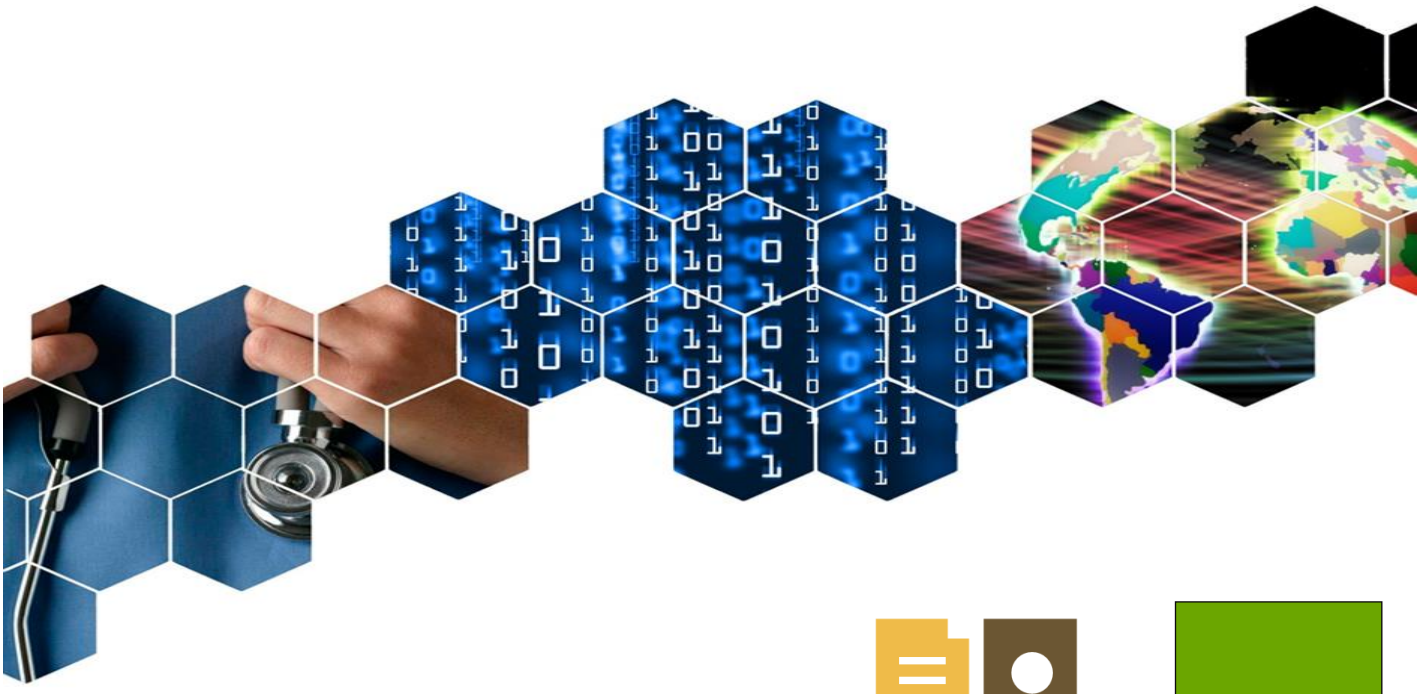
Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services

Contract 2013 63 02

Overview of the national laws on electronic health records in the EU Member States

National Report for Cyprus



07 April 2014

This Report has been prepared by Milieu Ltd and Time.lex under Contract 2013 63 02.

This report was completed by Haris Satsias, Nicoletta Epaminonda and Achilleas Demetriades of Lellos P. Demetriades Law Office LLC. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Executive Agency for Health and Consumers.

Milieu Ltd. (Belgium), rue Blanche 15, B-1050 Brussels, tel: +32 2 506 1000; fax: +32 2 514 3603; florent.pelsy@milieu.be; web address: www.milieu.be

Executive Summary

1. Stage of Development of EHRs in Cyprus

In Cyprus, eHealth is still at a very early stage. EHR systems have not been implemented on a full scale, but are in place at the two major General Hospitals of Cyprus, namely the Nicosia General Hospital and the Ammochostos General Hospital as well as at some local health centres. The Ministry of Health is the competent authority responsible for the general organisation of the healthcare system and the provision of public healthcare services, including the implementation of EHR policies. The Commissioner for the Protection of Personal Data is an independent governmental authority responsible for data protection issues in Cyprus, including health data in EHRs.

Even though in Cyprus eHealth activities are still at a very early stage, the Ministry of Health has completed the creation of infrastructure for electronic health records through the formalisation of procedures – namely, the creation of infrastructure for EHRs at the two major General Hospitals mentioned above, as well as some of the Health Centres in the two districts, and also the effective electronic management of material and of electronic prescriptions. In the Nicosia General Hospital, everything is fully computerised and most of the tasks, including ePrescriptions and the keeping of EHRs, is done electronically.

However, due to the fact that EHRs systems only exist in the two above-mentioned Hospitals, paper-based medical health records are still in use to some extent especially when a patient is referred from another hospital or health centre which does have an EHR system in place. The implementation of eHealth requires an amendment of the existing legal framework, raising awareness and a change of attitude. eHealth is considered to be the basis upon which the General Health System will be built.

The size of Cyprus as a country, as well as the high percentage of trained staff were considered to be a prescription for success; however, the delay and timid steps taken in that direction on a political level has left implementation of these systems incomplete. There is a growing consensus amongst Cypriot HCPs and society in general that there is an urgent need for the creation of electronic health records which will introduce efficiency and certainty into the healthcare system by the utilisation of new technologies. It is understood that EHRs have a plethora of advantages both for patients and for providers of health care services. The result will be the provision of a more efficient, viable and workable system of health care services.

2. Summary of legal requirements applying to EHRs

Cyprus relies on general health and data protection law and there is no specific legal framework that regulates EHRs and ePrescriptions. The main legislation that applies to EHRs is as follows:

- Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) (as amended);
- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005) (as amended); and
- The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013) (hereinafter referred to as "Cross-Border Healthcare Law").

Content of EHRs

First, there are no specific rules as to the content of EHRs. There are however, rules regarding the content of "medical files", which include files created electronically, and may be applied by analogy to EHRs. "Medical files", in accordance with the definition provided in the Patient Rights Law are

"files which are created on paper or electronically, or in any other way and which consist of information related to the physical (biological) or mental health or situation of the patient whose identity can be determined by those and which are created by or on behalf of the person who provides health services by way of profession". In practice, EHRs contain demographic data, laboratory tests, medical information, prescriptions, course of treatment, doctors' notes and the health history of the patient.

The Patient Rights Law does not distinguish categories of data and considers all data relating to a patient as confidential. Section 15(3) stipulates that all information and data which may determine the identity of the patient must be protected. In practice, however, EHRs are divided into separate categories of health data with different levels of access based on confidentiality. Doctors, Nurses and other staff have different access rights based on their specialisation and there is information which is considered as "more confidential" compared to other information e.g. demographic data is less confidential medical information in relation to a psychological disorder.

The Data Protection Law generally imposes upon the data controller the obligation to seek the patient's consent before the processing of his/her health data. It is generally prohibited to process, collect or share sensitive personal data. Health Data constitute sensitive personal data and therefore, unless one or more of the exceptions apply, the processing of such data is prohibited.

Requirements on the institutions that host EHRs

There are no specific national rules in relation to the hosting and management of data from EHRs. However, there are general rules about the collection, processing and protection of personal data and special categories of data such as sensitive data which include data regarding a person's health. Institutions hosting EHRs data are considered to be data controllers and are subject to the obligations set by the Data Protection Law and the Patient Rights Law.

A data controller who processes health data (sensitive data) is subject to more stringent requirements as to security in accordance with section 10 of the Data Protection Law which stipulates that the organisational (including qualified staff) and technical measures that need to be taken for the security of the data shall ensure a level of security which is appropriate/analogous to the risks involved in the processing and the nature of the data processed

Consent

The Data Protection Law generally imposes upon the data controller the obligation to seek the patient's consent before the processing of his/her health data. It is generally prohibited to process, collect or share sensitive personal data. Health Data constitute sensitive personal data and therefore, unless one or more of the exceptions apply, the processing of such data is prohibited.

