UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Alvar Ristikivi

Ensuring the Integrity of Electronic Health Records

Master's Thesis (30 ECTS)

Supervisors: Jaan Priisalu MSc
Raimundas Matulevičius PhD

Tartu 2018

Ensuring the Integrity of Electronic Health Records

Abstract

We are living in an era with an abundance of electronic data, yet the integrity and evidential value of these data are very hard to check. At present the problems like affecting the 2016 presidential elections in the USA or elections in the Europe by (social) media are highly topical. A few years ago such activity seemed completely improbable but it is entirely possible using contemporary means of data manipulation. Big data analysis as well is constantly reaching wider masses. The processing of sensitive genetic and health data has become an everyday issue. However, in order to ensure the complete authenticity of these data, it is necessary to guarantee their evidential value by certifying their initial source.

The initial source can only be certified by adding a digital signature or seal to a document containing health data, which should be done as close to its source as possible. It means that we can later rely on a medical document only if its compiler, the general practitioner, has digitally signed it.

Currently a major concern is that the format of electronic signing is changing and a large number of documents in old format have to be signed again. Thus, a solution should be found to the highly topical problem of how to ensure that the document has the original, unchanged evidential value also many years later.

Keywords: electronic health records, integrity, digital signature

CERCS: P170 Computer science, numerical analysis, systems, control

Elektroonsete terviseandmete terviklikkuse tagamine

Lühikokkuvõte:

Me elame ajastul, kus meie käsutuses on väga palju andmeid, kuid samas on nende andmete õigsust ja tõestusväärtust väga raske kontrollida. Nii on kasvõi Eurooopas või Ameerikas toimunud valimiste (sotsiaal)meedia abil mõjutamine asjakohane näide - aastaid tagasi ei võidud selle võimalikkusest mõeldagi, tänapäevase meedia abil aga küll. Samamoodi hakkab massidesse jõudma big data analüüs. Geeni- ja terviseandmete töötlemine on muutunud igapäevaseks, aga selleks, et tulemusi saaks 100% õigeteks pidada, on vajalik, et nende andmete tõestusväärtus oleks algallikas kinnitatud. Viimane on aga võimalik ainult digitaalse allkirja või tempiga, mis on antud võimalikult lähedal algallikale - meditsiinidokument peab olema allkirjastatud isiklikult perearsti poolt, sest ainult nii on võimalik seda tulevikus arvesse võtta.

Hetkel on suureks probleemiks ka asjaolu, et digitaalallkirjastamise formaat on muutumas. Seetõttu oleks väga palju vanas formaadis digiallkirju vaja ümber teha ja ühtlasi tagada, et hiljem on algse dokumendi tõestusväärtus sama, mis vastava dokumendi tegemise ajal.

Võtmesõnad: elektroonsed terviseandmed, terviklikkus, digitaalne allkiri

CERCS:P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

List of Abbreviations and Terms

BDOC	binary document
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
CLUSIF	Club de la Sécurité de l'Information Français
CSP	certification service provider
DDOC	digital document
DSG	document digital signature
EHR	electronic health record
EU	European Union
GP	general practitioner
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HWISC	Health and Welfare Information Systems Centre
IS	information system
ISO	International Organization for Standardization
ISKE	Infosüsteemide Kolmeastmeline Etalonturbe süsteem (Three-level baseline security system)
ISMS	Information Security Management Systems
ISSRM	information systems security risk management
IT	information technology
KSI	Keyless Signature Infrastructure
MEHARI	Method for Harmonized Analysis of Risk
MSP	medical service provider
NHIS	National Health Information System
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
RRL	risk reduction level
SRQ	sub-research question

Table of Contents

List of Figures

List of Tables

1 Introduction

Medical records in some form or other are as old as medicine itself. As stated by Luo [1, p. 20], "A medical record is an account of the patient's presenting symptoms, with annotations from the physician and other health professionals detailing their observations as well as discussions with the patient". In earlier times medical information of people was stored on paper in hand-written form. At first every doctor took his own notes, which were inaccessible to others, but later on different data pertaining to one person were collected together in one record. However, a major drawback of a paper-based record is that it can be in only one place at a time and has to be taken from one medical institution to other. Handwriting in such records is often poorly legible, which in turn may cause misunderstandings and flaws in making decisions about the treatment of patients. With the advancements in medicine and computer technology an idea of implementing computer-based medical records arose in the late 1960s [2]. Patient's health information in such records is stored in a digital form and can be shared between different health care providers through network-connected information systems. Electronic health records (EHRs) contain various medical data from all doctors treating one and the same patient, but also laboratory test results, information on medication, allergies, etc. All data are stored in only one modifiable file, which largely facilitates extracting data needed for the examination of a patient and making decisions about his/her health status and further treatment. Electronic health-care records must be preserved at least for the patient's lifetime or much longer for academic research.

However, as in the case of other kinds of information exchange via electronic channels, the EHRs may also be affected by threats from hackers, malicious workers, third parties, vulnerabilities or viruses – the information can be stolen, modified or used in some other adverse way causing harm to the patient. The increasing number of electronically stored medical records enhances also the possibility of threats to our security and privacy [3]. Thus, one of the key problems is ensuring the integrity of information, which is discussed in this master's thesis.

The integrity problems are very intense in present-day shared infrastructure. The researh of the European Union Agency for Network and Information Security about security and resiliance in e-health has found out that, according to the EC Directive on Critical Infrastructures, healthcare services have been recognized as a critical societal sector. Therefore, healthcare systems are considered as critical infrastructures that should be protected from all types of threats, including cyber security attacks [4]. However, many obstacles still need to be overcome "in the legal and semantic interoperability, standardization or electronic identification domains" [5].

The main aim of this master's thesis is to find out which methods can ensure the integrity of EHRs. Legal and cyber security aspects are analysed on the example of Estonia, the USA and European Union. The present state of the Estonian e-health infrastructure is considered. The business assets and risk analysis of the assets in the Estonian e-health infrastructure are discussed. Great attention is paid to security risk assessment, mitigation and control selection which are among the main issues in securing the integrity of EHRs.

The thesis is based on the assumption that the attributes of data authenticity, integrity and data origin verifiability are preserved by digital signature. The information transmitted over a transfer medium can be deliberately or accidentally modified, which may result in loss of data integrity. If the digital signature is used on the health information side, any modification on the signed content is immediately detectable [6].

To better understand cyber security challenges in the Estonian e-health infrastructure, the main focus of the thesis is on analysing the integrity of the EHRs. I chose the topic of the thesis due to my personal experience in dealing with medical records containing sensitive data at the National Health

Information System (NHIS) of Estonia. As very many EHRs from general practitioners (GPs) reach the NHIS in digitally unsigned form, they are vulnerable to any unauthorized modification, which may result in mistakes in patient treatment and may even have lethal consequences. In order to prevent such irreversible damage, measures should be taken to increase the integrity of EHRs of thousands of people, one of those measures being adding a digital signature to an EHR by the person or organization who initially creates that document.

1.1 Problem Statement

In Estonia, the NHIS is the main central state health information database managed by the Health and Welfare Information Systems Centre (HWISC). Doctors, medical service providers (MSPs) and GPs or health-care service providers are main data producers and data users. Medical service providers and the NHIS are connected over the data exchange layer named X-Road. General practitioners do not use X-Road infrastructure due to the lack of financial instruments, technical skills or infrastructure. Information systems of GPs are connected with the NHIS over a mini information portal which is managed by the HWISC. A digital signature or an e-seal added to an EHR can ensure the integrity of this EHR. Due to the lack of skills of software developers, a GP must sign every record manually. Thus GPs are not satisfied with this service and want it redesigned. The decision of the former Estonian E-health Foundation (present HWISC) committee to allow GPs to send digitally unsigned documents to the NHIS creates a security risk to patients data. Today GPs send out EHRs without a digital signature and the NHIS digitally signs them. This procedure, however, may not be secure and may make the unsigned documents vulnerable. The digitally unsigned EHRs are vulnerable to theft, unauthorized alteration or misuse during the transfer of patients' medical data from the system used by GPs to the NHIS. Due to the sensitivity of the information that the health-care system is dealing with, security is one of the major concerns that must be dealt with [7].

1.2 Research Methods

This thesis is a case study-based research relying on surveys and interviews. The current situation in the Estonian e-health infrastructure is analysed. The focus groups are security managers, chief information officers and GPs. The results are limited to Estonian context, as mainly persons from Estonia participated in this study. The reliability of the results was improved by including external experts in the process. The figures of the present thesis were compiled using Gliffy software and symbols in the standard Business Process Model and Notation, developed by the Object Management Group [8]. With the help of this standard, organizations can better understand and manage their business processes in a graphical notation.

1.3 Research Questions

The main research question of this thesis is:

How to guarantee the integrity of the EHR business process?

The main research question is subdivided into the following sub-research questions (SRQ):

SRQ1 – What assets are present in the Estonian e-health infrastructure?

SRQ2 – How to assess risks of assets in the Estonian e-health infrastructure?

SRQ3 – How to mitigate risks in the Estonian e-health infrastructure?

To find an answer to the main research question, first the present situation of the Estonian e-health infrastructure is described. Next the business and information system assets are analysed and the ways how information system (IS) assets support business assets and security criteria are discussed. Risk analysis of assets in the Estonian e-health infrastructure is provided, involving defining threat agents, attack methods, vulnerabilities and impacts. The analysis also includes security risk mitigation, risk assessment and control selection.

The results obtained in the study are validated through the survey that was conducted among specialists working in the E-health infrastructure. As the main question of my thesis is how to ensure the integrity of EHRs, I prepared a questionnaire and drew conclusions based on the answers that I received from the experts in the field of e-health.

The first sub-research question (SRQ1) is discussed in detail in Chapter 3. Several parties are operating in the Estonian e-health infrastructure through different ISs. By finding out how the responsibilities are shared between these parties, it can be understood what kind of information is transferred through different parties and how its confidentiality, integrity and availability is secured in different organizations.

The second sub-research question (SRQ2) is discussed in Chapter 4. It is very important to understand that the Estonian e-health infrastructure is not one organization but a much wider structure consisting of several organizations and governmental institutions, which can all be affected by the weaknesses of that system.

The third sub-research question (SRQ3) is dealt with in Chapter 5. In the Estonian e-health infrastructure some resources are shared but the organizations involved do not have the same security requirements. For that reason, for example, the NHIS must follow the highest security standards in order to ensure the integrity of EHRs. General practitioners, however, do not need to follow the same security requirements, which may breach the integrity and reliability of documents created by them.

2 Background

The main goal of this chapter is to give an overview of EHRs and to introduce risk management frameworks. The following questions are tackled:

- What standards and methods are used to assess security risks related to EHRs?
- What is security risk management?
- What security risk standards could be used for an EHR?
- What methods support the assessment of an EHR?

