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 the Republic of Estonia

13 May 2014

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

This report was completed by Mr Kaupo Lepasepp, Ms Mari Matjus and Ms Mari Haamer from law firm SORAINEN. 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 Estonia

Estonian e-health solutions are among the leading ones in Europe. Estonian e-health has at its core the Estonian National Health Information System (**ENHIS**): a national central electronic database for processing health records of all patients receiving healthcare services from any Estonian healthcare service provider. The ENHIS has been functioning since 1 September 2008. The ENHIS has a national scope. All officially recognised healthcare service providers have the obligation under the law to upload their patients' EHRs on ENHIS. The ENHIS is the national 'umbrella' system that exists side by side with electronic data systems of individual healthcare service providers. Data held on the ENHIS is referred to in this study as 'ENHIS data'.

Patients can view all of their EHRs stored on the ENHIS on the patient platform 'My E-Health'.[1] Other e-health solutions developed in Estonia include Digital Prescription (ePrescription), Digital Registration, Digital Stamp and Digital Image (see Section 1.1).

The main institutions behind the ENHIS are the Ministry of Social Affairs and the Estonian E-Health Foundation (**EHF**). The EHF is a legal entity founded by the Ministry of Social Affairs, the major hospitals, and trade associations of healthcare professionals. The Ministry is in charge of policy and strategy, and the EHF additionally manages the daily administration of the ENHIS. The national Data Protection Inspectorate supervises whether health data, including EHRs are processed in compliance with sensitive personal data protection rules.

A special regime of laws and regulations has been established in order to regulate ENHIS. The Health Services Organisation Act establishes the general basis for the functioning of ENHIS. On the other hand, there is no special regulatory regime applicable to EHRs recorded by healthcare service providers in their own local databases. Therefore general requirements for processing health records apply to EHRs that are not synchronised with the central database, ENHIS.

Documentation of healthcare services (i.e. the obligation to report on the provision of such services) is regulated by the Health Services Organisation Act and the Regulation on the Documentation of Provision of Healthcare Services and the Conditions and Arrangements for the Retention of these Documents.[2] The Personal Data Protection Act applies to all sensitive personal data protection issues related to EHRs.

It is a distinctive feature of Estonian e-health that uniform classifications, standards and nomenclatures required for describing diseases, symptoms, and conditions have been developed and published.[3] The development of these classifications, standards and nomenclatures is at an advanced stage and the EHF and the Ministry of Social Affairs organise the training of healthcare professionals in order to increase the usage of that uniform terminology.[4]

At present the health data of foreign patients who receive treatment in Estonian hospitals is already entered into ENHIS the same way as the health data of local patients. A few legal and technical barriers need to be tackled so that ENHIS data could be shared with foreign healthcare service providers as well. Therefore, the next legal developments in Estonian e-health are likely to involve the sharing of ENHIS data with foreign healthcare service providers, especially in countries where many

[1] https://m.digilugu.ee/login
[2] Regulation of 18 September 2008 on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents.
[3] http://pub.e-tervis.ee/
[4] Interview with the Ministry of Social Affairs on 28th February 2014.

Estonians reside, such as Finland, Ireland, and Australia.[5]

2. Summary of legal requirements applying to EHRs

Definition of EHRs

Even though there is no legal definition of EHRs in Estonia, the content of ENHIS data has been regulated in detail. A regulation[6] provides for a list of medical documents (e.g. ambulatory epicrisis, notice of counselling) that must be uploaded to ENHIS. Annexes to this regulation provide for these documents' detailed data content.

Protection of EHRs

Estonian law contains specific regulatory requirements on the security level of ENHIS, which refer to the security levels established for all information systems managed by public entities. The security level of ENHIS is classified as 'high' and the security measures used for ENHIS have to be audited every two years. The security level of EHRs that are a part of the local databases of individual healthcare providers must meet the general requirements ensuring confidentiality, integrity and availability of personal data.[7]

While there is no legal obligation for encryption of EHRs, EHRs need to be kept secure and confidential, and in practice both ENHIS data and the vast majority of EHRs that individual healthcare service providers process are encrypted. Healthcare service providers are not prohibited from using an interface or software that is provided by a private company and there are no restrictions for the location of the servers where the EHRs are kept.

Patient consent is not necessary in order to create EHRs or share EHRs for the purpose of providing healthcare. Estonian law provides patients with an opt-out for the sharing of ENHIS data: the patient can make all or particular EHRs inaccessible in ENHIS. In order to invoke that right, a patient must submit an application to his or her healthcare service provider (effective towards ENHIS data created by that provider) or to the Ministry of Social Affairs (effective towards all ENHIS data).

There is no specific legislation on sharing EHRs with healthcare institutions in other Member States by e-mail or by other means, except for ENHIS itself, which is today not accessible to foreign healthcare institutions. The patient who wishes to receive cross-border healthcare must be provided access to his or her health records or be able to have copies of these, so that he or she can provide health records to healthcare service provider in another state.[8]

Access and updating of EHRs

Any Estonian healthcare professional is able to access ENHIS data for any patient, if the healthcare service provider that employs the healthcare professional has a valid Estonian activity licence and unless a particular patient has prohibited access to his or her ENHIS data. ENHIS data must only be accessed for the purpose of providing healthcare services. Patients are the owners of their health data and can view the access log to their ENHIS data on the patient platform 'My E-Health'. Patients have as a rule full access to all of their ENHIS data.

Healthcare professionals have the legal obligation to update ENHIS when providing a healthcare service to a patient. Before gaining access to ENHIS data, the validity of the healthcare provider's activity licence and healthcare professional's registration are checked.

[5] Interview with the Estonian Data Protection Inspectorate on 28th February 2014.
[6] Regulation on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents.
[7] Personal Data Protection Act § 25 (1).
[8] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, Art 5 (d).

The legal framework applicable to EHRs that are part of the healthcare service provider's local database are more ambiguous. Healthcare providers are required to document the provision of healthcare services, yet this documentation does not have to be electronical.

Liability

Legal principles applicable to the civil liability of healthcare service providers are found in the Law of Obligations Act. Estonian legislation does not stipulate a more specific legal regime for the liability related to processing EHRs. Therefore, the general principles for malpractice apply.

The breach of confidentiality by healthcare professionals is a criminal offence under the Penal Code. If the patient's rights have been violated upon processing of personal data, he or she may claim damages in civil court.

Archiving and secondary use

ENHIS data is archived indefinitely. Archiving of ENHIS data is regulated by the Statute of Health Information System.

Secondary use of EHRs is allowed for scientific research or statistics and it is mainly regulated under the Health Services Organisation Act and the Personal Data Protection Act. The requirements for secondary use of EHRs depend on whether the data is anonymised or not. If the data is anonymised, it does not constitute personal data and therefore falls outside the scope of the Personal Data Protection Act. Anonymised (coded) health data is not personal data and can be used for scientific research or official statistics without the consent of the patient. There is therefore no opt-out system in this regard.

The patient can however opt-out of secondary use of non-anonymised ENHIS data. In order to do that, the patient must submit an application to his or her healthcare provider (to prohibit use of ENHIS data connected to that provider) or to the Ministry of Social Affairs (to prohibit use of all personal data in ENHIS).

Interoperability

Interoperability of EHRs is a technical issue that has not received much attention from the legislator. However, the law stipulates which particular EHRs need to be uploaded to ENHIS. Such EHRs are uploaded from the healthcare service provider's local database to ENHIS and for this reason a sufficient degree of interoperability is necessary.

EHRs and ePrescriptions

The Digital Prescription (ePrescription) database enables electronic processing of prescriptions. The Digital Prescription database and ENHIS are separate and independent from each other and exist in parallel. However, some of the content of the Digital Prescription database automatically synchronises with ENHIS, but that synchronisation is not reciprocal. [9] In order to see the full history of digital prescriptions, the patient has to log into the state platform www.eesti.ee.

In most cases healthcare professionals have access to both ENHIS and the Digital Prescription database. As an exception, pharmacists cannot access ENHIS, but they have access to the Digital Prescriptions database, where they can view only currently valid and open prescriptions.[10]

3. Good practices

Stakeholders gave a generally positive feedback on the current Estonian EHRs system.[11] Estonia has

[9] Interview with the Ministry of Social Affairs on 28th February 2014.
[10] Interview with the Ministry of Social Affairs on 28th February 2014.
[11] Interviews with the representatives of the East Tallinn Central Hospital on 28th February 2014 and on 3rd March 2014, interview with the Ministry of Social Affairs on 28th February 2014, interview with the Estonian Data Protection Inspectorate on 28th February 2014, interview with the Tartu University Hospital on 3rd March 2014.

been a pioneer in the field and the small size of the population has made implementation of a nation-wide central EHRs database easier to implement.

All stakeholders interviewed confirmed that hospitals strictly protect EHRs and have established internal rules on accessing EHRs and ENHIS. Hospitals take any infringement of such internal rules very seriously and have issued warnings or ended employment contracts on grounds of unauthorised access to EHRs.[12] The Data Protection Inspectorate finds out about such cases through submitted complaints.[13] All activities on ENHIS are recorded and can be tracked down.

The representative of the Estonian Data Protection Inspectorate also expressed the opinion that healthcare service providers are diligent in ensuring that all the requirements of processing patients' health data are followed. She pointed out that hospitals apply even stricter rules in order to protect patients' health data than the law requires.

The representative of the Data Protection Inspectorate explained that there is no need under Estonian law to obtain the patient's consent for processing his or her health data, as the law allows processing sensitive personal data by a healthcare service provider only if that is necessary for providing the healthcare service.[14] Patient's consent is necessary for any other use of health data, including EHRs. The patient may opt-out from recording EHRs, whereas according to a hospital representative, patients generally recognise the benefits of EHRs and do not choose to opt-out.[15]

The highest security measures need to be taken when dealing with EHRs, but the law does not stipulate whether EHRs need to be transferred in encrypted form or not. In practice Estonian healthcare service providers share EHRs among themselves in encrypted form, whereas they share EHRs with local and foreign patients, and foreign healthcare service providers, directly via e-mail in the non-encrypted form.[16]

4. Legal barriers

A hospital representative emphasised that the legislator should review the list of EHRs and their content that needs to be uploaded to ENHIS under the law, so that the content of that data would meet the actual needs of providing top quality healthcare services.[17] According to this representative, Estonian e-health has come a long way, but needs to be updated.

Healthcare service providers' local data systems contain more data than the ENHIS. According to both a hospital and the the Ministry of Social Affairs, there is still a gap between the EHRs that are accessible in the healthcare professionals' local institution and that are accessible to all healthcare professionals in ENHIS.[18] In practice this problem can be solved when the patient requests a copy of his or her EHRs from the healthcare service provider and sends this to another healthcare service provider.[19] Such pattern, however, undermines the idea of ENHIS: to reduce the need for a patient to carry his or her health data and make it accessible online in a central database.