Neither Data Protection Law nor Patient Rights Law requires materialised consent, but express consent as mentioned above. The term "consent" is defined in the Data Protection Law as follows:
"*'consent' means consent of the data subject, any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject* ***having been previously informed, consents to the processing of personal data concerning him".***

Taking into account the abovementioned definition of consent, it appears that there is a requirement to inform the patient of EHRs and the consequences of the consent or the withholding thereof.

There is no specific provision in the law as to the patient's giving of consent for the access by a health practitioner or a health institution outside Cyprus.

Neither Data Protection Law nor Patient Rights Law requires materialised consent, but express consent as mentioned above.

Creation, access to and updating of EHRs

Section 18 of the Patient Rights Law states that patients have the right to access, information and objection in relation to information which relate to him/her and are contained in the patient's medical record. The right to access contains the right to correct incorrect data, deletion of data and the locking of the record due to deficiencies or inaccuracy.

The right to access can be limited, rejected or suspended if the access will cause serious damage to the health of the patient or where it is possible to disclose information in relation to third parties or in relation to genetic information, where access will cause serious harm to the health of relatives.

There is an obligation on the data controller to keep records duly updated.

In relation to HCPs' access rights, in the two General Hospitals where an EHR system exists different health professionals have different access rights. Furthermore, there are certain kinds of sensitive data that are considered to be "more confidential" compared to others e.g. psychiatric or psychological disorders and sexually transmitted diseases. Furthermore, it appears that nurses have fewer access rights compared to doctors and for example cannot write prescriptions or order tests.

There are no specific rules on the identification and authentication of HCPs, but in practice, HCPs have their own username and password which allows them access to specific layers, or certain information in accordance with their access rights or privileges.

There are no specific national rules in relation to the hosting and management of data from EHRs. However, there are general rules about the collection, processing and protection of personal data and special categories of data such as sensitive data which include data regarding a person's health. Institutions hosting EHRs data are considered to be data controllers and are subject to the obligations set by the Data Protection Law and the Patient Rights Law.

Liability

There are no specific medical negligence requirements set by the law related to the use of EHRs. The legal principles of negligence are based on common law, and are non-exhaustively codified in section 51 of the Civil Wrongs Law, Cap.148. The Commissioner for the Protection of Personal data has, however, imposed administrative fines on numerous occasions on doctors and hospitals for loss of patients' medical files. Furthermore, section 26 of the Data Protection Law contains criminal offences as well as the penalties for the criminal offences in relation to its infringement.

Secondary use and archiving duration

One of the general rules of processing is that data should be retained in a form which allows identification of the data subject only for a period needed for the fulfilment of the purpose of their collection. After that period has lapsed the Commissioner may, by a reasoned decision, allow the retention of the data if he judges that the rights of the data subjects are not affected.

The archiving duration of EHRs has been identified as a very difficult issue in practice, by the Commissioner's office and it has not been resolved yet.

There are no specific national rules on archiving durations of EHRs but there are general rules contained in the Data Protection Law and the law does not mention anything about different archiving duration rules for different institutions. It depends on the circumstances of the specific institution or provider and on the discretion of the Commissioner.

Interoperability

There are no requirements in the law that refer to the interoperability of national EHRs with other Member States' EHRs systems. It is understood that the EHR system implemented in the two major hospitals as well as in some local health centres is centralised. Data Protection Law allows the transfer of data including health data to other Member States of the EU without the need for a permit or licence.

Links between EHRs and ePrescriptions

ePrescriptions are used in the two major public hospitals namely, General Hospital of Nicosia and General Hospital of Ammochostos as well as some local medical centres in the context of the IHIS which comprises 13 sub-systems and concerns the internal electronic operation of procedures in hospitals including the creation of EHRs, administration of patients, billing and administration of e-prescriptions and clinical examinations.

ePrescriptions are automatically filed in the patients' EHR. However, it appears that the existence of an EHR is not a precondition of the ePrescription system, nor is the existence of an EHR a prerequisite for the prescription to a patient using ePrescription.

The office of Commissioner for the Protection of Personal Data has granted an interconnection licence to the Pharmaceutical Services of the Ministry of Health and the Civil Registry of the Ministry of Interior and therefore the ePrescription system is connected to the registry which contains the demographic data of patients.

3. Good practices

Firstly, in the two General Hospitals where an EHR system exists, there are different access rights, depending on the position and capacity of the health professional. Furthermore, there are certain kinds of sensitive data that are considered to be "more confidential" compared to others e.g. psychiatric or psychological disorders and sexually transmitted diseases. In this way, the patients' sensitive data are more adequately protected due to the fact that the most sensitive data are only accessible to a very specific group of people.

The Ministry of Health has applied to the Commissioner for the Protection of Personal Data for an Interconnection Licence of the records retained by the Civil Registry and Migration Department with the records of patients in the two public hospitals where the system has been implemented. A licence has been issued and therefore there is access by the General Hospitals of Nicosia and Ammochostos in the demographic data retained by the Civil Registry and Migration department. By virtue of this interconnection, demographic data can be cross-referenced and their accuracy improved and maintained.

The Commissioner has made various suggestions to the Ministry of Health regarding good practices based on the Article 29 Working Group's Working Document on the processing of personal data relating to health in electronic health records. One of the suggestions was the implementation of a smart card which will contribute to the proper identification of patients and will further provide a mechanism for authentication and access of patients to their records. The creation of smart cards is one of the future goals of the Ministry of Health.

4. Legal barriers

The Office of the Commissioner for the Protection of Personal Data believes that the existing legal framework does not create any barriers to the development of EHRs. As to the transfer to other Member States, it is obviously allowed without any notification requirements to the Commissioner. The issue that needs to be addressed on a European level is the issue of interoperability. The office of

the Commissioner has identified a barrier only in relation to secondary uses, which is the need for a notification to the Commissioner.

Others believe that it is of paramount importance to revisit all related legislation due to the fact that it is based on paper based eras, to update it in order to be compatible with EU legislation and facilitate the use of EHR in all hospitals and medical practitioners (both public and private). For example the Private Health Institutions Law states that the patient files have to be kept in a book, i.e. on paper, and this might act as a barrier to the development of EHRs in the private sector.

One stakeholder expressed the opinion that the existing Data Protection Law places excessive administrative burdens on the General Hospitals that use EHRs since they have to apply for interconnection permissions every time they wish to seek access in a data base maintained for a different purpose.

It has been indicated to us that the ePrescriptions system will not be able to work properly and independently from paper based prescriptions unless an efficient system for the verification of electronic signatures is implemented.

It is also believed that we should turn to a more patient centric EHR system – the EHR should belong to the patient and a more patient centred philosophy will allow the development of EHRs.

All stakeholders agree that political decisiveness is needed in order to deploy EHRs in all sectors and in all regions as well as for their cross-border transfer.

Contents

1. GENERAL CONTEXT 10
1.1. EHR SYSTEMS IN PLACE 10
1.2. INSTITUTIONAL SETTING 10
1.3. LEGAL SETTING AND FUTURE LEGAL DEVELOPMENT 11
2. LEGAL REQUIREMENTS APPLYING TO EHRS IN CYPRUS 13
2.1. HEALTH DATA TO BE INCLUDED IN EHRS 13
2.1.1. MAIN FINDINGS 13
2.1.2. TABLE ON HEALTH DATA 14
2.2. REQUIREMENTS ON THE INSTITUTION HOSTING EHRS DATA 20
2.2.1. MAIN FINDINGS 20
2.2.2. TABLE ON REQUIREMENTS ON THE INSTITUTIONS HOSTING EHRS DATA 21
2.3. PATIENT CONSENT 24
2.3.1. MAIN FINDINGS 24
2.3.2. TABLE ON PATIENT CONSENT 25
2.4. CREATION, ACCESS TO AND UPDATE OF EHRS 29
2.4.1. MAIN FINDINGS 29
2.4.2. TABLE ON CREATION, ACCESS TO AND UPDATE OF EHRS 30
2.5. LIABILITY 35
2.5.1. MAIN FINDINGS 35
2.5.2. TABLE ON LIABILITY 36
2.6. SECONDARY USES AND ARCHIVING DURATIONS 39
2.6.1. MAIN FINDINGS 39
2.6.2. TABLE ON SECONDARY USES AND ARCHIVING DURATIONS 40
2.7. REQUIREMENTS ON INTEROPERABILITY OF EHRS 42
2.7.1. MAIN FINDINGS 42
2.7.2. TABLE ON INTEROPERABILITY OF DATA REQUIREMENTS 43
2.8. LINKS BETWEEN EHRS AND EPRESCRIPTIONS 44
3. LEGAL BARRIERS AND GOOD PRACTICES FOR THE DEPLOYMENT OF EHRS IN CYPRUS AND FOR THEIR CROSS-BORDER TRANSFER IN THE EU. 46

List of abbreviations

EHRs	Electronic Health Records
EU	European Union
HCP	Health Care Professional
IHIS	Integrated Health Information System

1. General context

1.1. EHR systems in place

EHR systems are in place at the two major General Hospitals of Cyprus, namely the Nicosia General Hospital and the Ammochostos General Hospital as well as at some local health centres. The Ministry of Health is the competent authority responsible for the general organisation of the healthcare system and the provision of public healthcare services, including the implementation of EHR policies.