2.1 Description of EHRs

Electronic health-care records have different forms depending on their purpose, kind of information stored, range of the information [9]. Among these, EHRs are widely used. According to the definition of the International Organization for Standardization (ISO) [10], an EHR is "a repository of patient data in digital form, stored and exchanged securely, and accessible by multiple authorized users. It contains retrospective, concurrent, and prospective information and its primary purpose is to support continuing, efficient, and quality integrated health". A patient's EHR is a "shared, integrated or interlinked (virtual) record of all his/her clinically relevant health and medical data independent of when, where and by whom the data were recorded" [5, p. 5].

An EHR is a digital version of a patient's paper-based medical chart. It is a real-time, patient-centred record which provides instant and secure information to authorized users. An EHR contains information from more than one health-care organization, such as laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, etc. The information is shared between all clinicians involved in a patient's care. The term "EHR" is widespread, but there exist also several other terms for EHR: "electronic patient record", "electronic medical record" and "computer-based patient record" [11]. The terms "electronic health record" and "electronic medical record" are often treated as synonymous. However, the National Alliance for Health Information Technology, USA, gives two different definitions, and differentiates also the personal health record [12]:

a) Electronic health record – "An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization" [12, p. 17].

b) Electronic medical record – "An electronic record of health-related information on an individual that can be created, gathered, managed and consulted by authorized clinicians and staff within one health care organization" [12, p. 16].

c) Personal health record – "An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual" [12, p. 19].

Although great progress has been made in the use of EHRs, this process may be quite complicated. The key factors affecting the adoption of electronic records are nation's overall healthcare system, the information technology (IT) status and strategies, national or regional approaches, connectivity issues, and stages of implementation, as well as the governance, funding, public policy, and legal and regulatory issues [13]. There is also resistance among doctors. Among many reasons brought

out by Ajami and Bagheri-Tad [14] we could mention the need of extra time, cost, computer skills, disruption of work flow, security issues, etc.

2.2 Benefits of EHRs

In comparison with paper-based medical records, EHRs have many benefits both for patients and health service providers. They enable an effective flow of information, making it available whenever and wherever it is needed, thus contributing to the delivery of better medical care. The benefits of EHRs have been widely discussed in medical circles in relation to the adoption of EHRs and are thus also considered in numerous published papers and respective webpages ([11,15]).

The following main benefits of EHRs can be listed [15]:

1. Improved health care – providing convenience in health care transactions and reliable and quick access to complete patient health information resulting in more coordinated and efficient care; enhanced decision support and medical information; real-time quality reporting, legible (unlike handwritten reports, which are often difficult to read), complete documentation; interfaces with labs, registries and other EHRs; safer, more reliable prescribing and a possibility of e-prescriptions electronically sent to pharmacy; patient portals with online interaction for providers.

2. Increased patient participation and improved care coordination – patients can get accurate information about their medical evaluations, self-care instructions and reminders for other follow-up care; appointment schedules can be made electronically and via e-mail, thus providing quick and easy communication between patients and service providers, enabling earlier identification of disease symptoms and improved diagnostics and patient outcomes.

2.3 Security of EHRs

A major issue with the implementation of EHRs is protecting their integrity, which is extensively covered in scholarly publications (see e.g. [16] and references therein) and webpages of different health-related governmental and local institutions, organizations, etc. As any malevolent modification of EHRs may cause great, sometimes irreversible damage to patient's health, countries have taken legal measures and issued regulations for ensuring the integrity of EHRs (e.g. [4,17–24]). The primary necessity, however, is to ensure a safe transfer, maintaining and exchange of medical data between institutions. For this purpose various methods have been implemented, including adding a digital signature to an EHR. A digital signature is widely used in Estonia, who has long been in at the forefront of digitizing medical services.

In the European Union (EU) all e-health organizations are dealing with local Data Protection Acts and European Union Data Protection directive stating that "Everyone has the right to the protection of personal data" [25]. Currently Directive 95/46/EC [17] and Framework Decision 2008/977/JHA [18] are used as legal framework in Europe. In January 2012, however, the European Commission put forward its EU Data Protection Reform. The aim of the reform was to make Europe fit for the digital age, to simplify the regulatory environment for business and to establish a harmonized data protection framework across the EU. The new rules are contained in the Regulation [19] and Directive [20] of the EU, which both will apply from May 2018.

In the United States the release of health-care information is legally regulated by the Health Insurance Portability and Accountability Act (HIPAA) adopted in 1996. The Privacy Rule of the HIPAA [21] defines the information that needs to be protected as the data concerning patient's health status, the provision of healthcare or payment for healthcare. It also gives instructions about how and under what circumstances protected health information can be disclosed. The use of such information for

marketing, fundraising or research is only permissible under patient's prior authorization in writing. The Privacy Rule also provides patients with access to their medical records.

The security of EHRs is regulated by the HIPAA Security Rule, which is aimed to protect all individually identifiable health information created, maintained or transmitted in electronic form by health-care providers. The rule specifies three types of safeguards that need to be implemented for this purpose [22]: (1) administrative (security management, security personnel, information access management, workforce training and management, evaluation of security policies), (2) physical (facility access and control, workstation and device security) and (3) technical (access control, audit controls, integrity controls, transmission security).

The health data and more sensitive patient communication data are protected by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which widens the scope of privacy and security protections provided by the HIPAA. The Act contains incentives related to healthcare IT in general (e.g. creation of a national health care infrastructure) and specific incentives designed to accelerate the adoption of EHR systems [26]. Cyber threats are graphically depicted in Figure 1.

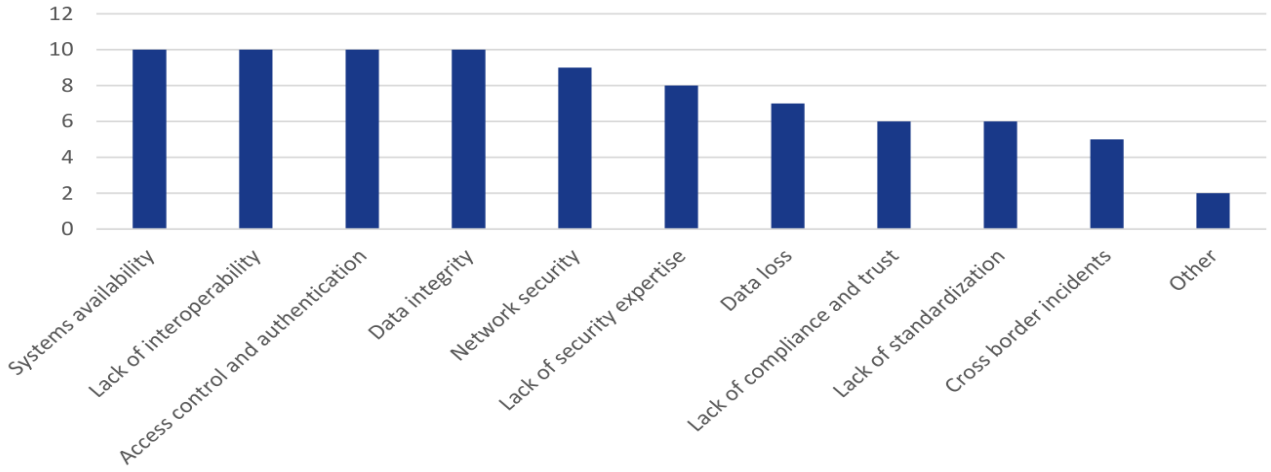

Figure 1: Cyber threats and challenges [6].

Nowadays the physical security of systems, firewalls, encryption technologies and access control mechanism are used to maintain the security of data [27]. However, we can spend a huge amount of finances and it is still not enough to prevent data breaches. The major cyber threats and security challenges in e-health are: systems availability, lack of interoperability, access control and authentication, data integrity, network security and data loss. In Estonia we are using a personal code, which is unique identification for every person. Every user is registered in the central authority, and the user can obtain a smart card. Access to data in the Estonian e-health infrastructure is granted in the case of therapeutic relationship. We must remember that the data integrity level is not the same as the security level [28]. The network architecture and network equipment (switches, firewalls, security patches, event logging systems, etc.) are not sufficient for the network security layer when we are dealing with personal e-health data. In Estonia we are using the X-Road infrastructure which gives an additional security level, between MSPs and the NHIS.

2.4 Standards and Regulations

Many standards are used in healthcare industry. The following main standards are regulating the EHRs:

- Health Level7 (HL7) Clinical Document Architecture – Health Level Seven International (HL7) is a not-for-profit standards developing organization founded in 1987. “Level Seven” refers to the seventh level of the ISO seven-layer communication model for Open Systems Interconnection to the application level [29];
- openEHR [30] – an open standard specification in the health informatics that describes how to manage, store, retrieve and exchange health data in EHRs [31].

These standards help to structure and markup clinical information for exchange between clinicians. From the security prospective the following standards must be followed by the organizations dealing with EHRs: ISO 18308:2011 [32], ISO/IEC JTC1/SC27 [33], ISO/TC 215 [34]. The most important standard is ISO 18308:2011 “Health informatics – Requirements for an electronic health record architecture” which is a set of technical and clinical standards for Electronic Health Record Architecture. This standard supports the use and exchange of EHRs between different health sectors and different countries [35].

2.5 Information Risk Management

Information is very valuable and important for private and state organizations, therefore it must be treated with utmost responsibility. Information risk management is an essential part of nowadays successful companies culture but its importance is often neglected by private companies as well as state-owned organizations.

According to Matulevičius [36, p. 17], “One important task during secure systems development is to understand what assets need to be protected against which risks, and how these risks could be mitigated by proposed security countermeasures”. Main parts of risk management are: risk identification, risk assessment and risk prioritization. The process of information risk management is depicted in Figure 2.

It is a common belief that information security means protecting the information at our disposal against cyber criminals. Yet, this issue needs to be considered from a wider aspect, involving also the protection of information against different force majeure risks such as flooding, storms and earthquakes. Information risk management in an organization should begin by implementing the documentation establishing the procedures necessary for fulfilling that task. The administration of the organization must initiate and control this process, and build up the procedure of monitoring everyday transactions.

Monitoring is particularly important in an organization dealing with confidential health data of people for securing the integrity of health data available in EHRs. When building up the new infrastructure from scratch, we can rely upon the Risk Management Framework. However, in situations with a substantial legacy from old systems and infrastructure, the Risk Management Frameworks need to be treated with caution.

2.6 Security Risk Management Standards

The security of the IS and the management of the security system are essential issues for all organizations who are interested to be successful. The easiest way of fulfilling the needs of IS security management is keeping track of security standards. Nowadays numerous security risk management standards are available, including different approaches to how and at what stage of the project to use them. We can expect that organizations who are participating in the Estonian e-health infrastructure have respectively planned, documented and functioning processes.

