SMART 2007/0059

—

Study on Legal Framework of
Interoperable eHealth in Europe

NATIONAL PROFILE ESTONIA

—

European Commission
Directorate General Information Society

Brussels

—

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Services Contract 30-CE-0162056/00-04

1.2 Reference Documents

[RD1]	Communication from the Commission, e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area, 2004 http://ec.europa.eu/information_society/doc/qualif/health/COM_2004_0356_F_EN_ACTE.pdf
[RD2]	eHealth Action Plan, Progress Report http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-ap-prog-report2005.pdf
[RD3]	Recommendation of the Commission on eHealth interoperability, http://ec.europa.eu/information_society/activities/health/docs/policy/20080702-interop_recom.pdf
[RD4]	Database of European eHealth priorities and strategies (Empirica), http://www.ehealth-era.org/database/database.html (country profiles)
[RD5]	European Observatory on Health Systems and Policies, Health Systems in Transition (HiT) country profiles, http://www.euro.who.int/observatory/Hits/TopPage
[RD6]	European Observatory on Health Systems and Policies, Patient Mobility in the European Union. Learning from experience, http://www.euro.who.int/observatory/Publications/20060522_4
[RD7]	Report on Priority Topic Cluster One and Recommendations: Patient Summaries, http://www.ehealth-era.org/documents/eH-ERA_D2.3_Patient_Summaries_final_15-02-2007_revised.pdf
[RD8]	Pilot on eHealth indicators: 'Benchmarking ICT use among General Practitioners in Europe (Empirica), final report: http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/

	gp_survey_final_report.pdf, Country profiles: http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm
[RD9]	Communication from the European Commission, "A Community framework on the application of patients' rights in cross-border healthcare", 2 July, 2008, http://ec.europa.eu/health-eu/doc/com2008415_en.pdf
[RD10]	Proposal for a Directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, http://ec.europa.eu/health-eu/doc/com2008414_en.pdf
[RD11]	European Commission, IDABC, eID interoperability for public government services (with country profiles): http://ec.europa.eu/idabc/en/document/6484/5938
[RD12]	European Commission, IDABC, eSig-Web (Electronic signatures applications in public government services – country overviews): http://ec.europa.eu/idabc/en/chapter/6000
[RD13]	Legally eHealth, Study on Legal and Regulatory Aspects of eHealth,http://www.ehma.org/projects/default.asp?NCID=140
[RD14]	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
[RD15]	Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf
[RD16]	International Encyclopedia of Medical Law (editor: Herman Nys), http://www.ielaws.com/medical.htm, (with country monographs)

2 Glossary

2.1 Definitions

In the course of this Study, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- **Authorization:** refers to:
  - the permission of an authenticated entity (e.g. a person) to perform a defined action or to access a defined resource/service
  - or: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to perform a defined action or has access to a defined resource.
- **Data authentication**: information provided for verification, with more or lesser degrees of certainty, of the origin and the integrity of data.
- **eHealth**: a very broad term that encompasses many different activities related to the use of the information and communication technology (ICT) for healthcare. Many of these activities focus on administrative functions such as claims processing or records storage. However, there is an increasing use of e-health related to patient and clinical care.
- **Electronic health record**: a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes;
- **Electronic signature**: data in electronic form which are attached or logically associated with other electronic data and which serve as a method of data authentication.
- **ePrescription**: a medicinal prescription, as defined by Article 1(19) of Directive 2001/83/EC47, issued and transmitted electronically
- **Healthcare**: the prevention, treatment, and management of illness and the preservation of mental and physical well being through the services offered by the medical, nursing, and allied health professions. Health care embraces all the goods and services designed for people's health, including preventive, curative and palliative infections, whether directed to individuals or to populations.
- **Health professional**: a doctor of medicine or a nurse responsible for general care or a dental practitioner or a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on

the recognition of professional qualifications or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC.

- **Identification**: using claimed or observed attributes of an entity (e.g. a person) to distinguish the entity in a given context from other entities it interacts with (= entity authentication).
- **Identifier**: attribute or set of attributes of an entity (e.g. a person) which uniquely identifies the entity in a given context.
- **Identity management**: Identity management (ID management) is a broad administrative area that deals with identifying entities in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.
- **Patient**: any natural person who receives or wishes to receive health care in a Member State;
- **Patient summary**: subsets of electronic health records that contain information for a particular application and particular purpose of use, such as an unscheduled care event or ePrescription;.
- **Registration**: process in which a partial identity is assigned to an entity and the entity is granted a means by which it can be authenticated in the future.
- **Telemedicine**: exchange of medical information from one site to another via electronic communications with the purpose to improve patients' health status.

2.2 Acronyms

EHR ..... Electronic Health Record

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

GP..... General Practitioner

HiT ..... Health in Transition

OCSP ..... Online Certificate Status Protocol

PKI..... Public Key Infrastructure

SSCD..... Secure Signature Creation Device

TTP ..... Trusted Third Party

MoSA ..... The Estonian Ministry of Social Affairs

PIC ..... Personal Identity Code

EMA..... Estonian Medical Association

3 Introduction

3.1 General overview of the Estonian healthcare system

A comprehensive overview of the Estonian healthcare system can be found in the Estonian HiT country report published by the European Observatory on Health Systems and Policies (written by Maris Jesse *et al.*).
http://www.euro.who.int/Document/E85516.pdf (150 p.)

From this report, we reproduce the following important observations, however the report was published in 2004 and thus some updates are made to the original text:

"The main bodies responsible for planning, administration, regulation and financing in Estonia are the Ministry of Social Affairs ("MoSA"), the Health Care Board (Tervishoiuamet), the State Agency of Medicines (Ravimiamet), the Health Protection Inspectorate (Tervisekaitseinspektsioon) and the Estonian Health Insurance Fund (Eesti Haigekassa)."
Through the Ministry of Social Affairs and its agencies, the state is responsible for development and implementation of overall health policy, including public health policy, and for supervision of health service quality and access. Its main function is regulation. The healthcare division [of MoSA] has been subdivided into three administrative departments: the Health Care Department, responsible for healthcare, investment and drug policy; the Public Health Department, responsible for public health policy, prevention programmes and health protection legislation; the Health Information and Analysis Department and from the beginning of 2008 E-Health Department was created.
"In the area of health, the general responsibilities of MoSA include health policy formulation, monitoring population health and shaping the organization of the national health system by determining the scope of primary, secondary, tertiary and public health services.
Four subordinate health agencies operate under the ministry. The ministry's healthcare division coordinates the activities of the Health Care Board, the State Agency of Medicines, the Health Protection Inspectorate and the National Institute for Health Development (Tervise Arengu Instituut), although each agency is directly responsible only to the Minister.
The Government plays a planning and regulatory role in approving the development plan for the hospital network, setting healthcare prices and approving regulatory acts involving wider public health issues.
The main role of the Estonian Health Insurance Fund is acting as a purchasing agency, and its responsibilities include: contracting healthcare providers; paying for health services; reimbursing pharmaceutical expenditure; paying for some sick leave and maternity benefits.
Estonia has two administrative levels: state and municipal. County government represents the state regionally but without any legal power. In terms of health, county governors have responsibilities in primary care, announcing family doctor vacancies and approving their appointments. They also assign the service areas for family doctors within their respective

