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 Malta

February 2014

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

This report was completed by Emma Psaila. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Consumers, Health and Food Executive Agency (Chafea).

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 Malta

Malta has an e-Government platform with an increasing number of services being made available. The main national document addressing eHealth is the National Information Communication and Technology (ICT) Strategy for Malta of 2008.[1] Although Malta has set up two eHealth portals, one providing more general information (called "eHealth") [2] and one specific for online access to health records (called 'myHealth')[3] there is currently no comprehensive eGovernment or eHealth legislation in place. Provisions in general legal instruments such as the Health Act and Data Protection Act and a number of documents referring to Malta's eHealth strategy, support electronic health record (EHR) systems.

Through the myHealth record system[4] patients and the physicians they choose can access key parts of personal health records through any computer connected to the Internet. The patients must have a working Government electronic identity (e-ID) and be subscribed to the myHealth system for their data to be available.

There is no specific institution created solely for the purposes of implementation of EHRs in Malta. Rather, a number of bodies working in the fields of health or data protection are relevant. These include the Ministry for Health, in particular its eHealth Strategy and Projects section of the Information Management Unit, the Malta Information Technology Agency (MITA) and the Information and Data Protection Commissioner.

2. Summary of legal requirements applying to EHRs

- Health data included in EHRs

There is no specific legislation on EHRs in Malta; consequently there are no rules on their content. In practice, the designers of EHR software and prevailing clinical and administrative practice have driven the content of EHRs.[5] Patients can access specific medical and non-medical information through the myHealth system.

There is no definition of EHR or patient's summary. However, Malta is taking part in the epSOS project and presumably the epSOS project's definition of patient summary applies.

Whilst no specific rules on the use of common terminology in EHRs were identified, it is noted that Malta is a member of the International Health Terminology Standards Development Organisation (IHTSDO). This has facilitated Malta's activity in the epSOS project in relation to the use of a subset of SNOMED CT concepts in a number of epSOS value sets.

- Requirements on the institutions hosting EHRs

No specific national rules on the hosting and management of data from EHRs were identified. In the case of Government-managed EHRs, the data and IT security rules set by MITA (the Government's IT agency) apply. Similarly, there are no specific obligations that apply to institutions hosting and managing data from EHRs. These must nevertheless conform to the requirements of relevant national law such as the Data Protection Act and the Professional Secrecy Act.

[1] The Smart Island: The National ICT Strategy for Malta 2008-2010, available at: http://www.rcc.gov.pt/SiteCollectionDocuments/e-Gov-Malta.pdf.
[2] www.ehealth.gov.mt
[3] https://www.myhealth.gov.mt.
[4] https://www.myhealth.gov.mt/help.
[5] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

There is no need for a specific authorisation requirement to host or process data from EHRs. However, the data controller must notify the Information and Data Protection Commissioner before processing data.

There is no obligation to have information in EHRs encrypted and there are no specific auditing requirements for institutions hosting and processing EHRs.

- Patient consent

There are no specific national rules on consent from the patient to set up EHRs. However, the rules of the Data Protection Act apply: personal data may only be processed if the data subject has unambiguously given his consent. Sensitive personal data, which includes health data, can only be processed in specific cases if the data subject has explicitly consented to the processing or has made the data public.

Similarly, although there are no specific requirements in relation to informing the patient about the purposes of EHRs and the consequences of the consent or withholding consent to create EHRs, patients can exercise their right to information and other relevant rights under the Data Protection Act.

As regards patient consent to EHRs being accessed by a health practitioner or health institution outside Malta, this currently takes place in the context of the epSOS project. Patients abroad and in need of emergency care at a health institution taking part in epSOS, can give temporary permission to a physician abroad to access an electronic summary of health data about them that has been processed by Government hospitals in Malta. For access to be given, patients must first fill in and sign a consent form. Patients will also be asked to sign another consent form at the foreign health institution.[6]

There are no specific rules on patient consent to share data in a cross-border situation. However, this would be covered by the general rules on transfers of personal data to third countries as found in the Data Protection Act and in the Third Country (Data Protection) Regulations. The requirement of the data subject's consent applies also with respect to sharing data in a cross-border situation.

- Creation, access to and update of EHRs

No specific national rules regarding who can create EHRs and where they can be created were identified. Similarly, no rules dealing specifically with access and update to EHRs were found. However, as a general rule under the Data Protection Act, data subjects have the right to access, the right to rectify and, where applicable, the right to erase data concerning them.

There are no explicit provisions providing for different categories of access for different health professions. However, patients and physicians can choose who can access health data through the myHealth portal[7] and most systems are secured by role-based access control.[8]

Patients can request a copy of the content of their health records, in line with the right of access entrenched in data protection legislation.[9] Through the myHealth system patients can download specific parts of their EHR (e.g. hospital discharge letters).[10] However, it is not currently possible for them to update their record, modify and erase EHR content.

Role-based access control is used to give differentiated access to Government health professionals

[6] https://ehealth.gov.mt/download.aspx?id=9168
[7] Information available on the help page of the myHealth portal: https://www.myhealth.gov.mt/help.
[8] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[9] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[10] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

according to their job role. Access is authorised according to need.[11] Health professionals who provide emergency care are allowed full access to EHR content even if it is not possible to obtain prior patient consent.[12]

According to the Data Protection Act, if personal data is processed the data controller must provide the data subject with written information about to which recipients or categories of recipients the information is disclosed.

There is no specific identification code system for cross-border healthcare purposes, the national ID number system is used. However, Malta is an active participant in epSOS, through which physicians in other participating countries are provided access to the national patient summary of patients who have consented to take part in the project.[13]

- Liability

Maltese law does not set specific liability requirements related to the use of EHRs. The Data Protection Act foresees liability for persons who breach its requirements and process personal data in contravention of its provisions. Moreover, the Civil Code rules on liability based on fault could apply.

The Health Care Professions Act contains provisions on professional misconduct or breach of ethics by a health care professional. In addition, health practitioners can be held liable for breach of professional secrecy under the Criminal Code and the Professional Secrecy Act. The Criminal Code also provides for the involuntary (or negligent) commission of offences, that is, where the harm results from the imprudence, carelessness, unskillfulness in an art or profession, or non-observance of regulations. Therefore health practitioners could be held criminally liable should their unskillfulness result in a criminal damage.

No provision providing for the liability of patients for erasing key medical information in EHRs was found. Similarly, there is no specific provision to the effect that physicians can be held liable because of input errors. Liability would need to be based on the general legal provisions.

Government contracts with hosting providers make provision for data protection in line with the requirements of the Data Protection Act.[14] Hosting institutions may be held liable in case of defect of their security/software systems.

There are no liability rules related specifically to the misuse of secondary use health data. However, it is noted that the Information and Data Protection Commissioner must order rectification if he/she finds that personal data has been processed in an unlawful manner. If rectification is not effected or if the matter is urgent, the Commissioner may prohibit the controller of personal data from processing the data in any manner other than to store that data.