According to a hospital representative and a doctor, a major problem experienced by healthcare professionals regarding ENHIS is poor quality or lack of informative data in it. Some healthcare professionals do not enter all the necessary information in ENHIS and therefore the next healthcare

[12] Interview with the East Tallinn Central Hospital on 28th February 2014, interview with the Estonian Data Protection Inspectorate on 28th February 2014.
[13] Interview with the Estonian Data Protection Inspectorate on 28th February 2014.
[14] Interview with the Estonian Data Protection Inspectorate on 28th February 2014.
[15] Interview with the East Tallinn Central Hospital on 3rd March 2014.
[16] Interview with the Estonian Data Protection Inspectorate on 28th February 2014.
[17] Interview with the East Tallinn Central Hospital on 3rd March 2014.
[18] Interview with the East Tallinn Central Hospital on 28th February 2014, interview with the Ministry of Social Affairs on 28th February 2014.
[19] Interview with the East Tallinn Central Hospital on 3rd March 2014.

professionals treating the patient may not be aware of all the procedures conducted.[20] This could potentially end in offering unsuitable treatment to patients. It is possible that such providing of an unsuitable healthcare service in good faith has already occurred, but has never become public due to discretion of settlements.

A doctor and a hospital representative have both suggested that the healthcare professional's ENHIS interface needs to be modernised and made more user-friendly.[21] Doctors are concerned about the slow functioning, such as loading of a new page, of ENHIS, which wastes valuable minutes from the already limited appointment slot for each patient.[22] Meanwhile, from the patient's point of view the patient platform 'My E-Health' is fast and user-friendly.[23]

According to the Ministry of Social Affairs, the main difficulty for Estonia in implementing ENHIS has been the lack of an existing role model, given Estonia's pioneer position in the field. In addition to the technical solution, Estonia has had to invent from scratch the uniform standards, classifications and nomenclatures. Additionally, from the Ministry's perspective, the training of healthcare professionals and persuading them to use these unified standards, classifications and nomenclatures in making entries to ENHIS takes time and effort.[24]

The Ministry of Social Affairs expressed the view that Estonia and ENHIS are politically and technology-wise ready to share ENHIS data with healthcare service providers in other Member States. However, as she perceived, due to the advanced technological level of ENHIS, many Member States lack the capacity to cooperate regarding ENHIS.[25] The Data Protection Inspectorate expressed the view that there were no direct legal barriers under Estonian law for cross-border transfer of EHRs and ENHIS data between healthcare service providers in different Member States[26].

However, in order to gain access to the patient's ENHIS data, the healthcare service provider must have a valid (Estonian) activity licence, and the healthcare professionals must have a valid healthcare professional's licence. Foreign health institutions therefore currently cannot access ENHIS. Moreover, the most convenient method for logging into ENHIS is by using the Estonian national Identification Card. To log into ENHIS in this manner, the healthcare professional needs the Identification Card and a device for reading the chip on the Identification Card. Alternative way of logging in does exist: using PIN-codes, while logging in with the Identification Card is more convenient.

The hospital representative confirmed that foreign patients who have received treatment at Estonian healthcare service providers currently have their data on the hospital EHRs system. She also pointed out as a concern that there is currently no system that would enable exchange of EHRs with healthcare service providers abroad. Patient's health records are handed or e-mailed to them directly at the end of treatment. There is room for establishing a system for sharing EHRs with foreign patient's local doctors in other countries.[27]

[20] Interview with the East Tallinn Central Hospital on 28th February 2014, interview with the Tartu University Hospital on 3rd March 2014.
[21] Interview with the East Tallinn Central Hospital on 3rd March 2014, interview with the Tartu University Hospital on 3rd March 2014.
[22] Interview with the East Tallinn Central Hospital on 3rd March 2014.
[23] According to practical experience of Ms Mari Matjus, one of the authors of this report.
[24] Interview with the Ministry of Social Affairs on 28th February 2014.
[25] Interview with the Ministry of Social Affairs on 28th February 2014.
[26] Interview with Estonian Data Protection Inspectorate on 28th February 2014.
[27] Interview with the East Tallinn Central Hospital on 28th February 2014.

Contents

List of abbreviations

EHRs	Electronic Health Records
EHF	The Estonian E-Health Foundation
ENHIS	Estonian National Health Information System
ENHIS data	Data held on the Estonian National Health Information System

1. General context

1.1. EHR systems in place

The Estonian National Health Information System (**ENHIS**) is a national central electronic database for processing health records of all patients receiving healthcare services from any Estonian healthcare service provider. According to the legal definition, the ENHIS is a database that forms part of the state information systems and in which data related to healthcare is processed, with the purpose of concluding and performing healthcare service agreements, ensuring the quality of healthcare services, protection of patient's rights and public health, including registering the current status of public health and the management of the healthcare sector.[28]

The purpose of the ENHIS is to provide an effective exchange platform of EHRs (including from a time-sensitive perspective) for different healthcare service providers, patients and other stakeholders involved. The ENHIS has been functioning since 1 September 2008.

The ENHIS has a national scope, covering the entire Estonian territory. All officially recognised healthcare service providers have the obligation under the law to record their patients' EHRs on the ENHIS. Healthcare service providers have to conclude a contract with the Estonian E-Health Foundaton (**EHF**) in order to access the ENHIS. The ENHIS is used by all healthcare service providers: hospitals and clinics (despite their public or private ownership), general practitioners, dentists and other healthcare professionals working for these institutions and professionals. The notion of healthcare professional is defined under Estonian law in a different way than Directive 2011/24/EC as Estonian law excludes pharmacists. The ENHIS is not restricted to particular types of patients.

ENHIS is the national 'umbrella' system that exists side by side with electronic data systems of individual healthcare service providers. Most healthcare service providers have their own electronic systems for recording EHRs.[29] The law provides for the type of health data that needs to be uploaded to the ENHIS. Such data is uploaded from the healthcare provider's own system to the ENHIS automatically. Synchronisation occurs overnight or by manual order. Individual healthcare service providers' data systems therefore contain more information than the ENHIS.

The patient can view her electronic health records (**EHRs**) on the **patient platform 'My E-Health'** (*Minu e-tervis*)[30]. Identification of the patient takes place by logging in with an electronic national identification card or through mobile phone based identification (mobile-ID).

In addition to viewing patient's EHRs, the 'My E-Health' platform allows access to **Digital Registration**: the patient can digitally book doctor's appointments from different healthcare service providers. It is planned that in the future, Digital Registration solution will display the waiting period until the appointment.

The **Digital Stamp** solution enables general practitioners to upload data to the ENHIS without having to digitally sign every document separately. The purpose is to save doctors' time.

The **Digital Prescription** (e-Prescription) database enables to process prescriptions electronically. The patient presents his ID card in any pharmacy and the pharmacist accesses the digital prescription online. According to one of the stakeholders interviewed, the Digital Prescription database is connected to the ENHIS, as some of its content is automatically transferred to the ENHIS, but in order

[28] Healthcare Services Organisation Act and Associated Acts Amendment Act § 59¹ (1).
[29] Interview with the East Tallinn Central Hospital on 28th February 2014.
[30] https://m.digilugu.ee/login

to see the full history of digital prescriptions, the patient has to log in to the state platform www.eesti.ee.

The **Digital Image** project involves access to medical images, such as X-ray, and reduces the need for duplicated clinical analysis. According to a press release of the Ministry of Social Affairs of February 2014, the database of digital images developed by major hospitals will become accessible to all healthcare service providers and will be integrated to the state information systems.[31] The launching of the E-Ambulance solution, which would connect the alarm centre, the ENHIS, ambulance stations and emergency medical care departments, is scheduled for summer 2014.

The elements presented above do not constitute an exhaustive list of e-health solutions being developed in Estonia as the Ministry of Social Affairs and EHF are working on introducing more digital solutions.

1.2. Institutional setting

The main institutions behind the ENHIS are the Ministry of Social Affairs and Estonian e-Health Foundation (**EHF**). The national Data Protection Inspectorate supervises whether health data, including EHRs are processed in compliance with rules for sensitive personal data protection.

Ministry of Social Affairs

The department of e-health of the Ministry of Social affairs is responsible for organization and coordination of e-health projects and their implementation, as well as administration and development of the ENHIS standardisation of medical databases and classifications, and their integration in the healthcare system.[32]

The Ministry works closely with its subordinated unit – EHF. The Ministry is in charge of policy and strategy, and EHF additionally manages the daily administration of the ENHIS. The data controller for the ENHIS is the Ministry of Social Affairs. EHF is the person authorised to process data.[33]

EHF

The EHF was established in 2005 by the following stakeholders:

- Ministry of Social Affairs
- North Estonia Medical Centre
- Tartu University Hospital Foundation
- East Tallinn Central Hospital
- Estonian Hospitals Association
- Estonian Society of Family Doctors
- Union of Estonian Emergency Medical Services.[34]

The activity objectives of the EHF are guided by the goal provided in its Statute to develop and manage the components of the ENHIS and to coordinate necessary activities related to achieving these goals.[35] The EHF's main fields of activity are the development and administration of the ENHIS, classifiers, standards and nomenclatures, and developing its own organisation and its cooperation with international partners.

The EHF participates in:

- EHTEL/ELO (European Health Telematics Associations /EHTEL-Like Organizations)

[31] The Ministry of Social Affairs webpage, available at http://www.sm.ee/aktuaalne/uudised/b/a/pildipank-muutub-avatuks-koigile-raviasutustele.html
[32] Statute of E-health Department § 2 (1).
[33] Statute of E-health Department § 3 (1) and (2).
[34] Webpage of EHF, available at http://www.e-tervis.ee/index.php/en/2012-07-22-13-35-31/organization
[35] Statute of the E-Health Foundation § 2.

network that is active as an e-health competency network in Europe;
- European Commission's working group, i2010 SubGroup on eHealth;
- project 'CALL for InterOPErability'(CALLIOPE).

In 2007, the EHF initiated the Estonian Telemedicine Association which acts as a sub-organisation of the Finnish Society of Telemedicine and eHealth. The goal of this association is to connect the promoters of Estonian telemedicine and eHealth through discussion forum and cooperation.[36]

Data Protection Inspectorate

The Estonian Data Protection Inspectorate is the national supervisory authority of data protection. Health data, including EHRs, fall in the scope of sensitive personal data for which stricter regulatory requirements are applicable.[37]

1.3. Legal setting and future legal development

Current legal setting

A special regulatory regime has been established to regulate the ENHIS. It consists of several legal acts, both parliamentary laws and administrative regulations.

Chapter 5^1 of the **Health Services Organisation Act of 9 May 2001** establishes the most general regulatory requirements for the functioning of the ENHIS. It is also the basis for enforcing the government regulations concerning the ENHIS, which are mentioned below. It defines the ENHIS, establishes general principles for forwarding data to the ENHIS and granting access to ENHIS data and also establishes the ENHIS ethics committee.

