: Publications Office of the EU. P. 26.
[233] Ad hoc Committee on Data Protection (CAHDATA), Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CM (2018)2- final, 18 May 2018.
[234] Protocol amending the Convention 108. Article 8(1).
[235] Ibid. Article 8.
[236] Ibid. Article 12.
[237] Ibid. Article 17.
[238] Ibid. Article 11.
[239] Z. v. Finland, ECtHR, App. No. 22009/93, 25 February 1997.

and family life' as guaranteed by Article 8 of the ECHR.[240] The "protection of personal data" was sufficiently recognized in the case. However, it is worth noting that the Court justified that the information disclosed should be protected not because it constituted "personal data" within the meaning of Convention No. 108, but because it belonged to sensitive data.[241] The Court held that the disclosure of such information may significantly affect the personal and family life of individuals.[242] Furthermore, the ECtHR linked the relevant protection to the principle of 'confidentiality', and described it as constituting a safeguard against certain types of communication or disclosure.[243]

The ECtHR has also played an important role in protecting patients' records. I v. Finland concerned an HIV-positive applicant whose confidential medical records were illegally accessed by her colleagues.[244] In this case, the applicant complained that the regional health authorities failed to provide sufficient protection to prevent unauthorized access to medical data. The ECtHR pointed out that according to the existing case law, Article 8 of the ECHR not only obliges States to refrain from interfering with the right to respect private life, but also may have positive obligations in respect of effective private or family life.[245] These obligations may involve measures to ensure respect for private life, even in the context of their personal relationships.[246]

4.2 EU legal framework on privacy and data protection

The legal instruments developed by the Council of European and the EU generally converge in protecting privacy and personal data, but they also differ in some respects. In the EU primary law, Article 16 of the TFEU stipulates the general EU competence of legislation on data protection issues. Another relevant legal instrument is the Charter of Fundamental Rights of the EU, in which

[240] Ibid, para 95.
[241] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing, p. 101.
[242] Z. v. Finland, ECtHR, App. No. 22009/93, 25 February 1997, para 96.
[243] Ibid, para 96.
[244] I v Finland, ECtHR App. No. 20511/03, 17 July 2008.
[245] Airey v Ireland, ECtHR, App. No. 6289/73, 9 October 1979, para 32.
[246] X and Y v the Netherlands, ECtHR, App. No. 8978/80, 26 March 1985, para 23.

Articles 7 and 8 recognize the respect for private life and the right to data protection, and emphasize that both of these rights are basic human rights. In addition, the main secondary EU law instrument for data protection is the General Data Protection Regulation (GDPR), which replaced the Data Protection Directive in May 2018.

4.2.1 EU Primary Law

4.2.1.1 Article 16 TFEU

As basic values of a democratic society, privacy and data protection are bound by law. Through legislation, judicial review and supervision of independent authorities, the EU Treaties give EU a broad role in protecting citizens' fundamental rights. Thus, the Union is able to play a constitutional role in defending privacy and data protection, because the necessity of such protection is stipulated at the constitutional level.

Prior to the entry into force of the Lisbon Treaty, legislation on data protection in the field of freedom, security and justice was divided into the first pillar (European Communities) and the third pillar (Police and Judicial Co-operation in Criminal Matters).[247] The former involved data protection for private and commercial purposes and used a Community integration method, while the latter related to data protection for law enforcement purposes and at the intergovernmental level. Thus, the two 'pillars' followed different rules for the decision process of data protection. The pillar structure disappeared with the entry into force of the Lisbon Treaty, which provided a firmer foundation for the development of more effective data protection system.[248] Article 16 of the TFEU, which relates to Articles 7 and 8 of the EU Charter,[249] sets the EU's mandate on privacy and data protection as fundamental right of individuals. More precisely, Article 16 (1) of the TFEU provides that everyone has right to the protection of personal data concerning them.[250] The wording of this article seems to imply that it applies to the processing of all personal data, including personal and commercial purposes, as well as in the area of police and judicial cooperation, and the processing of personal health data should also be included. This interpretation can gain further

[247] https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection
[248] Ibid.
[249] Articles 7 and 8 of the EU Charter are briefly analyzed in the next section.
[250] TFEU, Article 16(1).

support from the disappear of the three-pillar structure of the EU with the entry into force of the Lisbon Treaty. Article 16(1) of the TFEU, and Article 7 and 8 of the EU Charter lay down the right of data protection, which should be guaranteed by the EU and finally controlled by the CJEU. Besides, Article 16 (2) of the TFEU empowers the EU legislator to set the rules for the protection of individuals with regard to the processing of personal data, as well as the rules for the free movement of such data.[251] The EU provides this obligation in its constitution is unique.

Article 16 TFEU gives the Union a specific task to ensure the protection of personal data, in addition to the general responsibilities of the EU and the Member States acting within the legal scope of the EU, TFEU should also respect the fundamental rights set in the Charter. The EU Charter lays down that where the EU take actions, the fundamental rights of individuals should be respected. Furthermore, Article 16 TFEU determines that the Union should take action to ensure the fundamental right to data protection.

Given the enormous challenges of the information society and the era of big data, there is need for ambitious methods.[252] The successful implementation of the Article 16 TFEU mandate is essential for individuals whose fundamental rights are threatened. Additionally, if the EU can successfully realize the ambition of Article 16 TFEU and can effectively promote respect for privacy and data protection rights, then this will increase trust in the EU to a greater extent. Whether the EU can successfully carry out the tasks lay down in Article 16 TFEU depends on the way in which the EU tries to reconcile the requirements of legitimacy and effectiveness.[253] The successful implementation of the EU mandate in the area of privacy and data protection can demonstrate the EU's ability to protect fundamental rights not only within the Union, but even in the global environment. In order to protect privacy and data, not only through law, the EU can also play a role by successfully exercising its responsibilities.

[251] TFEU, Article 16(2).
[252] Hijmans, H. (2018). *The European Union as Guardian of Internet Privacy – The Story of Art 16 TFEU*. Springer International Publishing, p. 512.
[253] Ibid, p. 129-130.

Furthermore, Hielke Hijmans believes that Article 16 TFEU can benefit from the understanding of fundamental rights such as privacy and data protection, as well as other fundamental rights related to the changing environment of the Internet.[254] Nowadays, in the environment of high-frequency use of the Internet and electronic systems, all processing of personal data may affect personal privacy. For example, healthcare providers disclose or transmit unauthorized patient health data through the Internet when patients cross-border healthcare, which not only violates the privacy of patients, but also violates the rules of data protection. Hence, privacy and data protection often affect each other, and it is difficult to discuss and analyze them as separate fundamental rights.

4.2.1.2 EU Charter of Fundamental Rights

Another primary law that would further better guarantee the right to data protection in Article 16 TFEU is the European EU Charter of Fundamental Rights. In 2000, the EU Charter was officially proclaimed by the Presidents of the European Parliament, the Council and the Commission at the European Council. According to the preamble of the Charter, it reaffirms 'the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Community and by the Council of Europe and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights'.[255] At the same time, it asserted that the protection of fundamental rights should be strengthened by making these rights more visible in the Charter in accordance with social changes, social progress and the development of science and technology.[256] When the Lisbon Treaty came into force in December 2009, the Charter was legally binding on EU Member States. Since then, the formal status of human rights in the EU legal order has changed. It acquired the status of primary EU law and its provisions have

[254] Hijmans, H. (2018). *The European Union as Guardian of Internet Privacy – The Story of Art 16 TFEU*. Springer International Publishing, p. 560.
[255] EU Charter, Preamble.
[256] Ibid.

"the same legal value" as treaty provisions.[257] The incorporation of the EU Charter into the EU law enhances the role of human rights in EU law. The Charter covers the political, economic, civil and social rights of people within the EU by integrating the common international obligations and constitutional traditions of all Member States. The EU Charter also safeguards so-called 'third-generation' fundamental rights, such as data protection and bioethics, including the prevention of the misuse of large data sets collected by organizations on individuals' online. Nowadays, different organizations will use big data analysis to enhance competitiveness, innovation, market forecasting, scientific research and decision-making.

Article 51 of the EU Charter sets out that all Member States and EU institutions must respect and guarantee all the rights of the Charter when implementing EU law.[258] Therefore, when actions are taken within the scope of EU law, it is binding on EU institutions and Member States. The European Commission supervises the EU Member States' compliance with the EU charter under the control of the CJEU, and can initiate infringement proceedings in case of breach. All EU law provisions and national laws should be interpreted in accordance with EU Charter obligations.[259] Consequently, a significant function of the EU Charter is to guide the implementation and interpretation of EU laws, including the GDPR.

From 2000 to 2009, the EU Charter had no legally binding force and was still on the verge of legal limbo. Nevertheless, EU legislators demonstrated that they are aware that the text contained at least two separate provisions, particularly those relating to the protection of personal data, although it might not be sure of the relationship between them. There are two Articles of the EU Charter directly related to the protection of personal data: Article 7 on the right to respect private and family life, and Article 8 on the right to protection of personal data. Article 7 of the EU Charter is regarded as a relevant article consistent with Article 8 of the ECHR. Although some European countries had recognized the right to data protection, this is the first time that a supranational

[257] Article 6 (1) TEU.
[258] EU Charter, Article 51
[259] Carrera, S., Fuster, G. G., Guild, E., & Mitsilegas, V. (2015). Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights. Brussel : CEPS.

instrument has established these two rights. The preamble to the e-Privacy Directive,[260] also states that it seeks 'to ensure full respect for the rights set out in Articles 7 and 8 of that Charter'.[261]

Privacy rights and right to data protection are closely related, but they are not the same. The scope and limitations of these two rights are different.[262] As mentioned in Opinion 4/2007 on Personal data of Article 29 Working Party: "the Charter of Fundamental Rights of the European Union enshrines the protection of personal data in Article 8 as an autonomous right, separate and different from the right to private life referred to in Article 7".[263]

Article 7 of the EU Charter states that 'everyone has the right to respect for his or her private and family life, home and communications.'[264] This provision undoubtedly echoes Article 8 of the ECHR. At the same time, the Charter 's Article 7 needs to be combined with Article 52 of the charter to consider the scope of guaranteed privacy rights. In this sense, Article 52(1) of the Charter sets out that any limitation on its recognized rights must be provided by law, respect the essence of the right and, 'subject to the principle of proportionality', be made only if necessary and genuinely meets the objectives of general interest recognized by EU or the need to protect the rights and freedoms of others.[265] As interpreted by the ECtHR, this provision echoes, to some extent, the definition of legitimate interference in respect of the right to private life authorized by Article 8 (2) of the ECHR, but it is not identical. For example, Article 52(1) of the EU Charter extends the possible purposes foreseen in Article 8 (2) of the ECHR to justify limitations to meeting any EU objective of general interest.[266] These objectives may include those purpose not explicitly specified in Article 8 (2) of the ECHR as legitimate grounds justifying to interfere with respect of the right to private life.

---

[260] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201/37).
[261] Directive 2002/58/EC, Recital 2.
[262] See Joined Cases C-402/05 P and C-415/05 *P Kadi and Al Barakaat International Foundation v Council and Commission*, ECLI:EU:C:2008:461, para. 285.
[263] http://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf
[264] EU Charter, Article 7.
[265] EU Charter, Article 52(1).
[266] Fuster, G. G., & Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. International Review of Law, *Computers & Technology, 26(1),* 73-82.