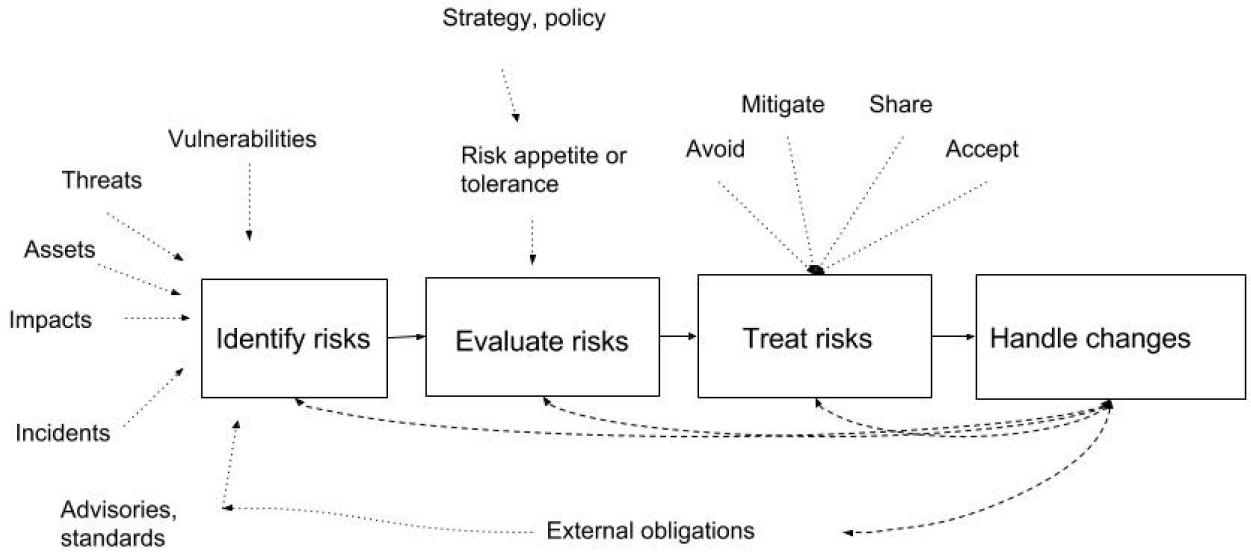

Figure 2: Information risk management [37].

2.6.1 ISO/IEC 27005: Information Security Risk Management

The ISO/IEC 27005 standard [38] describes the information security risk management process and its tasks. The second edition of the standard was published in 2011. This standard is based on the general corporate or enterprise-wide risk management standard ISO 31000:2009 “Risk management – Principles and guidelines”. The information security risk management process consists of the following stages:

- establishment of the risk management context, including the scope, compliance obligations and methods to be used and relevant policies;
- risk assessment – identifying, analysing and evaluating relevant information risks by considering the information assets, threats, existing controls and vulnerabilities and on that basis determining the likelihood of security incidents or security incident scenarios and the “level of risk”;
- risk treatment – several risk treatment tasks are needed to reach the best state in terms of residual risk; the effectiveness of risk treatment depends directly on risk assessment;
- risk acceptance – organization managers must accept residual risks;
- risk communication – sharing information with the stakeholders through the process; the whole process should be clearly documented so that all participants understand it;
- risk monitoring and review – monitoring and reviewing risks, risk treatments, identification and responding to changes.

The ISO/IEC 27005 information security risk management process is graphically depicted in Figure 3.

2.6.2 Information Security Risk Management Standard by the US National Institute of Standards and Technology

The Cybersecurity Framework of the US National Institute of Standards and Technology (NIST), founded in 1901 within the US Department of Commerce, provides a framework and methodology of computer security guidance for private sector organizations and for critical infrastructure in the United States of America. The first version of the NIST standard was published by the NIST in 2014 [39]. The NIST framework has three main parts [40]:

- The core – "a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors"; these allow for "communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level". The core consists of five components (functions) aimed at managing cyber security risk: identify, protect, detect, respond and recover. Each function has key categories and subcategories which are matched with existing standards, guidelines and practices.
- The tiers – we can find them from companies outcomes, and they are related to companies business needs. The following tiers are distinguished: tier 1: partial; tier 2: risk informed; tier 3: repeatable; tier 4: adaptive.
- The profiles – the organizations current status and road map towards the NIST.

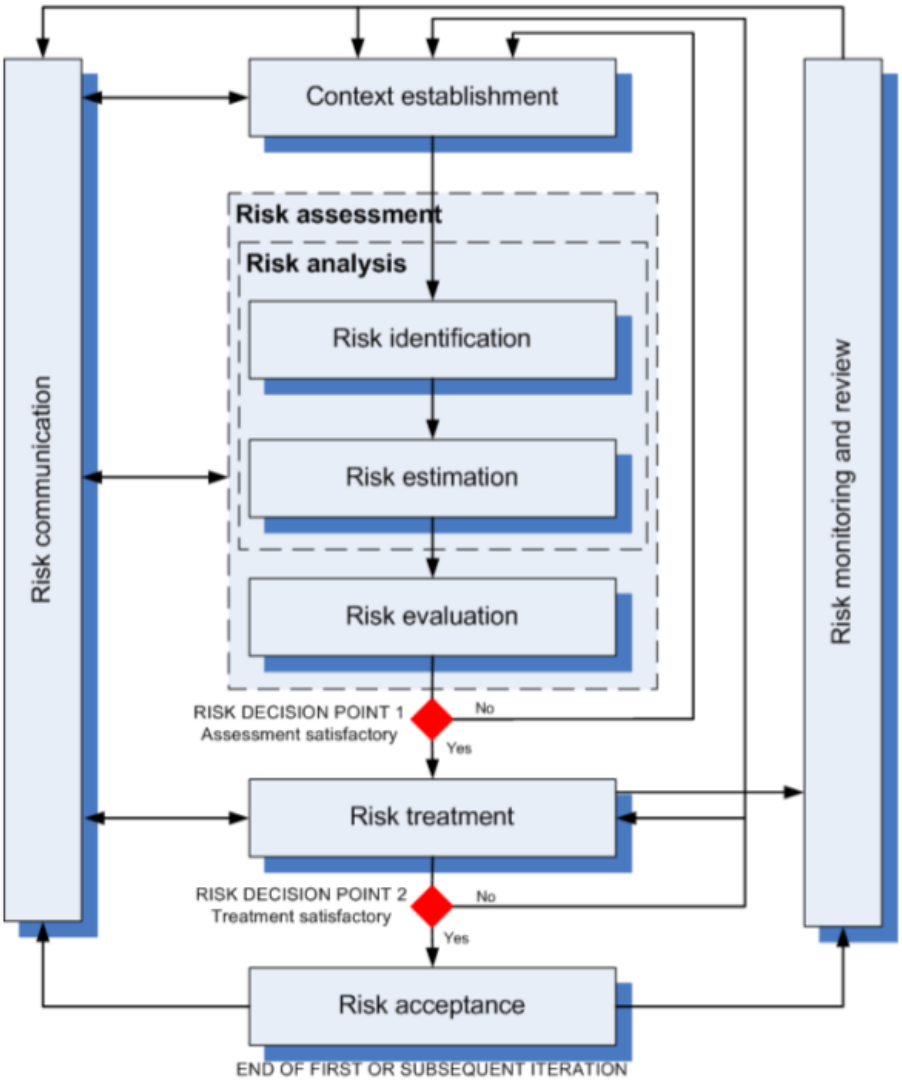

Figure 3: The ISO/IEC 27005 information security risk management process [38].

The standard NIST SP 800-30, entitled “Risk Management Guide for Information Technology Systems”, deals with the risk assessment procedure and provides a baseline for conducting effective risk management. It proposes two complementary processes: “risk assessment” and “risk mitigation”. The “risk assessment” process has nine components: system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendation and results documentation [41]. The “risk mitigation” process is composed of seven steps: prioritizing actions, evaluating recommended control options, conducting cost benefit analysis, selecting controls, assigning responsibility, developing safeguard implementation planning and implementing selected controls.

2.6.3 The Risk Management Framework by the German Federal Office for Information Security

The IT-Grundshutz is a set of German standards issued by the German Federal Office for Information Security (BSI) [42], containing methods, processes, procedures, approaches and measures for information security. The IT-Grundshutz is composed of three standards: BSI Standard 100-1: Information Security Management Systems (ISMS), BSI-Standard 100-2: IT-Grundshutz Methodology and BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz. Main parts of ISMS are: planning the information security risk processes, implementing the policy for information security, performance review in the information security process and eliminating discovered flaws and weaknesses. The participants in the ISMS are shown in Figure 4.

Figure 4: Components of the ISMS [43].

2.7 Security Risk Management Methods

The CLUSIF (Club de la Sécurité de l'Information Français) study from 2004 found that more than 200 security risk management methods had been registered [41]. These methods have their strengths but also weaknesses. There exist different conceptions and also lack of interoperability between methods. The selection of the proper method depends on the organization. However, more than one method should be used to resolve the task of protecting the integrity of EHRs.

2.7.1 Information System Security Risk Management Domain Model

According to Matulevičius [36, p. 17], “A domain model for information systems security risk management (ISSRM) is developed through a survey of security-related standards, security risk man-

agement standards, and security risk management methods". Main parts of the ISSRM domain model are the following concepts:

- asset-related – through this concept it is determined which organization assets must be protected. The assets can be divided into several parts, for example business assets or organizational assets;
- risk-related – definition of risk and components;
- risk treatment – a conception of how to treat risk; it can be divided into four subcategories of risk treatment: risk avoidance, risk reduction, risk transfer and risk retention.

All concepts are related to each other. A Universal Modeling Language class diagram showing how various risk components are linked to each other is represented in Figure 5.