counties. Municipal governments no longer have any legal responsibility for funding or organizing healthcare.
Healthcare providers are autonomous. Services can only be provided by individuals or institutions operating as private legal entities: a limited liability company, a foundation or a private entrepreneur. Most hospitals are either limited liability companies owned by municipal governments, or foundations established by the state, municipalities and other public agencies. In this sense they are owned and managed by public institutions, either on a commercial (limited liability company) or non-profit (foundation) basis. Most ambulatory providers are privately owned. All family doctors are private entrepreneurs or salaried employees of private companies; these companies are restricted to providing only primary care services. The only areas of direct state control include county governors deciding on family doctor service areas within their region and the Ministry of Social Affairs deciding on the number of ambulance units to be financed by the state budget. The state's influence on specialized care and independent nursing care is limited standard-setting and public financing.
The majority of healthcare funding comes from public sources – roughly three quarters of total expenditure on healthcare. Most of this public revenue is raised from the working population and employers through an allocated payroll tax equal to 13% of wages, which accounts for two thirds of total expenditure on healthcare.
The proportional payroll tax ensures redistribution of healthcare resources from higher-income groups to lower-income groups and from the healthy to those in poor health. However, the health system does not guarantee the same level of access to the entire population. There are differences between the rights of the insured – about 94% of the population – and the uninsured."

3.2 Use of ICT in the Estonian healthcare sector

A recent (2007) status of the use of ICT by *general practitioners* in Estonia has been drafted in the framework of the European Pilot Study on eHealth indicators: 'Benchmarking ICT use among General Practitioners in Europe" (Empirica):
http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm
From the Estonian country brief, we take over the following key findings:
"Estonia is one of the EU27 member states where the highest rates of infrastructure availability are attained. 100% of the Estonian GP practices use a computer. The same share of practices disposes of an Internet connection. In Estonia, broadband represents the most usual form of access to the Internet with 72% of GP practices resorting to broadband connections. GPs in Estonia also show extremely high use rates of security features.
In the areas of storage of administrative data and the use of computers in consultation with the patient, Estonia can be compared with top EU27 performers. 98% of GPs in Estonia store administrative patient data and 94% use a computer in consultation with the patients. This amount to one of the highest usage rates across Europe. With respect to the use of Decision Support Systems (DSS), Estonia also scores highly above average with 94% of the GPs reporting using a Decision Support System for prescribing or diagnosis. Virtually all Estonian GP practices store at least some sort of electronic medical patient information. When it comes

to the electronic transfer of patient data, Estonia shows a slightly weaker performance, the only exception being the transfer of lab results from laboratories to GP practices, where Estonia equals the EU27 average of around 40%. Only 1% of Estonian GP practices however transfer either medical or administrative patient data to other care providers. The use of eHealth applications today seems to be well in line with the history of the Estonian eHealth strategies. A rather mature eHealth strategy had already been launched in 2000. At the same time, all primary care practices were obliged to procure computers and Internet connections. Today these infrastructure prerequisites have not only been purchased, but are moreover heavily used, as shown by the high rate of Estonian GPs using a PC in consultation with the patients.

In Estonia, the reception of laboratory results by GP practices (39%) corresponds to the average score of the EU27 Member States. With regard to the transmission of data towards other care providers, Estonia scores substantially lower as only 1% of Estonian GPs make use of this option, as compared to 10% on average in the EU27.

Data transfer via networks concerns not only medical data, but can also be used for administrative purposes, i.e. for data exchanges between the GP practice and reimbursers or other care providers. Estonia scores well below the EU average of 10% for the exchange of administrative data with other carers, which is used by only 1% of Estonian GP practices. The networked exchange of administrative data with reimburses is also used in no more than 5% of the GP practices (as compared to 15% on average in the EU27).

With relation to the use of security features Estonian GP practices follow the general pattern found in the EU27, however scoring substantially above average for all security issues. In Estonia virtually all of the GP practices resort to password protection access which places Estonia on the top of the frontrunner group. The situation for the use of passwords for the protection of transmitted files is similar: password protection is used by 76% of GP practices in Estonia, as compared to the significantly lower EU27 average of 57%.

The encryption of transmitted files is a security feature that is used by only 42% of GP practices in the EU Member States. In Estonia, this figure is doubled as up to 85% of GP practices use encryption technology for the transmission of data files. With respect to the use e-signatures, Estonia scores highly above average with 58% of GP practices resorting to this security measure."

3.3 National eHealth strategy

An overview of the Estonian eHealth policy can be found in the March 2007 "eHealth ERA fact sheet: Estonia." Available at: http://www.ehealth-era.org/database/documents/factsheets/Estonia.pdf

For our Study, the following observations are adapted from this fact sheet:

"Estonia has a well developed eGovernment Service infrastructure that is also being used in the eHealth domain. In particular, 80% of the 15 – 75 year old population have an electronic identity card. The card has the ability to handle the functions of authentication, signature and encryption which gives it a central role in data protection and security risk management in the health service arena."

Additional information about the ID card can be found at: http://www.id.ee/?lang=en
"Since 2000, the eHealth strategy of the Estonian Ministry of Social Affairs (MoSA) is based on three pillars:

- establishment of a nationwide integrated electronic health record system, also known as the "Electronic Health Record Project of Estonia (2005 – 2008)",
- a strong focus on standardisation and in particular on interoperability [HL7; SNOMED; LOINC; DICOM, ICD 10 *etc.*], and
- the use of the existing IT infrastructure.

The strategy foresees a comprehensive central register of the health information for all 1.35 million Estonians from birth to death. The register is intended to facilitate the exchange of all types of health data between healthcare providers. It is also meant to support centralised healthcare management and strategic planning through better quality and accuracy of the necessary data for organising healthcare. Responsibility for implementation has been entrusted to the private non-profit Estonian eHealth Foundation (Eesti E-Tervise Sihtasutus). It was set up by the hospitals and professional associations in October 2005 following an initiative of MoSA. The main goals of this foundation are the development and governance of nationwide eHealth projects, and the coordination of the unification of Estonian healthcare provider information systems. The main drivers of eHealth development in Estonia are central public administration and public-private partnership (PPP)."
More information about the eHealth Foundation can be found at: http://www.e-tervis.ee
"Future activities of Estonia's eHealth strategy are ambitious. A system of medical information that registers all the health data of every citizen from birth to death is without international precedent. As it evolves into maturity the Electronic Health Record Project initiative will bring together or provide access to the patient clinical data in systems of all medical centres. This includes hospitals, general practitioners, emergency care institutions and pharmacies, as well as the information system of the Health Insurance Fund, and other registers and databases. The Electronic Health Record Project initiative will also support the provision and usage of eHealth services for and by the public in Estonia. All patients will be able to securely access and review their medical data and make it available to the healthcare professionals they are dealing with. This also includes the ability to – via the Internet – obtain appointments online, submit prescription renewal requests, and exchange test results such as blood pressure readings. The realisation of the digital health record project requires not just implementation of advanced information technology across a deeply complex system. It is widely recognised that significant efforts will be required in re-organising existing organisational and service delivery structures and in establishing an innovation friendly ethos."