Four government regulations have been adopted on the basis of chapter 5^1 of the Health Services Organisation Act:

1) **Regulation of 14 August 2008 on the Statute of Health Information System** (establishes the ENHIS and regulates data protection aspects);
2) **Regulation of 17 September 2008 on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents**;
3) **Regulation of 21 August 2008 on Types of Medical Images, Requirements of Information Technology therefor and Conditions and Procedure for Making them Available**;
4) **Regulation of 12 September 2008 on Health Information System Ethics Committee Rules of Procedure, Number and Procedure for Appointment of Members of the Committee**.

For EHRs recorded by the healthcare providers themselves, no special regulatory requirements have been adopted and thus the general regulatory requirements on personal data protection and documentation of provision of healthcare services apply.

Documentation of provision of healthcare services is regulated by the Health Services Organisation Act[38] and a government regulation which has been adopted on the basis of the same Act: **Regulation of 18 September 2009 on Documentation of Provision of Health Services and Conditions and Arrangements for Retention of these Documents**. The regulation mainly concerns health records with different types of content e.g. health card, ambulance card, dental care card. The regulation does not contain data protection rules, but refers to the Personal Data Protection Act. There are no regulatory requirements concerning EHRs specifically in either of those legal acts.

[36] Webpage of EHF, available at http://www.e-tervis.ee/index.php/en/2012-07-22-13-35-31/activities
[37] For more information see the webpage of the Estonian Data Protection Inspectorate, available at http://www.aki.ee/en
[38] Health Services Organisation Act § 4^2.

The **Personal Data Protection Act of 15 February 2007** applies as a general law to all personal data protection issues related to EHRs insofar as there are no more specific regulatory requirements in other legal acts (e.g. Statute of Health Information System). The Data Protection Inspectorate monitors compliance with the Personal Data Protection Act and guidelines issued by the Inspectorate are useful in interpreting the Act. For example, guidelines on processing personal data in scientific research have been issued by the Inspectorate.

The **Regulation of 20 December 2007 on the System of Security Measures for Information Systems** establishes security classes for information systems. The security class of ENHIS is also established on the basis of this regulation.

The legal principles for the civil liability of the providers of medical services are provided in the Law of Obligations Act. Estonian legislation does not currently regulate or prescribe a more specific legal regime for the liability related to the use of EHR systems. Therefore, the general principles for negligence/malpractice apply.

The **Law of Obligations Act of 26 September 2001** provides for the general regulatory requirements of the provision of healthcare services agreement. It establishes the confidentiality obligation of the healthcare service provider and healthcare professionals[39], the obligation to document the provision of healthcare services[40] and the liability of healthcare service providers[41]. It also provides the legal principles for the civil liability of the providers of medical services.

Digital prescriptions are regulated under **Regulation of 18 February 2005 on the Conditions and Procedure for the Issue of Prescriptions for Medicinal Products and for the Dispensing of Medicinal Products by Pharmacies and the Format of Prescriptions**. This regulation establishes:

1. The conditions and procedure for the issue of prescriptions for medicinal products and for the dispensing of medicinal products on the basis of prescriptions or order forms, including for the preservation and registration of medical prescription forms, order forms and accompanying documents;
2. The format of prescriptions;
3. The conditions and procedure for the dispensing of medicinal products on the basis of the prescriptions of the EU Member States, EEA Member States and the Swiss Confederation.[42]

Finally, the **Penal Code of 6 June 2001** prescribes criminal liability for confidentiality breaches and the **State Liability Act of 2 May 2001** provides the basis for claiming compensation if rights are violated in the process of performance of a public duty.

Future legal development

There was a consensus among the stakeholders interviewed that the legal framework for EHRs and cross-border processing of EHRs is sufficient and adequate. It ensures the protection of patients' rights and is flexible enough to accommodate new digital solutions that do not exist yet today. Therefore, we are not aware of planned changes in national laws in the field.

There are no direct legal barriers under Estonian law for cross-border transfer of EHRs and it is a matter of political agreement between Member States and of technical implementation.[43] The Ministry of Social Affairs is working towards such cooperation between Member States and inter-governmental negotiations regarding transfer of EHRs are ongoing with Finland, Ireland and Australia. Such

[39] Law of Obligations Act § 768.
[40] Law of Obligations Act § 769.
[41] Law of Obligations Act § 770.
[42] Conditions and Procedure for the Issue of Prescriptions for Medicinal Products and for the Dispensing of Medicinal Products by Pharmacies and the Format of Prescriptions §1 (1).
[43] Interview with Estonian Data Protection Inspectorate on 28th February 2014.

developments may result in **international treaties** providing a legal ground for forwarding and receiving EHRs from other countries with sufficient level of protection for health data.

List of relevant national legislation

Laws

- Health Services Organisation Act (*Tervishoiuteenuste korraldamise seadus*)
  - Adopted on 9 May 2001
- Personal Data Protection Act (*Isikuandmete kaitse seadus*)
  - Adopted on 15 February 2007
- Law of Obligations Act (*Võlaõigusseadus*)
  - Adopted on 26 September 2001
- Penal Code (*Karistusseadustik*)
  - Adopted on 6 June 2001
- State Liability Act (*Riigivastutuse seadus*)
  - Adopted on 2 May 2001

Regulations

- Statute of Health Information System (*Tervise infosüsteemi põhimäärus*)
  - Adopted on 14 August 2008
  - Regulation no 131 of the Government of the Republic
- Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents (*Tervise infosüsteemi edastatavate dokumentide andmekoosseisud ning nende säilitamise tingimused ja kord*)
  - Adopted on 17 September 2008
  - Regulation no 53 of the Minister of Social Affairs
- Types of Medical Images, Requirements of Information Technology therefor and Conditions and Procedure for Making them Available (*Meditsiiniliste ülesvõtete liigid, neile esitatavad infotehnoloogilised nõuded ning kättesaadavaks tegemise tingimused ja kord*)
  - Adopted on 21 August 2008
  - Regulation no 47 of the Minister of Social Affairs
- Health Information System Ethics Committee Rules of Procedure, Number and Procedure for Appointment of Members of the Committee (*Tervise infosüsteemi eetikakomitee töökord, komitee liikmete arv ja määramise kord*)
  - Adopted on 12 September 2008
  - Regulation no 51 of the Minister of Social Affairs
- Documentation of Provision of Health Services and Conditions and Arrangements for Retention of these Documents (*Tervishoiuteenuse osutamise dokumenteerimise ning nende dokumentide säilitamise tingimused ja kord*)
  - Adopted on 18 September 2009
  - Regulation no 56 of the Minister of Social Affairs
- System of Security Measures for Information Systems (*Infosüsteemide turvameetmete süsteem*)
  - Adopted on 20 December 2007
  - Regulation no 252 of the Government of the Republic
- Conditions and Procedure for the Issue of Prescriptions for Medicinal Products and for the Dispensing of Medicinal Products by Pharmacies and the Format of Prescriptions
  - Adopted on 18 February 2005
  - Regulation no 30 of the Minister of Social Affairs
- Statute of Estonian Cancer Registry (*Vähiregistri põhimäärus*)
  - Adopted on 26 May 2011
  - Regulation no 69 of the Government of the Republic
- Statute of Estonian Medical Birth Registry (*Meditsiinilise sünniregistri põhimäärus*)
  - Adopted on 26 May 2011
  - Regulation no 68 of the Government of the Republic

- Regulation on Establishment of Myocardial Infarction Registry and Statute of Maintenance of the Registry (*Müokardiinfarktiregistri asutamine ja registri pidamise põhimäärus*)
    - Adopted on 15 December 2011
    - Regulation no 156 of the Government of the Republic
- Statute of Estonian Tuberculosis Registry (*Tuberkuloosiregistri põhimäärus*)
    - Adopted on 26 May 2011
    - Regulation no 70 of the Government of the Republic

2. Legal requirements applying to EHRs in Estonia

2.1. Health data to be included in EHRs

2.1.1. Main findings

The Regulation on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents provides for a detailed list of documents that must be uploaded to the ENHIS. Annexes to this Regulation provide for the detailed data content of these documents.

According to § 2 (1) of this Regulation, data regarding healthcare services provided to the patient and for the purpose of healthcare management, including for keeping registers required under the law and containing data on health status, must be uploaded to the ENHIS.

According to § 2 (2) of this Regulation, the following documents regarding the healthcare service provided to the patient must be uploaded to the ENHIS:

1) ambulatory epicrisis;
2) stationary epicrisis;
3) doctor's letter entitling the patient for a medical procedure or appointment with another doctor;
4) reply to doctor's query and letter entitling the patient for a medical procedure or appointment with another doctor
5) notice of opening an ambulatory medical case;
6) notice of opening a stationary medical case;
7) notice of closing an ambulatory medical case;
8) notice of closing a stationary medical case;
9) notice on assessment of development;
10) notice of immunisation;
11) notice of side effects of immunisation;
12) notice of physical examination;
13) notice of counselling;
14) notice of growing.

EHRs have not been legally defined in Estonia. The EHF has published uniform classifications, standards and nomenclatures required for describing diseases, symptoms, conditions etc. on the ENHIS.

Patients are identified through their national identification numbers.

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?)	Regulation on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents (last amended: 21 August 2010) § 2 and 3	According to § 2 (1) of the Regulation, data regarding healthcare services provided to the patient and for the purpose of healthcare management, including for keeping registers provided under the law and containing data on health status, must be uploaded to the ENHIS. According to § 2 (2), the following documents regarding the healthcare service provided to the patient are uploaded to the ENHIS: 1) ambulatory epicrisis; 2) stationary epicrisis; 3) doctor's letter entitling the patient for a medical procedure or appointment with another doctor; 4) reply to doctor's query and letter entitling the patient for a medical procedure or appointment with another doctor 5) notice of opening an ambulatory medical case; 6) notice of opening a stationary medical case; 7) notice of closing an ambulatory medical case; 8) notice of closing a stationary medical case; 9) notice on assessment of development; 10) notice of immunisation; 11) notice of side effects of immunisation; 12) notice of physical examination; 13) notice of counselling; 14) notice of growing. Under paragraph 3, the data that must be contained in the documents listed above (paragraph 2) are detailed in the Regulation's Annexes.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	Annex 1 to the Regulation on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents (last amended: 21 August 2010):	The data that must be uploaded to the ENHIS does not only contain medical information as required under the Annexes to the Regulation. Annex 1 to the Regulation defines the data that must be included in ambulatory epicrisis documents. This data includes information relating to the patient's employer and profession.