- Secondary uses and archiving duration

Maltese law does not provide rules on the archiving durations of EHRs. However, according to the Data Protection Act, the controller of personal data must ensure that personal data are not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

Health data can be used for secondary purpose as long as there is a legal basis for it. There is no specific legislation regulating whether certain health data cannot be used for secondary use. Relevant

[11] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[12] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[13] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[14] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

activity is guided by sectoral best practice and ethical considerations.[15] Similarly, Maltese law does not state who will be entitled to use and access this data.

- Requirements on interoperability of EHRs

The myHealth record system enables patients and the physicians they choose to gain electronic access to key parts of personal health records. No obligations to develop interoperability of EHRs were identified in Maltese law. There are no requirements in the law that refer to the interoperability of national EHRs with EHR systems of other Member States.

- Links between EHRs and ePrescriptions

There is no ePrescriptions system in place in Malta.[16] Therefore there is nothing to report on links between EHRs and ePrescriptions.

3. Good practices

The absence of specific legal provisions results in a lack of good legal practices to report on in relation to the deployment of EHRs in Malta and for their cross-border transfer in other EU Member States.

4. Legal barriers

Although general legislation could cover a number of issues relevant to EHRs, the absence of specific obligations tailored to the circumstances prevailing in the health sector could result in legal barriers to the deployment of EHRs. For example, the absence of specific requirements on the interoperability of EHRs could be considered as a barrier thereto.

[15] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[16] According to information available on the epSOS website: http://www.epsos.eu/epsos-services/eprescription.html.

Contents

List of abbreviations

EHRs	Electronic Health Records
e-ID	Electronic identity
epSOS	European Patients Smart Open Services
ICT	Information Communication and Technology
IHTSDO	International Health Terminology Standards Development Organisation
IT	Information Technology
MITA	Malta Information Technology Agency
SNOMED CT	SNOMED Clinical Terms

1. General context

1.1. EHR systems in place

Malta has an e-Government platform in place with an increasing number of services being made available. The main national document addressing eHealth in Malta is the National Information Communication and Technology (ICT) Strategy for Malta of 2008.[17] Between 2008 and 2010 Malta was to pursue its eHealth strategy aimed at facilitating the extensive use and application of ICT in public and private healthcare institutions. Although Malta has set up two eHealth portals, one providing more general information (called "eHealth")[18] and one specific for online access to health records (called 'myHealth')[19] there is currently no comprehensive eGovernment or eHealth legislation in place. Provisions in general legal instruments and a number of documents that refer to Malta's eHealth strategy, support electronic health record (EHR) systems. These documents include the National Broadband Strategy which sets out the strategic target to develop an eHealth system; an information leaflet on eHealth targeting eHealth related services by presenting government support and the dedicated eHealth portal; and the National ICT Strategy that lays out the plan for 2008 to 2010 and aims to encourage eHealth developments and facilitate ICT use in the healthcare sector.[20]

The myHealth record system[21] enables patients and the physicians they choose to gain access to key parts of personal health records through any computer connected to the Internet. The patients must have a working Government electronic identity (e-ID) and be subscribed to the myHealth system for their data to be available in the system. The e-ID is necessary to ensure full security and privacy for personal health data. If a patient wishes to give a physician access to his/her data through myHealth, even he/she needs to have an e-ID.

Through the myHealth system patients can:

- Access their Mater Dei Hospital[22] case summaries (inpatient discharge letters from 2008 onwards). The case summaries are recorded by physicians at Mater Dei Hospital. These become available through myHealth 24 to 48 hours after being finalised.
- Ask one or more physicians to be their physicians in the myHealth system, thus allowing them direct electronic access to their personal health data and allowing patients to access results and reports released to them by their physicians in myHealth.
- Access their lab results (Haematology, Biochemistry, Immunology, Toxicology, Histology, Cytology, Microbiology, Virology and Blood Bank) and medical image reports (reports on X-rays, CT scans, MRI scans, ultrasound, etc.), after they have been seen and released by their physician (from 2008 onwards). The lab results and medical image reports are issued by the Laboratory Information System and Radiology Information System used by Government hospitals and health centres. These become available in myHealth within 25 hours of release. Rarely, results or reports may be updated at source; these updates are highlighted to physicians through the myHealth system.
- Access their current Pharmacy of Your Choice entitlement data.[23]
- Access data on their clinic appointments at Government hospitals. The appointments are those

[17] The Smart Island: The National ICT Strategy for Malta 2008-2010, available at: http://www.rcc.gov.pt/SiteCollectionDocuments/e-Gov-Malta.pdf.
[18] www.ehealth.gov.mt
[19] https://www.myhealth.gov.mt
[20] Information obtained from 'eHealth Strategies', Restall B, Giest J, Dumortier J, Artmann J, Country Brief : Malta (October 2010), available at : http://ehealth-strategies.eu/database/documents/Malta_CountryBrief_eHStrategies.pdf.
[21] Information in this and the following paragraphs has been obtained through the help page of the myHealth portal: https://www.myhealth.gov.mt/help. myHealth is the Government of Malta's portal for online access to health records.
[22] Malta's main public hospital.
[23] The Pharmacy of Your Choice Scheme is a service facilitating access to the national pharmaceutical care service through collaboration with community pharmacies. Those entitled to pharmaceutical items can apply at a pharmacy they choose to collect medicines from there. (Source: https://www.gov.mt/en/Services-And-Information/Business-Areas/Health%20Services/Pages/Medicine.aspx).

recorded on the Patient Administration System used in all Government hospitals.
- Set up email notifications about results and text message reminders for their appointments.

Physicians approached to be myHealth physicians can choose whether or not to accept patient requests. They may leave requests pending until the patient communicates with them first through other channels. If a physician accepts a request, the physician-patient link in myHealth continues for as long as both patient and physician wish. A patient may remove a myHealth physician at any time, but cannot re-create the link without first asking again for the physician's approval. Patient-physician links in myHealth are meant specifically to facilitate electronic access to health data. They do not constitute registration between the physician and the patient for wider healthcare delivery purposes.

The myHealth system does not create or have its own health data. Rather, it facilitates access to existing health data stored in Government healthcare systems. Questions regarding availability, completeness or quality of the data accessed through the myHealth system would therefore need to be tackled at source. Patients can choose who can access health data through this portal.

1.2. Institutional setting

There is no specific institution created solely for the purposes of implementation of EHRs in Malta. Rather, a number of bodies working in the fields of health or data protection are relevant and are described below.

- Ministry for Health

The Ministry for Health is the main body responsible for eHealth issues. It is in charge of implementing the Government's eHealth strategy. The Minister responsible for health is assisted by a number of Departments set up by the Health Act[24] in 2013. These are the:

(i) Department for Policy in Health

The Department for Policy in Health is the chief adviser to the Minister responsible for health on matters related to the Government's health policies and particularly to advise the Minister on the development of policy and coordination of strategic plans, on the design and implementation of action plans, and on the evaluation of outcomes in order to contribute to the sustainability of public health and health care services. The head of this Department is the Chief Medical Officer to Government. The Department must exercise those functions and fulfil the duties and responsibilities emanating from law, and in particular those that the Minister may establish by regulations.[25] These functions and responsibilities are set out in the Functions and Responsibilities of Department for Policy in Health Regulations[26] and include advising upon strategies and objectives for the health system, conducting health technology assessments and the administration of health entitlement policies.