The following is adapted from an introductory material published by the eHealth Foundation and is available at: http://www.digilugu.ee/DL_projekti_tutvustavad_materjalid_ENG.pdf (14.05.2008)

"From the information technology aspect, the Estonian healthcare landscape is quite varied and uneven. Most healthcare providers have already deployed an information system or use IT solutions developed by other providers. At the same time the information systems implemented by various healthcare providers are not mutually compatible and cannot exchange information with each other. A public healthcare information system is designed to solve this flaw by creating central infrastructure for exchanging medical information. The "heart" of the eHealth information system is a centrally managed electronic health record that is a central database of the most important medical information and provides the necessary information to various partners.

MoSA fulfils the coordinating and directing role in developing the national Health Information System. Currently four eHealth projects are under development: Electronic Health Record (EHR), Digital Images, Digital Registration and Digital Prescription. The implementation of these four projects will create a unified national Health Information System that will be linked with other public information systems and registers and will in its IT solution use the existing public information technology solutions.

IT system for EHR is a unique health information system in the world that encompasses the whole country and connects existing IT systems of healthcare providers. The EHR database will include the most important personal data, medical records, visits and other health-related information of the patient. With the help of EHR, medical doctors will be able to exchange documents that are produced in the course of the treatment and allow doctors to make enquiries of time-critical and general information about the patient. The information system stores the medical history of the patient and enables the doctors who are treating the patient access to this specific information.

In the next few years, the EHR project will be one of the largest and most extensive applications for electronic ID cards in Estonia that is developed on the initiative of the state and that will offer new functions for the electronic ID cards. The system is one of the most practical public administration services and will make the daily life of people notably more convenient in the same way as other popular solutions such as the Electronic Tax Office, Electronic School Database or Electronic Elections. The objectives to be achieved as a result of implementing the EHR information system:

• To provide a more timely and competent medical service to patients since the medical doctors will be able to operatively obtain information about the patient's medical condition.
• Patients will obtain a comprehensive overview of the use of his or her personal medical information by medical establishments, the state and other participants in the EHR project.
• Medical statistics will become notably more timely, accurate and comprehensive, enabling better and more efficient healthcare planning and organization.
• Medical doctors will be better informed of the health status of patients and will have more comprehensive information on the patients' medical records.

Data provided in the EHR can be used only for the treatment of patients and for checking the patient's medical condition, assessment of medical quality and for national statistics. The partners in the information system are medical establishments or other legal persons who have entered into the accession contract with the eHealth Foundation and have the right to use EHR data and exchange of medical information through the EHR system. EHR will offer the

partners authorized access to the persons' health data and create the opportunity for digital forwarding of medical documents between healthcare establishments.
Persons can access their health data by using their electronic ID cards at all times and from all computers with Internet access through the patient's portal." Bank eID and Mobile-ID solutions can also be used to gain access to health data.
To implement the eHealth projects, changes in the legal system had to be made. A draft Health Information System Act was drawn up in 2006 and it was to be implemented as a separate legal act, however it was never presented to the Parliament. Instead the current Health Services Organisation Act (Tervishoiuteenuste korraldamise seadus) was amended and expanded to facilitate the required legal framework needed for the implementation of the eHealth projects. The said amendments were adopted by the Parliament on 20.12.2007 and will enter into force on 01.09.2008.
The norms stipulate 01.01.2013 as the final date when the Health Information System must be fully in use. Further, the Minister of Social Affairs must issue a detailed timeline for the implementation of the Health Information System. In fact several provisions delegate authority to the Government and the Minister of Social Affairs to issue more detailed regulations. The newly adopted norms should therefore be seen as a backbone to the whole eHealth legal framework. At the time of writing this report the regulations that are to be issued by the Government and the Minister of Social Affairs were not available, because the provisions that delegate authority to issue such regulations have not yet entered into force.
The Health Information System is an official database in the sense of section 43^1 of the Public Information Act (Avaliku Teabe Seadus). The Health Information System is also part of the national information system in the sense of section 43^2 of the Public Information Act and is connected to it via a secure data exchange layer (X-Road see below section 7.2). The chief processor of the Health Information System database is MoSA. The Government has the obligation to adopt regulations establishing the Health Information System and its statutes.
The purpose of processing healthcare related data in the Health Information System is to conclude and fulfil healthcare provision agreements, to ensure the quality of the healthcare services and patients' rights as well as the protection of public health, to keep registers that contain data about the state of health and to control health policy.
It will be mandatory for the healthcare providers to input data to the Health Information System. In the broadest sense it will be necessary to provide data:

- required for the administration of waiting lists;
- required to make available the medical images (see below 3.5);
- about the healthcare services provided to the patient (including data concerning state of health).

The Minister of Social Affairs has the obligation to specify the categories of the said data as well as the conditions and regulations concerning the retention of such data. It is mandatory to use the classifications and address details of the national information system in order to ensure the quality of data.

Of great importance are the norms that regulate access to the Health Information System. The patients have full access to their personal data in the Health Information System, with a single exception that a healthcare provider may deny access to the patient for a period of up to six months for the purpose of protecting the life and health of the patient. The argumentation behind making such an exception is to preclude the patient of learning about data entered into the Health Information System before the healthcare provider has had an opportunity to explain the meaning of such data to the patient. This provision was added as a consequence of broad discussions with professional and patient associations.
The healthcare providers have access to the personal data in the Health Information System for the conclusion and performance of the healthcare provision agreement.
The patients have the right to deny healthcare providers access to their personal data in the Health Information System, and they also have the right to ask the healthcare provider to immediately apply access restrictions to the personal data.
Forensic experts of the national forensic institution have access rights to the Health Information System for the purposes of determining the nature of a person's injuries under the Code of Criminal Procedure and for the performance of a forensic autopsy.
Other persons have access rights to personal data in the Health Information System if such a right is stipulated in law.
The new regulatory framework also foresees the creation of a special ethics committee that assesses the necessity and justification of extracting personal data from the Health Information System for the purposes of scientific research and statistics. The special ethics committee also has the obligation to draw up guidelines of good practice. The decisions of the ethics committee are not binding, the Estonian Data Protection Inspectorate has the final say, however it has an obligation hear out the position of the ethics committee.
Changes were also made to several other legal acts that will also enter into force on 01.09.2008, most notably changes to the Medicinal Products Act (Ravimiseadus) regarding ePrescriptions (Digital Prescriptions project, see below 3.6 and 8). The Transplantation of Organs and Tissues Act (Elundite ja kudede siirdamise seadus) was amended to enable persons to express their will to donate organs or tissues after death, by confirming it with a digital signature through the Health Information System. The Establishing of the Cause of Death Act (Surma põhjuse tuvastamise seadus) was amended to enable persons to express their will to donate their bodies after death for scientific purposes, by confirming it with a digital signature through the Health Information System. The Blood Act (Vereseadus) was also amended to enable recipients to express their will relating to blood transfer, by confirming it with a digital signature through the Health Information System.

3.4 Regulatory framework for patients' summaries

Patients' summaries have been a matter of intense discussion. The draft acts contained a clause for time critical health related personal data that could be accessed in emergency situations. However, the legal framework that was adopted leaves the supreme authority to the patient to determine what kind of personal data can be accessed and what cannot be accessed

by healthcare providers and no exceptions are made for emergency situations. If a patient asks the healthcare provider to close access to the personal data already in the Health Information System or to data that is generated during a visit, the healthcare provider has an obligation to explain the possible consequences of closing access to such data.