In addition, Article 52 (3) of the EU Charter establishes that the Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. [267] It is clear from this provision that since Article 7 of the EU Charter mirrors Article 8 of the ECHR, the meaning of the two provisions should be considered the same to the extent that they correspond to each other. The rights guaranteed by Article 7 of the EU Charter shall correspond to those guaranteed by Article 8 of the ECHR. This means, therefore, that the limitations that might legitimately be imposed on Article 7 rights of the Charter are equivalent to the intervention described in Article 8 (2), of the ECHR.[268]

The case law of ECtHR on Article 8 of the ECHR provides crucial guidance on its scope and the requirements applicable to legitimate interferences in respect of the right to privacy life. The CJEU in Luxembourg, in its Rundfunk judgment, specifically emphasized the relevance of Article 8 of the ECHR and the right to privacy for the interpretation of EU personal data protection.[269]

Before the creation of the EU Charter, EU law recognized those basic rights accredited by international treaties (such as ECHR) signed by Member States, and those rights identified as common to the constitutional tradition of Member States. The EU institutions then considered that it was necessary to strengthen this fundamental rights protection system by developing a specific list of EU rights, which need to include the rights that have been confirmed to exist, and also recognize some that are considered non-existent but are deemed necessary according to the needs of the contemporary.[270] Hence, the EU established the right to protect personal data under Article 8 of the Charter.

[267] EU Charter, Article 52 (3).
[268] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing, p. 206.
[269] See Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v. Österreichischer Rundfunk*, ECLI:EU:C:2003:294, para. 68.
[270] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing, p. 206.

Article 8 of the EU Charter states that everyone has the right to the protection of personal data concerning him or her. The individual rights under Article 8 of the Charter could have an important impact on the protection of patient data in cross-border healthcare. Although the right of data protection guarantees a data protection system beyond individual rights, the individual rights of data subjects are still a significant part of the system.[271]

Article 8 of the Charter enshrines that personal data can only be processed according to the legal ground provided by law or the consent of the individual concerned.[272] This involves the principle that legal processing can only be based on legitimate ground. It can be understood that such ground could be the individual's consent, otherwise it must be a ground laid down by law. In addition, circumstances where a legal basis is required to process personal data generally applies to any data processing activity, including the collection, storage, or access of data.[273] In fact, there are some rights that are not mentioned in Article 8 of the EU charter, such as the right to obtain information, and the confidentiality obligation. These rights as data subjects can also be regarded as elements of established principles of processing personal data.[274] Moreover, It is necessary for private sectors to process and ultimately store data on legitimate ground, and when public authorities want to access data held by private sectors, such access should also be based on legitimate ground.[275] Finally, it also states that individuals have the right to access and rectify inaccurate data,[276] and that compliance with personal data protection rules should be monitored by an independent data protection authority.[277] [278]

[271] Bredenoord, A. L., Mostert, M., Van Delden, J. J. M., Van Der Slootb, B. (2018). From privacy to data protection in the EU: Implications for big data health research. european Journal of health law, 25(1), 43-55.
[272] EU Charter, Article8 (2).
[273] Ibid.
[274] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing, p. 205.
[275] Carrera, S., Fuster, G. G., Guild, E., & Mitsilegas, V. (2015). Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights. Brussel : CEPS.
[276] EU Charter, Article8 (2).
[277] Ibid. Article8 (3).
[278] The CJEU has underlined the importance of the independence requirement and made several rulings on this issue. See Case C-518/07 *European Commission v Federal Republic of Germany*, ECLI:EU:C:2010:125; C-614/10, *European Commission v Republic of Austria*, ECLI:EU:C:2012:631.

This Article is also applicable the provision of Article 52 (1) of the Charter, which describes possible legal limitations on the rights it establishes. In principle, Article 52(3), which applies to EU Charter rights corresponding to ECHR rights, has nothing to do with Article 8 of the Charter. The reason is that it cannot be insisted that there is a right in the ECHR corresponding to the right to protect personal data, which is already reflected in Article 7 of the EU Charter. It is a right other than respect for the right to private life. However, the case law of ECtHR on limitations on data processing under Article 8 of ECHR is directly related to the interpretation of Article 8 of the EU Charter.[279]

As mentioned in the preamble to the EU Charter, it is necessary to make the fundamental rights of the EU 'more visible' in order to enhance the protection of those rights.[280] However, some scholars believe that the Charter does not reaffirm or make the data protection right more obvious.[281] It can be understood that such a data protection right was actually created in addition to privacy right. It is rooted in pre-existing instruments. In addition, in the case law of the CJEU, the impact of the right to data protection as an independent right has become increasingly apparent.[282] Moreover, Article 1(2) of the GDPR clearly states that the data protection Regulation 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.' We can also see that common terms such as 'design privacy' and 'privacy impact assessment' have been replaced by 'design data protection'[283] and 'data protection impact assessment'[284] in GDPR. This shows that data protection has become particularly important as a separate right in the EU.

[279] It can be found that the CJEU refers to the case law of the ECtHR when the rights to respect private life and personal data protection enshrines in Articles 7 and 8 of the EU Charter is applied: Legal Service of the European Parliament (2015), Legal Opinion in Reference to Questions Relating to the Judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* – Directive 2006/24/EC on Data Retention – Consequences of the Judgment, p. 9.
[280] EU Charter, Preamble.
[281] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer International Publishing. p. 2.
[282] Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law, 3(4), 222-228.
[283] Article 25, GDPR.
[284] Article 25, GDPR.

In the context of this rapid development of technology and big data, In March 2017, the European Parliament voted on a non-legislative resolution about the fundamental rights implications of big data in 2017, including privacy, data protection, non-discrimination, security and law enforcement. The resolution seeks to promote cooperation between authorities, regulators and the private sector, as well as the use of security measures such as anonymity technology, default privacy, encryption and mandatory privacy impact assessment.[285]

Nowadays, the EU and its Member States need to fulfil their obligations on the right to data protection under the GDPR and both public authorities and private sector need to interpret GDPR according to the fundamental rights. However, increasing emphasis on data protection in GDPR does not necessarily reduce the relevance of privacy, especially in the context of health research and cross-border healthcare. After all, the data involved in cross-border medical care are often sensitive to private life, such as data concerning health and genetic data. Therefore, for patients in cross-border healthcare, both privacy right and right to data protection add important layer of protection to medical records.[286] We will discuss in detail below how the GDPR protects patients' medical records in cross-border healthcare.

4.2.2 EU secondary Law – GDPR

After a long and intense reform, the EU adopted a new Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) on 27 April 2016. It is one of the greatest achievements in recent years and now recognized as law across the EU. Since then, Data Protection Directive of 1995 had been replaced, which was adopted at a time when the internet was in its infancy. This data protection Regulation and the e-Privacy Directive can jointly provide stronger protection for patient's health data, especially when EHRs are transmitted across borders.

[285] European Parliament (2017). Report on fundamental rights implications of big data: Privacy, data protection, non-discrimination, security and law- enforcement (2016/2225- INI).
[286] Bredenoord, A. L., Mostert, M., Van Delden, J. J. M., Van Der Slootb, B. (2018). From privacy to data protection in the EU: Implications for big data health research. *European Journal of health law*, 25(1), 43-55.

The GDPR is the most comprehensive and progressive data protection legislation in the world, which was fully applicable to the whole EU. It has been updated to cope with the implications of the digital era and to create new rights for individuals in the digital environment. Globally, data protection laws are growing faster and faster. Many of these laws are strongly influenced by the EU rules, which have long been considered the gold standard in data protection law. Through the GDPR, the EU reaffirms its protection of the fundamental rights and freedoms of individuals, especially the rights related to the protection of personal data, including the specific fundamental rights for the protection of personal data provided in the TFEU and Charter of Fundamental Rights of the EU.[287]

In terms of legal principles, the GDPR maintains the approach of previous Directive 95/46/EC, which sets out general principles to be followed in any case of personal data processing, as well as for the purpose of archiving in the public interest, regardless of the type of personal data, including the processing of sensitive personal data. The GDPR outlines seven important data protection principles in Article 5 that must be followed when processing personal data.[288] In general, these principles involve:

- **Fairness, lawfulness and transparency** - personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.[289]
- **Purpose limitation**- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[290] It must be clearly stated what this purpose is and only collect the data needed to accomplish it.
- **Data minimization**- personal data processed is adequate, relevant and limited to the necessary data related to the processing purpose.[291]
- **Accuracy**- every reasonable step must be taken to update, erased or rectified incorrect or incomplete data without delay.[292]

[287] GDPR, Recitals 1
[288] GDPR, Article 5.
[289] GDPR, Article 5(1)(a).
[290] GDPR, Article 5(1)(b).
[291] GDPR, Article 5(1)(c).
[292] GDPR, Article 5(1)(d).

- **Storage limitation**- stored in a form that allows identification of the data subject for no longer than the time required to process personal data.[293]
- **Integrity and confidentiality**- using appropriate technical or organizational measures to secure personal data, prevent unauthorized or illegal processing, and prevent accidental loss, destruction or damage. [294] This principle can be implemented technically using coding techniques such as pseudonymisation, cryptography or anonymization technics.
- **Accountability**- this is a new principle under the GDPR, which states that the controller should be responsible for and be able to demonstrate compliance with the general principles of data processing.[295] This requires, in particular, that the controllers or their representatives in the EU, as well as processors maintain clear and secured records of any data processing activities that have been performed in order to demonstrate compliance with the GDPR.

These principles are essential to protect citizens' health data. According to the interpretation of the Regulation, 'data concerning health' is defined as personal data relating to the past, current or future physical or mental health of a natural person, including the provision of health care services, which reveal the health status of the natural person.[296] In addition, data concerning health is classified as special categories of personal data (called sensitive data) .[297] Health data that merit higher protection should only be available and processed for health-related purposes if it is necessary to achieve the benefits of natural persons and society.[298] EU or national legislation should provide for specific and appropriate measures to protect the fundamental rights and personal data of citizens, and allow Member States to impose further conditions on the processing of health-related data. However, when these conditions apply to the cross-border processing of health data, the free movement of such personal health data within the EU should not be impeded.[299]

[293] GDPR, Article 5(1)(e).
[294] GDPR, Article 5(1)(f).
[295] GDPR, Article 5(1)(g).
[296] GDPR, Recitals 15.
[297] GDPR, Article 9(1).
[298] GDPR, Recitals 53.
[299] Ibid.