Questions	Legal reference	Detailed description
	Data Content of ambulatory epicrisis. Annex 2 to the Regulation above: data content of stationary epicrisis. Annex 9 to the Regulation above: data content of notice on assessment of development; Annex 10 to the Regulation above: data content of notice of immunisation; Annex 11 to the Regulation above: data content of notice of immunisation; Annex 12 to the Regulation above: data content of notice of physical examination; Annex 13 to the Regulation above: data content of notice of counselling; Annex 14 to the Regulation above: data content of notice of growing.	Annex 2 to the Regulation defines the data that must be included in stationary epicrisis documents. This data includes information relating to the patient's actual place of residence, patient's employer and profession. Annex 9 to the Regulation defines the data that must be included in notice on assessment of development. This data includes information relating to the patient's employer and profession, description of work conditions, educational institution. Annex 10 to the Regulation defines the data that must be included in notice of immunisation. This data includes information relating to the patient's employer and profession, description of work conditions, educational institution. Annex 11 to the Regulation defines the data that must be included in notice of immunisation. This data includes information relating to the patient's employer and profession, description of work conditions, educational institution. Annex 12 to the Regulation defines the data that must be included in notice of physical examination. This data includes information relating to the patient's employer and profession, description of work conditions, educational institution. Annex 13 to the Regulation defines the data that must be included in notice of counselling. This data includes information relating to the patient's employer and profession, description of work conditions, educational institution, situation of the family, health habits, psychosocial background and development, mental background and development. Annex 14 to the Regulation defines the data that must be included in notice of growing. This data includes information relating to the patient's employer and profession, description of work conditions, educational institution, patient's actual place of residence.

Questions	Legal reference	Detailed description
Is there a definition of EHR or patient's summary provided in the national legislation?	Regulation on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents (last amended: 21 August 2010) § 2 and 3 and annexes.	There is no legal definition of EHRs in Estonia. There is no definition of patient's summary in Estonia, however, the Regulation details the list of documents that must be uploaded to the ENHIS (e.g. ambulatory and stationary epicrisis).
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	Regulation on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents (last amended: 21 August 2010) § 2 and 3 and annexes.	Annexes to the Regulation provide for a very detailed list of data that has to be included per document type in each EHRs that must be uploaded to the ENHIS. Please see detailed description under questions 1 & 2 above.
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?		The EHF has developed over the years and published the classifications, standards and nomenclatures.44 The classifications, standards and nomenclatures are based on Estonian and medical terminology (Ancient Greek and Latin). The development of the classifications, standards and nomenclatures is at an advanced stage and the Ministry and the EHF arrange trainings for medical professionals on using that uniform terminology in EHRs.
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)?		Both a hospital and a Ministry representatives confirmed that the patient sees the very same data that the doctors see on the 'My E-Health' platform, except when the doctor has decided to 'hide' a document from the patient before communication of the content in a way that the healthcare professional finds suitable. A document can be hidden for up to 6 months (also see table 2.4.2 on access below).
Are there any specific rules on identification of patients in EHRs?	Statute of Health Information System (last amended: 24 July 2009) § 12	The data subject is considered as identified if: 1) the data subject exercises its rights through the state web platform www.eesti.ee;

[44] http://pub.e-tervis.ee/

Questions	Legal reference	Detailed description
		2) the data subject submits a digitally signed application to an e-mail address provided by the state in the www.eesti.ee web platform. 3) a duely authorised person has identified the data subject according to a procedure provided under the law; 4) the data subject has authenticated itself in the health information system platform through a secure means of authentification (national Identity Card, Mobile-ID).
Is there is a specific identification number for eHealth purposes?		The ENHIS uses a person's name and national identification number for identification. People can access ENHIS by logging in with their national Identity Cards (ID cards). The Identity Card is inserted in the computer or in a separate device for reading ID cards. In order to log in, the PIN-codes are needed as well. Both the Identity Cards and the accompanying PIN-codes are provided by the Police and Border Guard Board.

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

Estonian law contains specific regulatory requirements on the security level of the ENHIS, which refer to the general system of security levels established for all information systems managed by public bodies. The content of the required security measures is determined by detailed guidelines issued by the Ministry of Economic Affairs and Communication. Due to the sensitivity of the data managed under the ENHIS, its overall security level has been classified as 'H' (high), and as a result security measures used for ENHIS have to be audited every two years.

The required security level of EHRs that are a part of the documentation of individual healthcare providers is based on general requirements ensuring confidentiality, integrity and availability of the data.[45]

There is no encryption obligation established by law, but in practice both ENHIS and EHRs which individual healthcare providers share with other providers are encrypted.

[45] The Personal Data Protection Act § 25 (1).

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?		Described in more detail below.
Is there a need for a specific authorisation or licence to host and process data from EHRs?	Statute of Health Information System (last amended: 24 July 2009) § 3 (2) Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 42 (11)	The EHF (see Section 1.2) maintains, manages and develops the ENHIS according to the Statute of Health Information System, a government regulation. Therefore, only the EHF is authorised to fulfil these tasks connected to the ENHIS. Individual healthcare providers may also document the provision of healthcare services in the form of EHRs. No specific authorisation or licence is required from healthcare providers to use EHRs for documentation purposes. Healthcare providers are not prohibited from using an interface or software that is provided by a private company and there are no authorisations or licencing requirements. There are no restrictions in the law for the location of servers.
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)?	Statute of Health Information System (last amended: 24 July 2009) § 6 Regulation on System of Security Measures for Information Systems (last amended: 25 January 2009) § 7, § 9 Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 42 (11) Regulation on Documentation of Provision of Health Services and	The security measures that are used for the ENHIS must correspond to security classes, which are based on a general system of security classes which apply to all databases managed by public sector bodies. The necessary security measures are established by detailed guidelines published by the Ministry of Economic Affairs and Communication.46 The security classes of the ENHIS are established as follows (the numbers show security classes 0 – 3): - confidentiality – S2 i.e. confidential information: the use of data is only allowed to certain user groups, access is allowed in the case of justified interest. - integrity – T3 i.e. source of information, modifying and destroying

[46] More information on the general system of security levels on the webpage of the Estonian Information System Authority: https://www.ria.ee/iske-en

Questions	Legal reference	Detailed description
	Conditions and Arrangements for Retention of these Documents (last amended: 21 August 2010) § 1 (4) Personal Data Protection Act (last amended: (1 January 2011) § 25	data must always be recorded; constant control of whether the data is correct, complete and up to date - availability – K2 i.e. reliability 99% (around 2 hours of down time per week allowed), allowed increase in reaction time at peak capacity – minutes (1÷10). The overall security level of ENHIS is high (H) i.e. the highest level. This affects the frequency of the auditing obligation (see below in same table for details). As for EHRs created by individual healthcare providers, documents certifying the provision of healthcare services may be created and preserved as EHRs if preservation of the integrity and authenticity of the data is ensured during the prescribed retention period and the EHRs are arranged and described pursuant to the Archives Act. Also, general requirements from the Personal Data Protection Act must be fulfilled. A person that processes personal data is required to take organizational, physical and information technology security measures to protect personal data against accidental or intentional unauthorised alteration of the data (integrity of data), against accidental or intentional destruction and prevention of access to the data by entitled persons (availability of data) and against unauthorised processing (confidentiality of the data). Upon processing of personal data, the person that processes the data is required to: 1) prevent access of unauthorised persons to the equipment used for processing personal data; 2) prevent unauthorised reading, copying and alteration of data within the data processing system, and unauthorised transfer of data storage mediums; 3) prevent unauthorised recording, alteration and deleting of personal data and to ensure that it be subsequently possible to determine when, by whom and which personal data were recorded, altered or

Questions	Legal reference	Detailed description
		deleted or when, by whom and which data was accessed in the data processing system; 4) ensure that every user of a data processing system only has access to personal data permitted to be processed by him or her, and to the data processing to which the person is authorised; 5) ensure the existence of information concerning the transmission of data: when, to whom and which personal data was transmitted and ensure the preservation of such data in an unaltered state; 6) ensure that unauthorised reading, copying, alteration or erasure is not carried out in the course of transmission of personal data via data communication equipment, and upon transportation of data carriers; 7) organise the work of enterprises, agencies or organizations in a manner that allows compliance with data protection requirements. 8) The person that processes personal data is required to keep account of the equipment and software which are under their control and are used for processing of personal data, and record the name, type, location and name of the producer of the equipment and the name, version and name of the producer of the software, and the contact details of the producer.
In particular, is there any obligation to have the information included in EHRs encrypted?	Statute of Health Information System (last amended: 24 July 2009) § 6 (2)	ENHIS data is in practice encrypted, however, the obligation to encrypt ENHIS data is not directly required by law. The law only requires the level of security of the ENHIS to be 'high'.In practice healthcare providers forward EHRs to other healthcare providers in an encrypted form, however, there is no obligation established by law to encrypt EHRs which are part of the healthcare provider's own documentation.
Are there any specific auditing requirements for institutions hosting and processing EHRs?	Regulation on System of Security Measures for Information Systems (last amended: 25 January 2009) § 91 (1) Statute of Health Information System (last amended: 24 July 2009) § 6 (2)	Security measures system for the ENHIS must be independently audited every two years, as it is a database with security level H (high). There is no specific auditing requirement established by law for individual healthcare providers who use EHRs as a part of their documentation.

2.3. Patient consent

2.3.1. Main findings

Patient consent is not needed for creating EHRs or for processing EHRs for the purpose of providing healthcare. However, Estonian law has established an opt-out system for the sharing of EHRs in the ENHIS – the patient can prohibit sharing EHRs in the ENHIS with healthcare providers. To do that, the patient must submit an application to his or her healthcare provider (to prohibit access to ENHIS data connected to that provider) or to the Ministry of Social Affairs (to prohibit access to all personal data in the ENHIS).

There are no specific regulatory requirements on sharing EHRs with healthcare institutions in other Member States. The patient who wishes to receive cross-border healthcare must be provided with the option to have remote access to his or her treatment documents or to have copies of the documents so that they can provide the documents to the cross-border healthcare provider.