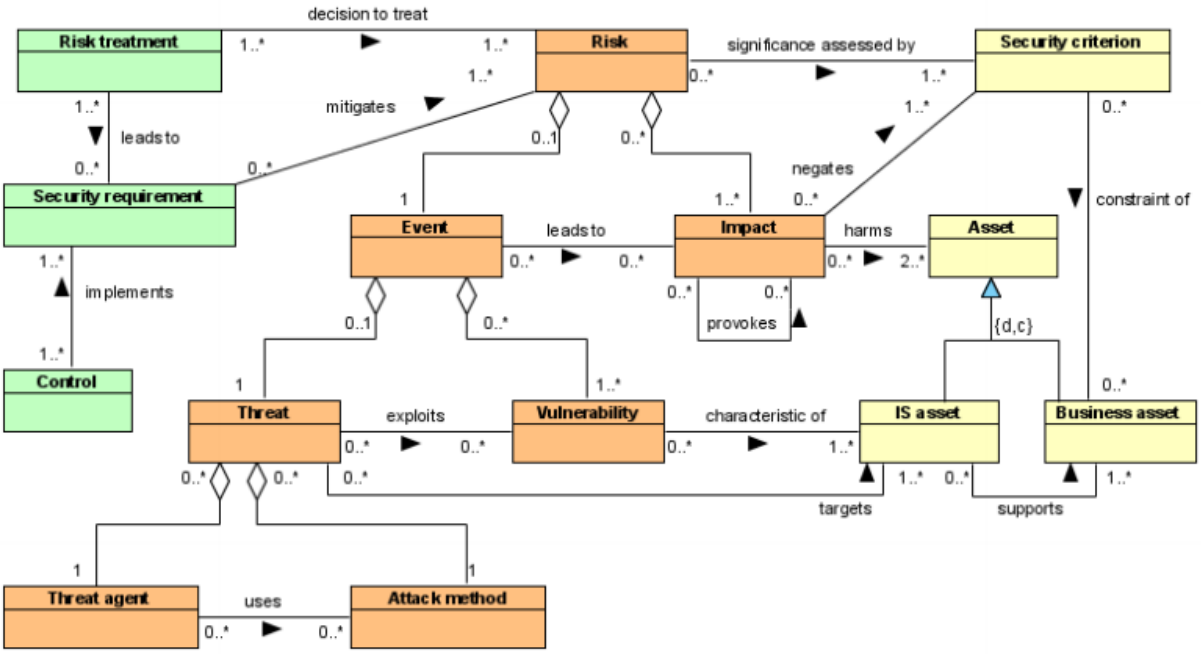

Figure 5: ISSRM domain model [44].

The main advantage of ISSRM is that it facilitates communication between three main stakeholders who are concerned with IS security: IS developers, organization managers and organization clients [41]. Using the ISSRM approach, we can usually have three outcomes [41]: the improvement of IS security, better management of decisions about IS security investments and assessing the level of confidence, which is important for customers and partners.

2.7.2 MEHARI

MEHARI (Method for Harmonized Analysis of Risk) is a free, open source risk analysis assessment and risk management method established in 1996 by the CLUSIF, a French IS security professional association. MEHARI is based on two older methods – MARION (Méthode d'Analyse de Risques Informatiques Optimisée par Niveau) [45] and MELISA (Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes d'Armement), which are not maintained any more [41]. MEHARI is like a toolbox designed for security management, consisting of the following modules:

1. Security stakes analysis and classification – analysing assets of an organization. It starts from defining a malfunction value scale, identifying the main activities and their objectives. On the next step the resources of the IS are classified through the identification of elements and giving rankings from classification criteria (confidentiality, integrity, availability).
2. Evaluation guide for security services – assessing the security level of the IS and through this finding out main weaknesses of the system. It helps to make protection plans.
3. Risk analysis guide – identifying critical risks and analysing the risk situations.

   MEHARI's risk listings are illustrated in Figure 6.

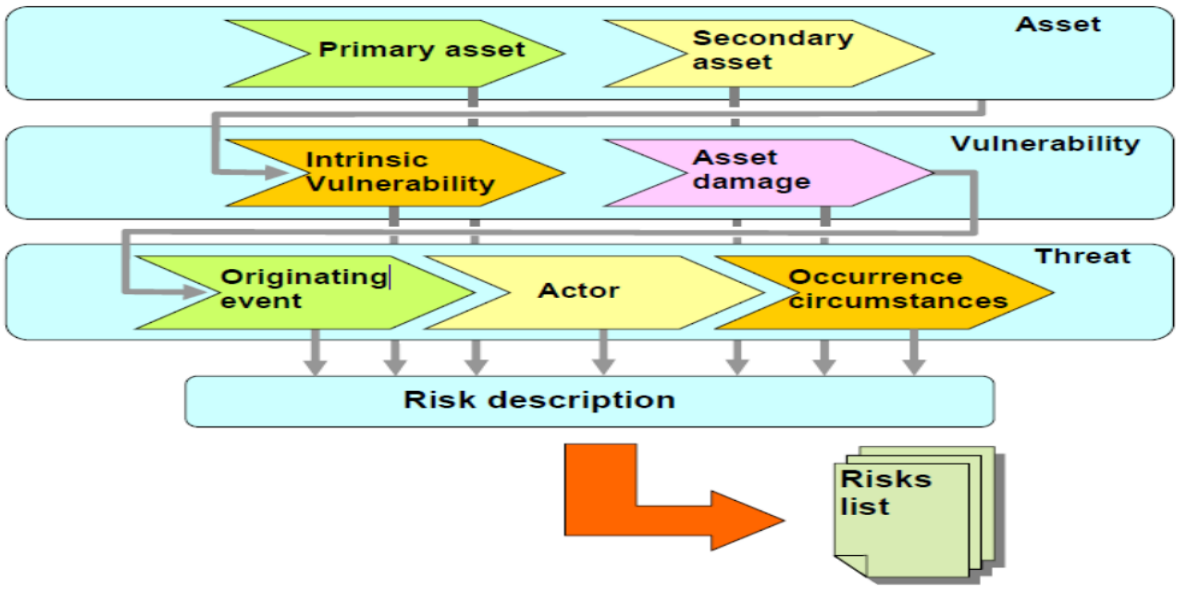

Figure 6: Risk process [46].

2.8 Summary

In this chapter I first gave a brief description and overview of benefits of EHRs. Next I discussed the problem of ensuring the security of EHRs, which is one of the major issues in health care. Numerous standards and methods for assessing and managing the security risks related to EHRs are available, some of which are dealt with in this chapter. I considered the following questions:

1. What standards and methods are used to assess security risks related to EHRs? – Risk management is a continuous, proactive and systematic process for assessing and managing Estonian e-health infrastructure risks in line with the accepted risk levels to provide reasonable assurance for achieving the stated project objectives. Many standards have been developed for information security management, but no methods are presented for implementing them. The ISO/IEC 27005 standard provides a general framework for risk management, but even there is much freedom for interpretation. **2. What is security risk management?** – It is necessary to understand what assets need to be protected and which measures could be applied to mitigate security-related risks. Main parts of risk management are: risk identification, risk assessment and risk prioritization. **3. What security risk standards could be used for an EHR?** – Three standards were presented in this chapter: the ISO/IEC 27005 standard, the NIST standard (issued by the US National Institute of Standards and Technology) and IT-Grundshutz (a set of standards issued by the German Federal Office for Information Security). **4. What methods support the assessment of an EHR?** – I discussed two risk

management methods – ISSRM and MEHARI. The main advantage of ISSRM is that it facilitates communication between IS developers, organization managers and organization clients. MEHARI consists of three modules: security stakes analysis and classification, evaluation guide for security services and risk analysis guide. It is a free, open source method of security management.

3 Present E-health Infrastructure in Estonia

The aim of this chapter is to give an overview of assets and security threats in organizations who are changing information in the Estonian e-health infrastructure. The assets are analysed and thereafter the assets involved in the Estonian e-health infrastructure are identified. In this chapter I provide an answer to SRQ1 – What assets are present in the Estonian e-health infrastructure? In the discussion below I consider the following problems:

- Which organizations take part in the Estonian e-health infrastructure and what is the responsibility of different parties?
- What kind of ISs are involved?
- How is an EHR transferred in the Estonian e-health infrastructure?

3.1 NHIS Infrastructure in Estonia

As mentioned above, the National Health Information System (NHIS) is the main central state health IS in Estonia. It is managed by the Health and Welfare Information Systems Centre (HWISC). The task of the NHIS is to collect medical data from the respective service providers, to store these data and enable their accessibility. The greatest group of data producers and receivers consists in other medical service providers (MSPs) who use this information in making decisions about the treatment of patients. The second biggest group of users is patients who examine their electronic health records in the patient portal. The data collected by the NHIS must comply with the security measure HT.34 of the instructions of ISKE (in Estonian *Infosüsteemide Kolmeastmeline Etalonturbe süsteem*), a three-level IT baseline security system that has been developed for the Estonian public sector, and the NHIS must guarantee their integrity. The obligation of transmitting data into the NHIS by MSPs has been laid down in the Health Services Organisation Act (adopted on 09 May 2001) [47], Statutes of the Health Information System (adopted on 14 August 2008) [48] and Decree No. 53 “Health Information System transmitted data of documents and their storage conditions and the procedure” of the Minister of Social Affairs of 17 September 2008 [49].

According to Article 2 of the statutes of the NHIS, a health IS is a set of data belonging to the national IS. Provision 1 of Article 1 of the Security Measures for the Information Systems Act (No. 252, adopted 20.12.2007) [50] establishes that a system of security measures is applied to all ISs and related information software that are used to process data contained in state-level or local databases. The parties of the Estonian E-health infrastructure are presented in Table 1.

Medical service providers send data to the NHIS and also receive data. Data exchange between the MSPs and the NHIS takes place via X-Road, the data exchange layer for ISs. Medical services are provided by large hospitals as well as small centres of GPs. The IT solutions used by them, however, are different. The logical scheme of the Estonian E-health infrastructure is presented in Figure 7. The GPs and doctors are using different software provided by MSP software developers or portals developed by HWISC developers for sending and receiving medical information. The MSP’s software and GP’s software can change information over the X-Road infrastructure or over the Mini information system portal. Citizens can see medical information of them and their relatives through the patient portal and can also share rights to their relatives.

Table 1: Parties of the Estonian e-health infrastructure.