(ii) Department for Healthcare Services

The mission of the Department for Healthcare Services is to ensure the effective and efficient operation and delivery of healthcare services with an emphasis on clinical and corporate governance, service delivery and quality review. The head of this Department is the Director General. The Department exercises those functions and fulfils the duties and responsibilities emanating from law, in particular, those that the Minister may establish by regulations.[27] These functions and responsibilities are set out in the Functions and Responsibilities of Department of Health Services Regulations[28] and include ensuring quality of services delivered through the public health system, coordinating between the health and social care systems and promoting research, teaching and training.

[24] Chapter 528 of the Revised Laws of Malta.
[25] Articles 4 and 5 of the Health Act.
[26] Subsidiary Legislation 528.01, Legal Notice 387 of 2013.
[27] Articles 6 and 7 of the Health Act.
[28] Subsidiary Legislation 528.04, Legal Notice 390 of 2013.

(iii) Department for Health Regulation

The mission of the Department for Health Regulation is to safeguard public health, licence, monitor and inspect the provision of healthcare services in order to ensure their quality and safety, and to recommend the standards to be met by healthcare providers and advise the Minister on matters relating to public health. The head of this Department is the Superintendent of Public Health. The Department exercises those functions and fulfils the duties and responsibilities emanating from law, in particular, those that the Minister may establish by regulations.[29] The Functions and Responsibilities of the Department of Health Regulation Regulations[30] set out these functions and responsibilities to include the formulation of regulations and standards in line with Government direction, the safeguarding of public health through the enforcement of legislation and the development of environment monitoring programmes aimed at reducing health hazards.

Every Department may request, collect and verify any information, data and statistics, as may be required for the performance of its functions. A Department will have access to all information which another Department or other entity, established by or under the Health Act holds. A Department may request all information from patients, relatives, personnel, and professionals, and from public and private healthcare providers, and such data will be given to it in cases of emergency, for reasons of public health and to safeguard the vital interest of the patient or a third person. In all other cases the informed consent of the patient is required. Every Department will have access to other statistics and data of an economic and social nature as required in order that it may perform its functions according to the Act. These requirements are without prejudice to Maltese data protection legislation.[31]

In addition, the Health Act set up the:

- Health Policy and Strategy Board to discuss and evaluate the policy, strategy developments and direction in the health sector and monitor and follow the implementation of the health policy and strategy adopted by the Government.[32]
- Council of Health to advise the Government on any matter related to health in Malta.[33]
- Advisory Committee on Healthcare Benefits to recommend the healthcare benefits to be provided by the public healthcare system and to maintain a publicly accessible list of such benefits regularly updated.[34]

- eHealth Strategy and Projects section of the Information Management Unit

The Ministry for Health established the eHealth Strategy and Projects section of the Information Management Unit to develop better ways of electronically collecting and exchanging health information. Specifically, its mission is to set the strategy, architecture and standards required for secure and interoperable e-health systems, as well as to promote the development of national EHRs, while maintaining high standards of privacy. This work supports improvement in healthcare safety, quality and efficiency.[35]

- Malta Information Technology Agency (MITA)

MITA is the central driver of the Government's ICT policy, programmes and initiatives. MITA's role is to deliver and implement the assigned programmes as set out in the National ICT Strategy of 2008 to 2010, and as directed by the Parliamentary Secretary for Competitiveness and Economic Growth from time to time.[36] MITA was mandated by the Government to provide the technical platform for the

[29] Articles 8 and 9 of the Health Act.
[30] Subsidiary Legislation 528.05, Legal Notice 391 of 2013.
[31] Article 13 of the Health Act.
[32] Article 15 of the Health Act.
[33] Article 17 of the Health Act.
[34] Article 23 of the Health Act.
[35] https://ehealth.gov.mt/HealthPortal/others/ehealth/ehsp.aspx
[36] https://www.mita.gov.mt/en/Pages/The-Agency.aspx

different eHealth services and the development of an eHealth strategy is one of its core priorities.[37]

- Information and Data Protection Commissioner

The office of the Information and Data Protection Commissioner is committed to protecting the individual's right to privacy, also enshrined in the Constitution of Malta, by ensuring the correct processing of personal data.[38] The Data Protection Act[39] gives the Commissioner a number of powers. These include:[40]

- Exercising control and verifying whether data processing is carried out in accordance with the Data Protection Act and regulations issued thereunder.
- Instructing the data processor and controller to take the necessary measures to ensure that the processing is in accordance with the Data Protection Act or regulations made thereunder.
- Ordering the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, or warning or admonishing the data controller.

Individuals who feel that a data controller has violated their privacy rights or who may require any information on data protection may forward the case/request to the office of the Commissioner.

1.3. Legal setting and future legal development

Malta relies on general health and data protection law as the legal setting for eHealth policies. The recently adopted Health Act (entered into force on 25 October 2013) sets out a number of patients' rights.[41] These include the right to:

- Receive information concerning their state of health and the health services and treatments available;
- Be provided in advance with clear information on the treatment options available and to be involved in discussions and decisions about the treatment to be given;
- Access their medical records in accordance with the Data Protection Act, provided this is not to the detriment of their overall wellbeing;
- Have their medical data processed in conformity with the Data Protection Act.

The Data Protection Act transposes Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, into Maltese law. It was fully brought into force on 15 July 2003. The main objectives of the Data Protection Act are:[42]

- The regulation of data controllers, the persons to determine the purposes and means of processing, who are obliged to process the personal data in accordance with inter alia the requirements and criteria established by law;
- The protection of privacy rights of an individual, including the right to information, the right of access and the right to rectify, block or erase personal data not processed in accordance with the Act.

The Act deals specifically with processing concerning health or medical purposes. According to its Article 15, sensitive personal data[43] may be processed for health and hospital care purposes, provided that it is necessary for:

(a) Preventive medicine and the protection of public health;
(b) Medical diagnosis;

[37] For further information see MITA Strategic Plan 2009-2012 available at: https://www.mita.gov.mt/MediaCenter/PDFs/1_MITA%20Strategic%20Plan%202009-2012%20(web).pdf
[38] https://secure3.gov.mt/socialpolicy/justice/departments/info_data_protection.
[39] Chapter 440 of the Revised Laws of Malta.
[40] Article 40 of the Data Protection Act.
[41] Article 27 of the Health Act.
[42] https://secure3.gov.mt/socialpolicy/justice/departments/info_data_protection.
[43] Article 2 of the Data Protection Act defines 'sensitive personal data' as personal data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life.

(c) Health care or treatment; or
(d) Management of health and hospital care services.

In such cases a health professional or other person subject to the obligation of professional secrecy must process the data.

Other health and data protection legislation that may be relevant to EHRs is listed below. Policy documents supporting the development of EHR systems in Malta are mentioned in Section 1.1 above.

Malta does not yet have a system in place for ePrescriptions.