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?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 41 (1), § 592 (1) 3)	Patient consent for setting up EHRs is not needed. Healthcare providers, who have the obligation to maintain confidentiality arising from the law, have the right to process personal data required for the provision of a health service, including sensitive personal data, without the permission of the patient. This includes creating EHRs whether the healthcare providers document the provision of healthcare services for their own purposes, or forwarding this information to the ENHIS and therefore creating ENHIS data.
Is a materialised consent needed?		Patient consent is not required, therefore there are no provisions on materialising such consent.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	Statute of Health Information System (last amended: 24 July 2009) § 13 (1) 2) Personal Data Protection Act (last amended: 1 January 2011) § 19 (1) 2)	If the patient requests it, the Ministry of Social Affairs must inform the patient of the purposes of processing his or her personal data in the ENHIS. The information must be given within five working days. It is not specified how and to whom exactly the request must be made. Also the healthcare provider must inform the patient of the purposes of processing of personal data in the form of EHRs as a part of the healthcare provider's documentation if the patient requests it. This obligation arises from the general regulatory requirements of the Personal Data Protection Act. As explained above, the patient cannot prohibit the creation of EHRs.
Are there specific national rules on consent from the patient to share data?		As explained below, Estonian law has established an opt-out system for patients concerning the sharing of ENHIS data and other EHRs. This means that initial patient consent to share data for

Questions	Legal reference	Detailed description
		the purpose of providing healthcare services is not required.
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 41 (1), § 592 (1) 3)	Healthcare providers, who have the obligation to maintain confidentiality arising from the law, have the right to process personal data required for the provision of a health service, including sensitive personal data, without the permission of the patient. This includes forwarding the patient's health data to the ENHIS, which is compulsory for healthcare providers, as well as processing their own EHRs.
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 41 (1), § 593 (3), § 593 (4) Statute of Health Information System (last amended: 24 July 2009) § 16	The patient has the right to prohibit the access of a healthcare provider to personal data in the ENHIS. Initially, the patient's healthcare provider(s) have access to the patient's personal data without the patient's explicit consent. Therefore, Estonian law establishes an opt-out system for sharing patient data in the ENHIS. Under the Statute of Health Information System § 16 (1), the patient can prohibit access to certain documents or to all personal data in the ENHIS. Under the Statute of Health Information System § 16 (2), through the healthcare service provider, the patient has the right to prohibit access only to records created under the healthcare service provision agreement (i.e. the documents that the same healthcare service provider had created in the process of healthcare service provision). To do that, the patient must submit an application to his or her healthcare provider (to prohibit access to ENHIS data connected to that provider) or to the

Questions	Legal reference	Detailed description
		Ministry of Social Affairs (to prohibit access to all personal data in the ENHIS). If the application is submitted to the healthcare service provider, it must be in written form. If the application is submitted to the Ministry of Social Affairs, it can be done online on the patient platform 'My E-Health.'47 Identification of the patient takes place by logging in with thenational Identity Card or through mobile phone based identification (mobile-ID). On the 'My E-Health' platform, the patient has several options: (1) to deny access to all data on the ENHIS for 'the doctor' (probably meaning any healthcare professional who would otherwise be able to access the patient's EHRs), whereas as a warning is displayed if the patient clicks on the respective box; (2) to deny access to individual ambulatory epicrises for 'the doctor'; (3) to deny access to 'time-sensitive data' for 'the doctor'. 'Time-sensitive' data includes allergies, serious or chronical diseases and pharmaceuticals that the patient currently takes. The patient can also grant access to his or her ENHIS data to other persons e.g. family members. The regulatory requirements on sharing the healthcare provider's own documentation in the form of EHRs are less clear than the requirements on ENHIS data. The same initial principle applies – initial patient consent for sharing EHRs is not required, if the EHRs are shared for the purpose of

[47] https://m.digilugu.ee/login

Questions	Legal reference	Detailed description
		providing healthcare. However, Estonian law does not provide a clear possibility for patients to prohibit the sharing of the healthcare provider's own documentation in the form of EHRs for the purpose of providing healthcare.
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?	Statute of Health Information System (last amended: 24 July 2009) § 13 (1) 2)	If the patient requests it, the Ministry of Social Affairs must inform the patient of the purposes of sharing his or her personal data in the ENHIS. As discussed above, the patient can prohibit access of his or her healthcare providers to his or her ENHIS data. There is no clear legal requirement to inform the patient of the consequences of prohibiting access to his or her ENHIS data. If the patient clicks on the respective box in the patient portal 'My E-Health' in order to deny access to all data on the ENHIS for 'the doctor', a warning appears, which says that by denying access to data the patient takes responsibility for possible decrease in the quality of treatment.
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)?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 41 (1), § 593 (2), § 505 (5) Statute of Health Information System (last amended: 24 July 2009) § 9 (1), § 9 (4)	Patient consent is not required for the processing and sharing of ENHIS data by their healthcare providers. The law does not specify whether only Estonian healthcare providers have access to the patient's ENHIS data or EHRs which are part of healthcare providers' own documentation. However, in order to have automatic electronic access to the patient's ENHIS data, the healthcare provider must have a valid Estonian activity licence. Therefore foreign health institutions do not have automatic access to the patient's ENHIS data.

Questions	Legal reference	Detailed description
		When accessing ENHIS, the validity of the healthcare professional's licence is checked, as well. The patient who wishes to receive cross-border healthcare must be provided with an option to have remote access to his or her treatment documents or to have copies of the documents so that they can provide the documents to the cross-border healthcare provider.
Are there specific rules on patient consent to share data on a cross-border situation?	Personal Data Protection Act (last amended: 1 January 2011) § 12 Statute of Health Information System (last amended: 24 July 2009) § 9 (1), § 9 (4)	At the moment, only healthcare providers that have a valid Estonian activity licence, and healthcare professionals who have a valid healthcare professional's licence, can access ENHIS data online. There are no regulatory requirements specifically on sharing ENHIS data with healthcare institutions in other Member States. However, if the patient has expressly consented to sharing EHRs with healthcare institutions in other Member States, sharing is allowed. This option is based on the principles established in the Personal Data Protection Act, according to which any type of data processing that the data subject (patient in this case) expressly consents to, is allowed. In the case of sensitive personal data, the consent must be obtained in a format which can be reproduced in writing. The ENHIS web page does not provide any technical options specifically for sharing data with healthcare providers in other Member States or for obtaining patient consent for this type of sharing.

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

All healthcare professionals are able to access ENHIS data on all patients, unless the patient has prohibited access to his or her ENHIS data. However, ENHIS data must only be accessed for the purpose of providing healthcare. There are no differences in the right to access ENHIS data of different types of healthcare professionals. Patients and the EHF can monitor who has accessed patients' ENHIS data, they can view the log on the ENHIS website. Patients can view their own ENHIS data, modify and add information for which they are the source (e.g. contact information) and also authorise other persons to access their ENHIS data. Healthcare professionals are able to restrict patients' access to ENHIS data for a limited period, e.g. if they wish to inform the patient of a particular illness themselves.

Healthcare professionals have the obligation to update ENHIS data. Before gaining access to ENHIS data, the validity of the healthcare provider's activity licence and the validity of the healthcare professional's licence are checked.

Regulatory requirements concerning EHRs that are a part of the healthcare provider's own documentation are less clear. The healthcare providers are required to document the provision of healthcare and this can be done in the form of EHRs, but it can also be done non-electronically. In any case, the regulatory requirements are quite similar to the requirements on ENHIS data i.e. the patient must be allowed to access his or her personal data and information on who else has accessed his or her personal data.

There may be legal barriers to cross-border healthcare in the regulatory rules and technical access to ENHIS data. First, if a foreign healthcare provider seeks access to ENHIS data, the validity of the healthcare provider's Estonian healthcare professional's licence is checked. Second, the most convenient method for logging into ENHIS is by using the Estonian Identity Card. We acknowledge, however, that an alternative method, using PIN-codes, exists. This can be considered as a legal or at least technical barrier to cross-border healthcare in the EU.

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?	Personal Data Protection Act (last amended: 1 January 2011) § 27 (1) Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 41 (1)	General requirements from the Personal Data Protection Act apply to creating EHRs. All persons who fulfil these general requirements can create EHRs, Estonian law does not establish a limited list of persons who can create EHRs. As EHRs contain sensitive personal data, they can only be created by persons who are registered for processing of sensitive personal data at the Data Protection Inspectorate.
Are there specific national rules on access and update to EHRs?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 592, § 593 Statute of Health Information System (last amended: 24 July 2009) § 4, § 5, § 8 - § 11, § 13 - § 15	Only a limited number of persons can submit data to the ENHIS. Data on provision of healthcare services is provided by healthcare providers, but additional data can also be provided by other persons. For example, the Estonian Health Insurance Fund provides information on whether the patient is insured or not. Patients have access to their own ENHIS data and may request access to EHRs held by general practitioners. They can only update non-medical information such as contact information, etc.
Are there different categories of access for different health professionals?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 3 (1), § 41 (1), 593 (2) Statute of Health Information System (last amended: 24 July 2009) § 9 (1), § 9 (2)	EHRs should be accessed by healthcare professionals only for the purpose of providing treatment. In practice, ENHIS data of all patients (who have not prohibited access to their data) is accessible to all healthcare professionals. However, as all activity is logged, healthcare professionals who view EHRs for another purpose than providing healthcare can be held liable. Access to ENHIS data is granted to all persons who are healthcare professionals under Estonian law: doctors, dentists, nurses, and midwives, provided they are registered with the Health Board. Therefore, all healthcare professionals who are connected to providing healthcare to a specific patient have the right to access the patient's EHR in the ENHIS. The same rules apply to EHRs which are part of the healthcare institution's own documentation – they may only be accessed for the

Questions	Legal reference	Detailed description
		purpose of providing healthcare. Also note that certain State's officials can be granted access to anonymised ENHIS data for secondary use purposes (see Section 2.6).
Are patients entitled to access their EHRs?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 593 (1) Statute of Health Information System (last amended: 24 July 2009) § 13, § 4 (1) Personal Data Protection Act (last amended: 1 January 2011) § 19	Patients are entitled to access their EHRs on the patient platform 'My E-Health'. General rules from the Personal Data Protection Act apply to EHRs which are part of the healthcare provider's own documentation. The patient is also entitled to access these EHRs. However, the doctor has 5 days since the end of stationary treatment to submit health data to the ENHIS, which is why the patient may not be able to access that data immediately.
Can patient have access to all of EHR content?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 593 (1) Statute of Health Information System (last amended: 24 July 2009) § 13 Personal Data Protection Act (last amended: 1 January 2011) § 19	Patients can have access to all of their EHRs, but in order to protect a patient's life or health the healthcare provider may set a time limit of up to 6 months upon forwarding data to the ENHIS in the course of which the patient can only first examine his or her personal data through a healthcare professional. This restriction only applies to patients and not to other healthcare providers.
Can patient download all or some of EHR content?		In the case of corss-border healthcare, the patient must have remote access or be able to have copies of treatment documents. If the treatment documents are already remotely accessible via the patient platform 'My E-Health', the law does not require that the documents must also be downloadable. In practice, it is not possible to download EHRs from the patient platform 'My E-Health', but it is possible to print individual EHRs.

Questions	Legal reference	Detailed description
Can patient update their record, modify and erase EHR content?	Statute of Health Information System (last amended: 24 July 2009) § 14, § 17	The patient has the right to modify or update ENHIS data but only with regard to the type of information that is based on the patient's testimony (e.g. contact information). The patient can make declarations of intention on the patient platform 'My E-Health' concerning: - granting and prohibiting access to personal data; - donating organs and tissues after death; - donating his or her body to scientific research and study after death; - consenting to blood transfusions; - choosing a contact person; - authorising other persons to buy prescription medicinal products for them. Whether the patient can modify EHRs which are part of the healthcare provider's own documentation is not regulated by law.
Do different types of health professionals have the same rights to update EHRs?		Any healthcare professional under Estonian law (i.e. doctors, dentists, nurses, and midwives, provided they are registered with the Health Board) have the same rights to update EHRs.
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 593 (1), (2) Personal Data Protection Act (last amended: 1 January 2011) § 10 (1)	Only healthcare providers and patients themselves are entitled to access non-anonymised ENHIS data. Also forensic experts of a state forensic institution are entitled to access ENHIS data of a deceased person for ascertaining the characteristics of injuries. All other persons (including insurance companies, banks) are not entitled to access to ENHIS data or any other type of EHRs.
Are there exceptions to the access requirements (e.g. in case of emergency)?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 41	All healthcare professionals who are providing healthcare services to a patient have the right to access the patient's ENHIS data and other EHRs without the patient's consent. Therefore normally there is no problem with access to EHRs also in the case of emergencies.