Patient	The person whose data are entered into the electronic health record, stored and processed
General practitioner	A doctor with required training, practising in general medicine, not in any specific branch of medicine, treating patients of all ages, collecting information and creating electronic health records
Doctor	A doctor with required education and skills, practicing in a special branch of medicine, collecting information and creating electronic health records
Medical service provider	Organization providing medical services
National Health Information System	Health and Welfare Information Systems Centre
Medical software developer	The company developing the software used by general practitioners or other doctors
Ministry of Social Affairs	The Ministry directing, controlling and funding medicine in Estonia

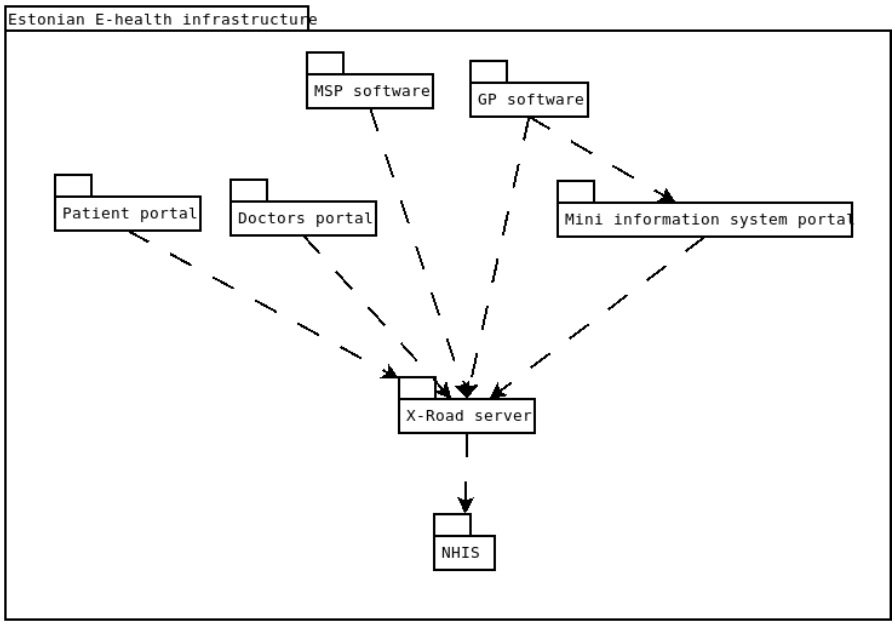

Figure 7: Estonian e-health infrastructure.

3.2 Digital Signature in Estonia

The Digital Signatures Act, adopted by the Parliament of Estonia on 8 March 2000, establishes that the digital signature is equivalent to the hand-written signature [51,52]. The digital and the hand-written signature must be equally valid in the private as well as in the public sector. The Digital Signatures Act also regulates the activity of the Certification Service Provider (CSP) in Estonia. The CSP in Estonia is the company SK ID Solutions AS. According to the Act, the CSP is obliged to provide the control of the validity of certificates. The following protocols are used: Certificate Revocation List – a shared list of suspended and revoked certificates (for description see [53]), Lightweight Directory Access Protocol – includes all valid certificates (see [54]), Online Certificate Status Protocol (OCSP) – the most used service offered by the CSP [55].

3.3 Usage of Digital Signatures with EHRs

Ink-based signatures have long been part of he documentation process in health care [56], but the use of digital signatures is gaining importance. The Document Digital Signature (DSG) Content Profile is a technical integration framework issued by the Integrating Health-care Enterprise. The DSG defines general methods of the use of the digital signature with EHRs. There are three types of digital signatures: (1) an enveloping signature – document contains both the signature block and the content, (2) a detached signature – this approach includes only references to the signed content and (3) a submission set signature – manifest of all the other documents included in the submission set.

3.4 Security Assets of the Estonian E-health Infrastructure

The NHIS must also fulfil the requirements set by ISKE. The first version of the ISKE implementation manual was completed in 2003, but it has been repeatedly revised later [57]. The NHIS has been assigned the integrity level T3. It means that the evidential value of data must be confirmed by a digital signature, whereas the signer is responsible for the accuracy of data. The integrity level T3 requires ensuring the evidential value of data (including documents sent to the NHIS by MSPs). Among other things, the independent evidential value for all other interested parties must be guaranteed. A most secure way to achieve it is to use a digital signature, as laid down in the security measure HT.34 of the present ISKE. If it is not possible to employ a digital signature, the three-level IT baseline security system requires using alternatives (security measures), which must ensure functionally equal integrity. Government Regulation No. 273 of 12 August 2004 [58] makes ISKE compulsory for state and local government organizations dealing with databases/registers.

However, the requirement of ISKE is not clearly worded and thus there are different possible interpretations as to who must sign a document and why. From the register we can see that this requirement can be met in at least two ways: (1) the data are signed by their source when the data are entered into the register and (2) the data are signed by the keeper of the register when the data are entered into the register.

The former way is more suitable for the register keepers because it lowers their responsibility. When the other way is used, the register keeper must take additional measures in order to prove why a certain entry was made. Still, besides fulfilling the ISKE requirement, the register keeper's signature has another function – it shows that the data were not altered between their entry into the register and sending out from the register.

The ISKE requirements can be satisfied in either way, yet, the outcome is different. The NHIS is currently using the former way – all data entered into the register by an MSP are provided with a

digital signature or an e-seal. By fulfilling the ISKE requirement, also the actual security problem is solved. The application of the second way does not contribute to the solution of the security problem (proving the source of data) but is used solely for satisfying the ISKE requirement.

In principle a similar scheme exists between MSPs. However, differences occur between big and small MSPs, and dentists.

3.5 Information Exchange in the Estonian E-health Infrastructure

Processing patient personal data in the MSP: When the patient arrives at the MSP, the registrar collects different personal data: the patient's name, address, phone number, e-mail address, relationships and submits these data to the MSP database. Personal data are very valuable for the patient and also for the MSP and constitute a very important business asset. The personal information about the patient is contained in the data object called *registered patient personal information* business asset which is supported by two system assets: *the input interface used by the registrar to submit the data* and *the database, where the registered patient data are stored*. Here we have an additional system asset, the MSP computer network that we can call the transmission medium through which the registrar can submit registered patient information from the input interface to the MSP database. The security criterion of this business asset is the confidentiality of patient registered data. Table 2 provides an overview including the registration of patient data by the MSP registrar and the business asset – registered patient personal information, also the process of patient registration in the MSP. The security criterion is the confidentiality of patient personal information, for example, the address is important only for persons who need to know it.

Table 2: Registered patient personal information asset identification.

Business asset 1	**Registered patient personal information**
IS assets	**Patient registration process;** **Patient management;** **Patient;** **MSP network;** **Registrar**
Process description: how do IS assets support business asset(s)	Patient registration process: • Patient goes to the registrar • Patient provides an identification document • Patient provides personal data • Patient pays for the visit
Security criterion	Confidentiality of patient registration data

Processing patient health information: This data object is generated during the patient's visit to the GP. The respective document contains data about the patient, all personal information and also information about the clinical data that were found during the visit. The creation of patient health information represents the IS asset which supports the business assets *patient health information* and *clinical data* about the registered patient. A malevolent attacker, however, may be able to manipulate the patient medical data and thus change patient clinical information.

The process described in Table 3 shows how the patient goes to the GP and how the patient health information is generated. It starts with clinical observation of the patient and finishes with compiling the patient health information and transferring it to the NHIS. The most important aspect related

to this process is guaranteeing the integrity and confidentiality of the patient health information provided by the GP.

Table 3: General practitioner compiling patient health information.

Business asset 2	**Patient health information**
IS assets	**Creation of patient health information;** **Sending patient health information;** **Infrastructure**
Process description: how do IS assets support business asset(s)	Creation of the EHR by the GP: • Patient comes to the GP office • GP makes observations • GP starts compiling patient health information • GP finishes patient health information
Security criteria	Confidentiality of patient health information; Integrity of patient health information

Sending the EHR created by the GP without a digital signature to the NHIS: After the patient has visited the GP and the GP has created the EHR information, the following assets lie in the exchange of data between the MSP and NHIS. Table 4 shows how the EHR is created by the GP and transferred to the NHIS. The main security criterion in this process is the integrity of the EHR. If the EHR is not digitally signed when composed, it is possible to change data during the transport process.

Table 4: EHR transfer to the NHIS asset identification.

Business asset 3	**EHR information**
IS assets	**Sending the EHR to the NHIS;** **Digital signature;** **Infrastructure**
Process description: how do IS assets support business asset(s)	Sending the EHR to the NHIS by the GP: • GP creates the EHR • GP sends the EHR to the NHIS • NHIS receives the EHR • NHIS makes validity controls • NHIS saves the EHR to the database
Security criteria	Confidentiality of the EHR; Integrity of the EHR

Processing the EHR signed with an e-seal of the MSP: Medical service providers use their own ISs into which doctors insert the data contained in EHRs provided by them. Before the EHR information is sent to the NHIS, these are digitally signed in the IS of the MSP using the MSP's e-seal. Next the data are sent from one MSP to another, via the X-Road infrastructure. The X-Road infrastructure signs all the outgoing messages and the X-Road infrastructure of the HWISC archives the incoming messages into the cryptographically protected log (see Table 5).

The use of the e-seal is justified due to the necessity of meeting the requirements set by ISKE. The NHIS has been assigned the highest integrity level. In that case ISKE requires that the data be pro-

vided with a digital signature or an e-seal ensuring their evidential value. The data are transferred between two MSPs over the X-Road infrastructure. One MSP sends a query over X-Road and the other MSP receives this query over the X-Road infrastructure. In between, the query passes through three security servers. A digital trace about this process should be left in each server and the metadata of the query are additionally saved in the central server of the Information System Authority.

Table 5: Transfer of an EHR from the MSP to the NHIS.

Business asset 4	**EHR information**
IS asset	**MSP infrastructure**
Process description: how do IS assets support business asset(s)	Sending the EHR to the NHIS by the MSP: • MSP creates the EHR • IS of the MSP adds an e-seal • MSP sends the EHR to the NHIS through the X-Road infrastructure • NHIS receives the EHR • NHIS makes validity controls • NHIS saves the EHR to the database
Security criteria	Confidentiality of the EHR; Integrity of the EHR

3.6 Requirements on Ensuring the Integrity of EHRs

Data integrity is the assurance that the data involved are accurate, consistent and up-to-date. It must be ensured that the data are authentic and not affected by unauthorized changes. According to ISKE, security level T3 of integrity requires that the information source, its change and destruction must have evidential value; it is necessary to check that the data are correct, complete and up-to-date in real time. The requirements of ISKE applying also to the NHIS, and which are audited, state that the digital signatures and/or digital seal, meeting the requirements established in the Digital Signatures Act of Estonia [51] can be applied to separate data, whole databases, etc. However, it is up to the NHIS to decide which evidential value its data must have and on this basis to judge either to use the person's digital signature or an e-seal. It is forbidden to use the digital signature with the data and documents of evidential value (security level T3) which do not comply with (in particular concerning the infrastructure) the requirements established in the Digital Signatures Act of Estonia. Technical data and metadata can be left without a digital signature or an e-seal.

3.7 Problems and Risks Related to EHRs Signed with an e-Seal

If the GP does not add a digital signature to an EHR, which would prove the authenticity of data, the e-seal is attached to it in the system of the NHIS. Thus the requirements of ISKE are formally fulfilled. In addition, this enables sending out digitally signed data to the GP. An e-seal is an alternative to X-Road, making it possible to verify that the data sent out by the NHIS correspond to the data that were once saved in the NHIS database. The application of the e-seal by the NHIS requires also changing the contracts made between the service providers.