At present, due to the lack of a General Health System or universal healthcare coverage system, there is a dual system of healthcare services – namely, the private system and the public system. The Private system comprises private clinics, private hospitals and independent doctors and physicians. The Public healthcare system consists of the 5 General Hospitals (one in each district), suburban outpatient departments, health centres, and rural health centres.

Even though in Cyprus eHealth activities are still at a very early stage, the Ministry of Health has completed the creation of infrastructure for electronic health records. In the public sector there is an EHR system in place at the two major General Hospitals mentioned above, as well as some of the Health Centres in the two districts. The EHR system is part of what is called an Integrated Health Information System (hereinafter referred to as "IHIS") which consists of 13 different subsystems and to our knowledge the computerization process has been completed and is now at the operational support stage. Apart from EHR system, the IHIS also includes computerized systems for lab tests, billing, e-prescription and is intended to cover the key elements of hospital activities. However, due to the fact that EHRs systems only exist in the two above-mentioned Hospitals, paper-based medical health records are still in use to some extent especially when a patient is referred from another hospital or health centre which does have an EHR system in place.

The Ministry of Health's future goals as to eHealth include:

a) The creation of Regional Health Networks for the exchange of information in real time between all the hospitals, Health Centres, and private doctors. These networks will provide the ability to the healthcare service providers to have access to the right information at any time so as to improve the quality of health care.
b) With the creation of a regional health network the following will be offered :
- Instant access to prescriptions and results of lab tests
- Immediate transfer of data for each patient
- A complete medical file
- Telemedicine, telecare, arrangement of appointments.

1.2. Institutional setting

The competent authority at a general level is the Ministry of Health, and is responsible for the general organisation of the public healthcare system, including the implementation of eHealth policies.

The Commissioner for the Protection of Personal Data (hereinafter referred to as "Commissioner") is an independent governmental authority responsible for data protection issues in Cyprus, including health data in EHRs. The Office of the Commissioner was established in 2002 after the enactment of the Law for the processing of Data of Personal Character (Protection of the Individual) of 2001 (hereinafter referred to as "Data Protection Law"). The Data Protection Law applies both in the public and in the private sector including the Police. The Office of the Commissioner consists of nine Officials and four administrators.

Officials from the Commissioner's Office have visited the two General Hospitals where EHR systems

have been implemented and have made various practical suggestions for the improvement of personal data protection.

1.3. Legal setting and future legal development

There is no specific legal framework; Cyprus relies on general health and data protection law to regulate EHRs and ePrescriptions.

The main legislation regulating EHRs is as follows:

- Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) (as amended);
- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005) (as amended); and
- The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013) (hereinafter referred to as "Cross-Border Healthcare Law").

Data controllers who collect sensitive data in the context of EHR systems must comply with the general data protection rules set out in the Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended (hereinafter referred to as "Data Protection Law"). The Data Protection Law transposes Directive 95/46/EC into the Cypriot legal order, lays down general data protection principles, imposes certain obligations on data controllers and also sets out the rights conferred on data subjects.

Principles such as those of purpose, data quality, relevance, retention, the data subject's right to be informed, rights of access and security related obligations are contained in the Data Protection Law and apply in the context of EHRs. It is understood that all data enclosed in an EHR are considered to be sensitive data and are therefore subject to the special protection regime.

Furthermore, the Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005) (hereinafter referred to as "Patient Rights Law") sets out certain requirements and imposes obligations upon the Health Institution or Health Care Services Provider in relation to patients' medical files, which also apply by analogy to electronic health records.

The opinions in relation to the adequacy of the existing legal framework are divided. On the one hand, there are those who believe that the existing legal framework is adequate and it can be used efficiently. On the other hand, there are those who claim that there is a lack of legal certainty and there is a need for a specific legal framework regulating the use of EHRs, as there are various deficiencies in the present legal framework. They believe that the lack of a complete and specific legal framework acts as a hindrance to the full utilisation of EHRs and to their cross border transfer.

The Office of the Commissioner for the Protection of Personal Data believes that the existing legal framework does not create any barriers to the development of EHRs. As to the transfer to other Member States of the EU, it is obviously allowed without any notification requirements to the Commissioner. The issue that needs to be addressed on a European level is the issue of interoperability. The office of the Commissioner has identified a barrier only in relation to secondary uses for research, i.e. the need for a notification to the Commissioner.

Others believe that it is of paramount importance to revisit all related legislation due to the fact that it is based on a paper-based era, to update it in order to be compatible with EU legislation and facilitate the use of EHR in all hospitals and medical practitioners (both public and private). For example the Private Health Institutions Law states that the patient files have to be kept in a book, i.e. on paper, and this might act as a barrier to the development of EHRs in the private sector.

One stakeholder expressed the opinion that the existing Data Protection Law places excessive

administrative burdens on the General Hospitals that use EHRs since they have to apply for interconnection permissions every time they wish to obtain access in a data base kept for different purposes.

It is also believed that we should turn to a more patient centric EHR system: the EHR should belong to the patient and a more patient-centred philosophy will allow the further development of EHRs.

All stakeholders agree that political decisiveness is needed in order to deploy EHRs in all sectors and in all regions as well as for their cross-border transfer.

2. Legal requirements applying to EHRs in Cyprus

2.1. Health data to be included in EHRs

2.1.1. Main findings

There are no specific rules pertaining to the content of EHRs. There are however, rules regarding the content of "medical files", which include files created electronically, may be applied by analogy to EHRs.

"Medical files", in accordance with the definition provided in the Patient Rights Law are "files which are created on paper or electronically, or in any other way and which consist of information related to the physical (biological) or mental health or situation of the patient whose identity can be determined by those and which are created by or on behalf of the person who provides health services by way of profession".

As to the content of medical files, section 17(1) of Patient Rights Law stipulates that the responsible provider of health services is obliged to keep medical records which demonstrate the course of a patient's treatment. These data should contain:

- detailed data which determine the identity of the patient and of the responsible provider for health services,
- and medical information pertaining to the treatment received by the patient,
- the patient's previous medical history, to the degree which it is known,
- the diagnosis of the present medical situation of the patient and the course of treatment which will be provided.

There is a qualification in s. 17(1), namely, that the personal notes of the health service provider are not part of the medical record.

In practice, EHRs contain demographic data, lab tests, medical information, prescriptions, treatment, doctor's notes and the health history of the patient.

The Patient Rights Law does not distinguish categories of data and considers all data relating to a patient as confidential. Section 15(3) stipulates ***that all information and data which may determine the identity of the patient must be protected***. In practice, however, EHRs are divided into separate categories of health data with different levels of access based on confidentiality. Doctors, Nurses and other staff have different access rights based on their specialisation and there is information which is considered as "more confidential" compared to other information e.g. demographic data is less confidential medical information in relation to a psychological disorder.

Furthermore, even though there are no specific rules on the use of a common terminology or coding system which identifies diseases, disorders, symptoms etc. in practice there is a coding system in place called DRG (Diagnosis Related Group). It is understood that the DRG has 1734 different codes and is used in all EHRs.

2.1.2. Table on health data

N.B. – The official language of any laws or parts and/or passages thereof is the Greek language. The translation of the relevant laws or passages thereof into English is unofficial.