Questions	Legal reference	Detailed description
	(1) Personal Data Protection Act (last amended: 1 January 2011) § 14 (1) 3)	Under the Personal Data Protection Act, all persons have the right to access someone else's personal data without their consent in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible.
Are there any specific rules on identification and authentication for health professionals? Or are they aggregated?	Statute of Health Information System (last amended: 24 July 2009) § 9 (4)	If a healthcare professional wants to access ENHIS data, the validity of the healthcare provider's activity licence and the validity of the healthcare professional's licence are checked before granting access to EHRs. Healthcare professionals access ENHIS data by logging in with their national Identity Cards or by using PIN-codes provided. This can be considered as a legal or technical barrier to cross-border healthcare service.
Does the patient have the right to know who has accessed to his/her EHRs?	Statute of Health Information System (last amended: 24 July 2009) § 13 (1) 5) Personal Data Protection Act (last amended: 1 January 2011) § 19 (1) 5)	The patient has the right to know who has accessed his or her ENHIS data. The patient can view on the patient platform 'My E-Health' who has accessed her ENHIS data. The Personal Data Protection Act establishes the same right as regards to the EHRs which are a part of the healthcare provider's own documentation. However, in practice, the healthcare providers do not keep such detailed records about accessing EHRs as the records which are available in the ENHIS.
Is there an obligation on health professionals to update EHRs?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 592 (1), § 42 (11) Statute of Health Information System (last amended: 24 July 2009) § 4 (1) Regulation on Documentation of Provision of Health Services and Conditions and Arrangements	The healthcare providers have the obligation to update the ENHIS. The healthcare providers also have a separate obligation to document the provision of healthcare services and this can also be done in the form of EHRs. However, it can also be done non-electronically.

Questions	Legal reference	Detailed description
	for Retention of these Documents (last amended: 21 August 2010) § 2 (5), § 1 (4)	
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 41 Statute of Health Information System (last amended: 24 July 2009) § 17 (1) 1)	Data relating to the patient's state of health who is in hospital (including the patient's EHRs) may be accessed by those closest to him or her, except if the patient has prohibited access to the data or a body conducting an investigation has prohibited access to the data in the interests of preventing a criminal offence, of apprehending a criminal offender or ascertaining the truth in a criminal proceeding. It is unclear, who falls under the term "those closest to him or her". On the patient platform 'My E-Health', the patient can authorise other persons to access his or her ENHIS data. Doctors who are providing a second opinion to the patient are also considered to be providing healthcare to the patient and can access the patient's ENHIS data.
Is there in place an identification code system for cross-border healthcare purpose?		There is no identification code system in place for cross-border healthcare purposes.
Are there any measures that consider access to EHRs from health professionals in another Member State?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 505 (5)	At the moment, health professionals in other Member States can access a patient's EHRs through the patient i.e. if the patient logs in to the patient platform 'My E-Health' and shows his or her EHRs to the healthcare professional. Patients who wish to receive or who receive cross-border health services must be provided with the option to have remote access to their treatment documents (i.e. electronically) or to receive copies of the documents. This applies also to EHRs which are a part of the healthcare provider's own documentation.

2.5. Liability

2.5.1. Main findings

The legal principles for the civil liability of the providers of medical services are provided in the Estonian Law of Obligations Act. Estonian legislation does not currently regulate or prescribe a more specific legal regime for the liability related to the use of EHR systems. Therefore, the general principles for negligence apply.

As a general rule, the providers of healthcare services and qualified doctors and dentists, and nurses or midwives providing healthcare services independently, who participate in the provision of healthcare services and operate on the basis of an employment contract or other similar contract entered into with a provider of healthcare services will be liable only for the wrongful violation of their own obligations, particularly for errors in diagnosis and treatment and for violation of the obligation to inform patients and obtain their consent. Culpability is a prerequisite for such liability. A healthcare professional will also be personally liable besides the provider of healthcare services for performance of a contract for the provision of healthcare services (joint and several liability). Providers of healthcare services will also be liable for the activities of persons assisting them and for any defects in the equipment used upon provision of healthcare services.

If there is an error in diagnosis or treatment and a patient develops a health disorder which could probably have been avoided by ordinary treatment, the damage is presumed to have resulted from the error. Important aspects here are the fault, the harm, and the causality between these two elements. The burden of proof lies with the patient, and in order to avoid liability, the medical service provider must have followed all of its other obligations, including the duty to notify and to maintain confidentiality. The burden of proof regarding circumstances which are the bases for the liability of the provider of healthcare services lie with the patient unless the provision of healthcare services to the patient is not documented as required. Therefore, the proper documentation of the provision of healthcare services is important.

In addition to civil liability, the Penal Code prescribes criminal liability for the breach of confidentiality of secrets which have become known in the course of professional activities relating to the health, private life or commercial activities of another person by a person who is required by law to maintain the confidentiality of such information, as well as for the illegal disclosure of sensitive personal data.

For breaches of data protection requirements, the medical service providers can be held liable under the Personal Data Protection Act. If the rights of a data subject have been violated upon processing of personal data, the data subject has the right to demand compensation for the damage caused to him or her:
1) on the basis and pursuant to the procedure provided by the State Liability Act if the rights were violated in the process of performance of a public duty, or
2) on the basis and pursuant to the procedure provided by the Law of Obligations Act if the rights were violated in a private law relationship.

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 of Obligations Act (last amended: 9 December 2013) § 770 Penal Code (last amended: 8 March 2014) § 157, 1571 Personal Data Protection Act (last amended: 1 January 2011) § 43	Estonian legislation does not prescribe any special liability regime relating to the use of EHRs. Therefore, the general rules for liability of providers of healthcare services apply. Providers of healthcare services and qualified doctors and dentists, and nurses or midwives providing healthcare services independently, who participate in the provision of healthcare services and operate on the basis of an employment contract or other similar contract entered into with a provider of healthcare services, will be liable for the wrongful violation of their own obligations, particularly for errors in diagnosis and treatment and for violation of the obligation to inform patients and obtain their consent. Under the Estonian Penal Code, any disclosure of information obtained in the course of professional activities and relating to the health, private life or commercial activities of another person by a person who is required by law to maintain the confidentiality of such information is punishable by a fine ranging between EUR 3,200 and EUR 16,000,000 or imprisonment of up to 3 years. Additionally, the illegal disclosure of sensitive personal data, enabling access to such data or transfer of such data for personal gain or if significant damage is caused thereby to the rights or interests of another person that are protected by law is punishable by a fine ranging between EUR 3,200 and EUR 16,000,000 or imprisonment of up to 3 years.
Can patients be held liable for erasing key medical information in EHRs?	Statute of Health Information System (last amended: 24 July 2009) § 14, § 16	Patients are not able to erase medical data from the ENHIS, and may only modify those elements relating to the patient's testimony (e.g. contact information). However, patients can close the use of their medical data, either wholly or partially. The medical data will still be collected into the EHR system, but it is not available to the medical service providers. This limits the possible liability of the doctor, who will not have full

Questions	Legal reference	Detailed description
		information regarding the health records of the patient. Therefore, any negative consequences will be attributed to the patient. Nevertheless, the healthcare professional is still expected to act diligently and act in the best interests of the patient, even if no medical data on the patient is available.
Can physicians be held liable because of input errors?	Law of Obligations Act (last amended: 9 December 2013) § 770	The general liability regime applies whereby providers of healthcare services and healthcare professionals will be liable for the wrongful violation of their own obligations, particularly for errors in diagnosis and treatment and for violation of the obligation to inform patients and obtain their consent. Therefore, as proper documentation is an obligation of a healthcare service professional, input errors that result in health disorder of the patient could result in the liability of the physician. Prerequisite for this liability standard is culpability, which is defined as recklessness, gross negligence and intent.
Can physicians be held liable because they have erased data from the EHRs?	Law of Obligations Act (last amended: 9 December 2013) § 770	There is no special regime on the deletion of medical data from EHRs. Provider of medical services must document the provision of healthcare services to each patient pursuant to the applicable legal requirements and preserve the corresponding documents. As a general rule, the burden of proof regarding circumstances which are the bases for the liability of the provider of healthcare services lie with the patient unless the provision of healthcare services to the patient is not documented as required. Proper documentation is therefore necessary in order to avoid the burden of proof being set on the medical service provider. Similarly to the explanation in the previous section, a healthcare professional can be held liable in case he or she has erased medical data from EHRs and this result in health damage to the patient.
Are hosting institutions liable in case of defect of their security/software systems?	Personal Data Protection Act (last amended: 1 January 2011) § 25, § 43	The person that processes personal data is required to take organizational, physical and information technology security measures to protect personal data against accidental or intentional unauthorised alteration of the data, accidental or intentional destruction and prevention of access to the data by entitled persons and against unauthorised processing.

Questions	Legal reference	Detailed description
		Violation of the requirements regarding security measures to protect personal data or violation of other requirements for the processing of personal data if a precept issued to the person by the Data Protection for the elimination of the violation is not complied with is punishable by a fine of up to EUR 32,000 for legal persons.
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?		As the Estonian legislation does not prescribe for a special liability regime relating to EHRs activities, there are no measures in place to limit the risks to healthcare professionals in that regard.
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	Personal Data Protection Act (last amended: 1 January 2011) § 43 Penal Code (last amended: 8 March 2014) § 157, § 1571	Violation of the requirements regarding security measures to protect personal data or violation of other requirements for the processing of personal data if a precept issued to the person by the Data Protection Inspectorate for the elimination of the violation is not complied with is punishable by a fine of up to EUR 32,000 for legal persons. In addition, criminal liability is possible for the violation of obligation to maintain confidentiality of secrets which have become known in the course of professional activities, and for the illegal disclosure of sensitive personal data. These can be punished with a fine ranging between EUR 3,200 and EUR 16,000,000 or imprisonment of up to 3 years.
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?	Law of Obligations Act (last amended: 9 December 2013) § 762	There is no explicit obligation to access the medical records in EHRs before making decisions involving the patient. Under the general regime, the healthcare services must, at the very least, conform to the general level of medical science at the time the services are provided and the services must be provided with the care which can normally be expected of providers of healthcare services. Such level of care may include accessing EHRs prior to taking a decision involving the patient.
Are there liability rules related to the misuse of secondary use of health data?	Personal Data Protection Act (last amended: 1 January 2011) § 23, § 43 Penal Code (last amended: 8 March 2014) § 157, § 1571	The general data protection legislation applies. If the rights of a data subject have been violated upon processing of personal data, the data subject has the right to demand compensation for the damage caused to him or her: 1) on the basis and pursuant to the procedure provided by the State Liability Act if the rights were violated in the process of performance of a public duty, or

Questions	Legal reference	Detailed description
		2) on the basis and pursuant to the procedure provided by the Law of Obligations Act if the rights were violated in a private law relationship. Violation of the requirements for the processing of personal data if a precept issued to the person by the Data Protection for the elimination of the violation is not complied with is punishable by a fine of up to EUR 32,000 for legal persons. In addition, criminal liability can be engaged for the violation of the obligation to maintain confidentiality of secrets which have become known in the course of professional activities, and for the illegal disclosure of sensitive personal data. These can be punished with a fine ranging between EUR 3,200 and EUR 16,000,000 or imprisonment of up to 3 years.