3.8 Summary

This chapter gave an overview of assets and security threats in organizations who are changing information in the Estonian e-health infrastructure. In the analysis main attention was paid to identifying assets in the Estonian e-health infrastructure. The following aspects were considered:

1. Which organizations take part in the Estonian e-health infrastructure and what is the responsibility of different parties? – I defined seven parties: patients, GP, doctor, MSP, NHIS, medical software developer and Ministry of Social Affairs. **2. What kind of ISs are involved?** – There are ISs used by the MSP and developed by different companies, X-Road infrastructure, portals managed by the HWISC and the NHIS database managed by the HWISC. **3. How is an EHR transferred in the Estonian e-health infrastructure?** – The EHRs created by doctors using the MSP's IS are sent over the X-Road infrastructure to the NHIS database, where all needed validation and controls are done.

4 Risk Analysis of Assets in the Estonian E-health Infrastructure

This chapter deals with SRQ2 – How to assess risks of assets in the Estonian e-health infrastructure? The analysis provides answers to the following questions:

- What are the threat agents in the Estonian e-health infrastructure?
- What kind of vulnerabilities are affecting organizations in the Estonian e-health infrastructure?
- What kind of attack methods can be used against organizations participating in the Estonian e-health infrastructure?
- What are risk impacts for the organizations involved?

Below, the ISSRM Domain Model is applied to the analysis of security risks identified in issuing EHRs by GPs and MSPs and sending them to the NHIS, and to the management of patient personal data in the MSP local network. An answer to the question about ensuring EHR integrity is obtained. The security modelling languages are assessed by using the three concepts of the ISRM domain model [41]: assets-related, risk-related and risk treatment-related concepts.

Among other aspects, the information dealt with gives an insight into the interested parties, possible threat agents, attack vectors, motivation of the attackers, etc. I try to find out how the threat agent is able to carry out the attack method. Further I identify vulnerabilities and the impact of the attack. Using this information it is possible to describe the ways how the interested parties can attack the Estonian e-health infrastructure.

4.1 Analysis of the Risk to the *Registered Patient Personal Information* Asset

One possible way (including threat agents, the attack method, risk components) of attacking and misusing registered patient personal information is described in Table 6.

Table 6: Registered patient personal information – risk and threat analysis.

	Risk 1
Threat agent	Hacker Motivation: needs patient personal information Resources: access to the network Expertise: knows how to find information
Attack method	Attacker gets access to the IS of the MSP Attacker changes patient personal information
Vulnerability	Weakness in the MSP network
Impact	Loss of trust in the MSP. Loss of confidentiality of patient information. Patient information is stolen
Risk 1	Hacker uses information to pretend to be anybody else, or to sell private information to interested persons. Loss of network security

4.2 Analysis of the Risk to the *Patient Health Information* Asset

One possible way of attacking the patient health information business asset, where an MSP worker is the threat agent, is presented in Table 7. The attack method and related risk components of EHR information assets are described.

Table 7: Patient health information – risk and threat analysis.

	Risk 2
Threat agent	MSP worker Motivation: to get access to patient health information and to change it Resources: access to the GP's personal computer Expertise: knowledge about the GP's work process is built up
Attack method	Changing patient health information Sending changed patient health information to the NHIS
Vulnerability	Weakness in the MSP's IS
Impact	Loss of the integrity of patient health information. Negation of the integrity of the EHR Loss of trust in the MSP
Risk 2	MSP worker changes patient health information, and thus the diagnosis, causing risk to person's life

4.3 Analysis of the Risk to the *EHR Information* Asset Created by the GP

In this chapter the risks affecting the EHR information during its transfer from the GP to the NHIS are described (Table 8). There is one threat agent, the hacker.

Table 8: EHR created by the GP – risk and threat analysis.

	Risk 3
Threat agent	Hacker Motivation: changing the EHR information during the transfer Resources: access to the network Expertise: network hacking
Attack method	Hacker gets access to the network
Vulnerability	Weakness in the MSP's health IS
Impact	Hacker gets access to the patient EHR and can change the diagnosis
Risk 3	Hacker changes the diagnosis, which causes loss of integrity of the EHR and poses risk to person's life through wrong treatment

We can see from Table 8 that the goal of the hacker is to compromise and change the EHR in the site where the person's health record is stored. Through the network attack and expert knowledge in this area it is easy for the hacker to make changes in the EHR because the integrity of the EHR is not ensured when it is created.

This attack is possible because the GP does not add the digital signature to the EHR. The e-seal will only be added to the EHR in the NHIS, and thus the NHIS stores the changed EHR with wrong health data, bearing the e-seal of the NHIS. The next party asking for this information does not suspect that this document was changed during its transfer from the GP to the NHIS database.

4.4 Analysis of the Risk to the *EHR Information* Asset Created by the MSP

In this chapter the risks affecting the EHR information during its transfer from the MSP to the NHIS are described (Table 9). There is one threat agent, the hacker.

Table 9: EHR created by the MSP – risk and threat analysis.

	Risk 4
Threat agent	Hacker Motivation: changing the EHR information in the MSP infrastructure Resources: access to the MSP infrastructure Expertise: knowledge of hacking computers
Attack method	Hacker gets access to the MSP computers Hacker changes the EHR EHR is changed before the MSP provides the e-seal
Vulnerability	Weakness in the transfer media
Impact	Hacker gets access to the patient EHR and can change the diagnosis
Risk 4	Hacker changes the diagnosis, causing loss of the integrity of the EHR and posing risk to person's life through wrong treatment

Table 9 shows that the goal of the hacker is to compromise and change the EHR in the site where the person's health record is stored. Using the network attack and expert knowledge in this area, the hacker can easily make changes in the EHR because the integrity of the EHR is not ensured when it is compiled.

This attack is possible because the MSP does not put a digital signature on the EHR during creating the EHR. The e-seal will be added to the EHR only when the MSP sends the EHR to the NHIS, and thus the NHIS stores the altered EHR with wrong health data, bearing the e-seal of the MSP. The next party asking for this EHR does not suspect that this EHR was changed after compiling it in the MSP infrastructure.

4.5 Summary

This chapter provided answers to the following questions. **1. What are the threat agents in the Estonian e-health infrastructure?** – Two possible threat agents are (a) a hacker and (b) another MSP worker. **2. What kind of vulnerabilities are affecting organizations in the Estonian e-health infrastructure?** – Four major vulnerabilities were defined: (a) weakness in the MSP network, (b) weakness in the MSP's IS, (c) weakness in the MSP's health IS, (d) weakness in the transfer media. **3. What kind of attack methods can be used against organizations participating in the Estonian e-health infrastructure?** – The following attack methods are possible: (a) a hacker gets access to the network through the man-in-the-middle attack, (b) an MSP worker changes patient medical information or sends changed patient medical information to the NHIS, (c) a hacker gets access

to the network through weakness in the MSP's health IS, (d) a hacker gets access to the MSP computers and changes the EHR or the EHR is changed before the MSP adds the e-seal. **4. What are risk impacts for the organizations involved?** – The risk impacts include (a) loss of the confidentiality of patient information or theft of patient information, (b) loss of the integrity of patient medical information and negation of the integrity of the EHR, (c) changing the patient EHR and the diagnosis by the hacker, (d) loss of trust in the MSP.

5 Security Risk Mitigation, Risk Assessment and Control Selection

This chapter deals with security controls and evaluation of risks in the Estonian e-health infrastructure. The analysis provides an answer to SRQ3 of the thesis – How to mitigate risks in the Estonian e-health infrastructure?

Some resources are shared in the Estonian e-health infrastructure but the organizations involved do not have the same security requirements. For that reason, for example the NHIS must follow very high security standards in order to ensure the integrity of EHRs. General practitioners, however, do not need to meet the same security requirements, which may breach the security and reliability of documents issued by them. Below, the following problems related to security requirements set on the Estonian e-health system and the security controls that can be implemented to satisfy these requirements are discussed:

- What are the security requirements for the Estonian e-health system?
- What kind of security controls can be implemented to fulfil the security requirements?
- What security controls should be applied in order to fulfil the security requirements for integrity, availability and confidentiality set on the HNIS by the law?

5.1 Security Risk Mitigation

The risks identified in Chapter 4 can be managed and mitigated by applying security requirements and controls. An overview of security controls and requirements enabling the reduction of risks to an acceptable level is given in Table 10.

Table 10: Security requirements and controls.

Risk	Security requirement	Control description
Risk 1	Monitoring and logging the activity in the MSP network and personal computers	Using secured connections and encryption of the database for patient registration. Auditing database queries logs
Risk 2	Monitoring and logging the activity of MSP workers	Using stronger passwords or smart cards for authentication
Risk 3	Ensuring the integrity of the EHR when the GP creates it	Using the digital signature, digital seal or KSI time stamp when creating the EHR
Risk 4	Ensuring the integrity of the EHR when the MSP creates it	Verifying the received EHR with the previous original received (with Blockchain cryptographic digest)

As seen from Table 10, the following security requirements are needed to reduce risks:

Risk 1 – monitoring and logging the activity in the MSP network and personal computers. In order to satisfy this security requirement, we must apply control. This security control needs additional technical staff and servers for logging and analysis of logs. Risk treatment cost to ensure this control is 3.

Risk 2 – monitoring the activity of MSP workers. For this purpose a stronger password and authentication with a smart card are applied. Risk treatment cost to ensure this control is 4.

Risk 3 – ensuring the integrity of the EHR when the GP compiles it. To achieve this, a digital signature, an e-seal or Keyless Signature Infrastructure (KSI) time stamp must be used on creating the EHR. Risk treatment cost to ensure this control is 5.

Risk 4 – ensuring the integrity of the EHR when the MSP compiles it. To this end, the received EHR must be verified with the previous original received. Risk treatment cost to ensure this control is 5.

To mitigate security risks, we must take various countermeasures depending on the character of risk. For Risk 1 we must use a security network and up-to-date network equipment. All equipment must be configured by employing strong passwords and keys, which makes it difficult for hackers to log in. Strong passwords and keys are necessary on network devices, personal computers and software. The software of the MSP IS must be tested against security requirements before implementing it and all vulnerabilities must be repaired before using it in the production. In the case of Risk 2 the MSP infrastructure must use a personal computer with the latest security patches installed, and employ a complex password or card for authentication. Mitigation of Risk 3 involves using security network protocols and up-to-date network equipment with all security patches installed. All equipment must be configured using strong passwords and keys, so that hackers cannot log in easily. The digital signature of the GP attached to the EHR is also a very good countermeasure preventing this document from malevolent modification. For Risk 4 it is necessary to use security network protocols, install all security patches, and employ a complex password or card for authentication. Here as well the digital signature of the GP is a very good countermeasure against changing the EHR.