3.5 Regulatory framework for telemedicine

The following is adapted from http://www.digilugu.ee/DL_projekti_tutvustavad_materjalid_ENG.pdf (14.05.2008):
"The objective of the digital image project is to create a technical platform to enable all Estonian healthcare providers including family physicians to join a uniform information system and image databank including transmission of large-volume medical research results. The unified image database will have an interface to the Electronic Health Record which will make it possible to monitor changes in the health condition over several years and involve foreign experts for providing an opinion on complex cases. In addition, the patient will no longer have to make repeated visits because of lost images or take X-ray images to various doctors. The digital image will also increase the efficiency of using video recordings made with complicated diagnostics equipment.
One of the largest problems of healthcare in Estonia today is long waiting lines of patients and the need for patients seeking vacant appointments at a specialist doctor to call or visit all medical establishments. A centrally administered digital registration system will be developed. It will be interfaced with the existing information systems that are already used for registration of patients in the medical establishments. The digital registration enables patients and family physicians to look for the first available appointment of all medical doctors in some specific area of Estonia or nationwide and to book the suitable time over the web portal. The online system will also enable to change and cancel existing bookings. To make a booking, the patient needs to have a referral which will avoid situations were the same patient makes appointments with several doctors of the same specialization. During the project the existing registration systems used by healthcare providers will not be replaced with the new ones. The digital registration will be a new opportunity that, when deployed, will operate in parallel with the current patient registration system in which patients can make appointments either by phone or physically on site. Instead of replacing the existing systems, uniform standards will be developed on the basis of which the existing systems will be interfaced with the central web portal."

The newly adopted legal framework addresses only the most general issues related to the said projects while leaving the specific and technical details for the Minister of Social Affairs to regulate. The healthcare providers are required by law to provide data for the digital images project as well as the digital registration project. The Estonian Health Insurance Fund is allowed to conclude remuneration agreements only with healthcare providers who comply with requirements of the digital registration project.

3.6 Regulatory framework for electronic prescriptions

The following is adapted from http://www.digilugu.ee/DL_projekti_tutvustavad_materjalid_ENG.pdf (14.05.2008):
"Unlike other eHealth projects, the Digital Prescription project is coordinated not by the Estonian eHealth Foundation, but by the Estonian Health Insurance Fund (Haigekassa). Digital prescription will simplify the life of the medical doctors, the pharmacist and the patients. Around 8 million prescriptions are issued in Estonia every year that now will be digitalized as a result of the digital prescription project. In the course of the project, a central system will be developed that will store the incoming prescriptions (messages) and issue, on the basis of a request, the prescriptions of the specific patient to the information system of pharmacies. The system will free the patient from the need to have the prescription at hand and from the risk of losing it. When the project is implemented, the doctors and pharmacies will save a lot of time and paper spent on issuing prescriptions since the system will automatically check different data that is needed. In addition, the system will provide feedback for the doctor on whether the medicine was taken out or not. Digital prescriptions will protect the doctors from unforeseeable costs related to inaccurate use of subsidies. When the system is implemented the Health Care Board, the State Agency of Medicines, the Health Insurance Fund and the Ministry of Social Affairs will obtain rapid and accurate reporting and the information system of the issuer of the prescription will receive an automatic confirmation from the information system of the Health Insurance Fund about the applicable subsidy."

Along with the adoption of amendments to the Health Services Organisation Act amendments were made to the Medicinal Products Act. Most notably Digital Prescription Centre (Retseptikeskus) an official database in the sense of section 43^1 of the Public Information Act will be established. All healthcare providers are obliged to issue prescriptions digitally, except when not possible for objective reasons (*e.g.* house calls). The legal framework relating to ePrescriptions is discussed in more detail below in section 8.

3.7 Overview of relevant legislation

In order to facilitate the Health Information System from the legal point of view amendments to the Health Services Organisation Act were adopted by the Parliament on 20.12.2007 and these will enter into force on 01.09.2008. These norms provide the legal backbone to the whole eHealth project because they contain the most important principles regarding the Health Information System and several provisions that delegate authority to the Government and the Minister of Social Affairs to issue more detailed regulations. The Health Services Organisation Act should be seen as the most important legislative act in the eHealth domain. Other relevant legal acts include the Law of Obligations Act (Võlaõigusseadus), which contains provisions that regulate the healthcare service provision agreements, and the general obligations and rights of healthcare providers and patients. The Public Information Act sets out the general legal framework of the official databases. The Identity Documents Act (Isikut tõendavate dokumentide seadus) is relevant, because it contains provisions regarding the

electronic identity card (ID card). All permanent residents of Estonia must have an ID card. The ID card contains two certificates, one for authorization purposes and one for digital signatures. The Digital Signatures Act (Digitaalallkirja seadus) contains more specific regulation regarding digital signatures.
The Personal Data Protection Act (Isikuandmete kaitse seadus) is relevant to the eHealth projects, containing the provisions that regulate the use of (sensitive) personal data.
Also relevant to the Digital Prescriptions and the Digital Registration projects are the Health Insurance Act (Ravikindlustuse seadus) and the Medicinal Products Act.
The Transplantation of Organs and Tissues Act, the Establishing of the Cause of Death Act, the Blood Act are also relevant to the eHealth projects.

4 Regulatory framework for the healthcare profession

4.1 Legal conditions for the practice of healthcare

The practice of medicine is regulated by the Health Services Organisation Act and the Law of Obligations Act.

According to the Health Services Organisation Act health services are the activities of healthcare professionals for the prevention, diagnosis or treatment of diseases, injuries or intoxication in order to reduce the malaise of persons, prevent the deterioration of their state of health or development of the diseases, and restore their health. The Minister of Social Affairs has issued a regulation according to which the diagnosis and treatment of the diseases listed in the International Statistical Classification of Diseases and Related Health Problems Tenth Revision (ICD-10), and the performing of surgical procedures listed in the Nordic Medico-Statistical Committee, Classification of Surgical Procedures (NOMESCO NCSP) are considered to be health services.

Healthcare professionals are doctors, dentists, nurses and midwives, who must be registered with the Health Care Board. The registration gives the right to provide healthcare services. "A right to practice a profession means access to a profession or to an occupation as a possibility to compete on the labour market. The right to practice a profession does not automatically guarantee employment - it is subject to a final decision from the employer. In order to provide healthcare services in Estonia, being registered is compulsory. For registration, a healthcare professional striving for professional activity in Estonia must fill in a registration form and send it to the Health Care Board."
(http://www.tervishoiuamet.ee/public/files/Registration_Procedure01.2007.pdf). In addition, a copy of the document certifying the person's qualifications must be filed with the Health Care Board. Before submitting a registration form, an appropriate state fee must be paid by the applicant. The Health Care Board will verify the validity of the presented data about the person's qualifications and in one month's time it will deliver the registration decision. A person will not be registered as a healthcare professional if false information was knowingly filed or the person has been revoked of the right to practice in the profession applied for.

Within the scope of the Health Services Organisation Act healthcare providers are healthcare professionals or legal persons providing health services. Within the scope of the Law of Obligations Act healthcare providers are legal persons providing health services.

The provision of emergency medical care, the provision of specialised medical care and the independent provision of nursing are activities that require applying for an activity licence from the Health Care Board.