2.6. Secondary uses and archiving durations

2.6.1. Main findings

There are special regulatory requirements in Estonian law concerning the archiving of EHRs in ENHIS which requires ENHIS data to be archived indefinitely. Archiving of EHRs in ENHIS is regulated by the Statute of Health Information System. For health data archived in other databases, the archiving period does not depend on whether the health data is electronic or not – general requirements apply, which are dependent on the content of the data.

As ENHIS data is archived indefinitely, the question of destroying data at the end of the archiving period does not arise. For other types of health records, which must be archived for a certain period, the general principle of purposefulness arising from the Personal Data Protection Act applies. According to the principle of purposefulness, the person that processes the data must immediately delete or close personal data which is not necessary for achieving the purposes for which the data was collected or for which it is further processed.

Secondary use of EHRs is allowed for scientific research or statistics and it is mainly regulated by the Health Services Organisation Act and the Personal Data Protection Act. The requirements for secondary use of EHRs depend on whether the data are anonymised or not. If the data are anonymised, it is not considered to be personal data and thus the general requirements of the Personal Data Protection Act do not apply. If the EHRs are not anonymised, the data can be used only if a permit has been issued by the Data Protection Inspectorate for the secondary use. When issuing the permit, the Data Protection Inspectorate considers whether the applicant has fulfilled various requirements e.g. whether the data processing is justified by predominant public interest and whether the applicant has sufficient security measures in place.

If the patient has consented to secondary use of non-anonymised EHRs, less strict requirements apply and a permit issued by the Data Protection Inspectorate is not required. However, the person that processes the data must still register the processing of sensitive personal information.

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?	Statute of Health Information System (last amended: 24 July 2009) § 7 Regulation on Documentation of Provision of Health Services and Conditions and Arrangements for Retention of these Documents (last amended: 21 August 2010) § 4 Statute of Estonian Cancer Registry (has not been amended) § 14 Statute of Estonian Medical Birth Registry (has not been amended) § 15 Regulation on Establishment of Myocardial Infarction Registry and Statute of Maintenance of the Registry (has not been amended) § 13 Statute of Estonian Tuberculosis Registry (has not been amended) § 14	EHRs in ENHIS are archived indefinitely. For the documentation that the healthcare providers keep themselves, the archiving period does not depend on whether the documentation is electronic or not. General archiving durations apply, these depend on the content of the health record. Also in the case of more specific national registries (e.g. Estonian Cancer Registry), the archiving period does not depend on whether the data is electronic or not.
Are there different archiving rules	Statute of Health	Different rule applies depending on whether the data controller is the

Questions	Legal reference	Detailed description
for different providers and institutions?	Information System (last amended: 24 July 2009) § 7, § 3 (1) Regulation on Documentation of Provision of Health Services and Conditions and Arrangements for Retention of these Documents (last amended: 21 August 2010) § 4 Statute of Estonian Cancer Registry (has not been amended) § 14 Statute of Estonian Medical Birth Registry (has not been amended) § 15 Regulation on Establishment of Myocardial Infarction Registry and Statute of Maintenance of the Registry (has not been amended) § 13 Statute of Estonian Tuberculosis Registry (has not been amended) § 14	Ministry of Social Affairs or a healthcare provider. Data controller: Ministry of Social Affairs EHRs in the ENHIS are archived indefinitely. In the case of more specific national registries (e.g. the Estonian Cancer Registry), the archiving period does not depend on whether the data is electronic or not. Data controller: a healthcare provider The archiving period does not depend on whether the health records are electronic or not. General archiving durations apply, which depend on the content of the health record.
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?	Personal Data Protection Act (last amended: 1 January 2011) § 24 1) Statute of Health	A person that processes personal data is required to immediately delete or close personal data which is not necessary for achieving the purposes for which the data was collected or for which it is further processed.

Questions	Legal reference	Detailed description
	Information System (last amended: 24 July 2009) § 7	This does not concern the ENHIS, where data is archived indefinitely and therefore the archiving duration does not end.
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
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	Personal Data Protection Act (last amended: 1 January 2011) § 16 Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 591 (1), § 593 (51), § 593 (52), § 593 (6), § 594 (3)	Secondary use of health data is only allowed under specific conditions (see below).
Are there health data that cannot be used for secondary use?		Every health data can be used for secondary use.
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 594 (3), § 594 (1) Personal Data Protection Act (last amended: 1 January 2011) § 16, § 4 (1), § 27 (1), § 15 (1), § 28	Secondary use of ENHIS data is allowed for the purposes of scientific research or statistics, but it must be authorised by the Ministry of Social Affairs. For secondary use of anonymised ENHIS data, only the approval of the Ministry of Social Affairs is required. No other requirements apply, as anonymised health data is not considered as 'personal data'. For secondary use of non-anonymised ENHIS data, a permit from the Data Protection Inspectorate is also required. The following requirements must be fulfilled in order to get this permit. It is required that the person has taken sufficient security measures for the protection of the personal data, has registered the processing of sensitive personal data, and that the Data Protection Inspectorate has

Questions	Legal reference	Detailed description
		verified compliance with data protection requirements before the commencement of the processing of the personal data. The Data Protection Inspectorate must also hear the opinion of the ENHIS Ethics Committee. Processing of non-anonymised ENHIS data is only permitted if, after removal of the data enabling identification, the goals of data processing would not be achievable or it would be unreasonably difficult. There must be predominant public interest for such processing and the obligations of the data subject must not be changed as a result of the processing and the rights of the data subject must not be excessively damaged in any other manner. The patient should generally be notified that his or her health data is being processed. The aforementioned requirements apply only if secondary use of health data takes place without the consent of the patient. If the patient consents to secondary use, the requirements do not apply, however, the processing of sensitive personal data must still be registered with the Data Protection Inspectorate. The registration application must include the name and contact details of the data controller; a reference to the legal grounds of the processing of personal data; the purposes of processing of personal data; the categories of personal data; the categories of persons whose data are processed; the sources of personal data; persons or categories of persons to whom transmission of personal data is permitted; place or places of processing of personal data; the conditions for transfer of personal data to foreign states; a detailed description of the organisational, physical and information technology security measures for the protection of personal data. The aforementioned requirements also apply if the secondary use concerns health records collected by the healthcare providers themselves. In that case, the application to use the data must be submitted to the healthcare provider, not to the Ministry of Social

Questions	Legal reference	Detailed description
		Affairs. Furthermore, the ENHIS Ethics Committee is not involved. However, the regulatory requirements concerning the secondary use of the data collected by the healthcare providers themselves are less clear than the requirements concerning the use of ENHIS data.
Does the law say who will be entitled to use and access this data?	Health Services Organisation Act (last amended: 25 April 2014, partially to come into effect on 1 August 2014) § 593 (51), § 593 (52), § 594 (1), § 594 (3) Personal Data Protection Act (last amended: 1 January 2011) § 16	The law contains specific regulatory requirements for the use of ENHIS data by certain officials/employees of government bodies (see below). Otherwise the persons, whom are allowed to secondary use of health data, are not specified. The following persons can use the data in a strictly anonymised form in order to make surveys, analyses and to organise health statistics necessary for the management of health policy and performance of international obligations: - officials of the Ministry of Social Affairs engaging in the analysis of data concerning health statistics; - employees of an institution administered by the Ministry of Social Affairs engaging in health statistics. Under the Health Services Organisation Act § 593 (51), these persons have access to the following personal data of a patient directly in the ENHIS in a way which does not enable the identification of a patient: - data on the person of a patient; - data on the health service provider; - data on in-patient health services; - data on out-patient health services, including day care; - data on diagnosis; - data on the indicators describing a patient's health status; - data on medicinal products; - data on operations, analysis, examinations and procedures performed. The law does not specify which data can be accessed this way regarding

Questions	Legal reference	Detailed description
		the person of a patient.
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	Personal Data Protection Act (last amended: 1 January 2011) § 4 (1), § 16 Statute of Health Information System (last amended: 24 July 2009) § 16	Anonymised (coded) health data can be used for scientific research or official statistics needs without the consent of the patient, as it is not considered personal data. There is therefore no opt-out system in this regard. The patient can however opt-out of secondary use of non-anonymised health data from the ENHIS. To do that, the patient must submit an application to his or her healthcare provider (to prohibit use of ENHIS data connected to that provider) or to the Ministry of Social Affairs (to prohibit use of all personal data in ENHIS). The legislation on whether the patient can prohibit the use of non-anonymised health data which has been collected by the healthcare providers themselves is unclear. The more likely interpretation is that the patient can also prohibit secondary use of such data.

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

The ENHIS exists side by side with electronic databases of individual healthcare service providers. According to one stakeholder interviewed, most healthcare service providers have their own electronic systems and databases for recording EHRs.[48] Most of such hospitals use the system called ESTER. As emphasised before, hospitals are not prohibited from using an interface or software that is provided by a private company and there are no authorisations or licencing requirements. There are also no restrictions in the law for the location of servers.

The law provides which type of health data needs to be also uploaded to the ENHIS. Such data is automatically uploaded from the healthcare provider's own system to the ENHIS, synchronising overnight, or by manual order. Therefore sufficient level of interoperability of such EHRs is necessary. Interoperability of EHRs is a technical issue and has not been directly regulated under legal acts.

[48] Interview with the East Tallinn Central Hospital on 28th February 2014.

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?		All healthcare service providers must upload the required EHRs on the ENHIS, so their own electronic databases must be adapted to be compatible with the ENHIS. However, there is no explicit requirement of interoperability in the law.
Are there any specific rules/standards on the interoperability of EHR?		No
Does the law consider or refer to interoperability issues with other Member States systems?		No

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

The Digital Prescription (ePrescription) database enables to process prescriptions electronically. It is a separate database from the ENHIS and the two databases exist in parallel.