The fundamental right of patients to protect their health data is an important issue in a variety of situations, such as healthcare obtained through e-health, treatment provided in a cross-border healthcare context, and a variety of medical-related research. On the one hand, health data are 'sensitive data' and subject to additional protection under EU law. It can be inferred that unauthorized disclosure of personal health-related information is likely to have a negative effect on the patient's personal, family life and even future career. On the other hand, the processing of health data is critical to the safety of patients, the normal provision of medical services, and the conduct of related research such as clinical trials and epidemiological studies. Also, policy and research on the processing of health data can improve public health. Thus, it can be considered that the use of patients' personal health data plays a positive role in advancing medical research and healthcare practice to some extent. Due to the electronic health records of patients include all data relating to the health of the individual, the nature of the data is particularly sensitive to fundamental rights and freedoms and may pose serious risks in the process, so health data merits special attention and protection.[300]

Article 9 (1) GDPR prohibits the processing of a series of special categories of data including health data. Nevertheless, the prohibition is still subject to the exceptions provided in Article 9 (2) GDPR, which provides a legal basis for the processing of sensitive personal data. When explicit and unambiguous consent is given for "one or more specified purposes"[301] or "it is necessary to protect the vital interests of the data subject",[302] the processing is lawful. Furthermore, sensitive data can be processed when the 'processing is necessary for the purposes of preventive or occupational medicine, . . . medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional'.[303] Other grounds for handling sensitive data in the health domain relate to 'reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of

[300] European Patients Forum. The new EU Regulation on the protection of personal data: what does it mean for patients. A guide for patients and patient's organisations.
[301] GDPR, Article 9 (a).
[302] GDPR, Article 9 (c).
[303] GDPR, Article 9 (h).

quality and safety of health care and of medicinal products or medical devices'.[304] Finally, the data processing is allowed when: necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall respect the essence of the right to data protection and provide measures to safeguard the fundamental rights and the data subject's interests.[305]

The consent rule derogates from the prohibition on the processing of health data under Article 9 (2) (a) of GDPR, which itself has been derogated from in Article 6 (4) GDPR. Article 6 (4) GDPR provides that the processing of another purpose is lawful if it is compatible with the purpose for which the personal data are initially collected.[306] This provision should in turn linked to the provisions of Article 5 (1) (b) GDPR, that is, "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not considered to be incompatible with the initial purposes".[307] Therefore, a comprehensive reading of Articles 6 (4) and 5 (1) (b) GDPR suggests that if health data is processed for the purpose of a secondary research, processing is legal for it is per se consistent with the initial purpose, even though the data processing is not based on the consent of the data subject.[308]

Prior to the implementation of GDPR, the Directive 95/46/EC on the protection of personal data made a significant contribution to the harmonization of EU data protection rules.[309] Nevertheless, with the development of modern technology, the EU is aware of the need for a new data protection regulation to take into account the changes caused by new technologies. For example, the Internet and electronic means are increasingly used in healthcare and telemedicine. New technologies (such as e-health) provide a great deal of opportunities for more efficient collection, use, and sharing of health data, as well as improve the quality, safety, and efficiency of healthcare systems. However,

[304] GDPR, Article 9 (j).
[305] GDPR, Article 9 (j).
[306] GDPR, Article 6 (4).
[307] GDPR, Article 5 (1) (b).
[308] Schneider, G (2019). Disentangling health data networks: a critical analysis of Articles 9(2) and 89 GDPR, *International Data Privacy Law*, Volume 9, Issue 4, P. 268. https://doi.org/10.1093/idpl/ipz015
[309] Hustinx, P (2014). EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation.

they undoubtedly pose new challenges for privacy and data security. In 2015, the special Eurobarometer on Data Protection showed that most citizens felt uncontrollable about what happened to their data.[310] Therefore, the new GDPR attempts to solves this problem by empowering EU citizens with more information and rights. The Directive 95/46/EC did not directly apply to EU Member States only through the provisions of national law to comply with the it (which causes many differences in interpretation between Member States), but GDPR as a regulation can directly apply to Member States.[311] In addition to the specific exceptions in the text of the GDPR allowing Member States to take further measures, the same provisions apply to the whole EU. This has a positive impact on the development of cross-border healthcare and the promotion of cross-border medical research.

4.2.3 Soft Law

Soft law refers to non-legally binding instruments, such as opinions, recommendations, codes of conduct, guidelines and communications. Although they are not legally binding, they can set standards and play an important role in increasing the value of international agreements or other legally binding instruments. Soft law can produce certain legal effect. It is believed that soft law may affect the development and implementation of policies precisely because it exercises informal 'soft' influences through projects, which illustrate the possibilities and generate persuasiveness. Therefore, soft law is sometimes seen as a more flexible tool to achieve policy goals. The recommendations and resolutions of the Council of Europe are also soft law and represent the views of the Parliamentary Assembly of the Council of Europe.

The opinion of the European Data Protection Supervisor (EDPS) is also soft law, which is an independent supervisory authority dedicated to protecting personal data and privacy. EDPS needs to advise EU institutions and bodies on all matters related to the processing of personal data. In particular, the European Commission needs to seek the views of EDPS on legislative proposals,

[310] Special Eurobarometer 431 on Data Protection, June 2015: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

[311] Díaz Díaz, E. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions. Church, Communication and Culture, 1(1), 206-239.

international agreements and acts that have an impact on data protection and privacy.[312] It will also intervene before the ECJU to provide expert advice on the interpretation of data protection laws. Also, the opinions and recommendations of the Article 29-Working Party play a crucial role in protecting personal data.[313] It is an advisory body composed of representatives from the data protection authorities of EU Member States, the European Data Protection Supervisor as well as a representative of the European Commission. However, the mission of the Article 29 working group was replaced by the European Data Protection Board (EDPB) until May 25, 2018.[314] The EDPB consists of the head of each Data Protection Authority and of the EDPS or their representatives. The European Commission participated in the EDPB meeting without voting rights.[315]

4.3 Exchange of EHRs across the EU

4.3.1 EHR in the EU

Citizen's EHR is crucial to cross-border healthcare in the EU. If patients can check their own EHR in the Member States of treatment during cross-border healthcare, or healthcare professionals can check the EHR of patients in telemedicine, the treatment efficiency of patients and the work efficiency of healthcare providers will be greatly improved. In the series of policies introduced in the third Chapter, it is obvious that the significant role of e-health in the healthcare system has been widely recognized at the EU and Member States levels. The European Commission is supporting the implementation of e-health in the healthcare system through different activities and initiatives, including the deployment of EHR. At the same time, significant investments have been made in the deployment of EHR over the decades. In the 1990s, this work mainly focused on efforts to maximize the development and application of EHR in the local / regional / national healthcare system or healthcare point.[316] Although this work is still ongoing, the current focus is to create conditions and develop legal certainty for cross-border access to health data. However, whether it is the focus of work in the early stage or the task currently being concentrated, the main

[312] https://edps.europa.eu/about-edps_en.
[313] The composition and purpose of Article 29 Working Party was set out in Article 29 of the Data Protection Directive.
[314] GDPR, Recitals 139.
[315] GDPR, Articles 63 to 76 and Recitals 135 to 140.
[316] Peetso, T. (2017). Addressing eHealth at the EU Level. In *New Perspectives in Medical Records Meeting the Needs of Patients and Practitioners*, Springer International Publishing.

goal of both is to enable healthcare professionals to quickly access and share patients' important information (the patient's own health data), so as to improve the efficiency and quality of patients' access to healthcare. The following EU-wide documents and projects aim to support this objective:

1. The Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems, which provides guidelines for interoperable EHR systems and allows cross-border exchange of patient health data within the Community for the legitimate healthcare purposes. It is the first document published by the European Community providing the steps that EU Member States should take to set up a compatible EHR system.
2. The European Commission issued the Green Paper on mobile Health on 10 April 2014. Some mHealth instruments may facilitate access EHR and support data management, and thus help to improve health outcomes.[317] The results of public consultation of Green Paper on mHealth showed that attention should be paid to legal clarity, privacy and safety, patient safety.[318]
3. On 6 May 2015, the European Commission published the Communications for 'The Digital Single Market strategy', which aimed to complete the work of the DSM as one of the ten political priorities of the Commission.[319] The strategy includes 16 initiatives, some of which directly or indirectly enhance the development of e-health.
4. The e-health Action Plan 2012-2020 also covers actions related to the EHR. Firstly, the Action Plan seeks to find an e-health interoperability framework based on the e-health roadmap and the general European interoperability framework. The e-health (including EHR) interoperability has four layers: semantics, technology, organizational and legal, which are the regular and significant items in e-health network agenda. Secondly, the European Commission launched a study under the Health Programme 2014-2020 to review the laws of Member States on EHR in order to make recommendations on the legal level of interoperability for e-health network.[320] This study showed that there were significant differences in some aspects of EHRs deployed in Member States with an interoperable

[317] Ibid.
[318] https://ec.europa.eu/digital-agenda/en/news/mhealth-europe-preparing-ground-consultation-results-published-today.
[319] https://ec.europa.eu/digital-agenda/en/news/digital-single-market-strategy-europe-com2015- 192-final
[320] 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.

infrastructure that allowed different healthcare providers to access and update patient's health data to ensure their healthcare continuity.[321] In terms of the methods adopted to regulate EHR, some Member States have formulated specific rules for EHR, while others are based on the general legislation on health records and data protection.[322] In addition to discussing the national laws regulating the EHR, the study also discussed the security, access and update, patient consent, patient's rights to data, liability of health professionals, secondary use of health data and archiving. In view of these aspects, the final report also gives corresponding recommendations at the national and EU levels. Thirdly, research and innovation on health care for the ageing population in the implementation of the strategy of 'European Innovation Partnership on Active and Healthy Ageing' aims to provide personalized care for the ageing population. Obviously, comprehensive EHR plays a core role in personalized health care.

However, many European citizens currently would like to have more access to their own health data during cross-border healthcare, which is often limited, because these data are usually difficult to track and scattered. If a person is not in his/her home country, his/her medical information is not accessible, which may have adverse effects on his/her diagnosis and treatment. Following its mid-term review on the implementation of the DSM strategy, the Commission conducted a public consultation.[323] Through this consultation, the important challenges of digital health were identified and the need for further work was basically recognized. The heterogeneity of EHRs is considered to be one of the main barriers to the exchange of health data and the promotion of digital health care in Europe. Meanwhile, it also faces the challenges of access to health data and the lack of technical interoperability. The consultation also identified issues related to the electronic sharing of health data, such as the cybersecurity risks, risk of privacy breaches, and data quality. Therefore, one of the priorities of the Communication on enabling the digital transformation of health and care in the DSM is to enable EU citizens to securely access and share their health data across borders. This shows that the Communication also aims to encourage and

[321] Ibid.
[322] Ibid.
[323] Public Consultation on Transformation of Health and Care in the Digital Single Market, carried out between July and October 2017.Available at: https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market_en

develop the exchange of patients' EHRs to improve the efficiency and continuity of cross-border healthcare for patients.

At present, this exchange is limited to e-Prescriptions and patient summaries, excluding EHRs. Most citizens are not yet able to access or securely share their health data across borders. The Committee believes that it is necessary to gradually expand these two use cases by supporting the development and adoption of the European EHR exchange format. In February 2019, the European Commission adopted a Recommendation on the European Electronic Health Record exchange format, which supports the EU's digital transformation of healthcare by seeking to unlock cross-border health data flow.[324] The Recommendation seeks to enable citizens to securely access and exchange their health data between EU Member States. In particular, it aims to create a European format that can help citizens quickly access their health data and share it with healthcare professionals, for instance, when receiving emergency treatment in another Member State. Currently, in addition to the patient summaries and e-Prescriptions in the health records can be interoperated between EU Member States, the European Commission recommends that Member States extend health information into three new areas of EHR: laboratory results, medical imaging and report, as well as hospital discharge reports.