Questions	Legal reference	Detailed description
Are there specific rules on the content of EHRs? (or regional provisions, agreements, plans?)	- The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. - Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). - The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013).	There are no specific rules pertaining to the content of EHRs. There are however, rules regarding the content of "medical files" which include files created electronically and may be applied by analogy to EHRs. Medical files in accordance with the definition provided in Patient Rights Law are "files which are created on paper or electronically, or in any other way and which consist of information related to the physical (biological) or mental health or situation of the patient whose identity can be determined by those and which are created by or on behalf of the person who provides health services by way of profession". Section 17(1) of Patient Rights Law stipulates that the responsible provider of health services is obliged to keep medical records which **demonstrate the course of a patient's treatment**. These data should contain: - **detailed data which determine the identity of the patient** and of the responsible provider for health services, - **and medical information pertaining to the treatment received by the patient,** - **the patient's previous medical history, to the degree which it is known,** - **the diagnosis of the present medical situation of the patient and the course of treatment which will be provided.** There is a qualification in s. 17(1), namely, that the personal notes of the health service provider are not part of the medical record. The Cross-Border Healthcare Law defines the term "medical file" as "all

Questions	Legal reference	Detailed description
		the documents which contain data, assessments and information of any kind in relation to the condition and clinical examination of the patient during the whole procedure of the treatment".
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). - The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	It appears that the data that have to be contained in a medical file (which can be electronic or paper based) are not restricted to purely medical information. S. 17(1) of the Patient Rights Law stipulates that the responsible provider of health services is obliged to keep medical records which **demonstrate the course of a patient's treatment**. These data should contain: - **detailed data which determine the identity of the patient** and of the responsible provider for health services; - medical information pertaining to the treatment received by the patient; - the patient's previous medical history, to the degree which it is known, - the diagnosis of the present medical situation of the patient, and - the course of treatment which will be provided**.** There is a qualification in s. 17(1), namely, that the personal notes of the health service provider are not part of the medical record Furthermore, it is known that the Commissioner for the Protection of Personal Data has provided an interconnection of records licence to the Ministry of Health based on which it can have access to the records of the Civil Registry and Migration Department of the Ministry of Interior. Therefore, it appears that apart from purely medical information, EHRs also contain demographic information. In practice, EHRs contain demographic data, lab tests, medical information, prescriptions, treatment, doctor's notes and the health history of the patient.
Is there a definition of EHR or	- Law on the	Medical Files in accordance with the definition provided in the Patient

Questions	Legal reference	Detailed description
patient's summary provided in the national legislation?	Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). - The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013). - The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	Rights Law are "files which are created on paper or electronically, or in any other way and which consist of information related to the physical (biological) or mental health or situation of the patient whose identity can be determined by those and which are created by or on behalf of the person who provides health services by way of profession". The Cross-Border Healthcare Law defines the term "medical file" as "all the documents which contain data, assessments and information of any kind in relation to the condition and clinical examination of the patient during the whole procedure of the treatment". Even though there is no express definition of the term EHR in the national legislation, the definition provided in the Working Document on the processing of personal data relating to health in electronic health records (EHR) of the Article 29 Working Party is generally used as guidance ("a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in an electronic form and providing for ready availability of these data for medical treatment and other closely related purposes").
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). - The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as	There are no requirements about the content of EHR specifically but there are requirements as to the contents of patients' "medical records" which can be either paper based or electronic. S.17(1) of the Patient Rights Law stipulates that the responsible provider of health services is obliged to keep medical records in which **the course of a patient's treatment is demonstrated**. The medical record shall contain: - detailed data which determine the identity of the patient and of the responsible provider for health services; - medical information pertaining to the treatment received by the patient; - the patient's previous medical history, to the degree which it is

Questions	Legal reference	Detailed description
	amended. - The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013).	known, - the diagnosis of the present medical situation of the patient, and the course of treatment which will be provided. Section 36(1) of the Cross Border Health Care Law provides that if the Ministry of Health decides to nominate a National Authority of Electronic Health (NAEH) which will cooperate and exchange information with other Member States in the context of a voluntary network which connects the relevant national authorities for electronic health, that NAEH is responsible for creating a non-exhaustive catalogue of data that must be included in a patient summary. These data will be used by HCPs so that the continuity of cross border healthcare and safety of patients is ensured. Also the NAEH has to apply effective methods to ensure the use of medical information for public health and research. We are not aware of the nomination of such a NAEH yet. In practice, EHRs contain demographic data, results of laboratory tests, medical information, prescriptions, treatment, doctor's notes and the health history of the patient.
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?	- The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013).	There are no specific rules on the use of a common terminology or coding system which identifies diseases, disorders, symptoms etc., but in practice there is a coding system in place called DRG (Diagnosis Related Group). It is understood that the DRG has 1734 different codes and is used in all EHRs. Section 36(1) of the Cross Border Health Care Law provides that if the Ministry of Health decides to nominate a National Authority of Electronic Health (NAEH), which will cooperate and exchange information with other Member States in the context of a voluntary network which connects the relevant national authorities for electronic health, that NAEH is responsible for creating a non-exhaustive catalogue of data that must be included in a patient summary. These data will be used by HCPs so that the continuity of cross border healthcare and safety of patients is ensured.

Questions	Legal reference	Detailed description
		Also the NAEH has to apply effective methods to ensure the use of medical information for public health and research. We are not aware of the nomination of such a NAEH yet.
Are EHRs divided into separate categories of health data with different levels of confidentiality (e.g. data related to blood type is less confidential than data related to sexual diseases)?	- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). - The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	In practice EHRs are divided into separate categories of health data with different levels of access based on confidentiality. Every doctor or nurse has different access rights and when usernames and passwords are created for each doctor he/she is given different privileges of access. This is done for purposes of protection of confidentiality but also for efficiency and economic purposes. It is understood that patient information in relation to psychological disorders and data for sexually transmitted diseases such as HIV is more confidential compared to, for example, demographic data. Only specialised doctors or the doctor responsible for treating the specific patient have access to the "more confidential data". Furthermore, it was explained to us that, for example, a dentist does not have access to health data which are not within the sphere of his/her specialisation and therefore a dentist or a nurse will not be able to write a prescription for heart medicine or order a pap-test. The Patient Rights Law does not distinguish categories of data and considers all data relating to a patient as confidential: Section 15(3) stipulates ***that all information and data which may determine the identity of the patient must be protected***. Section 15(1)(a) of the Patients' Rights Law provides that all the information regarding the medical condition of the patient, the diagnosis, prognosis and therapy, and "**every other data of personal character"** are kept confidential, even after the patient's death and may not be disclosed to any person or authority.

Questions	Legal reference	Detailed description
		Subsection (b) states that the responsible provider of health services or any employee of a health institution must not disclose **any information regarding a patient** which may come into his/her knowledge during the exercise of his/her responsibilities or profession. According to section 17 the directors of the medical institution or the responsible provider of health services, depending on the specific case, have the responsibility for retaining in a secured manner, updated medical records in accordance with the Law for the Processing of Personal Character Data (Protection of the Individual) (Law no. 138(I)/2001) as amended. The Data Protection Law states that the data controller is responsible for taking measures which are analogous to the dangers connected to the processing and the nature of the data. In other words, Data Protection Law distinguishes between different kinds of data – i.e. personal data and sensitive data – depending on the risk posed to data subjects. For the processing of sensitive personal data there must be additional safeguards.
Are there any specific rules on identification of patients in EHRs?	- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	There are no specific rules regarding the identification of patients in EHRs but the Patient Rights Law, section 17(1), stipulates that the medical file (which can be electronic or paper based) has to contain detailed information which determines the identity of the patient. In practice ***identity card numbers*** are used to identify patients in EHRs. Also there is another kind of identification method which uses what is called an "episode number" which is used throughout Cyprus.
Is there is a specific identification number for eHealth purposes?		In practice ***identity card numbers*** are used to identify patients in EHRs. Also there is another kind of identification method which uses what is called an "episode number" which is used throughout Cyprus

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

There are no specific national rules in relation to the hosting and management of data from EHRs. However, there are general rules about the collection, processing and protection of personal data and special categories of data such as sensitive data which include data regarding a person's health. Institutions hosting EHRs data are considered to be data controllers and are subject to the obligations set by the Data Protection Law and the Patient Rights Law.