According to the Law of Obligations Act 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 healthcare providers. If necessary, a healthcare provider must refer a patient to a specialist or involve a specialist in the treatment of the patient.

The Law of Obligations Act regulates the healthcare service provision agreement and the rights and duties of healthcare service providers and patients therein (see section 6 below).

4.2 Control over the practice of medicine

According to the Health Services Organisation Act supervision over compliance with the requirements for healthcare providers is exercised by county governors and officials authorised by the Health Care Board. A county governor exercises supervision over the activities of family physicians practising in the county. Supervision over the activities of family physicians, providers of emergency medical care, providers of specialised medical care and independent providers of nursing is exercised by the officials authorised by the Health Care Board.

The Health Service Quality Expert Commission is an advisory committee of the Health Care Board. It has the authority to: give an assessment to the quality of healthcare services provided to the patient; propose to the Health Care Board to initiate supervisory proceedings, propose to healthcare providers to assess the qualifications of healthcare professionals or to send them to refresher courses; propose to the healthcare providers to change their organisation of work; propose to the Health Care Board to revoke licences of healthcare providers; propose to the Health Care Board to refuse issuing licences to healthcare providers; propose to the Estonian Health Insurance Fund to review the remuneration agreements concluded with healthcare providers. The opinions and proposals of the Health Service Quality Expert Commission are not binding legally, they are only an assessment to the quality of the medical services provided, and they do not create rights or obligations and cannot thus be appealed. The supervisory proceedings carried out by the Health Care Board can be disputed by the patients.

The Minister of Social Affairs has issued a regulation on the Quality Assurance Requirements for Health Services.

"The Estonian Medical Association (Arstide Liit) is a voluntary nongovernmental organisation. The aims of the EMA are to protect the professional and economic interests of physicians, to participate in the creation of health policy and improve healthcare in Estonia. The main activities of the association are quality assurance in healthcare, protection of its members in the labour market, postgraduate and continuous medical education affairs, co-operation with other medical organisations in Estonia and abroad, dealing with problems of medical ethics, reorganisation of the certification system of medical specialists in Estonia." (http://www.arstideliit.ee/en/index.html). The EMA has developed an ethics code which is considered to be the most important ethics code applicable to Estonian medical doctors. Naturally, patients have the right of recourse directly to the courts, so the court system must also be considered as part of the control structures of the medical profession.

4.3 Professional liability

In the broadest sense liability can be divided into penal liability and civil liability.

Penal liability can further be divided into criminal liability and liability for misdemeanours. Criminal liability can only be attributed to natural persons unless the penal code expressly stipulates criminal liability of a legal person. In most cases the general rules apply. However, there are some provisions in the penal code, which are more specific to the health sector. For example inducing a person to use doping by prescribing medicine to be used as doping in sports; unlawful termination of pregnancy, *i.e.* termination of pregnancy without consent or performing the termination later than allowed by law; causing the spread of infectious disease; transplantation without consent; performing unlawful medical trials etc. are all considered criminal offences. Providing healthcare services without registration or licence can be a misdemeanour or a criminal offence depending on the circumstances.

Civil liability can arise from the breach of contractual obligations or from non-contractual obligations. According to the Law of Obligations Act section 770 healthcare providers and healthcare professionals are liable only for the wrongful violation of their obligations, particularly for errors in diagnosis and treatment and for violation of the obligation to inform patients and obtain their consent. This means that the healthcare provider (usually a legal person) and the healthcare professional (individual) are both responsible jointly and severally, an important exception to the general rule that only parties to the contract can be held responsible, since the health services provision agreement is concluded between the patient and healthcare provider (*i.e.* legal entity).

Healthcare providers are also liable for the activities of persons assisting them and for any defects in the equipment used upon provision of healthcare services. The burden of proof regarding circumstances which are the bases for the liability of the healthcare provider and healthcare professionals lies with the patient unless the provision of healthcare services to the patient is not documented as required. 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. In this case, the burden of proof regarding the damage resulting from the health disorder also lies with the patient.

A violation is considered wrongful if carelessness, gross negligence or intent is evident. Carelessness is failure to exercise necessary care. Gross negligence is failure to exercise necessary care to a material extent. Intent is the will to bring about an unlawful consequence upon the creation, performance or termination of an obligation.

Non-contractual liability does not arise from the breach of an obligation but arises when the legal rights of persons are violated. Treatment without consent of the patient is an example, in such a case a healthcare provider must prove that it had the consent of the patient or that coercive treatment was lawful in order to be released from liability.

4.4 Professional secrecy

The most important provision regarding professional secrecy in the current Estonian law is section 768 of the Law of Obligations Act, which stipulates that healthcare providers and persons participating in the provision of healthcare services must maintain the confidentiality of information regarding the identity of patients and their state of health which has become known to them in the course of providing healthcare services or performing their official

duties and they must ensure that the information contained in documents created in the course of providing healthcare services does not become known to other persons unless otherwise prescribed by law or by agreement with the patient. It is permissible to deviate from this duty to a reasonable extent if failure to disclose the information could result in the patient significantly damaging oneself or other persons. The term "information regarding the identity of patients" can be interpreted extensively as to include all personal data which becomes known during the course of providing healthcare services.

The Penal Code criminalises the 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.

The Code of Criminal Procedure and the Code of Civil Procedure both have special regulations that allow healthcare professionals, who are obliged under law to keep information obtained in the course of professional activities confidential, to refuse from giving statements regarding such information within the named procedures.

5 Processing of personal health data

5.1 Short overview of personal data protection legal framework

The current Estonian Data Protection Act was adopted on 15.02.2007 and entered into force on 01.01.2008, replacing the old Data Protection Act. Both acts – the new and old one – are based on directive 95/46/EC. Generally, the provisions of the Data Protection Act conform to the articles of the Directive, having the same terminology, concepts, principles and rules.
Some nationally specific provisions relevant to processing health related personal data have been adopted, these relate to the transposition of Art 8 and the use of health related data for scientific and statistical purposes.
Some provisions relating to processing of personal data concerning health are incorporated to the Health Services Organisation Act.

5.2 Transposition of article 8 of Directive 95/46/EC

The processing of special categories of personal data in the sense of Article 8 of Directive 95/46/EC has been transposed to the Estonian Data Protection Act by differentiating between personal data and sensitive personal data. The term personal data includes any information relating to an identified or identifiable natural person, independent of the type or format of such information.

According to the Data Protection Act subsection 4 (2) sensitive personal data is:

- data revealing political opinions or religious or philosophical beliefs, except data relating to being a member of a private legal person registered pursuant to the procedure provided by law;
- data revealing ethnic or racial origin;
- data relating to the state of health or disability;
- data relating to genetic information;
- biometric data (images of iris, finger and palm prints; genetic data);
- data relating to sexual life;
- data concerning membership in trade unions;
- data about committing an offence or having fallen victim of an offence, before the beginning of a public trial, delivery of an official judgment or the termination of proceedings in the same matter.

Processing of personal data without the data subject's consent is prohibited, unless otherwise provided by law. Stricter regulations apply when processing sensitive personal data, most notably the processing of sensitive personal data has to be registered with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon). Alternatively, the data controller who

wishes to process sensitive personal data has to appoint a person who is responsible for the processing of personal data and inform to the Data Protection Inspectorate the name and contact details of such a person.