Additionally, the highest standards of security and data protection are essential for the development and exchange of EHR, which are also the core of this Recommendation. The GDPR requires the protection of patient health data to ensure its confidentiality, availability and integrity. The exchange of EHR requires full compliance with the GDPR. Therefore, the system must be secure and trusted, and data protection integrated by design and by default. This is based on a range of digital solutions across Europe, as well as common methods by governments and institutions. Besides, the Directive on security of network and information systems (the NIS Directive) provides a series of measures to ensure that the network and information systems (including health information systems) are secure to a certain extent.[325] Access, security and trust in EHR systems

[324] Commission Recommendation a European Electronic Health Records exchange format. Brussel, 6.2.2019 C (2019) 800 final.
[325] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union 2016 O.J. (L 194/1).

should also be strengthened through the use of secure electronic identification and authentication means as set out in the elDAS Regulations. The elDAS Regulation provides that under the electronic identity authentication scheme of Member States, citizens can obtain online public services (including medical services and health data) from abroad by using recognized electronic identity authentication means. It also sets rules for trust services such as electronic signatures and electronic seals in order to minimize the risk of possible tampering and abuse, so that health data can be managed and exchanged more secure.

The specification for the EHR exchange format should be based on open standards and appropriate technical expertise. The European Commission also needs to monitor the cross-border interoperability of EHR systems, and once implemented, the European EHR exchange format will be adopted throughout the EU.

The Commission also raises finding from the CEF and Horizon 2020 programmes for the European EHR exchange format and further development of infrastructure for e-health services. Health authorities can use targeted EU funding tools (e.g. the European Fund for Strategic Investments) to deploy interoperable EHRs at the national and regional level, so that citizens can access their health data. The European Commission will further support the e-health Digital Services Infrastructure to provide new services for citizens and healthcare providers, such as the exchange of EHRs using a standardized European EHR exchange format, and the use of health data from these patients for public health and research. It is also planned to mobilise funding from relevant projects to obtain further support to encourage cross-border exchange of health data and its possible expansion (especially to full EHR) between EU Member States.[326]

4.3.2 Patient's rights on the EHR

4.3.2.1 Information and access

The right of access is a data subject right, which gives people the right to access the data collected in the EHR and the information about how to process their personal data. This right is already

[326] Ibid.

mentioned in Article 8(2) of the EU Charter. The ECtHR held that the right to access information about personal data stem form the need to respect private life.[327] Under Article 15 of GDPR, patient have the right to know the purpose of his/her own medical data processing,[328] and have the right to access a copy of his/her own health records.[329] Additionally, the data controller must inform the patient of the details of the processing, such as how the data are required,[330] and with whom the data are shared[331].

Patient has the right of access to his/her health data which have been collected about themselves and to exercise this right at reasonable intervals to facilitate their access to his/her previous health information during cross-border healthcare. These health data include data in patient's medical records containing information such as diagnosis, test results, assessment by the healthcare professionals, and any treatment provided.[332] Hence, every patient should have the right to know and to obtain communications, particularly with regard to, for example, the purpose for which such health data are processed, the period for which data are processed (where possible), and the results of such processing.[333] Where possible, the controller shall provide remote access to the secure system so that the patient can have direct access to his or her personal health records, but this right shall not adversely affect the rights or freedoms of others.[334] In particular, there needs to be a balance between the right of access and copyright.[335]

The controller should also provide the means for making requests electronically, particularly in cases where personal data are processed electronically[336] (such as in the case of EHR). The patient's access request should be executed as soon as possible and not later than one month after

[327] See Case of Gaskin v. the United Kingdom, App No. 10454/83, 7 July 1989, para. 39.
[328] GDPR, Article 15(1)(a).
[329] GDPR, Article 15(3).
[330] GDPR, Article 15(1)(g).
[331] GDPR, Article 15(1)(c).
[332] GDPR, Recital 63.
[333] Ibid.
[334] Ibid.
[335] Sobolčiaková, A. (2018). Right of access under GDPR and copyright. *Masaryk University Journal of Law and Technology*, 12(2), 221-246.
[336] GDPR, Recital 59.

the request.[337] If necessary, it can be extended by two further months, but the reason for the extension shall be provided.[338]

Although patients have access to their EHRs, data controllers also need to take steps to prevent unauthorized access to health records. Therefore, it is important that the controller use all reasonable measures or technical means to verify the identity of the person providing an access authorization or making an access request, especially in the case of online services and online identifiers.[339] This is necessary to protect data and prevent data disclosure.

When healthcare providers or researchers want to access the patient's EHR, it is necessary to obtain the his/her consent (unless it is an exception within the scope of the law). In the processing of personal data concerning health in EHR, a free consent is considered to be a voluntary decision that he/she has the ability to make without any psychological, economic or social coercion. Hence, Therefore, in processing of health records, informed data subjects should make real choices within the scope of their autonomy in order to make a valid consent.

Nonetheless, there are still some restrictions on the right to access when personal data are stored by public authorities, In the case Leander v. Sweden, the ECtHR concluded that, in some cases, right to access may be restricted.[340] On the one hand, it overrides the legal interests of others. Data processed for scientific purposes, on the other hand, may not be subject to undue time restrictions.[341]

4.3.2.2 Rectification, erasure and data portability

Sometimes, patients will ask to correct or delete incorrect personal data from their EHRs. Hence, GDPR not only gives data subject the right to rectification, but also provides them the right to

[337] GDPR, Article 12(3).
[338] Ibid.
[339] GDPR, Recital 64.
[340] See Case of Leander v. Sweden, App No. 9248/81, 2 March 1987.
[341] See Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, ECLI:EU:C:2009:293, para 59.

erase the data. The retention of such data violates the laws of the Union or the Member State to which the data controller is subject. Right to rectification give the patients power to request modification of their personal data if they believe their personal data are inaccurate or not up to date.[342] From the essence of this right, it can ensure the data of patients to be updated effectively, and avoid the diagnosis mistakes of healthcare providers due to the wrong information. However, this is not an unconditional right and depends on the specific circumstances of each case. The relevant disputes can be resolved by adding supplementary statements to the patient 's medical record, and some inaccurate patient data should be recorded.[343] For instance, a patient thinks that the diagnosis of "anxiety disorders" in their medical records is inaccurate. The result of this diagnosis is the opinion of the healthcare provider, but the patient has the right to add an explanation to his/her medical record, stating that he/her does not agree with the diagnosis of the healthcare provider at the time, but the contemporaneous record and clinical diagnosis by healthcare provider need not be erased.

Another right to erase, known as the "right to be forgotten", refers to the patient's right to request the erasure of personal data when it is no longer needed for the purpose of collection or other processing.[344] When the consent is withdrawn by the patient himself/herself [345], or the patient objects to the processing of his or her personal data,[346] or the processing of the patient's personal data does not comply with this Regulation,[347] the basis for the legal processing of the data no longer exists. Nevertheless, if necessary, it is legal to further retain personal data in EHR. For example, data processing is based on the public interest in the field of public health,[348] or in order to fulfill legal obligations,[349] perform tasks for the public interest[350] or exercise the official authority given to the controller,[351] or archive for the public interest, scientific or historical research

[342] GDPR, Recitals 39, 59, 65, 73 and Article 5(1)(d), 16.
[343] ICGP Data Protection Working Group (2018). Processing of patient Personal Data: A Guideline for General Practitioners.
[344] GDPR, Article 17(1)(a).
[345] GDPR, Article 17(1)(b).
[346] GDPR, Article 17(1)(c).
[347] GDPR, Article 17(1)(d).
[348] GDPR, Article 17(3)(c).
[349] GDPR, Article 17(3)(b).
[350] Ibid.
[351] Ibid.

purposes,[352] defend legal claims.[353] In a word, according to the principle of accountability, the controller must prove that patients' health data processing has a legal basis, otherwise the processing must stop. Additionally, the right to erasure of health records is not an absolute right and restrictions may apply under Article 23.1(g) of GDPR. This need to be examined de facto.

In addition, according to the Article 20 of GDPR, patients have the right to obtain their personal data[354] and transfer their personal health data directly from one controller to another if technically feasible (data portability).[355] Unless otherwise required by national law, medical institutions(such as hospitals) and other healthcare providers must be prepared to provide patients with electronic health data in the appropriate format on request so that patients can choose to consult other healthcare providers.[356] Copies of patients' data records must be provided free of charge, except for further copies or in the case of "manifestly unfounded or excessive" requests for information.[357] This data portability is usually related to the control of personal data, which is part of the fundamental right of data protection under the Article 8 of the EU Charter. However, Article 8 of the EU Charter does not explicitly refer to the portability of data, while it explicitly includes the parallelism with other provisions of the GDPR.[358] Moreover, the right to data portability cannot be seen as an extension of the right of access explicitly referred to protected under the Article 8 (2) the EU Charter.[359] The scope of right to data portability extend beyond access to certain aspects, such as what is being provided to patients as well as in what format. GDPR does not require a specific file format for data portability, but Article 29 Data Protection noted that "a format that can only be read subject to costly licensing constraints would be considered inadequate".[360] Data portability enables patients to receive a copy for their own use and transfer data to another

[352] GDPR, Article 17(3)(d).
[353] GDPR, Article 17(3)(e).
[354] GDPR, Article 20 (1)
[355] GDPR. Article 20
[356] European Society of Radiology (ESR) (2017) The new EU General Data Protection Regulation: what the radiologist should know? Insights Imaging 8:295–299.
[357] GDPR, Article 15 (5).
[358] Graef, I., Husovec, M., Purtova, N. (2018). Data portability and data control: Lessons for an emerging concept in EU law. *German Law Journal*, 19(6), 1359-1398.
[359] See EU Charter, Artivle. 8(2), "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.".
[360] Article 29 Data Protection Working Party, "Guidelines on the right to data portability" Adopted on 13 December 2016.

controller in a 'structured, commonly used and machine-readable' format.[361] This makes data portability particularly suitable for the digital context and facilitates the cross-border exchange of EHR. Meanwhile, the more extensive right to data portability is only applicable to fewer situations compared with the generally applicable access rights. It can only be invoked if the processing is carried out by automated means,[362] based on consent[363] or on a contract.[364]

Patients are entitled to obtain a copy of their health records in a format that permits the data to be transferred to another healthcare provider. Healthcare service providers should provide health records in a technically feasible electronic format or in a format available to other healthcare professionals to facilitate the treatment of patients in another EU Member State (in cross-border healthcare). When EHRs are transferred, the protocol is a powerful tool to protect patient health data. The protocol for transfer of health records means that the receiving healthcare institution provides a signed patient consent to transfer health records from the sending healthcare institution.[365] To ensure that records are securely transmitted, tools such as secure email or systems can be used to enhance security during transmission.

4.3.3 Additional obligations of the controller and processor

Whether patients' health data are collected, stored, or accessed through a database or cloud computing capacity, the security of health records must be at the top of the priority list. The reason is that any misuse can have irreversible consequences for the patients. Hence, it is the responsibility of both the controller and the processor to implement appropriate technical and organizational measures to ensure and demonstrate the level of security appropriate to the risk, and to review and update such measures if necessary. [366] These measures may include encryption or pseudonymization where necessary, which are designed to implement data protection principles

[361] GDPR, Article 20 (1).
[362] GDPR, Article 20(1)(b).
[363] GDPR, Article 6(1)(a), 9(2)(a).
[364] GDPR, Article 6(1)(b).
[365] ICGP Data Protection Working Group (2018). Processing of patient Personal Data: A Guideline for General Practitioners.
[366] GDPR, Article 24 (1).

and to incorporate these necessary safeguards into the process in an effective manner to protect the patients' rights.[367] In the event of a physical or technical accident (such as failure of computers used to collect, store and access EHRs), secure technical measures are required to restore the availability and access of personal data in a timely manner.