The Data Protection Law generally prohibits the collection and processing of sensitive personal data (section 6). Sensitive personal data are defined in the Law as "Data concerning racial or ethnic origin, political convictions, religious or philosophical beliefs, participation in a body, association and trade union, health, sex life and sexual orientation as well as data relevant to criminal prosecutions and convictions". Section 6(2) prescribes various exceptions to the prohibition of processing of sensitive of personal data provided for in section 6(1). One of the exceptions concerns health/medical data and is as follows: "the processing concerns issues of medical data and is taking place by a person providing health services by profession and has a duty of confidentiality or is subject to relevant codes of conduct, on condition that the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or the management of healthcare services".

A data controller who processes health data (sensitive data) is subject to more stringent requirements as to security in accordance with section 10 of the Data Protection Law which stipulates that the organisational (including qualified staff) and technical measures that need to be taken for the security of the data shall ensure a level of security which is appropriate/analogous to the risks involved in the processing and the nature of the data processed.

2.2.2. Table on requirements on the institutions hosting EHRs data

Questions	Legal reference	Detailed description
Are there specific national rules about the hosting and management of data from EHRs?	- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). - The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	There are no specific national rules in relation to the hosting and management of data from EHRs. However, there are general rules about the collection, processing and protection of personal data and special categories of data such as sensitive data which include data regarding a person's health. A host and manager of EHRs is considered to be a data controller for the purposes of the Data Protection Law and therefore has the obligations of a data controller who processes sensitive personal data. Section 7(1) of the Data Protection Law imposes an obligation on data controllers to notify the commencement of processing or the operation of a filing system with the Commissioner for the Protection of Personal Data who is the Supervisory Authority in Cyprus. Section 7(6)(d) however, stipulates that the data controller is exempted from the obligation to notify when the processing takes place by doctors or other persons who provide health services and concerns medical data, as long as the data controller is bound by medical confidentiality or any other kind of confidentiality required by law or code of conduct and the data are neither transferred/disclosed nor communicated to third parties. However, the Law further provides that persons who offer health services, like clinics, hospitals, health centres, recovery and rehabilitation centres , insurance funds and insurance companies, as well as data controllers when the processing takes place in the context of telemedicine programmes are not exempted. The Data Protection Law imposes several obligations on data controllers including the obligation to ensure that the data are processed in fairly and lawfully, that are not processed in a way incompatible with the purpose for which they were collected, that they are accurate and up to date, that

Questions	Legal reference	Detailed description
		they are kept in a form which permits identification of a data subject for no longer than is necessary for the fulfilment of the purposes for which they were collected and processed. Furthermore, a data controller who processes health data (sensitive data) is subject to more onerous requirements as to security in accordance with section 10 of the Data Protection Law which stipulates that the organisation and technical measures that need to be taken for the security of the data shall ensure a level of security which is appropriate/analogous to the risks involved in the processing and the nature of the data processed.
Is there a need for a specific authorisation or licence to host and process data from EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	There is no need for a specific authorisation or licence to host and process data from EHRs. There are, however, as stated above, obligations of data controllers to notify the commencement of processing of data to the Supervisory Authority which is the Commissioner for the Protection of Personal Data. If the processing of the data from EHRs involves any combination or interconnection of registers or filing systems there is a need for an interconnection licence by the Commissioner for the Protection of Personal Data in accordance to section 8 of the Data Protection Law.
Are there specific obligations that apply to institutions hosting and managing data from EHRs (e.g. capacity, qualified staff, or technical tools/policies on security confidentiality)?	- Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). - The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	There are no specific rules in relation to EHRs but there are obligations that apply to institutions hosting and managing sensitive data and medical files. A data controller who processes health data (sensitive data) is subject to more stringent requirements as to security in accordance with section 10 of the Data Protection Law which stipulates that the organisational (including qualified staff) and technical measures that need to be taken for the security of the data shall ensure a level of security which is appropriate/analogous to the risks involved in the processing and the nature of the data processed.
In particular, is there any obligation	The Processing of Data of	There is no express obligation prescribed by the Data Protection Law to

Questions	Legal reference	Detailed description
to have the information included in EHRs encrypted?	Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	have the information included in the EHRs encrypted. The Commissioner for the Protection of Personal Data, however, suggested the use of encryption mechanisms as a technical measure for the security of the sensitive data contained in EHRs. Pursuant to the Data Protection Law and practice a data controller who processes health data (sensitive data) is subject to more onerous requirements with regard to security in accordance with section 10 of the Data Protection Law, which stipulates that the organisational and technical measures that need to be taken for the security of the data shall ensure a level of security which is appropriate/analogous to the risks involved in the processing and the nature of the data processed.
Are there any specific auditing requirements for institutions hosting and processing EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	There are no specific auditing requirements; however, the Office of the Commissioner for the Protection of Personal Data makes frequent visits to institutions hosting and processing EHRs in order to monitor compliance with the Data Protection Law.

2.3. Patient consent

2.3.1. Main findings

The Data Protection Law generally imposes upon the data controller the obligation to seek the patient's consent before the processing of his/her health data. It is generally prohibited to process, collect or share sensitive personal data without patient consent. Health Data constitute sensitive personal data and therefore, unless one or more of the exceptions apply, the processing of such data is prohibited.

Neither Data Protection Law nor Patient Rights Law requires materialised consent, but express consent as mentioned above. The term "consent" is defined in the Data Protection Law as follows:
"*'consent' means consent of the data subject, any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject* ***having been previously informed, consents to the processing of personal data concerning him".***

Taking into account the abovementioned definition of consent, it appears that there is a requirement to inform the patient of EHRs and the consequences of the consent or the withholding thereof.

There is no specific provision in the law as to the patient's giving of consent for the access by a health practitioner or a health institution outside Cyprus.

2.3.2. Table on patient consent

Questions	Legal reference	Detailed description
Are there specific national rules on consent from the patient to set-up EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	No, the general rules on data protection apply. According to the Data Protection Law processing of personal data can only take place if the express consent of the data subject is granted, unless one of exceptions listed s. 5(2) of the said law applies. The collection and processing of sensitive data (including health data) is generally prohibited by virtue of section 6(1) of the Data Protection Law. By way of exception to the section 6(1) prohibition processing of sensitive data is allowed when one or more of the exceptions listed in subsection 2 of section 6 apply. The main exception is when the data subject has provided his/her express consent. Another exception to the prohibition of the processing of sensitive data is as follows: "when the processing concerns health data and is carried out by a person who, by profession, provides healthcare services and is subject to a duty of confidentiality or to relevant codes of professional ethical conduct, assuming that the processing is necessary for the medical prevention, diagnosis, treatment, or the administration of health services" (s.6(2)(f)). Furthermore, section 16(1) of the Patient Rights Law provides that consent is needed in order to intrude in a patient's personal and family life.
Is a materialised consent needed?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	Neither Data Protection Law nor Patient Rights Law requires materialised consent, but express consent as mentioned above.

Questions	Legal reference	Detailed description
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	No specific requirements exist. In order for a data subject to be able to provide express consent he/she has to be informed of the purpose of processing and the consequences of consent or withholding of consent. The term "consent" is defined in the Data Protection Law as follows: "*'consent' means consent of the data subject, any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject* ***having been previously informed, consents to the processing of personal data concerning him".*** Taking into account the abovementioned definition of consent, it appears that there is a requirement to inform the patient of EHRs and the consequences of the consent or the withholding thereof. The Patient Rights Law (s. 18(1) – rights of patients in relation to health records) also provides that the patient has the right to object.
Are there specific national rules on consent from the patient to share data?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	According to section 15(2) of the Patient Rights Law the health institution or the responsible health service provider can disclose to a third party "medical information" if the patient provides his consent in writing. However, it will be deemed that the patient has provided consent if the information is disclosed to a person which participates in the patient's treatment. There are also further exceptions where consent is not required. Data can, for example, be disclosed to another health care services provider for the purpose of the patient's treatment, or where the medical data is disclosed to the health institution which provides healthcare to the patient or a member of the staff for the processing, filing or for a disclosure required by law. Patients' data can also be disclosed for the purpose of publication in medical journals, for research or for teaching purposes as long as the