Under subsection 14 (1) of the Personal Data Protection Act personal data may be processed without the data subject's consent if:

- processing is necessary for the performance of an obligation prescribed by law, international treaties, or regulations of the European Union;
- in individual cases when the data subject is incapable of giving his consent and processing is necessary for the protection of the life, health or freedom of the data subject or another person;
- processing is necessary for the performance or the ensuring of performance of the contract entered into with the data subject – this exception is not applicable to the processing of sensitive personal data.

Healthcare providers, who are subject under law to the obligation of professional secrecy, are allowed to process personal data, including sensitive personal data, if this is necessary for the purpose of providing the healthcare service (The Health Services Organisation Act subsection 4^1 (1)). So if the data subject forbids the processing of personal data, healthcare providers are still allowed to provide health services to the person and process his (sensitive) personal data. The data subject (patient) may of course refuse health services. In case of emergency care, health professionals are obliged under law to provide health services within the scope of their competence and available resources (the Health Services Organisation Act subsection 6 (2)).

Subsection 4^1 (1) of the Health Services Organisation Act does not exempt healthcare providers (legal entities; self-employed specialist care providers – *i.e.* data controllers) from the obligation to register the processing of sensitive personal data with the Data Protection Inspectorate.

The fact that health professionals have the right to process personal data, including sensitive personal data, does not grant them access to the information that the patient has closed access to in the Health Information System. This applies even in emergency care situations.

5.3 Other relevant rules regarding personal data protection

Subsection 4^1 (2) of the Health Services Organisation Act contains some additional clauses that relate to data protection. Access or transfer of the data concerning state of health of a hospitalized patient is allowed to persons who are closest to the patient (e.g. spouse, next of kin, life companion), unless the data subject has forbidden access to or transfer of such data or when an investigative body has closed access to such data for the purpose of preventing a crime, capturing a criminal or finding out the truth in criminal proceedings.

A judgment of the Supreme Court of Estonia dated 17.04.2007 № 3-3-1-98-06 has touched upon the processing of (health related) sensitive personal data. The Supreme Court confirmed that information published by the police about taking a person to the sobering-up centre is considered to be information about the state of health of that person. Such data indicates the degree of intoxication, which is information about the state of health of a person, and must therefore be considered to be sensitive personal data. The police did not have the data subject's consent nor did such a publishing right come from any legal act.
Failure to register the processing of sensitive personal data is considered to be a misdemeanour and a fine of EEK 18,000 (~EUR 1,150) can be made to natural persons or up to EEK 500,000 (~EUR 31,970) to legal entities.
Since 15.03.2007 the illegal disclosure of sensitive personal data has been criminalised. This applies only to natural persons, who may receive a pecuniary punishment or up to one year imprisonment for the illegal publishing, granting of access to or transfer of sensitive personal data for the purpose of personal gain and if the legal rights and interests of data subject have been significantly damaged.

6 Rights and duties of healthcare providers and patients

The rights and duties of healthcare providers and patients are regulated in chapter 41 (the healthcare service provision agreement) of the Law of Obligations Act. The relationship between the healthcare provider and the patient is subjected to a contract, which is to some extent regulated by imperative clauses of the law. Additionally the healthcare provider can be held responsible for non-contractual obligations. This chapter focuses on the rights and obligations arising from the healthcare service provision agreement.

6.1 Agreement for the provision of healthcare services

An agreement for the provision of healthcare services under the Law of Obligations Act is an agreement, whereby one person (healthcare provider) obliges, in the professional activities thereof, to provide healthcare services to another person (the patient), particularly by examining the patient in the interests of his health and in accordance with the rules of medicine, by consulting and treating the patient or offering obstetrical care to the patient, and by informing the patient of his state of health and of the progress and results of his treatment. Patient care within the framework of the provision of healthcare services and other activities directly related to the provision of healthcare services are considered to constitute provision of healthcare services.

Qualified doctors, and nurses or midwives providing healthcare services independently, and dentists who participate in the provision of healthcare services and operate on the basis of an employment contract or other similar contract with a healthcare provider are held jointly and severally liable with the healthcare provider for the performance of the healthcare service provision agreement.

Within the scope of the Law of Obligations Act healthcare service providers are legal persons providing healthcare services. The party to the agreement for the provision of healthcare services is always the healthcare provider as a legal person (*e.g.* hospital) and not the healthcare professional.

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 healthcare providers. If necessary, a healthcare provider must refer a patient to a specialist or involve a specialist in the treatment of the patient.

Any agreements which derogate from the provisions of chapter 41 (the healthcare service provision agreement) of the Law of Obligations Act to the detriment of the patient are void.

6.2 Obligation to conclude the agreement for the provision of healthcare services

Under the Law of Obligations Act the healthcare provider is obliged to provide healthcare services to a person who applies for healthcare services, unless the terms or conditions that the patient applies for are in conflict with provisions of law or the standard terms of an agreement for the provision of healthcare services. This is considered to be the primary obligation of the healthcare provider.

The patient has full freedom of choice whether to conclude the agreement at all and with which healthcare provider. The patient can also terminate the agreement without any limitations (this does not mean that financial obligations do not have to be performed by the patient), while the options for the healthcare provider to terminate the agreement are quite limited – the healthcare provider must have good reason to terminate the agreement. Even if the healthcare provider terminates the agreement, it must in case of necessity carry on the provision of healthcare services to the patient until the patient finds another healthcare provider.

6.3 Patient's duty to pay fee

The patient must pay an established, agreed or standard fee or, in the absence thereof, a reasonable fee for the provision of healthcare services. A fee may be demanded from a patient in so far as the expenses for providing healthcare services are not covered by sickness insurance or another person. This is considered to be the primary obligation of the patient.
Established fees are fees that arise from legal acts and that are not established by the healthcare provider – e.g. the price list of the Estonian Health Insurance Fund. Agreed fees are agreed upon by the patient and the healthcare provider. Healthcare fees can be agreed when established fees are inexistent or do not apply – *e.g.* when the patient is not an insured person in the sense of the Health Insurance Act, or the healthcare service provider has not concluded a remuneration agreement with the Estonian Health Insurance Fund.
A standard fee applies if the parties to the agreement for the provision of healthcare services have not agreed upon a fee or no established fees apply. A standard fee is usually derived from the price list of the Estonian Health Insurance Fund. If a standard fee cannot be determined the principle of reasonable fee applies.

6.4 Duty to obtain the informed consent of the patient

The healthcare provider must inform the patient of the physical examination results, the state of his health, any possible illnesses and the development thereof, the nature and purpose of the healthcare services to be provided, the risks and consequences associated with the provision of such healthcare services and of other available and necessary healthcare services. At the request of the patient, the healthcare provider must present the specified information in a format which can be reproduced in writing.
The healthcare provider is not allowed to promise that a patient will recover or that an operation will be successful.
A patient may be examined and healthcare services may be provided only with his consent. A patient may withdraw his consent within a reasonable period of time after granting consent. At the request of a healthcare provider, consent or an application to withdraw consent must be in a format which can be reproduced in writing.
Special provisions apply if the patient has restricted active legal capacity, is unconscious or incapable of exercising his or her will for any other reason.