Physical security plays an equally significant role in the security chain, so it cannot be ignored. In addition to implementing effective security measures on the data, it is also necessary to ensure that the healthcare professionals authorized to process the patients' health records have committed confidentiality or assumed appropriate statutory obligation of confidentiality.[368] The objective of personal data protection can only be achieved by fully stimulating data controller and processor through legal means to take necessary security measures to ensure effective implementation in practice.[369]

The controller and processor should not only undertake the obligations of data security, but also assume the liability of compensation in case of accident. They should compensate any damage that the natural person may suffer as a result of processing in violation of the GDPR,[370] unless the controller or processor proves that it is not liable for the damage.[371] The concept of damage should be interpreted broadly in accordance with the case law of the CJEU.[372] In fact, most of the obligations for data protection falls on the controller. If more than one controller or processor is jointly involved in the same process, each controller or processor shall be liable for all damages.[373] Any controller or processor who has paid all the compensation may subsequently claim back part of the compensation corresponding to their part of responsibility from other controllers or processors participating in the same processing.[374] For example, in some cases, an Internet services

[367] GDPR, Article 25 (1).
[368] GDPR, Article 28 (3) (b).
[369] Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International Journal of Law and Information Technology*, 26(1), 45-63.
[370] GDPR, Article 82 (1).
[371] GDPR, Article 82 (3).
[372] GDPR, Recital 146.
[373] GDPR, Article 82 (4).
[374] GDPR, Article 82 (5).

supplier or cloud storage provider[375] may assist controller in processing patient's health data. In this case, the allocation of responsibilities may be complicated. According to the Article 29 Working Party, the primary role of the controller is to allocate responsibility. More specifically, the controller should determine who is responsible for complying with the rules, and how data subjects exercise their rights in practice.[376] In any case, it is necessary to ensure that the data subject suffering from the damage is fully and effectively compensated.

4.3.4 Health records breach handling

Under Article 4 (12), 'personal data breach' is defined as:
'a breach of security results in leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'. In the medical field, typical examples of personal data leaks collected in patients' EHRs are as follows: [377]

- loss or theft of equipment storing data;
- improper access control results in unauthorized use;
- hacker / cyber-attack;
- human error of relevant personnel (e.g. sending health records to wrong data objects);

It should be noted that breaches also include unforeseen circumstances (such as information destruction caused by natural disasters), or accidental loss of personal data (such as loss of paper documents caused by fire). However, the use of electronic processing and access to health records is now the dominant way for healthcare professionals to record the health status of patients, which largely prevents the disclosure of data caused by these two conditions.

Although relevant departments and authorities will take certain security measures to ensure the data security, no matter how many appropriate technical and organizational protection measures

[375] Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing. Document 05/12/EN WP 196, Adopted July 1st 2012. Available at: http:// www.cil.cnrs.fr/CIL/IMG/pdf/wp196_en.pdf
[376] Ibid.
[377] ICGP Data Protection Working Group (2018). Processing of patient Personal Data: A Guideline for General Practitioners.

are implemented, patients should always be aware that their data is not completely safe[378] and there is a risk that their sensitive data will be disclosed. If health records breach occurs and is not handled properly in a timely manner, it may adversely affect the natural person, such as identity theft, loss of control over his/her personal data, economic loss, damage to reputation, or any other significant social disadvantage to the natural person concerned.[379] Therefore, in case of patient's health records breach, the controller shall notify the supervisory authority competent without delay and within 72 hours after having become aware, if feasible.[380] Unless the controller can prove that the breach of the patient's data is unlikely to pose a risk to his/her rights and freedom under the principle of accountability.[381] In addition, when such breach may cause high risks to the rights and freedoms of patient, for example, the compromised EHRs were not encrypted and no measures can be taken to reduce the risk, healthcare professionals need to inform all the affected individuals.[382] The content of the notification should include the nature of the data breach,[383] the name and contact information of the data protection officer,[384] and possible consequences of the health records breach,[385] as well as the remedial measures taken by the controller to resolve the data breach.[386] The controller should not ignore that the leak of the patient's health record should be faithfully recorded, especially the impact after the breach and the corresponding remedies.

When patients receive cross-border healthcare, cross-border processing of personal health records is also involved. In accordance with Article 55 and Article 56 of GDPR, the controller is required to notify the lead supervisory authority[387] whenever a breach occurs in the context of cross-border processing and the need for notification. Thus, the question of which supervisory authority is the

[378] Raposo, V. L. (2016). Telemedicine: The legal framework (or the lack of it) in Europe. *GMS Health Technology Assessment*, 12, Doc03.
[379] GDPR, Recital 85
[380] GDPR, Article 33 (1)
[381] GDPR, Recital 85
[382] GDPR, Article 34 (1).
[383] GDPR, Article 33 (3)(a).
[384] GDPR, Article 33 (3)(b).
[385] GDPR, Article 33 (3)(c).
[386] GDPR, Article 33 (3)(d).
[387] The "lead supervisory authority" is the main authority responsible for dealing cross-border data processing activities, for instance, when the data subject complain about processing their personal data. It coordinates any investigations involving other "concerned" relevant" supervisory authority. See also WP29 Guidelines for identifying a controller or processor's lead supervisory authority. Available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

lead supervisory authority that needs to be notified is that the controller must make an assessment.[388] This will enable the controller to respond quickly to the breach and to fulfil its obligations under Article 33 of GDPR. It should be noted that the lead supervisory authority must be notified whenever there is a breach involving cross-border processing. However, it is possible that the controller may be vague and uncertain about the lead supervisory authority. If the controller has any questions about the identity of the lead supervisory authority, at a minimum, the local supervisory authority where the breach occurred should be notified.[389]

4.4 Privacy of cross-border EHR system

In 2007, the Article 29 Working Party issued the Working Document on the processing of personal data relating to health in EHR[390], and provided an explanation of privacy principles and the applicable data protection legal framework for EHR systems. The Document also described the data protection requirement for establishing the EHR system and recommended eleven specific legal protection measures to guarantee patients' data protection rights and health privacy.[391] Following the Article 29 Working Party guidance, the European Commission made Recommendations on privacy and data protection issues in the EHR systems for cross-border interoperability (cross-border EHR system Recommendation). Article 9 of GDPR prohibits, in principle, the processing of health-related sensitive data, but provides a limited exemption from this prohibition, especially when it is required for specific medical and healthcare purposes. The collection and processing of health data is particularly sensitive, and there must be a specific legal framework to address the privacy issues of these sensitive data. When implementing the cross-border interoperability of the EHR system, the processing of health-related personal data may

[388] Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679.
[389] Ibid.
[390] Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records 2 (Working Paper No. 131, 2007). Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp 131_en.pdf.
[391] Working Document on the processing of personal data relating to health in electronic health records provided recommendations on eleven topics, included respecting self-determination, identification and authentication of patients and health care professionals, authorization for accessing EHR in order to read and write in EHR, use of EHR for other purposes, organizational structure of an EHR system, categories of data stored in EHR and modes of their presentation, international transfer of medical records, data security, transparency, liability issues and control mechanisms for processing data in EHR.

create a significant new risk, which requires additional safeguards and counterbalances. Once the EHR goes online, it may not be enough to protect patients' privacy interests to maintain appropriate legal confidentiality standards in the traditional paper record environment. In addition, EU Member States should recognize that interoperable EHR systems increase the risk that health-related personal data may be accidentally exposed or easily shared to unauthorized parties.[392]

The cross-border EHR system Recommendation advocates the adoption of a comprehensive legal framework for the interoperable EHR system of Member States, which includes the protection of personal privacy in the EHR systems. This legal framework incorporates the fundamental principles of previous documents, [393] requires recognition and resolution of the sensitive nature of personal data relating to health, and provides for specific and appropriate safeguards to protect the fundamental right of personal data protection.[394] Combined with some of the requirements in the Recommendation, the current legal framework of cross-border EHR systems should especially:

- consider the alternatives of systems and storage of records according to the specific risks of data subject's rights and freedoms, so as to reflect the best practice;[395]
- make use of easy-to-use technology to let patients control and freely make decisions on the storage and disclosure of their health information, so as to ensure patients' right of self-determination. However, the decision of patients does not affect the possibility of healthcare providers to store patient data for treatment purposes;[396]
- require that EHR systems should be designed for limited personal data collection or non-collection, and use pseudonym options as much as possible. These aspects related to the required protection level should be reasonable;[397]
- provide for an assessment of the risk of information security breaches and the impact of personal data protection prior to the implementation of EHR systems;[398]

[392] Ibid. Article (12).
[393] Baumer, D. L., Chumney, W. M., Hiller, J., McMullen, M. S. (2011). Privacy and security in the implementation of health information technology (electronic health records): U.S. and E.U. compared. *Boston University Journal of Science & Technology Law*, 17(1), 39.
[394] Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review* 27(5):503-515.
[395] Cross-border EHR system Recommendation. Article(14)(a).
[396] Ibid. Article (14) (b).
[397] Ibid. Article (14) (c).
[398] Ibid. Article (14) (d).

- define which health-related information can or cannot be stored or processed electronically, and whether subsets of certain information (such as genetic data) are subject to stricter access controls;[399]
- limit that data processing can only be carried out by healthcare professionals who are reliable identified and subject to secrecy under professional or national regulations;[400]
- specify policies, security and technical rules for entities other than individuals to access EHR systems and use health data, which can be enforced by national data protection authorities and technologies;[401]
- inform patients about the implementation of EHR system so that patients can fully understand the structure of EHR and the nature of health data, and need to provide special groups (such as children and the elderly) with options to access understandable information about the systems;[402]
- provide special procedures to prevent patients from being under undue pressure to be illegally induced to disclose their personal health data in the systems;[403]
- ensure that the processing (including storage) of personal data in EHR systems is limited to jurisdictions that comply with GDPR;
- establish auditing procedures to ensure compliance with data protection obligations, such as reliable electronic identification and authentication system, and all records of data processing steps.[404]
- adopt security measures to guarantee the confidentiality of EHR systems, so as to prevent illegal alteration, destruction, unauthorized access or disclosure of personal health information in EHR systems (personal data breach).[405] In order to ensure the confidentiality of the system, breach notification procedure should be adopted. When the personal data breach may cause high risk to the rights and freedoms of patients, the

[399] Ibid. Article (14) (e).
[400] Ibid. Article (14) (f).
[401] Ibid. Article (14) (g).
[402] Ibid. Article (14) (h).
[403] Ibid. Article (14) (i).
[404] Ibid. Article (14) (k).
[405] Ibid. Article (14) (l).

controller shall inform the patients of the personal data breach in a timely manner without undue delay,[406] except in legal exceptions.[407]

Ideally, there should be a list of categories of healthcare professionals so that these professionals can access the EHR. Or it might be for each Member State to decide who should be considered as health professionals in the context of EHR exchanges within the EU.[408] Access to certain special categories of personal health data must be strictly controlled. It may be necessary to establish varying degrees of confidentiality as well as limit access to certain information to certain healthcare professionals. Then a system consisting of data modules or sealed envelopes can help achieve this goal.[409]

[406] GDPR, Article 34 (1).
[407] GDPR, Article 34 (3).
[408]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.
[409] Report of the eHealth Stakeholder Group (2013). Patient access to Electronic Health Records. Version June.