Questions	Legal reference	Detailed description
		information through which the patient's identity can be determined is not disclosed i.e. by retaining the patient's anonymity. Data can also be shared when there is a legal obligation or where there is a danger to the society but only after a patient's opinion is heard. The identity of the patient must always remain anonymous and information is disclosed up to a point to which it is necessary depending on the specific situation. Also when data is collected through third parties the data subject must be informed of the identity of the data controller , the purpose of collection and processing etc, unless the data is collected for historical purposes, or scientific research, or the notification of data subjects is impossible and assuming that the permission of the Commissioner has been granted
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	S.18 (1) of the Patient Rights Law states that the patient has the right to object to processing of his/her data. However, it is also stated that the right to object is subject to the application of sections 11-14 of the Data Protection Law which, however, makes no mention of the right to object to the processing of health data by doctors.
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	No specific rules exist. It is one of the basic principles of processing that the data are collected for specified, clear and legal purposes and are not subsequently processed in a manner which is inconsistent with the purposes they were collected for. If, in order to legally process data, the consent of the data subject must exist (unless an exception applies) it appears that if data are shared in order to be subsequently processed, without consent of the patient, the subsequent

Questions	Legal reference	Detailed description
		processing will not be legal. As to the right to object to the processing, it is unclear as to whether it applies in the context of EHRs.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	Section 11(2) of the Data Protection Law provides that the data subject has a right to be informed, including the right to be informed of the consequences of his/her refusal. Section 18 of the Patient Rights Law also provides that the patient has the right to be informed, to access the data and to refuse.
Can the patient consent to his/her EHRs being accessed by a health practitioner or health institution outside of the Member State (cross-border situations)?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	There is no specific provision in the law as to the patient's giving of consent for the access by a health practitioner or a health institution outside Cyprus.
Are there specific rules on patient consent to share data on a cross-border situation?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	There are no specific rules; however, general rules apply in relation to the disclosure of data to a third party. The Data Protection Law provides (s.9(4)) that transfer/transmission of data to Member States of the EU is free and no permission is needed from the Commissioner.

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

Creation of EHRs:

There are no rules as to who can create EHRS but there are rules as to who has to create health records or medical files (which can be electronic or digitised) e.g. section 17 of the Patient Rights Law ("the responsible health service provider has to keep medical records in which the course of the patient's treatment is demonstrated"). Furthermore, the Private Health Institutions Law states that patient health records which are fully updated have to be kept (books that have to be kept – Part XI of Appendix 1).

Access to EHRs:

There are general rules as to access and updating of personal data of patients or medical data.

Section 18 of the Patient Rights Law states that patients have the right to access, information and objection in relation to information which relate to him/her and are contained in the patient's medical record. The right to access contains the right to correct incorrect data, deletion of data and the locking of the record due to deficiencies or inaccuracy.

The right to access can be limited, rejected or suspended if the access will cause serious damage to the health of the patient or where it is possible to disclose information in relation to third parties or in relation to genetic information, where access will cause serious harm to the health of relatives.
There is an obligation on the data controller to keep records duly updated.

Section 12(1) of the Data Protection Law stipulates that everyone has a right to access his/her data and if the data controller does not reply within four weeks the data subject can file a complaint with the Commissioner.

In relation to HCPs' access rights, in the two General Hospitals where an EHR system exists different health professionals have different access rights. Furthermore, there are certain kinds of sensitive data that are considered to be "more confidential" compared to others e.g. psychiatric or psychological disorders and sexually transmitted diseases. Furthermore, it appears that nurses have fewer access rights compared to doctors and for example cannot write prescriptions or order tests.

There are no specific rules on the identification and authentication of HCPs, but in practice, HCPs have their own username and password which allows them access to specific layers, or certain information in accordance with their access rights or privileges.

2.4.2. Table on creation, access to and update of EHRs

Questions	Legal reference	Detailed description
Are there any specific national rules regarding who can create and where can EHRs be created?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Law for Private Health Institutions (Control of Establishment and Operation) of 2001 as amended (Law No. 90(I)/2001).	There are no rules as to who can create EHRS but there are rules as to who has to create health records or medical files (which can be electronic or digitised) e.g. section 17 of the Patient Rights Law ("the responsible health service provider has to keep medical records in which the course of the patient's treatment is demonstrated"). Furthermore, the Private Health Institutions Law states that patient health records which are fully updated have to be kept (books that have to be kept – Part XI of Appendix 1).
Are there specific national rules on access and update to EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	There are general rules as to access and update of personal data of patients or medical data. Section 18 of the Patient Rights Law states that patients have the right to access, information and objection in relation to information which relate to them and are contained in the patient's medical record. The right to access contains the right to correct incorrect data, deletion of data and the locking of the record due to deficiencies or inaccuracy. The right to access can be limited, rejected or stayed if the access will cause serious damage to the health of the patient or where it is possible to disclose information in relation to third parties or in relation to genetic information, where access will cause serious harm

Questions	Legal reference	Detailed description
		to the health of relatives. There is an obligation on the data controller to keep records duly updated.
	The Law for Private Health Institutions (Control of Establishment and Operation) of 2001 as amended (Law No. 90(I)/2001).	Section 12(1) of the Data Protection Law prescribes that everyone has a right to access his/her data and if the data controller does not reply within four weeks, the data subject can file a complaint with the Commissioner.
Are there different categories of access for different health professionals?	*Not applicable*	In the two General Hospitals where an EHR system exists different health professionals have different access rights. Furthermore, there are certain kinds of sensitive data that are considered to be "more confidential" compared to others e.g. psychiatric or psychological disorders and sexually transmitted diseases. Furthermore, it appears that nurses have less access rights compared to doctors and for example cannot write prescriptions or order tests.
Are patients entitled to access their EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	Pursuant to section 12 of the Data Protection Law, patients have the right to access their medical file and the data controller is obliged to reply in writing and provide a copy containing the personal data collected when this does not presuppose a disproportionate effort. The fee that the patient has to pay in order to access his/her file has to be returned if the data subject's application for access was justified.
	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	In practice, the actual medical file (original) is considered to be property of the hospital and any displacement outside of the premises of the hospital is strictly prohibited. The patient has a right to obtain a copy of the medical file by submitting an application to the Department of Medical Certificates upon payment of a fee (€17).
	The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013).	The Cross Border Health Care Law stipulates that the Ministry of Health as the Responsible Authority has to ensure that patients from other Member States of the E.U. who receive treatment in Cyprus and vice versa have the right to access to at least one copy of their medical

Questions	Legal reference	Detailed description
		file, either medical or paper based, as specified in the Data Protection Law and that they have a right to a summary of their treatment either in paper or electronically for the purpose of continuation of their treatment in other Member States.
Can patient have access to all of EHR content?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	Section 18 of the Patient Rights Law states that patients have the right to access, information and objection in relation to information which relate to him/her and are contained in the patient's medical record. The right to access contains the right to correct incorrect data, deletion of data and the locking of the record due to deficiencies or inaccuracy. The right to access can be ***limited***, rejected or stayed if the access will cause serious damage to the health of the patient or where it is possible to disclose information in relation to third parties or in relation to genetic information, where access will cause serious harm to the health of relatives.
Can patient download all or some of EHR content?	Not applicable.	EHRs cannot currently be downloaded. It also appears that the law is more paper-based.
Can patient update their record, modify and erase EHR content?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	Section 18 of the Patient Rights Law states that patients have the right to access, information and objection in relation to information which relate to him/her and are contained in the patient's medical record. The right to access contains the right to correct incorrect data, deletion of data and the locking of the record due to deficiencies or inaccuracy. In accordance with section 12(2) of the Data Protection Law, the data subject may request the deletion or locking of data which was not processed in accordance with the provisions of the law because of deficiencies or inaccuracy.
Do different types of health professionals have the same rights to update EHRs?	Not applicable.	The law does not specify between different types of health professionals. However, in practice different types of health professionals have different access rights and consequently different rights as to update of EHRs.
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational	Not applicable.	There are no explicit occupational prohibitions in the law.