List of relevant national legislation:

- Health Act, 25 October 2013, Chapter 528 of the Revised Laws of Malta (Act XI of 2013). The Health Act regulates the entitlement to, and the quality of, healthcare services in Malta, consolidates and reforms the Government structures and entities responsible for health and provides for the rights of patients.
  - Subsidiary Legislation 528.01, Functions and Responsibilities of Department for Policy in Health Regulations, 25 October 2013, Legal Notice 387 of 2013.
  - Subsidiary Legislation 528.04, Functions and Responsibilities of Department of Health Services Regulations, 25 October 2013, Legal Notice 390 of 2013.
  - Subsidiary Legislation 528.05, Functions and Responsibilities of the Department for Health Regulations, 25 October 2013, Legal Notice 391 of 2013.
- Health Care Professions Act, 21 November 2003, Chapter 464 of the Revised Laws of Malta (Act XII of 2003 as last amended by Legal Notice 234 of 2013). The Act regulates the practice of health care professions in Malta.
- Data Protection Act, 15 July 2003, Chapter 440 of the Revised Laws of Malta (Act XXVI of 2001 as last amended by Act XXV of 2012 and Legal Notice 426 of 2012). The Act provides for the protection of individuals against the violation of their privacy by the processing of personal data and for matters connected therewith or ancillary thereto.
  - Subsidiary Legislation 440.03, Third Country (Data Protection) Regulations, 4 July 2003, Legal Notice 155 of 2003, as amended by Legal Notice 426 of 2007.
- Professional Secrecy Act, 23 September 1994, Chapter 377 of the Revised Laws of Malta (Act XXIV of 1994, as last amended by Act X of 2004). The Act establishes general provisions protecting professional secrecy and makes consequential amendments to other laws.
- Civil Code, 11 February 1870, Chapter 16 of the Revised Laws of Malta (Ordinance VII of 1868 as last amended by Acts IV and VII of 2013). The Code was adopted to amend and consolidate the laws relating to persons and the laws respecting rights relative of things and the different modes of acquiring and transmitting such rights.
- Criminal Code, 10 June 1854, Chapter 9 of the Revised Laws of Malta (Order in Council of 30 January 1854 as last amended by Legal Notice 246 of 2013). The Code was adopted to amend and consolidate the penal laws and the laws of criminal procedure.

2. Legal requirements applying to EHRs in Malta

2.1. Health data to be included in EHRs

2.1.1. Main findings

There is no specific legislation on EHRs in Malta; consequently there are no rules on their content. Article 7 of the Data Protection Act transposes Article 6 of Directive 95/46/EC requiring that the data collected must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'.[44] This is transposed as a requirement on the data controller to ensure that personal data that is processed is adequate and relevant in relation to the purposes of the processing and that no more personal data is processed than is necessary having regards to the purposes of the processing.[45] This is relevant in the context of personal data in health records. In practice, the actual content of EHRs has been driven by the designers of EHR software and prevailing clinical and administrative practice.[46] Through the myHealth system, patients can access specific medical and non-medical information.

There is no definition of EHR or patient's summary. However, Malta is taking part in epSOS, a European Union pilot project aimed at improving the medical treatment of citizens travelling between European countries, by providing health professionals with data on patients needing health care. Patients abroad and in need of emergency care at a health institution taking part in the epSOS project, can give temporary permission to a physician abroad to access an electronic summary of health data about them that has been processed by Government hospitals in Malta.[47] Presumably the epSOS project's definition of patient summary applies.

No specific rules on the use of common terminology were identified. However, Malta is a member of the International Health Terminology Standards Development Organisation (IHTSDO). Membership in IHTSDO has facilitated Malta's activity in the epSOS project in relation to the use of a subset of SNOMED CT concepts in a number of epSOS value sets.

To log into the myHealth system, patients need to have an e-ID and password and be subscribed to the myHealth service. The e-ID is necessary to ensure security and privacy for personal data (see myHealth login page: https://www.myhealth.gov.mt/). If a patient wishes to give a physician access to his/her data through myHealth, the physician must also have an e-ID.

[44] Article 6(1) Directive 95/46/EC.
[45] Article 7(e) and (f) of the Data Protection Act.
[46] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[47] https://ehealth.gov.mt/download.aspx?id=9168.

2.1.2. Table on health data

Questions	Legal reference	Detailed description
Are there specific rules on the content of EHRs? (or regional provisions, agreements, plans?)		There is no specific legislation on EHRs in Malta. The general rules of the Health Act, Data Protection Act and legislation issued thereunder would apply. The designers of EHR software and prevailing clinical and administrative practice have driven the actual content of EHRs.[48]
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?		Malta has a Government portal for online access to health records, called myHealth. The myHealth record system enables patients and the physicians they choose to gain online access to key parts of personal health records.
Is there a definition of EHR or patient's summary provided in the national legislation?		There is no definition of EHR or patient's summary. Presumably the epSOS project's definition of patient summary is relevant, that is, a concise clinical document that provides an electronic patient health data set applicable both for unexpected, as well as expected, healthcare contact.[49] The epSOS patient summary is a standardized set of basic medical data that includes the most important clinical facts required to ensure safe and secure healthcare. This summarized version of the patient's medical data gives health professionals the essential information they need to provide care in the case of an unexpected or unscheduled medical situation (e.g. emergency or accident). The epSOS patient summary contains the following data: • General information about the patient (e.g. name, birth date, gender). • A medical summary consisting of the most important clinical patient data (e.g. allergies, current medical problems, medical implants, or major surgical procedures in the last six months). • A list of the current medication including all prescribed medicines that the patient is currently taking. • Information about the patient summary itself e.g. when and by whom it was generated or updated.[50]
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data		None identified.

[48] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[49] http://www.epsos.eu/faq-glossary/glossary.html?tx_a21glossary%5Buid%5D=542&tx_a21glossary%5Bback%5D=3438&cHash=c3253fb498000d121a8f017a12b5781f.
[50] http://www.epsos.eu/epsos-services/patient-summary.html.

Questions	Legal reference	Detailed description
or general reference to health data)?		
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?		No specific rules seem to exist. However, Malta is a member of the International Health Terminology Standards Development Organisation (IHTSDO). The setting and promotion of health data standards fall within the remit of the eHealth Strategy and Projects Office of the Information Management Unit of the Ministry for Health. For many years, the structuring of health data in EHRs in the government health sector in Malta depended mainly on the application of standard classifications for diagnoses and procedures. One of the eHealth Office's main 2012 projects involved the mapping of health data concepts to SNOMED CT concepts. Membership in IHTSDO has facilitated Malta's activity in the epSOS project in relation to the use of a subset of SNOMED CT concepts in a number of epSOS value sets. Affiliate Licensees have used SNOMED CT as a reference terminology as part of their data management activities. Malta currently has two registered Affiliate Licensees: Mater Dei Hospital (Malta's main acute and teaching hospital) and the Central Procurement & Supplies Unit (responsible for government procurement of pharmaceuticals and medical supplies).[51]
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)?		No requirements to this effect were identified. However, in practice it is noted that there is role-based access control to EHRs.[52]
Are there any specific rules on identification of patients in EHRs?		An e-ID is necessary to use e-Government services. The e-ID is an authentication mechanism for citizens and businesses to identify themselves to electronically access services from across government, including eHealth services. To log into the myHealth system, patients must have an e-ID and password and be subscribed to the myHealth service. The e-ID is necessary to ensure security and privacy for personal data. See myHealth login page:

[51] Information obtained from http://www.ihtsdo.org/members/malta/2013-update/.
[52] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
		https://www.myhealth.gov.mt/. If a patient wishes to give a physician access to his/her data through myHealth, the physician must also have an e-ID.
Is there a specific identification number for eHealth purposes?		As a general rule, their national identity number identifies patients in EHRs.[53]

[53] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

No specific national rules on the hosting and management of data from EHRs were identified. In the case of Government-managed EHRs, the data and IT security rules set by MITA (the Government's IT agency) apply.