Chapter V

5.1 Challenges

5.1.1 Lack of guarantees of privacy and confidentiality

Although recognizing that traditional paper health records do not adequately ensure data protection, one of the biggest challenges in EHRs is the security of the system in terms of privacy. Privacy and confidentiality issues have always been a priority in initiatives related to e-health, especially when transmitting sensitive data from patients. The concept of a centralized supranational/national central server has attracted people's attention.[410] This powerful server aims to store the EHRs of EU citizens in a central location.[411] However, it is important to note that the health care sector is a high-risk area and arguably one of the most affected sectors. If such a centralized system is destroyed due to virus infection or other reasons, there is a huge risk of losing or leaking all personal data. When health data disclosure is involved, the health information of these patients may be accessed and modified, and there is a risk of being used or sold for commercial purposes. On the top of that, EU citizens will lack trust in the health system and reluctant to use it. From the current perspective, the exchange and transmission of health electronic records during cross-border healthcare still have the risk of being leaked.

In the past decade, there has always been an incident in which the health records of patients have been leaked. In 2010, a computer virus destroyed hospital information system at Medical Center in Bakersfield, California. This makes the medical staff busy looking for paper records to keep the healthcare flowing.[412] In addition to accessing the hospital information system, viruses can also infect clinical monitoring devices and network devices used by healthcare providers, for example. There is a high risk of data leakage due to the large amount of sensitive private data stored on the computers of healthcare providers, which is usually unencrypted. According to statistics, the UK's

[410] Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review* 27(5):503-515.
[411] Ibid.
[412] McBride, M. (2011). Cyber-Attacks against Internet-Enabled Medical Devices are New Threat to Clinical Pathology Laboratories. Dark Daily. Available at: https://www.darkdaily.com/cyber-attacks-against-internet-enabled-medical-devices-are-new-threat-to-clinical-pathology-laboratories-215/

National Health System (NHS) was once responsible for nearly a third of data breaches.[413] In 2011, researchers at the London Health Programmes said that the unencrypted records of more than 8 million NHS patients had been lost.[414] Furthermore, the records of 1.13 million patients in the United States were damaged via 110 health data breaches in the first quarter of 2018.[415] These intrusions may be caused more by hacking incidents or deliberate human factors. Most of the leaked health records can be found and purchased online through illegal markets. It should be assumed that this happens more often than we hear, because companies or some services providers are often unwilling and not obliged to let their data breaches public. [416]

Although not all of these events occurred in the EU, they can also reflect or infer the risks of EHR storage and processing. If the security measures of the system are not in place, it is likely to endanger the trust of patients in the information society. Data breaches are becoming harder to prevent and track.

The EHRs pose a challenge in ensuring that only authorized healthcare professionals can access patient-related information for legitimate purposes. Data on the disclosure of health information indicates that threats may arise not only from unauthorized access to data for economic purposes, a lack of privacy and security policies, but also from people who are legally privileged to access information by insiders. For example, Rostad and Edsburg (2006) reported that 99% of healthcare professionals were given overriding rights, while only 52% needed it. The potential for misuse of patients' health data is high, and the risks increase significantly as the system become more interconnected. In this regard, consideration should be given to allowing only healthcare providers directly involved with the patient's condition to access a part of patient's EHR on a need-to-know basis. In view of the data security concerns of these threats, it is necessary to identify these threats that frequently arise in the health sector may contribute to the development of effective information security.

[413] Jowitt, T. (2010). NHS Tops ICO List for Most Data Breaches. Silicon.co. Available at: https://www.silicon.co.uk/workspace/nhs-tops-ico-list-for-most-data-breaches-7429
[414] Doyle, E. (June 15, 2011). NHS Researchers Lose Laptop with 8 m Patient Record. Silicon.co. Available at: https://www.silicon.co.uk/workspace/nhs-researchers-lose-laptop-with-8m-patients-records-31810
[415] https://protenus.com/press/press-release/113m-patient-records-breached-from-january-to-march-2018.
[416] Mulder, T., & Tudorica, M. (2019). Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law*, 28(3), 261-274.

Under the current legal framework of data protection, there is a general uncertainty about who and how to access and modify patient's medical data and who is responsible for it. In addition, it is still difficult for all parties to judge the degree of data protection and whether the degree of protection is sufficient to transfer data to other Member States. However, overly stringent security systems and data protection rules should not impede the transfer and sharing of data in cross-border health care, nor should they impede health services.[417] As long as effective security and informed consent rules and procedures are in place, and patients are informed these when their health records are processed in another Member State.

On the other hand, the lack of privacy and confidentiality is reflected in different levels of security between the Member States. For example, although Directive 2002/58/EC on Privacy and Electronic Communications is applied uniformly in EU, there are huge differences in the interpretation and implantation of certain elements of the Directive by the authorities and courts of Member States.[418] Some Member States may be very restrictive in their interpretation of the same legal rules, while others are more flexible. This also brings serious regulatory challenges to telemedicine, especially when healthcare providers and patients are not in the same Member States.

Directive 2011/24/EU and centralized EHR system will lead to increased information exchange between the healthcare providers in different Member States. These developments indicate that the protection of health data needs to be strengthened to prevent disclosure and misuse to unauthorized third parties.

5.1.2 Lack of interoperability and information

[417] Foster, G., Holbrook, A., Perera, G., Thabane, L., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. *International Journal of Medical Informatics*, 80(2), 94-101.
[418] Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review* 27(5):503-515.

From the perspective of a series of e-health initiatives launched by the EU, the EU is vigorously developing cross-border healthcare domain in order to make it more convenient for citizens to receive medical treatment, and also to benefit citizens in the electronic field. The EU is still evolving on interoperability in e-health (four areas: legal, technical, organizational, semantic) and usability standards. There is a link between the four aspects of interoperability. The issue of legal interoperability arises when cross-border healthcare requires healthcare professionals to access patients' EHR for effective diagnosis and treatment. However, the EU does not have uniform rules or legislation on EHRs, which will lead to different Member States may have different legal requirements on the content or use of EHRs. This also leads to legal uncertainty when the EHRs are transferred across borders, and it may also require a radical change in the technical composition of EHR implementation. The lack of EU rules in this area is also the most significant obstacle to a breakthrough in the EU e-health industry.

At present, many patients and healthcare professionals do not always know how the technology works or how to deal with these health data. Lack of sufficient information will hinder their acceptance of e-health solutions. In fact, health professionals and patients should be more informed and more involved in their own health decisions. It is worth considering whether the NCPs mentioned in Directive 2011/24/EU could consider some guidance to enhance citizens' awareness of the use of EHRs when receiving healthcare across borders, thus improving the efficiency and continuity of healthcare.

5.2 Recommendations

5.2.1 Guarantee privacy and data protection

It is necessary to ensure that the system security and data are adequately protected, so that e-health solutions can be trusted and accepted by healthcare professionals and patients. With regard to the privacy protection of EHRs, Member States are not allowed to provide higher levels of protection than GDPR for patients on their territory. Whether patient's consent is needed to create and share health data should be strictly in accordance with GDPR. If consent is required, then what type of

consent is required. This is a question that needs to be decided and needs to be further clarified at the EU level.

In the context of EHRs being able to transfer across borders, it is recommended to reach an agreement on certain issues based on a set of guidelines, such as the possibility of patients modifying or deleting data from the EHR. Such guidelines may take into account some exceptions to the provision of data. For example, consider the protection of the patient or the rights and freedoms of others when allowing access to the EHR to ensure that information harmful to him/her is not provided. Although GDPR provides that the data subjects have the right to modify and erase personal data, whether the careless modification of these health data will be harmful to the diagnosis and treatment of patients. With this in mind, it is also recommended to adopt a provision that patients should not be allowed to modify their health data from EHRs that have not been inputted, so that healthcare professionals in other Member States can rely on information available.[419] In addition, if patients have the right to erase their data, the healthcare providers should be notified that some data is losing.[420] This is to ensure that healthcare professionals can timely reference the patient's past condition to make an effective diagnosis.

The EU data protection legal framework should be necessary to clarify the rules regarding the use and processing of EHRs and liability issues. In order to increase the legal certainty of this aspect, it is necessary to clarify the specific consequences of the current liability regime of data controller set out in Article 82 of GDPR on the background of EHRs. This clarification can take the form of guidelines to determine how to avoid liability, and can be further illustrated by relevant examples of possible negligence and some suggested actions.

In addition, it is essential to ensure the highest level of quality and safety. The quality and safety of the technology used in the cross-border exchange of EHRs and the related services should be carefully evaluated by the competent authorities to ensure that the risks are minimized. These techniques should also ensure effective and reliable identification of healthcare professionals and

[419] 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.
[420] Ibid.

patients. And the good infrastructure is also a necessary condition. From a technical point of view, the running system should be secure enough to prevent hacker intrusion and accidental collapse.

5.2.2 Requirements on interoperability of EHRs

There are currently no jointly agreed rules on EHR interoperability at the European level. Member States that exchange health records across borders are also more often forced to develop their own bilateral solutions.[421] But in fact, the EU has made great effort, not only in the implementation of many European projects related to it, but also in the form of "soft law" to develop European EHR rules and frameworks. The EU has now achieved the cross-border exchange of e-prescriptions and patient summaries, which is undoubtedly a big step towards the real large-scale cross-border exchange of EHRs.

The design of EHR should be user-friendly, and end users should be best able to participate in the early development of technology.[422] Moreover, the information (especially the key information) contained in the EHR should be in easy-to-understand language and layout to facilitate the operation of patients or healthcare professionals. When implementing the EHR system, the needs of vulnerable populations such as children and disabled people should also be fully considered. For example, the EHR format needs to include items that are specific to the vulnerable groups or requirements that are particularly important to them. These requirements determine the incremental functionality (that is, functionality beyond the needs of adults or normal people) that EHRs should meet the needs of the special groups.

Recommendation on a European EHR exchange format is to promote cross-border interoperability of EHRs in the EU, making it more likely to achieve the exchange of health records. Therefore, the next step is to further explain the legal issues (such as security and privacy) related to cross-border EHR between Member States and the EU so that the legal barriers between the EU and

[421] Ibid
[422] Bratan, T., Greenhalgh, T., Hinder, S., Russell, J., Stramer, K. (2010). Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. *British Medical Journal (Online)*, 341(7782).

Member States and between Member States can be reduced, and the interpretation of the legal issues can be more unified. It is necessary to explore the issues when implementing the solution of cross-border transmission of EHRs, especially in the case of fundamental legal incompatibility.

At the EU level, it would be difficult to establish an entire law on the EHR to regulate patient' data. And, within the EU''s existing data protection and privacy framework, protection of the EHR should be adequate, although there is room for improvement. In the future, it is more likely that the EU will continue to propose recommendations in this regard to reduce the differences in health records among Member States and realize their exchange. It is necessary to reach agreement on general guidelines for EHR content, such as the categories of healthcare professionals who have access to the patient's EHR, including a solution for safety certifications of healthcare professionals and their authorizations. However, such an agreement is likely to be difficult to reach in the short term. The agreement reached by the e-health Network on the patient summary guidelines indicates the correct approach, which is a good precedent.[423] Actively monitoring the implementation of the guidelines by Member States is extremely important to their ultimate success. Once the agreement is reached, it will enable greater interoperability and a higher level of security for the exchange of EHRs in cross-border healthcare.

[423] Estelrich, A., Solbrig, H., Cangioli, G., Melgara, M., Chronaki, C. (2014). European Patient Summary Guideline and Continuity of Care Document: A comparison. *Computing in Cardiology*, 481-484.