6.5 Duty to maintain confidentiality

Healthcare providers and persons participating in the provision of healthcare services must maintain the confidentiality of information regarding the identity and state of health of patients which has become known to them in the course of providing healthcare services or performing their official duties and they must ensure that the information contained in documents created in the course of providing healthcare services does not become known to other persons unless otherwise prescribed by law or by agreement with the patient. It is permissible to deviate from this duty to a reasonable extent if failure to disclose the information could result in the patient significantly damaging oneself or other persons. The term "information regarding the identity of patients" can be interpreted extensively as to include all personal data which becomes known during the course of providing healthcare services.

The presence of another person during the provision of healthcare services is permitted only with the consent of the patient unless it is impossible to provide the healthcare services without the presence of the other person, it is impossible to obtain the consent of the patient and failure to provide the healthcare services would significantly damage the health of the patient.

6.6 Duty to document

Healthcare providers must document the provision of healthcare services to each patient pursuant to the established requirements and must retain such documents. The patient has the right to examine these documents and to obtain copies thereof at his own expense, unless otherwise provided by law. The Minister of Social Affairs has issued a regulation which lists the documents that prove the provision of healthcare services, the forms of such documents and the procedure rules for documenting.

Failure to document the provision of healthcare services properly reverses the burden of proof. Normally, the burden of proof regarding circumstances which are the bases for the liability of the healthcare provider and healthcare professionals lies with the patient. If the provision of healthcare services to the patient is not documented as required, the burden of proof lies with the healthcare provider to prove that the healthcare services have been properly rendered to the patient.

The newly adopted amendments to the Health Services Organisation Act regarding the Health Information System make it obligatory to healthcare providers to document the information about the provision of healthcare services and information about the state of health of patients into the Health Information System. The Minister of Social Affairs has yet to issue the exact data that has to be on such documents that are to be forwarded to the Health Information System, and the rules of retention and procedures regarding such data. It is mandatory to use the classifications and address details of the national information system in order to ensure the quality of data.

6.7 Duty of patient to provide information

A patient must inform the healthcare provider about all circumstances which, according to his best understanding, are necessary for the provision of healthcare services and must provide any assistance which the healthcare provider requires to perform the agreement.

.

7 Identity management in the health sector

Much of the information (quoted text) of this chapter has been adopted from IDABC-report "eID Interoperability for PEGS. Estonia" referenced under [RD9].

7.1 Overview

"The most important eIDM system in Estonia is based on the Estonian ID-card, a mandatory electronic identity card that is intended to facilitate access to eGovernment services for all Estonian citizens and residents as well as offering access to a variety of other services. The ID-card is mandatory for Estonian citizens from age 15 and up (younger than 15 have an option to apply for an ID-card) and all aliens residing permanently in Estonia on the basis of a valid residence permit or right of residence irrespective of their age. The ID-card has three main functions: visual identification, authentication and digital signing. The card contains a chip holding a personal data file and two certificates: one for authentication purposes, and one for qualified digital signatures. Qualified electronic signature is an advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device, as defined in the eSignatures Directive. The ID-card certificates are linked to the various registers through the Personal Identification Code (hereinafter: PIC), which functions as a unique identifier for Estonian citizens and residents in eGovernment services. The PIC is included as a serial number on the certificates of the eID card. The PIC is provided by the Population register of Estonia." The PIC will be used as the patient identifier in eHealth applications as well.

"Although the ID-card is an important eIDM system, it is not the most used system today. Estonia has relatively long tradition of Internet banking and nearly everyone has access to it. The main method to access Internet banks is using password cards. Banks are providing authentication services to 3rd parties, including eGovernment systems. It is estimated that over 90% of eGovernment transactions requiring authentication are performed thanks to the authentication service from Internet banks. The PIC has also here the function of unique identifier in the authorisation process. This situation is going to change in a few years – banks are going to drop authentication service to 3rd parties and reduce usage of password cards by gradually lowering transaction limits.

The latest eIDM system is Mobile-ID. There are high expectations in the field of Mobile-ID. It is expected that ease of use (no software installation is required) and mobility (no smartcard reader is required) will drive the use of this PKI-based authentication and digital signing mechanism.

The main legal acts concerning e-IDM systems are the Identity Documents Act, the Digital Signature Act regarding ID-card certificates and the Population Register Act regarding the PIC."

7.2 X-Road and the Health Information System

"The backbone of the eGoverment environment is the X-Road (X-Tee) network of distributed and central servers. X-Road is a platform-independent secure standard interface between databases and information systems (to connect databases and information systems) of the public sector, which has a common user interface and a standard authentication system. The X-Road enables secure access to nearly all Estonian national databases; ensures the necessary availability, integrity and confidentiality of electronic document exchange over the Internet servicing Estonian residents, the state and local government authorities. In this environment, information systems provide and also consume different e-services.

Access to the X-Road is enabled only to the authenticated user: 1) in the case of the citizen/resident with the ID-card, via Internet banking authentication service, or Mobile-ID; 2) in the case of civil servant with the ID-card or via the information system of the authority; 3) in case of the information system, on the basis of the certificate of the security server of X-Road."
The following is adopted from http://www.digilugu.ee/DL_projekti_tutvustavad_materjalid_ENG.pdf : "Information systems that are interfaced with the Health information System forward messages at the moment when the health event takes place, i.e. on the same moment when the information that forms the content of the messages is created and is stored in information system of the healthcare provider itself. The message exchange channel is X-Road (http://x-tee.riik.ee/portaal/). Healthcare providers are interfaced to the Health Information System via X-Road. Healthcare providers with less capable information systems can use their rights through the doctors' portal.
In the framework of Health Information System, also a patient's Internet portal will be developed through which a person can monitor which data has been collected; who, when and why has accessed the data in the Health Information System; and to determine who and in what extent can see the medical records. The patient can also ban access to the medical data or add remarks to the Health Information System (for instance, allow or plan blood transfusion or organ donation). In the patient's Internet portal the person can modify the personal data so that time can be saved during the visit or in registration.
The information system interfaced with Health Information System must have the following functionality:

- capability of interfacing with X-Road (requires publicly certified secure servers);
- capability of forwarding/reception of standardised medical records (message standards and classifiers shall be approved on a national basis and will made be publicly available);
- end users of the Health Information System must be registered in public registers.

The Health Information System is using the two-phased authorization system of X-Road for the authorization of end users: Health Information System authorizes the interfaced information systems and the authorization of end users is implemented on the basis of data from public registers."

Authentication of end users is carried out with the help of authentication mechanisms developed in the information systems of the electronic ID card, Internet Banks', Mobile-ID infrastructures and information systems of healthcare providers.