There is no need for a specific authorisation requirement to host or process data from EHRs. However, the Data Protection Act contains a notification obligation. The data controller must notify the Information and Data Protection Commissioner before processing data.

There are no specific obligations that apply to institutions hosting and managing data from EHRs. These must nevertheless conform to the requirements of relevant national law such as the Data Protection Act and the Professional Secrecy Act.

There is no obligation to have information in EHRs encrypted and there are no specific auditing requirements for institutions hosting and processing EHRs.

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?		No specific national rules were identified. It seems that the general rules on the processing of personal data contained in the Data Protection Act would apply. In the case of Government-managed EHRs, the data and IT security rules set by MITA (the Government's IT agency) apply (http://ictpolicies.gov.mt).[54]
Is there a need for a specific authorisation or licence to host and process data from EHRs?	Data Protection Act, Article 29 (last amended in 2012)	No such requirement was identified. However, the Data Protection Act contains a notification obligation. According to Article 29, the data controller must notify the Information and Data Protection Commissioner before carrying out any wholly or partially automated or manual processing operation or set of such operations intended to service a single purpose or several related purposes. The Commissioner keeps a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by the data controller. Individuals can consult the register to find out what processing of personal data is being carried out by a particular data controller.[55] The public register of data controllers is available on the website of the office of the Commissioner.[56] It includes Mater Dei Hospital and several other health institutions.
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)?	Data Protection Act, Article 26 (as introduced in 2003)	No specific obligations in relation to EHRs were identified. However conformance to relevant legislation (e.g. Data Protection Act, Professional Secrecy Act) is required.[57] According to Article 26 of the Data Protection Act on security measures, the controller must implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security that gives regard to the:

[54] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[55] http://www.idpc.gov.mt/article.aspx?art=123.
[56] http://www.idpc.gov.mt/public/dcregister.aspx.
[57] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
		(*a*) technical possibilities available; (*b*) cost of implementing the security measures; (*c*) special risks that exist in the processing of personal data; (*d*) sensitivity of the personal data being processed.
In particular, is there any obligation to have the information included in EHRs encrypted?		There is no specific legal obligation, but policies and guidelines are provided by MITA for the storage of this type of information.[58]
Are there any specific auditing requirements for institutions hosting and processing EHRs?		None identified.

[58] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

2.3. Patient consent

2.3.1. Main findings

There are no specific national rules on consent from the patient to set up EHRs. However, the rules of the Data Protection Act apply: personal data may only be processed if the data subject has unambiguously given his consent. Sensitive personal data, which includes health data, can only be processed in specific cases. It may be processed if the data subject has explicitly consented to the processing or has made the data public. A materialised consent is not needed.

Similarly, although there are no specific requirements in relation to informing the patient about the purposes of EHRs and the consequences of the consent or withholding consent to create EHRs, patients can always exercise their right to information and other relevant rights under the Data Protection Act.

As regards patient consent to EHRs being accessed by a health practitioner or health institution outside of Malta, this is currently being done in the context of the epSOS project. Patients abroad and in need of emergency care at a health institution taking part in the epSOS project, can give temporary permission to a physician abroad to access an electronic summary of health data about them that has been processed by Government hospitals in Malta. For access to be given, patients must first fill in and sign a consent form. Patients will also be asked to sign another consent form at the foreign health institution.[59]

There are no specific rules on patient consent to share data in a cross-border situation. However, this would be covered by the general rules on transfers of personal data to third countries as found in the Data Protection Act and in the Third Country (Data Protection) Regulations. The requirement of the data subject's consent applies also with respect to sharing data in a cross-border situation.

[59] https://ehealth.gov.mt/download.aspx?id=9168

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?	Data Protection Act, Articles 9 and 12 (as introduced in 2003)	There are no specific national rules on patient consent to set up EHRs. However, this situation would be covered by general rules. According to Article 9(a) of the Data Protection Act, personal data may be processed only if the data subject has unambiguously given his consent. With specific reference to sensitive personal data, which includes health data, Article 12 prohibits the processing of sensitive personal data except in specific cases. It may be processed if the data subject has given his/her explicit consent to the processing or if the data subject has made the data public.
Is a materialised consent needed?	Data Protection Act, Article 2 (last amended in 2012)	Article 2 of the Data Protection Act defines 'consent' as any freely given specific and informed indication of the wishes of the data subject by which s/he signifies his/her agreement to personal data relating to him/her being processed.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	Data Protection Act, Article 19 (as introduced in 2003)	No specific requirement in relation to EHRs was identified. However patients can always exercise their right to information and other relevant rights under the Data Protection Act.[60] According to Article 19 of the Act, the data controller must provide the data subject from whom data are collected with at least the following information: (a) the identity and habitual residence or principal place of business of the controller; (b) the purposes of the processing for which the data are intended; and (c) any further information relating to matters such as: (i) the recipients or categories of the recipients of data; (ii) whether the reply to any questions made to the data subject is obligatory or voluntary, as well as the possible consequence of failure to reply; and (iii) the existence of the right to access, the right to rectify, and, where applicable, the right to erase the data concerning him/her.
Are there specific national rules on consent from the patient to share	Data Protection Act, Articles 9 and 12 (as	The general rules of the Data Protection Act as described in the first row of this table would apply.

[60] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
data?	introduced in 2003)	
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?		None identified. However, some specific systems have built-in consent management features. For example, the myHealth system gives physicians access to patient data only if the patient has specifically recorded prior consent to this access in the system. In the patient summary system, release of data to the epSOS system (for cross-border exchange of data) is only allowed if the patient has given specific prior consent.[61]
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?		None identified. See above.
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?	Data Protection Act, Article 19(c) (as introduced in 2003)	There is no specific prior requirement to inform the patient.[62] However, the general rules of the Data Protection Act as described in the third row of this table should cover this situation. According to Article 19(c) of the Act, the data controller must provide the data subject from whom data are collected with information relating to matters such as: (i) the recipients or categories of the recipients of data; (ii) whether the reply to any questions made to the data subject is obligatory or voluntary, as well as the possible consequence of failure to reply; and (iii) the existence of the right to access, the right to rectify, and, where applicable, the right to erase the data concerning him/her.
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)?		This is currently being done in the context of the epSOS project. Patients abroad and in need of emergency care at a health institution taking part in the epSOS project, can give temporary permission to a physician abroad to access an electronic summary of health data about them that has been processed by Government hospitals in Malta. For access to be given, patients must first fill in and sign a consent form. Patients will also be asked to sign another consent form at the foreign health institution.[63] The existing consent procedure is specific to this project.[64]
Are there specific rules on patient	Data Protection Act,	There are no specific rules. However, the situation seems to be covered