Chapter VI Conclusion

So far, the adoption of e-health solutions has remained slow, with significant differences between Member States and regions. Therefore, further actions at the EU level is essential to accelerate the meaningful use of digital solutions in the European healthcare domain, such as guidelines for cross-border exchange of EHRs.

Compared with traditional handwritten health records, EHR can improve efficiency and accuracy, reduce costs, and generally boost the quality of cross-border healthcare services. However, the increased health information collected and transmitted will lead to a significant raise in the risk of misuse of such data and violation of privacy. In addition, the diversity of quality and safety levels in Europe is a major obstacle to cross-border EHR deployment. There are other issues that need to be addressed, including uniform standards, security, confidentiality, interoperability of systems or databases, liability and compliance with data protection rules and other legislation.

The rapid advances in technology and electronic data processing have increased the risk and vulnerability of processing personal data. There is no doubt that these different levels of risks may have a significant impact on the fundamental rights and freedoms of data subjects. The network environment exposes the patient’s health data to hacker attacks and other illegal forms of processing, which damages the privacy of patient. The study also found that the main source of privacy threats is internal factors rather than external factors.

Although wide adoption of EHR has many benefits, its implementation will be difficult to achieve unless existing security and privacy risks are reduced. In fact, most EU citizens still want more access to their own health data. They are also willing to share their data on treatment or research if appropriate safeguards are in place. Thus, it is crucial to embed privacy and data protection into the whole life cycle of EHR, and it must be from the initial design stage to the final processing. In addition, the use of incompatible formats and standards in EHRs will be improved.

As the patient's health records are sensitive data, there is a greater risk of leakage in cross-border processing. Taking this into account, supervisory authorities are responsible for supervising

hospitals or other related entities to comply with data protection and privacy rules. This regulatory action can be achieved through cooperation between national and EU supervisory authorities. However, the challenges faced cannot be solved only through legal means and law enforcement by supervisory authorities. This is also a social challenge to a large extent, and social organizations (such as patient organizations) can raise awareness of protecting personal health data through various forms of activities. In this way, the protection of individuals' fundamental rights and freedoms in the exchange of health records across borders can truly be achieved.

BIBLIOGRAPHY

EU Regulations

1. Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of ministers, in Strasbourg, 15.6.1999.
2. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326/391).
3. Consolidated version of the Treaty on the Functioning of the European Union,2012 O.J. (C326/47).
4. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 2000 O.J. (L 13/12).
5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') 2000 O.J. (L 178/1).
6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201/37).
7. Council Directive 65/65/EEC of 26 January 1965 on the approximation of provisions laid down by law, regulation or administrative action relating to medicinal products, 1965 O.J. (L22/369).
8. Council Directive 89/105/EEC of 21 December 1988 relating to the transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of national health insurance systems, 1989 O. (L40/8).
9. Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices, 1990 O.J. (L 189/17).
10. Council Directive 93/104/EC of 23 November 1993 concerning certain aspects of the organization of working time, 1993 O.J. (L 307/18).
11. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, 1993 O.J. (L169/1).
12. Council Directive on the approximation of the laws of the Member States concerning the colouring matters authorised for use in foodstuffs intended for human consumption, 1962 O.J. (Spec Ed 279).

13. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, 2011 O.J. (L88/45).
14. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union 2016 O.J. (L 194/1).
15. Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices, 1998 O.J. (L331/1).
16. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD).
17. Regulation (EEC) No 1408/71/EEC of the Council of 14 June 1971 on the application of social security schemes to employed persons and their families moving within the Community, 1971, O.J. (L149/2).
18. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance. 2012 O.J. (L 316/12).
19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016 O.J. (L 119/1).
20. Regulation (EU) No 282/2014 of the European Parliament and of the Council of 11 March 2014 on the establishment of a third Programme for the Union's action in the field of health (2014-2020) and repealing Decision No 1350/2007/EC, 2014 O.J. (L 86/1).
21. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014 O.J. (L 257/73).

Other Legal Documents

1. Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority. Adopted on 13 December 2016. Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102
2. Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679. Adopted on 3 October 2017 (At last Revised and Adopted on 6 February 2018). Available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827
3. Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR). Adopted on 15 February 2007. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp 131_en.pdf.
4. Article 29 Data Protection Working Party, Guidelines on the right to data portability. Adopted on 13 December 2016. Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099
5. Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing. Adopted July 1st 2012. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
6. Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format, 2019 O.J. (L39/18) 800 final.
7. Commission Recommendation of 2 July 2008 on Cross border interoperability of electronic health records systems, 2008 O.J. (L 190/ 37).
8. Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions eHealth Action Plan 2012-2020 – innovative healthcare for the 21st century SWD (2012) 414 final.
9. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century' COM (2012) 736 final.
10. Communication from the Commission to the Council, the European Parliament, the European

Economic and Social Committee and the Committee of the Regions - e-Health - making healthcare better for European citizens: an action plan for a European e-Health Area {SEC(2004)539} COM(2004)0356 final.

11. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Europe 2020 Flagship Initiative Innovation Union COM (2010) 546 final.

12. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Modernising social protection for the development of high-quality, accessible and sustainable health care and long-term care: support for the national strategies using the "open method of coordination" COM (2004) 304 final.

13. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – The EU Role in Global Health COM (2010) 128 final.

14. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Towards Social Investment for Growth and Cohesion including implementing the European Social Fund 2014-2020' COM (2013) 83 final.

15. Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society SWD (2018) 126 final.

16. European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)) 2018 O.J. (L 263/82).

17. Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All. COM (2017) 228 final.

18. Convention for the Protection of Human Rights and Fundamental Freedoms, (1950).

19. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (1981).

20. Green Paper on mobile Health ("mHealth") COM (2014) 219 final.

21. Public Consultation on Transformation of Health and Care in the Digital Single Market, carried out between July and October 2017.Available at: https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market_en

Cases

1. ECtHR, *Airey v Ireland*, App. No. 6289/73, 9 October 1979.

2. ECtHR, *I v Finland*, App. No. 20511/03, 17 July 2008.

3. ECtHR, *Liberty and others v. the United Kingdom*, App. No. 58243/00, 1 July 2008.

4. ECtHR, *S and Marper v. United Kingdom*, App. No 30562/04 and 30566/04, 4 December 2008.

5. ECtHR, *Taylor-Sabori v. the United Kingdom*, App. No. 47114/99, 22 October 2002.

6. ECtHR, *Tyrer v. the United Kingdom*, App. No. 5856/72, 25 April 1978.

7. ECtHR, *Uzun v Germany*, App. No. 35623/05, 2 September 2010.

8. ECtHR, *X and Y v the Netherlands*, App. No. 8978/80, 26 March 1985.

9. ECtHR, *Z. v. Finland*, App. No. 22009/93, 25 February 1997.

10. Judgment of 12 November 1996, *United Kingdom v Council (Working Time)*, C-84/94, ECLI:EU:C:1996:431.

11. Judgment of 15 July 1964, *Flaminio Costa v E.N.E.L.*, 6/64, ECLI:EU:C:1964:66.

12. Judgment of 16 May 2006, *Yvonne Watts v Bedford Primary Care Trust and Secretary of State for Health*, C-372/04, ECLI:EU:C:2006:325.

13. Judgment of 16 October 2012, *European Commission v Republic of Austria*, C-614/10, ECLI:EU:C:2012:631.

14. Judgment of 2 April 2009, *A.Menarini Industrie Farmaceutiche Riunite Srl and Others v. Ministero della Salute and Agenzia Italiana del Farmaco (AIFA) (C-352/07), Sanofi Aventis SpA v. Agenzia Italiana del Farmaco (AIFA) (C-353/07), IFB Stroder Srl v. Agenzia Italiana del Farmaco (AIFA) (C-354/07), Schering Plough SpA v. Agenzia Italiana del Farmaco (AIFA) (C-355/07), Bayer SpA v. Agenzia Italiana del Farmaco (AIFA) and Ministero della Salute (C-*

356/07), Simesa SpA v. Ministero della Salute and Agenzia Italiana del Farmaco (AIFA) (C-365/07), Abbott SpA v. Ministero della Salute and Agenzia Italiana del Farmaco (AIFA) (C-366/07), Baxter SpA v. Agenzia Italiana del Farmaco (AIFA) (C-367/07) and SALF SpA v. Agenzia Italiana del Farmaco (AIFA) and Ministero della Salute (C-400/07), Joined Cases C-352/07 to C-356/07, C-365/07 to C-367/07 and C-400/07, ECLI:EU:C:2009:217.

15. Judgment of 2 February 1989, *Ian William Cowan v Trésor public*, C-186/87, ECLI:EU:C:1989:47.

16. Judgment of 20 May 2003, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk*, Joined cases C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2003:294.

17. Judgment of 21 June 2012, *Marja-Liisa Susisalo and Others*, C-84/11, ECLI:EU:C:2012:374.

18. Judgment of 21 November 2018, *Novartis Farma SpA v Agenzia Italiana del Farmaco (AIFA) and Others*, Case C-29/17, ECLI:EU:C:2018:931.

19. Judgment of 21 October 2003, *Solvay Pharmaceuticals BV v. Council of the European Union*, T-392/02, ECLI:EU:T:2003:277.

20. Judgment of 28 April 1998, *Raymond Kohll v Union des caisses de maladie*, C-158/96, ECLI:EU:C:1998:171.

21. Judgment of 3 September 2008, *P Kadi and Al Barakaat International Foundation v Council and Commission*, Joined Cases C-402/05 P and C-415/05, ECLI:EU:C:2008:461.

22. Judgment of 30 April 1986, *Commission of the European Communities v French Republic (Doctors and Dentists)*, C-96/85, ECLI:EU:C:1986:189.

23. Judgment of 31 January 1984, *Luisi and Carbone v Ministero del Tesoro*, Joined Cases 286/82 and 26/83, ECLI:EU:C:1984:35.

24. Judgment of 5 May 1998, *United Kingdom of Great Britain and Northern Ireland v. Commission of the European Communities*, C-180/96, ECLI:EU:C:1998:192.

25. Judgment of 6 November 2003, *Criminal proceedings against Bodil Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

26. Judgment of 6 September 2012, *Deutsches Weintor eG v Land Rheinland-Pfalz*, C-544/10, ECLI:EU:C:2012:526.

27. Judgment of 7 February 1984, *Duphar BV and others v. The Netherlands State*, C-238/82, ECLI:EU:C:1984:45.

28. Judgment of 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07, ECLI:EU:C:2009:293.

29. Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

30. Judgment of 9 March 2010, *European Commission v Federal Republic of Germany*, C-518/07, ECLI:EU:C:2010:125.

Books

1. Artmann, J., Dumortier, J., Giest, S., Protti, D., Stroetmann, K. A., Stroetmann, V. N., Whitehouse, D. (2011). *European Countries on their journey towards national eHealth infrastructures*. Luxembourg: Publications Office of the European Union.

2. Baeten, R., McKee, M., Mossialos, E. (2002). *The impact of EU law on health care systems*. Brussels. P.I.E.-Peter Lang.

3. Baeten, R., Hervey, T. K., Mossialos, E., Permanand, G. (2010). *Health Systems Governance in Europe: The Role of EU Law and Policy*. Cambridge University Press.