5.2 Security Risk Assessment

I conducted interviews with experts in the area of e-health infrastructure security. The following risk components were estimated: business asset value, threat likelihood, vulnerability level and security objectives, in the range from 0 to 5. The minimum risk obtainable is 0, and the maximum risk obtainable is 45. It means that 0 and 45 represent the boundaries of the risks. The following formulas were used for calculations [59]:

Risk event = threat likelihood + vulnerability level – 1

Impact = maximum value of the security criterion

Risk level = risk event x impact level

Maximum risk = (5 + 5 – 1) x 5 = 45

Minimum risk = (0 + 0 – 1) x 0 = 0

Risk reduction level = Risk level 1 – Risk level 2

The collected data are presented in Table 11. The table provides information about the risk levels before and after applying security controls.

It is difficult to mitigate all security risks, because this needs substantial resources and finances. By applying the security control selection, we can find out which risks must be mitigated first.

Table 11: Risk metrics before and after risk treatment.

	Before risk treatment					After risk treatment				Risk reduction level	Business asset value	Cost of countermeasure
	Vulnerability level	Threat likelihood	Event potentiality	Impact level	Risk level 1	Vulnerability level	Threat likelihood	Event potentiality	Risk level 2			
Risk 1	3	2	4	3	12	2	1	3	9	3	2	3
Risk 2	3	4	6	3	18	1	3	4	12	6	3	2
Risk 3	4	2	5	4	20	1	1	2	8	12	4	4
Risk 4	5	2	6	4	24	1	1	2	8	16	5	5

5.3 Security Control Selection

It is very difficult to mitigate all security risks due to the lack of resources, time, etc. In order to choose security controls, we must have an excellent knowledge of the IS, it means we must know what security controls should be selected in first order. To do this trade-off analysis, we used the value of the business asset, countermeasure cost and the risk reduction level (RRL) – the information available in the three last columns of Table 11. On the basis of this information three graphs were prepared, including data on the RRL and business asset value, the RRL and countermeasure cost, and the countermeasure cost and business asset value. Figure 8 represents a graph about the RRL against business asset value. The desired situation is a high-value asset with a high risk reduction value. Such risks are observed in the quadrant with Risk 3 (R3) and Risk 4 (R4), representing high priority.

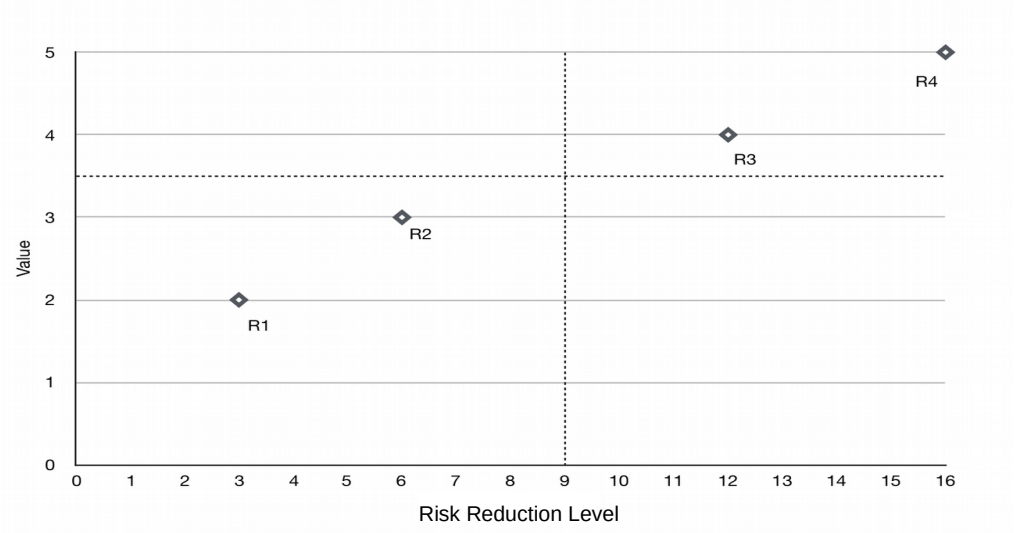

Figure 8: Risk reduction level against business asset value.

The medium-priority quadrants have a low business asset value and low RRL, determined for Risk 1 (R1) and Risk 2 (R2). Figure 9 shows a graph of the RRL against the cost of countermeasures. An ideal situation is characterized by a low cost value with a high risk reduction value. Risk 3 (R3) in the figure represents medium priority. The medium-priority quadrants have a high cost value with a high RRL and a low cost with low risk reduction values. This situation is seen in quadrants that comprise Risk 4 (R4) and Risk 3 (R3), and Risk 1 (R1) and Risk 2 (R2), respectively.

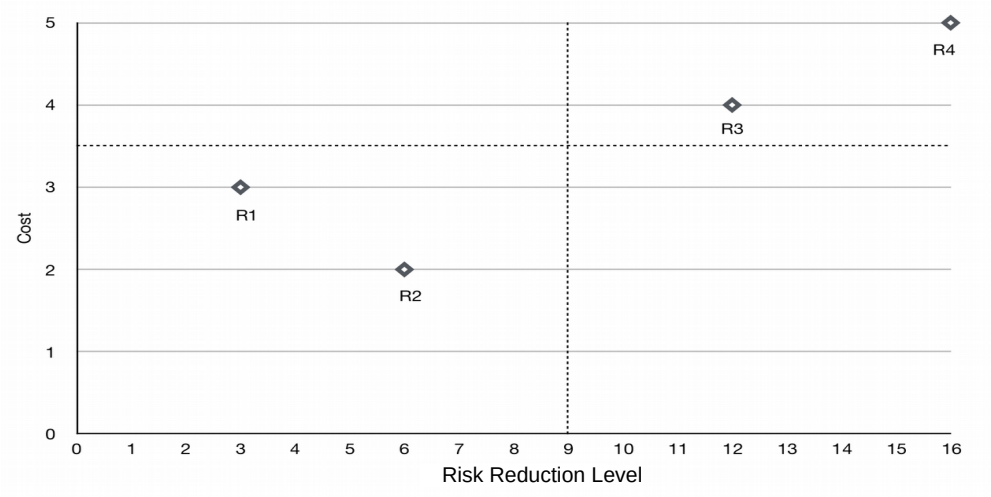

Figure 9: Risk reduction level against the cost of the countermeasure.

Figure 10 depicts the cost of the countermeasure against business asset value. Medium priority is observed in the quadrants combining high-value assets with a high cost of the countermeasure and low-value assets with a low cost of the countermeasure (respectively in the quadrant comprising Risk 3 (R3) and Risk 4 (R4), and in the quadrant with Risk 1 (R1) and Risk 2 (R2)). The ideal situation is a low-value asset with a high cost of risk treatment (in the quadrant with Risk 3 (R3) and Risk 4 (R4)).

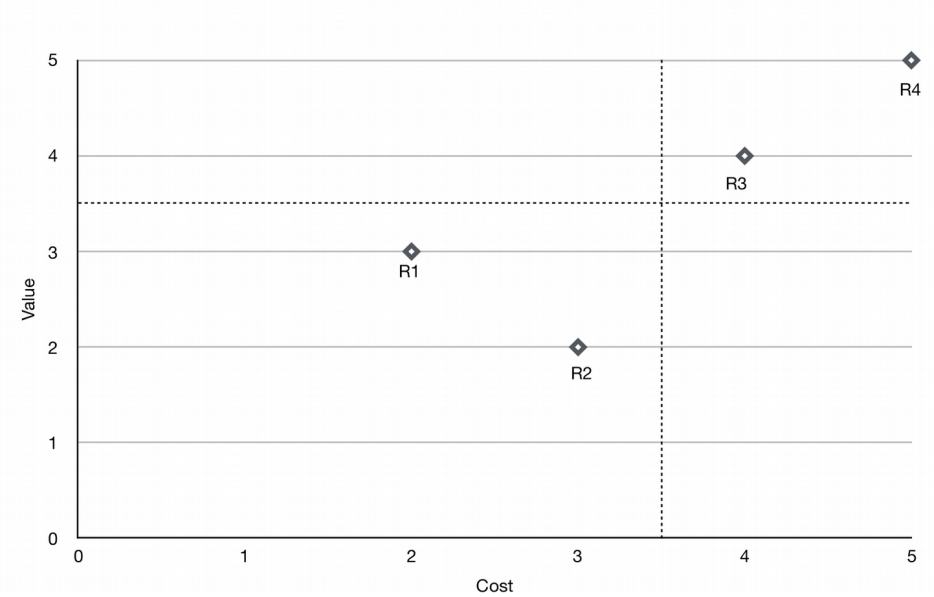

Figure 10: Cost of the countermeasure against the business asset value.

Table 12 presents the risk priorities derived from the graphs in Figures 8–10. Value 1 is assigned to low-priority risks, value 2 to medium-priority risks and value 3 to high-priority risks. Adding these values across the three graphs, a priority can be estimated that depends on the value of the business asset, cost of countermeasures and RRL. Risks R3 and R4 are high-priority risks and R1 and R2 are medium-priority risks.

Table 12: Risk versus priority.

	Value–RRL	RRL–cost	Value–cost		
	Graph 1	Graph 2	Graph 3		
Risk 1	1	2	2	5	Medium priority
Risk 2	2	1	1	4	Medium priority
Risk 3	3	3	3	9	High priority
Risk 4	3	3	3	9	High priority

5.4 Summary

The discussion presented in this chapter focuses on mitigating risks in the Estonian e-health environment. The risk reductions that could be achieved were considered through the estimated calculations and introducing security controls. The risk levels were calculated before and after the security controls were applied. The following problems were considered:

1. What are the security requirements for the Estonian e-health infrastructure? – It was found that with R1 and R2 the security requirement was to monitor and log the activity in the MSP network and personal computers. In the case of R3 and R4 the integrity of the EHR should be ensured when it is compiled by the GP. **2. What kind of security controls can be implemented to fulfil the security requirements?** – Security control in the case of R1 is to use secured connections and encryption of the database for patient registration auditing database queries logs. For R2, stronger passwords or smart cards should be used for authentication. In the case of R3 the digital signature, e-seal or KSI time stamp should be used on creating the EHR. In the case of R4 the received EHR should be verified with the previous original received, for example, by using Blockchain cryptographic digest. **3. What security controls should be applied in order to fulfil the security requirements for integrity, availability and confidentiality set on the NHIS by the law?** – It is necessary to use secured connections and encryption of the database for patient registration auditing database queries logs. The MSP workers should have stronger passwords or use smart cards for authentication, and use the digital signature, e-seal or KSI time stamp when compiling the EHR. The received EHR should also be verified with the original received. For this purpose, for example, Blockchain cryptographic digest can be used.