[61] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[62] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[63] https://ehealth.gov.mt/download.aspx?id=9168.
[64] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
consent to share data on a cross-border situation?	Articles 27 and 28 (as introduced in 2003) Third Country (Data Protection Act) Regulations, Legal Notice 155 of 2003 (4 July 2003)	by general rules: transfers of personal data to third countries are regulated by Articles 27 and 28 of the Data Protection Act, and by the Third Country (Data Protection) Regulations. The transfer to a third country of personal data that is undergoing processing or intended processing, may only take place subject to the provisions of the Data Protection Act and provided that the third country to which the data is transferred ensures an adequate level of protection. Therefore, the requirement of the data subject's consent as explained in the first row of this table applies also with respect to sharing data in a cross-border situation. A transfer of personal data to another country constitutes processing and as such must be notified to the Information and Data Protection Commissioner in the same way as other processing operations (Third Country (Data Protection) Regulations, Regulation 5). No restrictions or other formalities apply in relation to transfer of personal data to: EU or EEA Member States and third countries which are from time to time recognised by the EU Commission to have an adequate level of protection. The transfer of personal data to a third country that does not ensure an adequate level of protection requires an authorisation by the Commissioner. In order to approve the transfer, the Commissioner must at least be satisfied that the controller has provided adequate safeguards. Notwithstanding the above, a transfer of personal data to a third country that does not ensure an adequate level of protection may be effected by a data controller if the data subject has given his unambiguous consent to the proposed transfer, and in a number of cases including where it is necessary in order to protect the vital interests of the data subject.[65]

[65] http://idpc.gov.mt/article.aspx?art=121

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

According to Article 15 of the Data Protection Act, sensitive personal data may be processed for health and hospital care purposes, provided that it is necessary for: preventive medicine and the protection of public health; medical diagnosis; health care or treatment; or management of health and hospital care services. In such cases a health professional or other person subject to the obligation of professional secrecy must process the data. This is in line with Article 8(3) of Directive 95/46/EC.

No specific national rules regarding who can create EHRs and where they can be created were identified. Similarly, no rules dealing specifically with access and update to EHRs were found. However, as a general rule under the Data Protection Act, data subjects have the right to access, the right to rectify and, where applicable, the right to erase data concerning them.

There are no explicit provisions providing for different categories of access for different health professions. However, patients and physicians can choose who can access health data through the myHealth portal[66] and most systems are secured by role-based access control.[67]

Patients can request a copy of the content of their health records, in line with the right of access entrenched in data protection legislation.[68] Through the myHealth system patients can download specific parts of their EHR (e.g. hospital discharge letters).[69] However, it is not currently possible for them to update their record, modify and erase EHR content.

Role-based access control is used to give differentiated access to Government health professionals according to their job role. Access is authorised according to need.[70] In line with Directive 95/46/EC and with the Data Protection Act, health professionals who provide emergency care are allowed full access to EHR content even if it is not possible to obtain prior patient consent.[71]

According to the Data Protection Act, if personal data is processed the data controller must provide to the data subject written information in an intelligible form about to which recipients or categories of recipients the information is disclosed.

There is no specific identification code system for cross-border healthcare purposes in place. However, Malta is an active participant in the epSOS project, through which physicians in other participating countries are provided with access to the national patient summary of patients who have consented to take part in the project.[72]

[66] Information available on the help page of the myHealth portal: https://www.myhealth.gov.mt/help.
[67] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[68] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[69] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[70] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[71] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[72] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

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?		None identified.
Are there specific national rules on access and update to EHRs?	Data Protection Act, Articles 15, 19 and 21 (as introduced in 2003)	No rules dealing specifically with the access and update to EHRs were identified. However, according to Article 15 of the Data Protection Act, sensitive personal data may be processed for health and hospital care purposes, provided that it is necessary for: preventive medicine and the protection of public health; medical diagnosis; health care or treatment; or management of health and hospital care services. In such cases a health professional or other person subject to the obligation of professional secrecy must process the data. As a general rule data subjects have the right to access, the right to rectify and, where applicable, the right to erase data concerning them (Article 19(c)(iii) of the Data Protection Act). Article 21 of the Data Protection Act deals specifically with the right of access. The controller of personal data at the request of the data subject must provide to the data subject, without excessive delay and without expense, written information as to whether personal data concerning the data subject is processed. If such data is processed the data controller must provide to the data subject written information in an intelligible form about: (i) actual information about the data subject which is processed; (ii) where this information has been collected; (iii) the purpose of the processing; (iv) to which recipients or categories of recipients the information is disclosed; and (v) knowledge of the logic involved in any automatic processing of data concerning the data subject. The data subject's request must be made in writing to the controller of personal data and is to be signed by the data subject.
Are there different categories of access for different health professionals?		There are no explicit provisions. It is noted that patients and physicians can choose who can access health data through the myHealth portal.[73] Moreover, access is *de facto* limited to registered health professionals, insofar as clinical content of EHRs is concerned. Most systems are secured by role-based access control.[74]

[73] Information available on the help page of the myHealth portal: https://www.myhealth.gov.mt/help.
[74] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
Are patients entitled to access their EHRs?	Data Protection Act, Article 21 (as introduced in 2003)	Patients can request a copy of the content of their health records, in line with the right of access entrenched in data protection legislation.[75] See second row of this table.
Can patient have access to all of EHR content?		The myHealth record system enables patients and the physicians they choose to gain online access to key parts of personal health records.[76] The relevant physician must have released lab results and medical imaging reports for them to be accessible by the patient.
Can patient download all or some of EHR content?		Through the myHealth system patients can download specific parts of their EHR (e.g. hospital discharge letters).[77]
Can patient update their record, modify and erase EHR content?		Currently this is not possible.[78]
Do different types of health professionals have the same rights to update EHRs?		Role-based access control is used to give differentiated access to Government health professionals according to their job role. Access is authorised according to need.[79]
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)		None identified. *A priori* there are no specific occupational prohibitions but on the other hand, the default is 'no access', so in practice insurance company physicians and company physicians would not have access.[80]
Are there exceptions to the access requirements (e.g. in case of emergency)?		In line with Directive 95/46/EC and with the Data Protection Act, health professionals who provide emergency care are allowed full access to EHR content even if it is not possible to obtain prior patient consent.[81]
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*		There are no specific rules on identification and authentication for health professionals. For services provided on the Government network, access by health professionals is through the use of individual strong passwords by registered users of the corporate domain (Active Directory services). For services provided over the Internet, access is through the use of a personal national e-ID and password.[82]