4. Corrales, M., Fenwick, M., & Forgo, N. (2017). *New technology, big data and the law*. Singapore: Springer.

5. Den Exter, A. (2017). *Cross-border health care and European Union Law*. Erasmus University Press.

6. EU Agency for Fundamental Rights and Council of Europe, Council of Europe. (2018). *Handbook on European data protection law* 2018 edition, Luxembourg: Publications Office of the European Union.

7. *European Commission (2008). Legally eHealth putting eHealth in its European legal context*. (2008). Brussels: Publications Office of the European Union.

8. Fricker, S. A., Thümmler, C., & Gavras, A. (2015). *Requirements Eengineering for Digital Health*: Springer.

9. Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer International Publishing.

10. Gaddi, A., Capello, F., Manca, M. (2014). *eHealth, Care and Quality of Life*. Springer.

11. Gkoulalas-Divanis, A., Loukides, G. (2015). *Medical Data Privacy Handbook*. Springer

International Publishing.

12. Hervey, T. K., McHale, J. V. (2004). *Health Law and the European Union*. Leiden: Leiden Cambridge University Press.

13. Hervey, T. K., McHale, J. V. (2015). *European Union Health Law*. Cambridge University Press.

14. Hervey, T. K., Young, C. A., Bishop, L. E. (2017). *Research Handbook on EU Health Law and Policy*. Edward Elgar.

15. Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy*. Springer International Publishing.

16. Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometric Applications A Comparative Legal Analysis*. Springer Netherlands.

17. Kosta, E. (2013). *Consent in European data protection law*. Leiden. The Netherlands: Martinus Nijhoff Publishers.

18. Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford University Press.

19. Prosser, T. (2005). *The limits of competition law: markets and public services*. Oxford University Press.

20. Rinaldi, G. (2017). *New Perspectives in Medical Records Meeting the Needs of Patients and Practitioners* (1st ed. 2017. ed.). Springer International Publishing.

21. Schutze, R. (2018). *European Union Law*: Cambridge University Press.

22. WHO Globle Observatory for eHealth. (2012). *Legal Frameworks for eHealth: Based on the Findings of the Second Global Survey on EHealth*. World Health Organization.

Journal Articles

1. Baeten, R., Busse, R., Glinos, I. A., Legido-Quigley, H., McKee, M. (2012). Analysing arrangements for cross-border mobility of patients in the European Union: A proposal for a framework. *Health policy,* 108(1), 27-36. DOI:10.1016/j.healthpol.2012.07.001

2. Bahr, A., Claerhout, B., Coorevits, P., Daniel, C., De Moor, G., Dugas, M., Dupont, D., Kalra, D., Klein, G. O., Schmidt, A., Singleton, P., Sundgren, M. (2013). Electronic health records: new opportunities for clinical research. *Journal of Internal Medicine*, Vol. 274, pp. 547.

3. Baumer, D. L., Chumney, W. M., Hiller, J., McMullen, M. S. (2011). Privacy and security in the implementation of health information technology (electronic health records): U.S. and E.U. compared. *Boston University Journal of Science & Technology Law*, 17(1), 39.

4. Ben-Assuli, O., Flaumenhaft, Y. (2018). Personal health records, global policy and regulation review. *Health Policy*, 122(8), 815-826.

5. Berger, R., Gerard, S., Iriana, S., Krawiec, C., & Levi, B. (2020). What We Can Learn From Failure: An EHR-Based Child Protection Alert System. *Child Maltreatment*, 25(1), 61–69. https://doi.org/10.1177/1077559519848845

6. Bratan, T., Greenhalgh, T., Hinder, S., Russell, J., Stramer, K. (2010). Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. *British Medical Journal (Online)*, 341(7782). DOI:10.1136/bmj.c5814

7. Bredenoord, A. L., Mostert, M., Van Delden, J. J. M., Van Der Slootb, B. (2018). From privacy to data protection in the EU: Implications for big data health research. *european Journal of health law*, *25*(1), 43-55. DOI:10.1163/15718093-12460346

8. Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, 26(3), 213-228. DOI:10.1080/13600834.2017.1330740

9. Commers, M. J., Van Der Molen, I. N. (2013). Unresolved legal questions in cross-border health care in Europe: liability and data protection. *Public health*, 127(11), 987-993. DOI:10.1016/j.puhe.2013.08.020

10. Damjanovic, D., De Witte, B. (2008). Welfare Integration through EU Law: The Overall Picture in the Light of the Lisbon Treaty. *IDEAS Working Paper Series from RePEc*.

11. Díaz Díaz, E. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions. *Church, Communication and Culture*, 1(1), 206-239. DOI:10.1080/23753234.2016.1240912

12. Duncan, B. (2002). Health policy in the European Union: how it's made and how to influence it. *British Medical Journal*, 324(7344), 1027. DOI:10.1136/bmj.324.7344.1027

13. Foster, G., Holbrook, A., Perera, G., Thabane, L., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. *International Journal of Medical Informatics*, 80(2), 94-101. DOI:10.1016/j.ijmedinf.2010.11.005

14. Gleason, A. M. (2015). mHealth - Opportunities for Transforming Global Health Care and Barriers to Adoption. *Journal of Electronic Resources in Medical Libraries,* 12(2), 114-125. DOI: 10.1080/15424065.2015.1035565

15. Graef, I., Husovec, M., Purtova, N. (2018). Data portability and data control: Lessons for an emerging concept in EU law. *German Law Journal*, 19(6), 1359-1398.

16. Greer, S. L., Hervey, T. K., Mackenbach, J. P., McKee, M. (2013). Health law and policy in the European Union. *The Lancet,* 381(9872), 1135-1144. DOI:10.1016/S0140-6736(12)62083-2

17. Gunter, T. D., Terry, N. P. (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. *Journal of Medical Internet Research,* 7(1). DOI:10.2196/jmir.7.1.e3

18. Gutierrez, J., Kaboli, P. J., Kuperman, E. (2020). Using Telehealth as a Tool for Rural Hospitals in the COVID-19 Pandemic Response. *The Journal of rural health.* DOI:10.1111/jrh.12443

19. Kokott, J., Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law,* 3(4), 222-228. DOI:10.1093/idpl/ipt017

20. Lauritsen, S. M., Olsen, M. V., Larsen M. S., Kristensen, M. Lange, J., et al. (2019). Explainable artificial intelligence model to predict acute critical illness from electronic health records. *Nature Communications,* 11(1), 1-11. DOI:10.1038/S41467-020-17431-x

21. Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International Journal of Law and Information Technology*, 26(1), 45-63. DOI:10.1093/ijlit/eax024

22. Lymberis, A., Olsson, S., Whitehouse, D. (2004). European Commission activities in eHealth. *International Journal of Circumpolar Health,* 63(4), 310-316. DOI:10.3402/ijch.v63i4.17747

23. Marian, B. (2018). Considerations regarding Directive 2011/24/EU on the application of patients' rights in cross-border healthcare in EU member states. *Juridical Tribune Journal, 8*(3), 681-689.

24. Miller, A. P. (1986). Teleinformatics, transborder data flows and the emerging struggle for information: an introduction to the arrival of the new information age. *Columbia Journal of Law and Social Problems,* 20(1), 89-144.

25. Mulder, T., Tudorica, M. (2019). Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law*, 28(3), 261-274. DOI:10.1080/13600834.2019.1644068

26. Olimid, A. P., Olimid, D. A., Rogozea, L. M. (2018). Ethical approach to the genetic, biometric and health data protection and processing in the new EU General Data Protection Regulation (2018). *Romanian Journal of Morphology and Embryology*, 59 (2), 631-636.

27. Pakla, R. (2017). The Impact of Health Tourism and Cross Border Healthcare on EU Legislation. *Anglo-German Law Journal*, 3, 184-203.

28. Peeters, M. (2012). Free Movement of Patients: Directive 2011/24 on the Application of Patients' Rights in Cross-Border Healthcare, *European Journal of Health Law*, 19(1), 29-60.

29. Raposo, V. L. (2016). Telemedicine: The legal framework (or the lack of it) in Europe. *GMS Health Technology Assessment,* 12, Doc03. DOI:10.3205/hta000126

30. Raposo, V. L. (2020) The CJEU's ruling in the Novartis Farma case - Money, Health and Medicines", *Maastricht Journal of European and Comparative Law*. https://doi.org/10.1177/1023263X20904228.

31. Sobolčiaková, A. (2018). Right of access under GDPR and copyright. *Masaryk University Journal of Law and Technology*, 12 (2), 221-246. DOI: 10.5817/MUJLT2018-2-5

Other Resources

1. Aho E (2006) Creating an innovative Europe: Report of the independent expert group on R&D and innovation, European communities, Luxembourg.

2. Beaten, R., Footman, K., Glonti, K., Knai, C., McKee, M. (2014). Cross-border health care in Europe. World Health Organization.

3. Carrera, S., Fuster, G. G., Guild, E., & Mitsilegas, V. (2015). Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights. Brussel: Centre for European Studies (CEPS).

4. Doyle, E. (2011). NHS Researchers Lose Laptop with 8 m Patient Record. Silicon.co. Available at: https://www.silicon.co.uk/workspace/nhs-researchers-lose-laptop-with-8m-patients-records-31810

5. European Commission – Cross-border health project epSOS: what has it achieved? Available at: https://ec.europa.eu/digital-single-market/en/news/cross-border-health-project-epsos-what-has-it-achieved.

6. European Commission - EU health policy. Available at: https://ec.europa.eu/health/policies/overview_en

7. European Commission. e-health Governance Initiate: Joint Action EHGov & SEHGovIA Thematic Network. Available at: http://www.ehgi.eu/Download/eHGI%20Documentation%20eHealth%20Governance%20Initiative%20Factsheet(7-November-2011).pdf

8. European Commission - EU health programme. Available at: https://ec.europa.eu/health/funding/programme_en

9. European Commission. 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. Available at: http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf

10. European Court of Auditors (2018). Cross-border healthcare in the EU. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BP_CBH/BP_Cross-border_healthcare_EN.pdf

11. European Parliament (2014). The OMC Method of Coordination. At a glance October. Available at: https://www.europarl.europa.eu/EPRS/EPRS-AaG-542142-Open-Method-of-Coordination-FINAL.pdf

12. European Society of Radiology (ESR) (2017) The new EU General Data Protection Regulation: what the radiologist should know? Insights Imaging 8:295–299. DOI: 10.1007/s13244-017-0552-7.

13. ICTPSP. epSOS – legal and regulatory perspectoves. Available at: https://www.promisalute.it/servizi/gestionedocumentale/visualizzadocumento.aspx?ID=2461

14. Jowitt, T. (2010). NHS Tops ICO List for Most Data Breaches. Silicon.co. Available at: https://www.silicon.co.uk/workspace/nhs-tops-ico-list-for-most-data-breaches-7429

15. McBride, M. (2011). Cyber-Attacks against Internet-Enabled Medical Devices are New Threat to Clinical Pathology Laboratories. Dark Daily. Available at:

https://www.darkdaily.com/cyber-attacks-against-internet-enabled-medical-devices-are-new-threat-to-clinical-pathology-laboratories-215/

16. Report of the eHealth Stakeholder Group (2013). Patient access to Electronic Health Records. Version June. Available at: https://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5169

17. Smart Open Services for European Patients Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription - Recommendations D2.2.7, 06 June 2014.

18. Vanhercke, B., Zeitlin, J. (2014). Socializing the European Semester? Economic governance and social policy coordination in Europe 2020. In E. Political & G. Transnational.