Questions	Legal reference	Detailed description
physicians…)		
Are there exceptions to the access requirements (e.g. in case of emergency)?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	The Data Protection Law contains a disproportionate effort exception. The right to access can be limited, rejected or stayed if the access will cause serious damage to the health of the patient or where it is possible to disclose information in relation to third parties or in relation to genetic information, where access will cause serious harm to the health of relatives (section 18 of Patient Rights Law).
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*	*Not applicable.*	There are no specific rules on the identification and authentication of HCPs. In practice, HCPs have their own username and password which allows them access to specific layers, or certain information in accordance with their access rights or privileges.
Does the patient have the right to know who has accessed to his/her EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	Section 12(1)(c) stipulates that the data subject has the right to ask for and receive from the data controller, without extreme delay or cost, any disclosure to third parties to which the data have been notified and/or any deletion, locking, or correction that has taken place, unless this is impossible or the effort that is needed to do this is disproportionate.
Is there an obligation on health professionals to update EHRs?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	The obligation is on the "responsible provider of health services" not on health professionals (section 17). If however, the health professional, say in the private sector is a data controller he/she is obliged to keep the record updated and precise.
Are there any provisions for	Law on the Consolidation and	Section 18(2) provides that the patient can access his/her data through

Questions	Legal reference	Detailed description
accessing data on 'behalf of' and for request for second opinion?	the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	a legal representative. Other than the above, there are no specific provisions for accessing data on 'behalf of' and for request for second opinion.
Is there in place an identification code system for cross-border healthcare purpose?	The Application of the Rights of Patients in the Context of Cross-Border Healthcare Law (Law No. 149(I)/2013).	An identification code system is not in place. However, section 36(1) of the Cross Border Health Care Law provides that if the Ministry of Health decides to nominate a National Authority of Electronic Health (NAEH), which will cooperate and exchange information with other Member States in the context of a voluntary network, which connects the relevant national authorities for electronic health, that NAEH is responsible for creating ***a non-exhaustive catalogue of data that must be included in a patient summary***. These data will be used by HCPs so that the continuity of cross border healthcare and safety of patients is ensured. Also the NAEH has to apply effective methods to ensure the use of medical information for public health and research. To our knowledge NAEH has not been established yet.
Are there any measures that consider access to EHRs from health professionals in another Member State?	*Not applicable.*	No such measures are in place.

2.5. Liability

2.5.1. Main findings

Legal Principles on Medical Negligence/Malpractice in Cyprus

By way of introduction it has to be mentioned that the Cyprus legal system is based at large on the common law. The legal principles on negligence in Cyprus are based on common law and are codified in section 51 of the Civil Wrongs Law, Cap. 148. The codification is non- exhaustive and the principles of common law and equity apply provided that they do not conflict with the Constitution or with the Laws enacted by the House of Representatives.

As stipulated in section 51 of Cap.148, negligence consists of doing some act which under the circumstances a reasonable prudent person would not do or omitting or failing to do some act which a reasonable prudent, under the circumstances would do. In relation to professional negligence such as medical negligence, negligence consists of failing to use such skill or take such care in the exercise of the profession, trade or occupation as a reasonable prudent person qualified to exercise such profession, trade or occupation would in the circumstances use or take. The negligence of the defendant must cause damage and therefore a causal link must be proven between the act or omission and the damage caused. Furthermore, there has to be a duty of care.

There are no specific medical negligence requirements set by the law related to the use of EHRs. The Commissioner for the Protection of Personal data has, however, imposed administrative fines on numerous occasions on doctors and hospitals for loss of patients' medical files.

Other information on liability issues

Furthermore, a person whose human rights have been violated can sue in the District Court for the violation of Constitutional Rights and rights enshrined in the ECHR.

The Commissioner for the Protection of Personal Data can impose administrative sanctions by virtue of section 25 including an administrative fine of up to €30.000. Furthermore, there is a right to temporary judicial protection and a right to claim compensation if damage occurs due to the infringement of the provisions of the Data Protection Law. The Data Controller will not be obliged to compensate an injured party if it proves that it was not responsible for the event that caused the damage.

Furthermore, section 26 of the Data Protection Law contains criminal offences as well as the penalties for the criminal offences in relation to its infringement. For example, it is a criminal offence if anyone omits to file a notification for the commencement of processing with the Commissioner, or if someone combines databases without the permission of the Commissioner. Furthermore, it is a criminal offence for someone to intrude in a database without permission, or without permission, to delete, disseminate, disclose, modify, process etc data included in a filing system. Section 26 differentiates between committing the above crimes negligently and committing the crime in order to benefit himself or hurt a data subject.

2.5.2. Table on liability

Questions	Legal reference	Detailed description
Does the national legislation set specific medical liability requirements related to the use of EHRs?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Civil Wrongs Law, Cap. 148	No specific medical liability requirements exist in the law related to the use of EHRs. The general principles on medical negligence apply i.e. whether a doctor failed to use such skill or take such care in the exercise of his/her profession, as a reasonable prudent person qualified to exercise such profession, would in the circumstances use or take. Also the criminal and administrative offence provisions of the Data Protection Law apply. For example, if it is proven that a doctor ought to have considered all relevant information on EHRs and because of his/her omission damage had been caused, the patient will have an action based on negligence. Furthermore, pursuant to section 25 of the Patient Rights Law a healthcare provider who fails to keep medical records is guilty of a criminal offence and it is expressly stated in that section that there is no need to prove intent or professional negligence to prove the offence.
Can patients be held liable for erasing key medical information in EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	Patients can be held liable for erasing key medical information **only if access is illegal** (section 26(1)(e)).
Can physicians be held liable because of input errors?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Processing of Data of Personal Character (Protection of the	Physicians and/or the health institution where the physician is employed can probably be held liable if as a result of their input error the patient has suffered damage and there is a causal link between the input error and the damage.

Questions	Legal reference	Detailed description
	Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Civil Wrongs Law, Cap. 148	
Can physicians be held liable because they have erased data from the EHRs?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Civil Wrongs Law, Cap. 148	Physicians and/or the health institution where the physician is employed can probably be held liable if as a result of their input error the patient has suffered damage and there is a causal link between the input error and the damage. Furthermore, the patient can file a complaint with the Commissioner.
Are hosting institutions liable in case of defect of their security/software systems?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	The data controller is responsible for taking the necessary organisational and technical measures for the security of the data and their protection against destruction, loss, modification, illegal dissemination or disclosure and other forms of unlawful processing. The Commissioner may impose a fine for an administrative offence or criminal procedures may be initiated based on section 26 of the Data Protection Law against a data controller who did not conform with the provisions of the Data Protection Law.
Are there measures in place to limit the liability risks for health professionals (e.g guidelines,	*Not Applicable*	We are not aware of any measures in place that could limit the liability risks for HCPs. We were told by the Commissioner for the Protection of Personal Data that HCPs in the public sector receive training in relation to

Questions	Legal reference	Detailed description
awareness-raising)?		the data privacy issues.
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	Section 10 of the Data Protection Law imposes an obligation on Data Controllers to have in place adequate organisational and technical measures to prevent breach of access.
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Civil Wrongs Law, Cap. 148	Even though an obligation for health service providers to keep medical records exists, there is no obligation imposed by the law to consult the medical file before taking any decision. The Patient Rights Law provides that the health care services provider has to act in the best interests of the patient. General rules of negligence apply.
Are there liability rules related to the misuse of secondary use of health data?	Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005). The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Civil Wrongs Law, Cap. 148	If a person accesses a data base without permission and misuses data he/she is committing a criminal offence. If the intent was to cause harm to a data subject or personally profit or gain an illegal proprietary interest, the maximum sentence is 5 years of imprisonment or a monetary penalty of up to £5000 (€ 8543). A party who has suffered injury due to the misuse of his/her data can sue for negligence, violation of the right to privacy etc.

2.6. Secondary uses and archiving durations

2.6.1. Main findings

There are no specific national rules on archiving durations of EHRs but there are general rules contained in the Data Protection Law and the law does not mention anything about different archiving duration rules for different institutions. It depends on the circumstances of the specific institution or provider and on the discretion of the Commissioner.

One of the general rules of processing is that data should be retained in a form which allows identification of the data subject only for a period needed for the fulfilment of the purpose of their collection. After that period has lapsed the Commissioner may, by a reasoned decision, allow the retention of the data if he judges that the rights of the data subjects are not affected.

The archiving duration of EHRs has been identified as a very difficult issue in practice, by the Commissioner's office and it has not been resolved yet.

In relation to the destruction of data, the Data Protection Law in section 4(2) stipulates that data which were collected or are processed in breach of the provisions of section 4(1) (which includes the provision to keep data for a period necessary to fulfil the purpose of collection) have to be destroyed.