[75] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[76] Information available on the help page of the myHealth portal: https://www.myhealth.gov.mt/help.
[77] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[78] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[79] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[80] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[81] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[82] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
Does the patient have the right to know who has accessed to his/her EHRs?	Data Protection Act, Article 21(2)(iv) (as introduced in 2003)	No specific rules on access to EHRs were identified. However, the Data Protection Act states that if personal data is processed the data controller must provide to the data subject written information in an intelligible form about to which recipients or categories of recipients the information is disclosed (Article 21(2)(iv)).
Is there an obligation on health professionals to update EHRs?		There is no specific legal obligation, but there is a professional obligation.[83]
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?		In the case of the myHealth system, a patient may delegate another e-ID holder to access the system on his or her behalf. There is no provision to request a second opinion online.[84]
Is there in place an identification code system for cross-border healthcare purpose?		None identified. The national identity number is used for this purpose.[85]
Are there any measures that consider access to EHRs from health professionals in another Member State?		Malta is an active participant in the epSOS project, through which physicians in other participating countries are provided with access to the national patient summary of patients who have consented to take part in the project.[86] Patients abroad and in need of emergency care at a health institution taking part in epSOS, can give temporary permission to a physician abroad to access an electronic summary of health data about them that has been processed by Government hospitals in Malta.[87]

[83] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[84] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[85] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[86] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[87] https://ehealth.gov.mt/download.aspx?id=9168

2.5. Liability

2.5.1. Main findings

Maltese law does not set specific liability requirements related to the use of EHRs. The Data Protection Act foresees liability for persons who breach its requirements and process personal data in contravention of its provisions. Moreover, the Civil Code rules on liability based on fault could apply.

The Health Care Professions Act also contains provisions that might be relevant. The council of the specific health profession can investigate allegations of professional misconduct or breach of ethics by a health care professional falling under its supervision and can take measures where it finds that the health care professional is guilty of professional or ethical misconduct in any respect or has failed to abide by the professional and ethical standards applicable to him/her. In addition, health practitioners can be held liable for breach of professional secrecy under the Criminal Code and the Professional Secrecy Act.

Finally, the Criminal Code provides for the involuntary (or negligent) commission of offences, that is, where the harm results from the imprudence, carelessness, unskillfulness in an art or profession, or non-observance of regulations. Therefore health practitioners could be held criminally liable should their unskillfulness in exercising their profession result in a criminal damage.

No provision providing for the liability of patients for erasing key medical information in EHRs was found. Similarly, there is no specific provision to the effect that physicians can be held liable because of input errors. Liability would need to be based on the general legal provisions.

Government contracts with hosting providers make provision for data protection (both in terms of privacy and security), in line with the requirements of the Data Protection Act.[88] Hosting institutions may be held liable in case of defect of their security/software systems.

There are no liability rules related specifically to the misuse of secondary use health data. However, it may be relevant to note that if the Information and Data Protection Commissioner finds that personal data has been processed in an unlawful manner, the Commissioner must order rectification. If rectification is not effected or if the matter is urgent, the Commissioner may prohibit the controller of personal data from processing the personal data in any manner other than to store that data (Data Protection Act).

[88] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

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?	Data Protection Act, Articles 41A to 47 (added in 2012)	Maltese law does not set specific medical liability requirements related to the use of EHRs. The Data Protection Act foresees liability for any person who breaches its requirements and processes personal data in contravention of its provisions.
	Civil Code, Articles 1031 to 1033 and Article 1038	Moreover, the general rules on liability based on fault as found in the Civil Code could apply. According to Article 1031 of the Civil Code, every person is liable for damage that occurs through his/her fault. A person is considered to be in fault if, in his/her acts, s/he does not use the prudence, diligence and attention of a *bonus paterfamilias* (that is, a 'good father of the family') (Article 1032). Article 1033 of the Civil Code deals with culpable negligence and states that any person who, with or without intent to injure, voluntarily or through negligence, imprudence, or want of attention, is guilty of any act or omission constituting a breach of the duty imposed by law, is liable for any damage resulting therefrom. According to Article 1038 of the Civil Code, any person who without the necessary skill undertakes any work or service will be liable for any damage that, through his unskillfulness, he may cause to others.
	Health Care Professions Act, Articles 31 and 32	The Health Care Professions Act also contains provisions (Articles 31 and 32) that might be relevant. The relevant council of the specific health profession can investigate allegations of professional misconduct or breach of ethics by a health care professional falling under its supervision and can take measures where it finds that the health care professional is guilty of professional or ethical misconduct in any respect or has failed to abide by the professional and ethical standards applicable to him/her.
	Criminal Code, Article 257 (last amended in	In addition, it is noted that health practitioners can be held liable for breach of professional secrecy under Article 257 of the Criminal Code and the

Questions	Legal reference	Detailed description
	2007); Professional Secrecy Act, Article 3 (last amended in 2004)	Professional Secrecy Act. Finally, it is noted that the Criminal Code also makes provision for the involuntary (or negligent) commission of offences, that is, where the harm results from the imprudence, carelessness, unskillfulness in an art or profession, or non-observance of regulations. Therefore health practitioners could be held criminally liable should their unskillfulness in exercising their profession result in a criminal damage.
Can patients be held liable for erasing key medical information in EHRs?		No provision providing for the liability of patients for erasing key medical information in EHRs was found.
Can physicians be held liable because of input errors?	Criminal Code, Articles 337B to 337H (computer misuse) (last amended in 2010)	There is no specific provision to the effect that physicians can be held liable because of input errors. Liability can be based on the general legal provisions as described in the first row of this table. In addition, the computer misuse provisions in the Criminal Code may apply in specific cases.[89]
Can physicians be held liable because they have erased data from the EHRs?		There is no specific provision on liability for erasing data from EHRs. Liability would need to be based on the general legal provisions as described in the first row of this table.
Are hosting institutions liable in case of defect of their security/software systems?	Data Protection Act, Articles 26 (as introduced in 2003) and 42(2)(a) (last amended in 2012)	Government contracts with hosting providers make provision for data protection (both in terms of privacy and security), in line with the requirements of the Data Protection Act.[90] Article 26 of the Act requires the data controller to implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security. If the controller does not implement security measures in terms of Article 26, the Commissioner may impose an administrative fine (Article 42(2)(a)). According to the Fifth Schedule to the Act a level 2 fine can be imposed. According to the Third Schedule to the Act a level 2 fine is not less than EUR 250 but not more than EUR 2,500 or a daily fine of not less than EUR 25 but not more than EUR 250.

[89] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[90] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?		Maltese law does not contain specific provisions on liability risks for health professionals in relation to EHRs, therefore no measures to limit these liability risks were found.
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	Data Protection Act, Article 41B(4) (last amended in 2012) Criminal Code, Articles 337B to 337H (computer misuse) (last amended in 2010)	There is no specific national legislation. This would probably classify as a breach of the Data Protection Act punishable by a fine of not less than EUR 120 and not more than EUR 23,000 or to imprisonment for six months or to both such fine and imprisonment. Moreover, the computer misuse provisions of the Criminal Code may apply in specific cases.[91] Article 337C of the Criminal Code deals with unlawful access to, or use of, information.
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		There is no specific legal obligation, but there is a professional obligation.[92]
Are there liability rules related to the misuse of secondary use of health data?	Data Protection Act, Article 42 (last amended in 2012)	There are no liability rules related specifically to misuse of secondary use health data. However, it may be relevant to note that if the Information and Data Protection Commissioner finds that personal data has been processed in an unlawful manner, the Commissioner must order rectification, and if rectification is not effected or if the matter is urgent, the Commissioner may prohibit the controller of personal data to continue processing the personal data in any manner other than to store that data (Article 42(1) of the Data Protection Act). In the case of unlawful processing of personal data in contravention of Article 42(1), the Commissioner may impose an administrative fine. According to the Fifth Schedule to the Act a level 2 fine can be imposed. According to the Third Schedule to the Act a level 2 fine is not less than EUR 250 but not more than EUR 2,500 or a daily fine of not less than EUR 25 but not more than EUR 250.