7.3 The ID-Card

"A ministerial decision to introduce an ID-card was made in May 2000. First passports in Estonia were issued in 1992 with a lifetime of 10 years – it was a unique opportunity to renew the identification document system in Estonia by providing a new kind of document.
The decision was that the ID-card will be the mandatory (or: primary) identification document for Estonian citizens from age 15 and up (younger than 15 have an option to apply for an ID-card) and for all aliens residing permanently in Estonia on the basis of a valid residence permit or right of residence irrespective of their age. An alien receives an ID-card with the data of residence permit or right of residence. There are no separate residence permit cards. There are no sanctions for not having an ID-card, but the ID-card is provided as the "primary" identification document with the passport being optional.
It was decided that the ID-card will contain a contact chip with a personal data file (all data personalised to the visual card) and two certificates – one for the secure electronic authentication of persons and the second for creating a digital signature. The legal basis for the issuance and usage of certificates on ID-cards is the Identity Documents Act. The ID-card contains the certificates that enable digital authentication and digital signing, also personal keys that are corresponding to public keys that are generated into these certificates.
For more information about the terms of use for ID-card certificates, see http://www.pass.ee/index.php/pass/eng/id_card/terms_of_use_for_the_national_id_card_certificates . The terms of use for the ID-card are communicated to the ID-card applicant.
The Estonian legislation distinguishes between the authentication and digital signing. The general regulation (not application based) about digital signatures exists in the Digital Signature Act. The Digital Signature Act provides the necessary conditions for using digital signatures and the procedure for exercising supervision over the provision of certification services and time-stamping services. The Digital signature act was drafted in accordance with the European Councils regulation in EC 1999/93."
As of May 2008 over one million active ID cards have been issued. "Taking into account the population of Estonia (near 1.4 million) and the "addressable market" (people over 15 of age – roughly 1.1 million) one may say that the roll-out is completed."
"The physical card has the dimensions of ID-1 according to the International Civil Aviation Organization (ICAO) specifications. The card contains:
1) on the front side the card holder's signature and photo, and also name, PIC, birth time, sex, citizenship, card number, end of the date of card validity;
2) on the back side the card holder's birth place, card issuing date, residence permit details and other information (if applicable), card and holder data in machine readable zone (according to the ICAO standards).
All the above mentioned data except photo and handwritten signature are also present on the chip in electronic form, in a special publicly readable data file. The chip also contains two

certificates, allowing the authentication of the citizen and the use of a qualified electronic signature and their associated private keys protected with PIN codes. The certificates contain only the holder's name and PIC. In addition, the authentication certificate contains the holder's unique e-mail address.
It should be noted that, while the signature certificate is considered to be qualified, the authentication certificate has emphatically not been given this label. This choice was justified by concerns of legal certainty: the authentication certificate should not be used for signature purposes, and for this reason only the signature certificate is considered qualified. This way, parties are expected to take adequate precautions to ensure that the authentication certificate is not misused."

7.4 Bank eID

"The most popular method for authentication today is to use Internet bank authentication. Virtually all banks (5 major ones covering 99% of the banking customers) are providing authentication service to 3rd parties.
This works in practice as follows:
• the user logs into the Internet bank (using the appropriate method)
• the user selects "external e-service"
• user's PIC is securely communicated to the e-service
• user continues work with selected e-service

There are basically 3 methods for logging into Internet bank:
• password cards (with 24 codes) – around one million cards issued
• PIN-calculators – estimated 50 000 in use
• ID-card – over one million issued
Password-based authentication is the most (estimated – 90%) used method for Internet bank logging today. It is considered relatively secure as these password cards are issued personally in the bank office. Trustworthiness of banks is generally considered as good. Considering this, it is not surprising that number of eGovernment services make use of the bank authentication. Services like eTaxation and Citizen Portal are accessible through bank authentication. As a result, most (~86%) of the people declare their taxes via Internet. Citizen Portal represents a single point of access to ~70 governmental databases with more than 700 services."

7.5 Mobile-ID

The following is adapted from http://www.id.ee/blog_en/?p=20:
"The Mobile-ID service was launched by the joint effort of the Certification Centre and EMT (the biggest mobile carrier in Estonia), providing customers with a possibility to identify themselves and issue a digital signature by using a mobile telephone.
In order to use the service, a client needs to enter into a contract for use of the Mobile-ID service and replace the old SIM-card in the phone with a new one. Together with the new

SIM with added functionality, a client gets the usual PIN and PUK keys plus additional codes needed for Internet-based personal identification and issuing of digital signatures.
After signing the service contract, the Mobile-ID service must be activated, for this a client needs to use his or her ID-card and a card reader. Activation is needed for ensuring of maximum security, which is necessary, as the Mobile-ID can be used for gaining an access to bank accounts, for example, as well as for issuing a digital signature that has the same legal power as a handwritten signature."

8 Electronic prescription

Along with the adoption of Health Information System related amendments to the Health Services Organisation Act amendments were made to the Medicinal Products Act. These will also enter into force on 01.09.2008 and are directly related to the ePrescription (Digital Prescription) service. With the adoption of these amendments the basic legal framework was established for the application of the Digital Prescriptions project.

According to this new legal framework the Digital Prescription Centre (Retseptikeskus) will be established as an official database. It enables the issuing and processing of digital prescriptions for medicines and digital cards for medical devices. It also serves the purpose of generating medicinal statistics. The benefits for medicinal products and benefits for medical devices payable under the Health Insurance Act are also processed through this database. The Digital Prescription Centre is a separate database from the Health Information System, however it also makes use of the technical possibilities of X-Road (see above section 7.2).

Under the new norms all healthcare providers are obliged to issue prescriptions digitally, except when not possible for objective reasons (e.g. house calls). Persons who have the right to issue prescriptions have access to the Digital Prescription Centre. A proprietor of an activity licence for provision of pharmacy services has the obligation to immediately notify the Health Care Board of the conclusion or termination of an employment contract with a dispensing chemist or pharmacist. This is necessary for prevention of unauthorized access to the data in the Digital Prescription Centre.

A person whose data is being processed in the Digital Prescription Centre has the right to deny access to such data for the healthcare provider. The person has access to the personal data that is processed in the Digital Prescription Centre.

9 General assessment

The necessary basic legal framework that is required for the implementation of the eHealth projects of Estonia has been adopted and will enter into force on 01.09.2008. By 2013 the Health Information System must be fully operable, this is a realistic goal and there is a good chance that factually the whole system will be operable much sooner. In the short term several eHealth related regulations will be adopted by the Minister of Social Affairs and the Government. These will establish the detailed legal framework for the eHealth projects.
From the positive side the eHealth projects have greatly benefited from the already existing eGovernment technological infrastructure and a significant effort has been made to use standardised data sets. Use of international standards is the key to ensuring the interoperability of the information system. There are no special provisions that regulate possible future cross-border interoperability of the eHealth projects.
The Estonian legislator has established that the patient has full control over access rights to the personal data in the Health Information System – the patient can even block access to patient summaries, which cannot then be accessed even in emergency care situations. The privacy preferences of the patient are therefore paramount.
Overall the eHealth projects in Estonia are well on track and have an excellent maturity level.

Kaupo Lepasepp
Mihkel Miidla

19 June 2008

Annex: Contact details of National Correspondents

9.1 Primary Contact

Country	Estonia
Name	Kaupo Lepasepp
Organisation	Sorainen
Position	Senior Associate
Mailing Address	Pärnu mnt 15, 10141 Tallinn, Estonia
Work Phone	+372 640 0939
Fax	+372 640 0901
E-Mail	Kaupo.Lepasepp@sorainen.ee

9.2 Alternative Contact

Country	Estonia
Name	Mihkel Miidla
Organisation	Sorainen
Position	Associate
Mailing Address	Pärnu mnt 15, 10141 Tallinn, Estonia
Work Phone	+372 640 0959
Fax	+372 640 0901
E-Mail	Mihkel.Miidla@sorainen.ee