The Commissioner may, with a reasoned decision, allow the retention of the data for historical, statistical or scientific purposes if he is of the opinion that the rights of the data subjects will not be adversely affected (s.4(1)(c)). Also, the Patient Rights Law (s.15(2)(d)) provides that if the data is anonymised, it can be used, without consent, for publication in medical journals, teaching, etc.

2.6.2. Table on secondary uses and archiving durations

Questions	Legal reference	Detailed description
Are there specific national rules on the archiving durations of EHRs?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	There are no specific national rules on archiving durations of EHRs but there are general rules contained in the Data Protection Law. One of the general rules of processing is that data should be retained in a form which allows identification of the data subject only for a period needed for the fulfilment of the purpose of their collection. After that period has lapsed the Commissioner may, by a reasoned decision, allow the retention of the data if he judges that the rights of the data subjects are not affected. It must also be mentioned that the Patient Rights Law states that information contained medical files is kept confidential even after the patient's death. The archiving duration of EHRs has been identified as a very difficult issue in practice, by the Commissioner's office and it has not been resolved yet.
Are there different archiving rules for different providers and institutions?	Not Applicable	The law does not mention anything about different archiving rules. It depends on the circumstances of the specific institution or provider and on the discretion of the Commissioner.
Is there an obligation to destroy (...) data at the end of the archiving duration or in case of closure of the EHR?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	The Data Protection Law in section 4(2) stipulates that data which were collected or are processed in breach of the provisions of section 4(1) (which includes the provision to keep data for a period necessary to fulfil the purpose of collection) have to be destroyed.
Are there any other rules about the use of data at the end of the archiving duration or in case of closure of the EHR?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	The Commissioner may, with a reasoned decision, allow the retention of the data for historical, statistical or scientific purposes if he is of the opinion that the rights of the data subjects will not be adversely affected (s.4(1)(c)).
Can health data be used for secondary purpose (e.g. epidemiological studies,	The Processing of Data of Personal Character	S.4(1)(c) of Data Protection Law - see above.

Questions	Legal reference	Detailed description
national statistics...)?	(Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended. Law on the Consolidation and the Protection of the Rights of Patients of 2004 (Law No. 1(I)/2005).	The Patient Rights Law (s.15(2)(d)) provides that if the data is anonymised, it can be used, without consent, for publication in medical journals, teaching, etc.
Are there health data that cannot be used for secondary use?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	Not mentioned in the law but it appears that it will depend on the Commissioner's discretion.
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	The Processing of Data of Personal Character (Protection of the Individual) Law of 2001 (Law No. 138(I)/2001) as amended.	Section 6(1) states that the processing of sensitive data can take place without the consent of the data subject if in accordance with the decision of the Commissioner there are serious reasons of public interest and assuming that the necessary measures for the protection of the data subject are taken.
Does the law say who will be entitled to use and access this data?	*Not Applicable.*	The law does not say who is entitled to use and access the data.
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	*Not Applicable.*	There is no relevant provision in the law.

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

There are no requirements in the law that refer to the interoperability of national EHRs with other Member States' EHRs systems. However, section 36(1) of the Cross Border Health Care Law provides that if the Ministry of Health decides to nominate a National Authority of Electronic Health (NAEH), which will cooperate and exchange information with other Member States in the context of a voluntary network, which connects the relevant national authorities for electronic health, that NAEH is responsible for creating ***a non-exhaustive catalogue of data that must be included in a patient summary***. These data will be used by HCPs so that the continuity of cross border healthcare and safety of patients is ensured. Also the NAEH has to apply effective methods to ensure the use of medical information for public health and research. To our knowledge NAEH has not been established yet.

It is understood that the EHR system implemented in the two major hospitals as well as in some local health centres is centralised.

If a fully mature and interoperable eHealth system in Europe is to be achieved, an EU wide legal framework has to exist which will set the standards to achieve interoperability and uniformity of EHRs.

Data Protection Law allows the transfer of data including health data to other Member States of the EU without the need for a permit or licence.

2.7.2. Table on interoperability of data requirements

Questions	Legal reference	Detailed description
Are there obligations in the law to develop interoperability of EHRs?	Not Applicable.	No such obligation is imposed by the law.
Are there any specific rules/standards on the interoperability of EHR?	Not Applicable.	The EHR systems in the two hospitals are designed in order for EHRs to be interoperable with other Health institutions.
Does the law consider or refer to interoperability issues with other Member States systems?	Not Applicable.	The law does not consider or refer to interoperability issues with other Member States' systems. However, section 36(1) of the Cross Border Health Care Law provides that if the Ministry of Health decides to nominate a National Authority of Electronic Health (NAEH), which will cooperate and exchange information with other Member States in the context of a voluntary network, which connects the relevant national authorities for electronic health, that NAEH is responsible for creating ***a non-exhaustive catalogue of data that must be included in a patient summary***. These data will be used by HCPs so that the continuity of cross border healthcare and safety of patients is ensured. Also the NAEH has to apply effective methods to ensure the use of medical information for public health and research. To our knowledge NAEH has not been established yet.

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

ePrescriptions are used in the two major public hospitals namely, General Hospital of Nicosia and General Hospital of Ammochostos as well as some local medical centres in the context of the IHIS which comprises 13 sub-systems and concerns the internal electronic operation of procedures in hospitals including the creation of EHRs, administration of patients, billing and administration of e-prescriptions and clinical examinations.

ePrescriptions are automatically filed in the patients' EHR. However, it appears that the existence of an EHR is not a precondition of the ePrescription system, nor is the existence of an EHR a prerequisite for the prescription to a patient using ePrescription.

The office of Commissioner for the Protection of Personal Data has granted an interconnection licence to the Pharmaceutical Services of the Ministry of Health and the Civil Registry of the Ministry of Interior and therefore the ePrescription system is connected to the registry which contains the demographic data of patients.

2.8.2. Table on the links between EHRs and ePrescriptions

- ***Infrastructure***

Questions	Legal reference	Detailed description
Is the existence of EHR a precondition for the ePrescription system?	Not Applicable	The ePrescription system operates independently from EHRs in the context of the IHIS and it is therefore possible to have an ePrescription system without an EHR system.
Can an ePrescription be prescribed to a patient who does not have an EHR?	Not Applicable	Having an EHR is not a prerequisite for the ePrescription to a patient.

- ***Access***

Questions	Legal reference	Detailed description
Do the doctors, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?	Not Applicable	Doctors in hospitals where an EHR system exists can have access to the EHR of patients to whom the prescription is given, subject to the specific doctor's access rights.
Can those health professionals write ePrescriptions without having access to EHRs?	Not Applicable	It is possible to write electronic prescriptions without accessing the EHR or the paper based file.

3. Legal barriers and good practices for the deployment of EHRs in Cyprus and for their cross-border transfer in the EU.

The lack of specific legal provisions in relation to interoperability can be identified as a barrier to the cross border transfer of the EHRs in other Member States of the EU.

It has been indicated to us that the ePrescriptions system will not be able to work properly and independently from paper based prescriptions unless an efficient system for the verification of electronic signatures is implemented.

The Office of the Commissioner for the Protection of Personal Data believes that the existing legal framework does not create any barriers to the development of EHRs. As to the transfer to other Member States, it is obviously allowed without any notification requirements to the Commissioner. The issue that needs to be addressed on a European level is the issue of interoperability. The office of the Commissioner has identified a barrier only in relation to secondary uses, which is the need for a notification to the Commissioner.

Others believe that it is of paramount importance to revisit all related legislation due to the fact that it is based on paper based eras, to update it in order to be compatible with EU legislation and facilitate the use of EHR in all hospitals and medical practitioners (both public and private). For example the Private Health Institutions Law states that the patient files have to be kept in a book, i.e. on paper, and this might act as a barrier to the development of EHRs in the private sector.

One stakeholder expressed the opinion that the existing Data Protection Law places excessive administrative burdens on the General Hospitals that use EHRs since they have to apply for interconnection permissions every time they wish to seek access in a data base kept for different purpose.

It is also believed that we should turn to a more patient centric EHR system – the EHR should belong to the patient and a more patient centred philosophy will allow the development of EHRs.

All stakeholders agree that political decisiveness is needed in order to deploy EHRs in all sectors and in all regions as well as for their cross-border transfer.