According to one of the stakeholders interviewed, the Digital Prescription database is connected to the ENHIS, as some of its content is automatically transferred to the ENHIS, but in order to see the full history of digital prescriptions, the patient has to log in to the state platform www.eesti.ee. So Digital Prescription database and the ENHIS have part of their data in common.

The usage of the two databases by healthcare professionals is not interdependent, even though in most cases healthcare professionals have access to both. As an exception, pharmacists do not have access to ENHIS data. They have access to the Digital Prescriptions platform and can view only valid and open prescriptions, not any past ones.

It is not obligatory for doctors to have access to the ENHIS in order to write a regular prescription or ePrescription. However, all healthcare professional do have such access to patients' EHRs on the ENHIS.

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?		According to stakeholders, these two databases are separate and not interdependent. It is possible to have the ePrescription system without EHRs and the ENHIS.
Can an ePrescription be prescribed to a patient who does not have an EHR?		It is possible to prescribe ePrescription to a patient who does not have an EHR. However, as a rule all patients' EHRs at Estonian healthcare service providers are uploaded to the ENHIS.

- ***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?		Pharmacists do not have access ENHIS data. They have access to the Digital Prescriptions platform and can view only valid and open prescriptions, not any past ones.
Can those health professionals write ePrescriptions without having access to EHRs?		Health professionals are working also in their local healthcare service provider's electronic database. It is not obligatory for them to have access to the ENHIS in order to write a regular or ePrescription. However, all healthcare professional do have such access to patients' ENHIS data.

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

Stakeholders gave a positive feedback to the current system of EHRs in Estonia. The general consensus was that the legal framework is sufficient and that there is no need for over-regulation in the field. However, a few legal barriers exist for foreign healthcare providers and healthcare professionals who wish to use ENHIS data: the healthcare provider must have a valid Estonian activity licence in order to access the ENHIS. Several issues arise from other aspects than legal: technical, institutional and personal willingness and technical readiness of other countries to cooperate with our advanced databases.

Health data to be included in EHRs

The law provides which type of health data needs to be also uploaded to ENHIS. According to the representatives of one of biggest hospitals[49] and the Department of E-health of the Ministry of Social Affairs,[50] such data is uploaded from the healthcare provider's own system to ENHIS automatically, synchronising over the night, or by a manual order. Individual healthcare service providers' data systems therefore contain more information than ENHIS. Therefore there is still a gap of information in which health data is accessible to all healthcare service providers, but the representative of the hospital confirms that in practice that can be solved when the patient herself asks for her EHRs kept by the healthcare service provider.

The representatives of a hospital and the Ministry have confirmed that on 'My E-Health' platform the patient sees the very same information that the doctors see, except for if the doctor has decided not to make a diagnosis visible to the patient online for 6 months, before it has been communicated to the patient in person. That includes fatal diagnosis.

According to a representative of a hospital, the main problem that this hospital has experienced regarding EHRs is the lacking health data on ENHIS.[51] Some healthcare professionals do not insert all the necessary health data on ENHIS and therefore the healthcare professionals treating the patient afterwards are not aware of all the procedures that have been carried out. That could end in maltreatment of patients. The interviewee was not aware of any such case. It is possible that such maltreatment has occurred, but it has not become public because it has been settled between the patient and hospital in complaint proceedings.

Challenges to establishing ENHIS

According to the representative of the Ministry of Social Affairs the main difficulty for Estonia in establishing ENHIS and other EHRs has been the lack of prior example.[52] As Estonia has been a pioneer in the field, there have been no examples where to copy from. Estonia has invented the systems and standards, classifications and nomenclatures from scratch. Second, training of healthcare professionals and convincing them to use the unified standards, classifications and nomenclatures in order to mark the diagnosis and symptoms in ENHIS takes time and effort.

Patient consent and creation, access to and update of EHRs

All stakeholders interviewed have confirmed that hospitals strictly regulate which employee and under which conditions can access EHRs and ENHIS. Hospitals take any infringement of such internal rules

[49] Interview with the East Tallinn Central Hospital on 28th February 2014.
[50] Interview with the Ministry of Social Affairs on 28th February 2014.
[51] Interview with the East Tallinn Central Hospital on 3rd March 2014.
[52] Interview with the Ministry of Social Affairs on 28th February 2014.

very seriously and have issued warnings or ended employment contracts with employees who have accessed EHRs without authorisation.[53] All activities on ENHIS are recorded and every access can be tracked down.

The representative of Estonian Data Protection Inspectorate says that according to her experience healthcare service providers are diligent in ensuring that all the requirements of processing patients' health data are followed.[54] Strict internal procedures are in place and hospitals even apply stricter personal data protection rules than required by the law.

She points out that there have been a few cases of unauthorised viewings of EHRs and in these cases healthcare service providers react to it decisively.[55] Data Protection Inspectorate finds out about such cases through complaints submitted.

The representative of Data Protection Inspectorate explains that there is no need under Estonian law to ask for patient's consent for processing his or her sensitive personal data, as the law provides a ground for processing sensitive personal data by a healthcare service provider, as long as it is necessary for providing the healthcare service.[56] Patient's consent is necessary for any other use of health data.

The interviewee also believes that processing patients' health data and EHRs has been regulated sufficiently.[57] The law stipulates that the highest security measures need to be taken when dealing with EHRs, but does not prescribe whether EHRs need to be transferred in encrypted form or not. In practice healthcare service providers share EHRs in encrypted form, whereas EHRs are shared with patients and foreign healthcare service providers in a non-encrypted form.

Liability

The legal principles for the civil liability of the providers of medical services are provided in the Estonian Law of Obligations Act. Estonian legislation does not currently regulate or prescribe a more specific legal regime for the liability related to the use of EHR systems. Therefore, the general principles for negligence/malpractice apply. No interviewee has expressed the view that liability concerning EHRs should be different from that for other forms of negligence.

Secondary use and archiving duration

Majority of interviewees did not raise concerns regarding secondary use and archiving duration. One interviewee pointed out that the archiving obligation should be limited to reasonable time, whereas currently EHRs need to be kept indefinitely.[58] Secondary use of EHRs is allowed for scientific research or statistics and it is mainly regulated by Health Services Organisation Act and Personal Data Protection Act. The requirements for secondary use of EHRs depend on whether the data are anonymised or not. If the data are anonymised, it is not considered to be personal data and thus the general requirements of the Personal Data Protection Act do not apply. If the EHRs are not anonymised, the data can be used only if a permit has been issued by the Data Protection Inspectorate for the secondary use.

Links between EHRs and ePrescriptions and requirements on interoperability of EHRs

Interoperability of EHRs is a technical issue and according to our best knowledge the area has not

[53] Interview with the East Tallinn Central Hospital on 3rd March 2014, interview with Estonian Data Protection Inspectorate on 28th February 2014.
[54] Interview with Estonian Data Protection Inspectorate on 28th February 2014.
[55] Interview with Estonian Data Protection Inspectorate on 28th February 2014.
[56] Interview with Estonian Data Protection Inspectorate on 28th February 2014.
[57] Interview with Estonian Data Protection Inspectorate on 28th February 2014.
[58] Interview with the East Tallinn Central Hospital on 3rd March 2014.

been regulated under legal acts.

Interviewee from the Ministry of Social Affairs confirmed that Digital Prescription database is connected to ENHIS, as some of its content is automatically transferred to ENHIS, but in order to see the full history of digital prescriptions, the patient has to log in to the state platform www.eesti.ee.[59] So Digital Prescription database and ENHIS have part of their data in common.

She also explained that the usage of the two databases by healthcare professionals is not interdependent, even though in most cases healthcare professionals have access to both.[60] As an exception, pharmacists do not have access to EHRs on ENHIS. They have access to Digital Prescriptions platform and can view only valid and open prescriptions, not any past ones. When ENHIS was being established, the representatives of pharmacists did not raise the need for them to see the patient's all health data on ENHIS, as the pharmacist does not have the authority to change the doctor's prescription in any way.

A representative of a hospital pointed out that she does not see a problem in the fact that there are multiple databases in use simultaneously, such as Digital Prescription and ENHIS.[61]

It is not obligatory for doctors to have access to ENHIS in order to write a regular prescription or ePrescription. However, all healthcare professional can have such access to patients' EHRs on ENHIS.

In conclusion, there is room for discussion of whether to integrate these two systems and make the full history of regular prescriptions and ePrescriptions also visible on ENHIS.

Cross-border processing of EHRs

The representative of the Ministry expressed the view that Estonia and ENHIS are ready technically and politically to share EHRs with healthcare service providers in other EU Member States.[62] However, due to the advanced level of ENHIS many Member States are not technically ready to receive EHRs.

Additionally, in order to have access to the patient's ENHIS data, the healthcare provider must have a valid Estonian activity licence. Foreign health institutions therefore currently do not have access to the patient's ENHIS data. Moreover, the most convenient method for logging into ENHIS is by using the Estonian national Identification Card, for which the healthcare professional needs the Identification Card and the device for reading the chip on the Identification Card. Alternative way of logging in does exist: using PIN-codes, whereas logging in with the Identification Card is more convenient.[63]

There are no regulatory requirements specifically on sharing EHRs with healthcare institutions in other Member States through other means than the ENHIS. However, if the patient has expressly consented to sharing EHRs with healthcare institutions in other Member States, sharing by e-mail or by any other means is allowed. This option is based on the principles established in the Personal Data Protection Act, according to which any type of data processing that the data subject (patient in this case) expressly consents to, is allowed. In the case of sensitive personal data, the consent must be obtained in a format which can be reproduced in writing. The patient platform 'My E-Health' does not provide any technical options specifically for sharing data with healthcare providers in other Member States or for obtaining patient consent for this type of sharing.

A representative of a hospital confirms that foreign patients also have their data on the hospital EHR

[59] Interview with the Ministry of Social Affairs on 28th February 2014.
[60] Interview with the Ministry of Social Affairs on 28th February 2014.
[61] Interview with the East Tallinn Central Hospital on 28th February 2014.
[62] Interview with the Ministry of Social Affairs on 28th February 2014.
[63] Interview with the Tartu University Hospital on 12th May 2014

system.[64] She also points out as a concern that there is currently no system that would enable transfer of EHRs with healthcare service providers abroad. Patient's health records are given to them directly in the end of treatment and not to the doctor abroad. Therefore there is room for development for establishing a system for sharing EHRs with foreign patient's local doctors in other countries.

The representative of Data Protection Inspectorate was of the opinion that there were no direct legal barriers under Estonian law for cross-border transfer of EHRs between healthcare providers in different EU Member States.[65] It is a matter of political agreement between Member States and of technical implementation. As she has heard, the Ministry of Social Affairs is working towards such cooperation between Member States. Inter-governmental negotiations regarding sharing Estonian healthcare providers' health data are allegedly going on between Estonia and Finland, Ireland and Australia – all countries with large Estonian communities.

[64] Interview with the East Tallinn Central Hospital on 3rd March 2014.
[65] Interview with Estonian Data Protection Inspectorate on 28th February 2014.