[91] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[92] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

2.6. Secondary uses and archiving durations

2.6.1. Main findings

No specific rules on the archiving durations of EHRs were identified. However, it is noted that according to the Data Protection Act, the controller of personal data must ensure that personal data are not kept for a period longer than is necessary, having regard to the purposes for which they are processed. The Data Protection Act applies to the secondary use of EHR data.[93]

Health data can be used for secondary purpose as long as there is a legal basis for it. There is no specific legislation regulating whether certain health data cannot be used for secondary use. Relevant activity is guided by sectoral best practice and ethical considerations.[94] Similarly, Maltese law does not state who will be entitled to use and access this data.

[93] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[94] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

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?	Data Protection Act, Article 7(i) (as introduced in 2003)	No specific rules on the archiving durations of EHRs were identified. However, it is noted that as a general rule, according to Article 7(i) of the Data Protection Act, the controller of personal data must ensure that personal data are not kept for a period longer than is necessary, having regard to the purposes for which they are processed.
Are there different archiving rules for different providers and institutions?		No relevant rules were identified.
Is there an obligation to destroy data at the end of the archiving duration or in case of closure of the EHR?		No such requirement was identified.
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?		No relevant rules were identified.
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	Data Protection Act, Articles 8 and 16 (as introduced in 2003)	Health data can be used for secondary purpose as long as there is a legal basis for it (e.g. Malta Statistics Authority Act,[95] Notification of Cancer Act[96]).[97] According to Article 8 of the Data Protection Act, the processing of personal data for historical, statistical or scientific purposes is not incompatible with the purposes for which the information was collected. However, the controller must ensure that: (a) appropriate safeguards are in place where personal data processed for historical, statistical or scientific purposes may be kept for a period longer than necessary having regard to the purposes for which they are processed; or (b) personal data kept for historical, statistical or scientific purposes will not

[95] Chapter 422 of the Revised Laws of Malta; the Act provides for the establishment of the Malta Statistics Authority, and for the exercise of regulatory functions regarding resources relating to the collection and publishing of official statistics.
[96] Chapter 154 of the Revised Laws of Malta; the Act makes provision for the notification of cancer. Every medical practitioner attending on or called in to visit a patient must, on becoming aware that the patient is suffering from cancer, send to the Superintendent of Public Health a certificate stating the name, age, occupation and address of the patient and the type of cancer from which the patient is suffering as well as the organ, tissue or site which is affected by the disease.
[97] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

Questions	Legal reference	Detailed description
		be used for any decision concerning a data subject. Article 16 of the Act states that sensitive personal data (includes health data) may be processed for research and statistics purposes, provided that the processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data is disclosed.
Are there health data that cannot be used for secondary use?		There is no specific legislation. Relevant activity is guided by sectoral best practice and ethical considerations.[98]
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?		There is no specific legislation. Relevant activity is guided by sectoral best practice and ethical considerations.[99]
Does the law say who will be entitled to use and access this data?		There is no specific legislation.
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?		None identified.

[98] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[99] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

The myHealth record system enables patients and the physicians they choose to gain access to key parts of personal health records through any computer connected to the Internet. No obligations to develop interoperability of EHRs were identified in Maltese law. There are no requirements in the law that refer to the interoperability of national EHRs with EHR systems of other Member States.

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?		None identified.
Are there any specific rules/standards on the interoperability of EHR?		None identified.
Does the law consider or refer to interoperability issues with other Member States systems?		None identified.

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

There is no ePrescriptions system in place in Malta.[100] Therefore the tables in Section 2.8.2 have not been completed.

[100] According to information available on the epSOS website: http://www.epsos.eu/epsos-services/eprescription.html.

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?		No
Can an ePrescription be prescribed to a patient who does not have an EHR?		No

- ***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?		No
Can those health professionals write ePrescriptions without having access to EHRs?		No

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

As indicated in the previous sections, there is no specific Maltese legislation with respect to EHRs. Although general legislation could cover a number of issues relevant to EHRs, the absence of specific obligations tailored to the circumstances prevailing in the health sector could result in legal barriers to the deployment of EHRs. For example, the absence of specific requirements on the interoperability of EHRs could be considered as a barrier thereto. The absence of specific legal provisions also results in a lack of good legal practices for the deployment of EHRs in Malta and for their cross-border transfer in other EU Member States.

The following paragraphs summarise the situation with respect to a number of issues dealt with by this report, based on stakeholder feedback.

- Health data to be included in EHRs

Although Malta has not yet adopted any specific national legal requirements on EHR content, the groundwork has already been done for cross-border exchange of EHR data. In fact, Malta is an active participant in the epSOS project and is active in its Operational Pilot. In this role, it is already exchanging data with other participating countries (e.g. Portugal, Spain). The national patient summary dataset includes the epSOS patient summary minimum dataset.[101]

- Requirements on the institutions hosting EHR data

Maltese law does not currently set any specific authorisation requirements on the institutions that host the data from EHRs. The general rules contained in the Data Protection Act, Professional Secrecy Act and computer misuse provisions in the Criminal Code apply. In practice this general legislation does not appear to have inhibited the hosting of eHealth data. Hosting providers (including MITA, which is the Government's principal IT agency) have been required to adhere to the relevant parts of the Government's general ICT policy framework (http://ictpolicies.gov.mt).[102]

- Patient consent

In the absence of specific legal requirements, the matter of patient consent has not had significant impact on the development and/or implementation of EHRs. However, there is a growing awareness of the need to have a structured and explicit approach towards the management of patient consent for access to EHRs. The best example of this to date is the myHealth system, in which patients can exercise online real-time control over access by individual professionals to their health data.[103]

- Creation, access to and update of EHRs

Ever since health IT systems started to be developed in Malta, personal identification (of both patients and health professionals) has been based on the national ID number, and appears set to remain so. Authentication and authorisation has so far been based on passwords, issued either through the national e-ID system or other Government systems, and related role-based access. In the future it is likely to be based more on token-based digital certificates and signatures. The EU has already successfully demonstrated models of cross-border interoperability (through projects such as epSOS), but so far cross-border access to EHRs by health professionals is achieved through ad hoc bilateral

[101] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[102] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[103] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.

arrangements on a case-by-case basis.[104]

- Liability

Liability issues have not yet arisen.[105] The absence of provisions catering specifically for liability issues related to EHRs could constitute a legal barrier.

- Secondary use and archiving duration

The practice in Malta has been to retain EHR data for as long as possible, based on the principle that it may be required to deliver continuity of care in the long term. Secondary use of EHR data is allowed for specific academic and research purposes on a case-by-case basis, after formal consideration by a research ethics committee, or for statistical purposes where there is a legal basis for it.[106]

[104] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[105] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.
[106] Stakeholder response on behalf of the Ministry for Health, eHealth Office and MITA.