6 Survey and Validation

In this thesis I described the present situation of the Estonian e-health infrastructure, defined the parties who are playing an important role in that infrastructure, analysed the usage of the digital signature with EHRs and considered the role of ISKE and information exchange. Next I discussed four business assets: registered patient personal information, patient health information, EHR information created by the GP and EHR information created by the MSP. Then I made risk analysis of assets using the ISSRM Domain Model, where I brought out threat agents, attack methods, vulnerabilities and impact, and also discussed risk mitigation, risk assessment and security control selection.

In the last step I made a survey to validate the correctness of my findings. The process and results of the survey are presented below.

6.1 Problem Statement

Proceeding from my research questions, I defined risk and conducted a survey in order to assess the likelihood of the risks. The results of the survey are used to validate the correctness of my findings and to show how big is the deviation between my results and expert opinions.

6.2 Development and Testing of the Questionnaire

When participants in interviews were defined and the design of the questionnaire was completed, the planning and setup of interviews were finished. A personal invitation was sent to each interviewee. The schedule of the interviews depended on the availability of time. The interviews were conducted in office meeting rooms without disruption.

The target audience for the survey was selected from the specialists working with the Estonian e-health infrastructure. Out of the large number tools available for making the survey, I chose Surveymonkey that fitted best with my thesis. In my research the correctness of the survey is much more important than statistical analysis, because due to the small number of experts in that area, it is impossible to get statistical data for analysis.

Three versions of the questionnaire were tested over the time frame from December 2017 until March 2018. The final version was developed based on the interviews that were documented.

Several interviews were conducted in December 2017 with the representatives from the Estonian e-health infrastructure. The Chief Security officer at the HWISC, Mr. Urmo Laaneots gave a valuable feedback on my questionnaire.

6.3 Results and Observations from Interviews

Hereby I discuss the results obtained from the interviews and the process of analysing these results. All information collected from the interviews was documented in the best way possible. The interviews were conducted face to face. I made audio recordings and transcripts of all verbal communication and data obtained from notes. The whole set of information was compiled soon after the interview was finished, to ensure that all feelings and information were fresh and emotions were not forgotten.

The correctness of answers is the most important part of interviews. In order to achieve it, the following issues should be taken into account.

- **Questionnaire problems:** The proper design of the questionnaire requires a large amount of background work. We can try to mitigate this problem but it is impossible to eliminate it. The questions must be worded with utmost care so that all persons would understand them in the same way.
- **Questionnaire length:** The questionnaire must be short and very clear. There must be a balance between time and the number of questions.
- **Question-order effect:** Randomizing questions are not working in software engineering; instead, logical adherence must be used. The questions must be asked in logical order, which helps categorizing the data.
- **Time limitation:** This problem is common with e-mail-based questionnaires when we are unable to get an answer in the right time cycle.
- **Domain knowledge:** I tried to resolve this problem by choosing experienced persons to answer the questionnaire, involving experts in the study area.

6.4 Presentation of Main Results

The main audience of my study consists of experts in e-health cyber security. The five persons who participated in the interviews are highly educated and also experienced in that area. Figure 11 shows that two interviewees have been engaged in e-health cyber security for more than 7 years, two up to 3 years and one participant has been working in that field for 5–7 years.

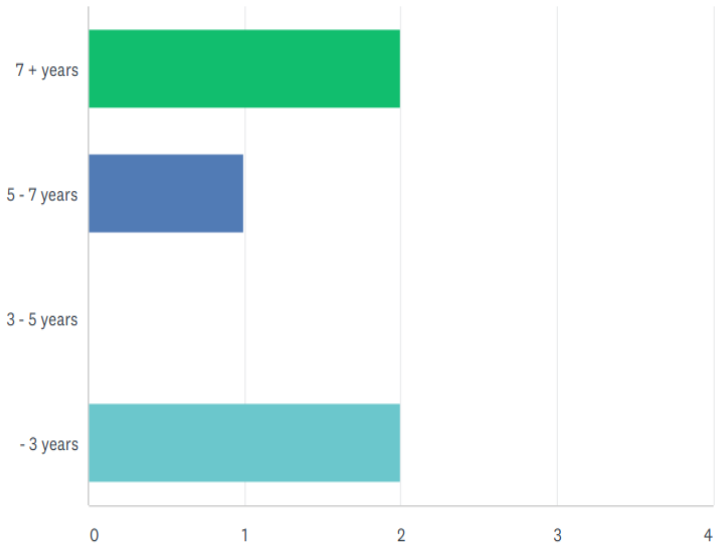

Figure 11: Working experience.

The educational level of the participants in the interviews varied as well: one has a master's degree, three have a bachelor's degree and one has no academic degree (Figure 12). All of them have been working in this industry for a long time and are thus highly experienced.

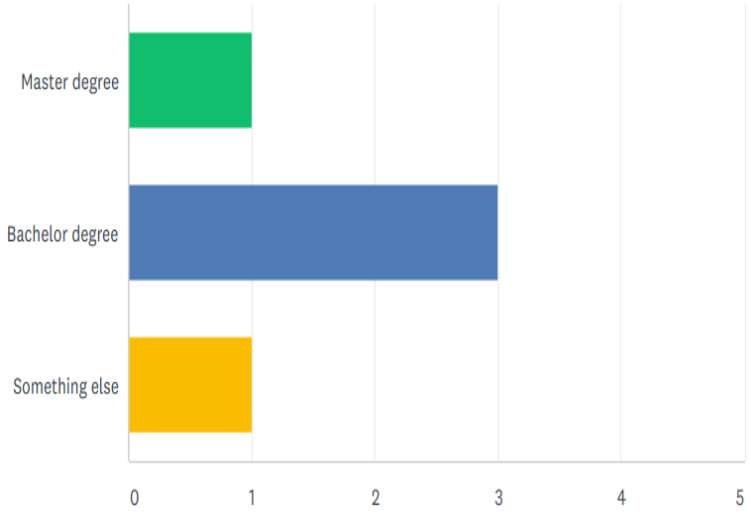

Figure 12: Educational level.

6.5 Ensuring the Integrity of EHRs

The main question of my thesis is how to ensure the integrity of EHRs in the Estonian e-health infrastructure. Is it enough that the HWISC adds an e-seal to every EHR issued by GPs, without checking the data in the EHR? To resolve this problem, I conducted a survey and asked experts to answer the following five questions.

The **first question** is related to business asset 1:

- How likely will the confidentiality of registered patient information be compromised by the hacker in the IS of the MSP?

The process behind this question includes the registration of patient data by the MSP registrar and the business asset – registered patient personal information, also patient registration in the MSP. The opinions of the experts varied: one expert considered it very likely that somebody could change the EHR in the MSP's IS, one expert considered it potentially likely and three experts said it was potentially not likely (Figure 13).

The **second question** is related to business asset 2:

- How likely will the EHR be compromised inside the IS of the MSP by another MSP worker?

The process involved starts with clinical observation of the patient and finishes with creating the EHR information by the GP and transferring it to the NHIS. As I stated earlier, EHR integrity is not ensured when the document is left digitally unsigned by the GP. This triggered my second question.

One of the experts answered that such a possibility was potentially likely and four experts considered such a possibility potentially not likely (Figure 14). A hacker able to perform this kind of attack must have very high know-how and excellent technical equipment.

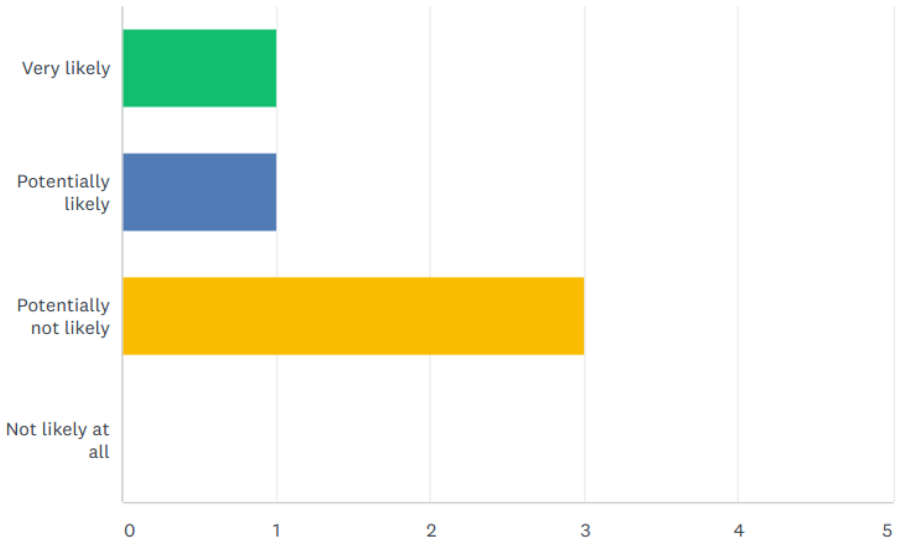

Figure 13: The likelihood that the integrity of the EHR will be compromised by the hacker in the MSP's IS.

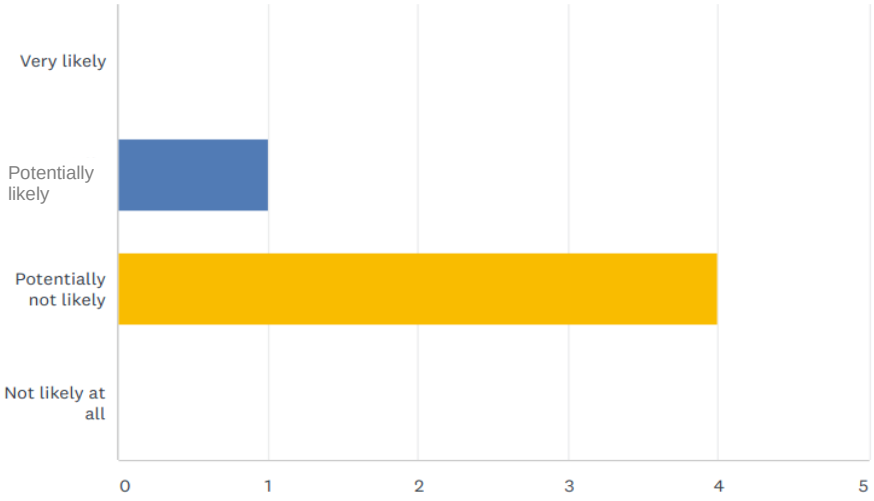

Figure 14: The likelihood that the integrity of the EHR will be compromised inside the MSP's IS.

The **third question** is related to business asset 3:

- How likely will the EHR become compromised during the transfer from the MSP infrastructure to the HWISC infrastructure?

After the patient has visited the GP and the GP has compiled the EHR, the following assets lie in the exchange of data between the MSP and NHIS. Three experts considered the possibility that the EHR becomes compromised during its transfer potentially likely and two experts considered it potentially not likely (Figure 15).

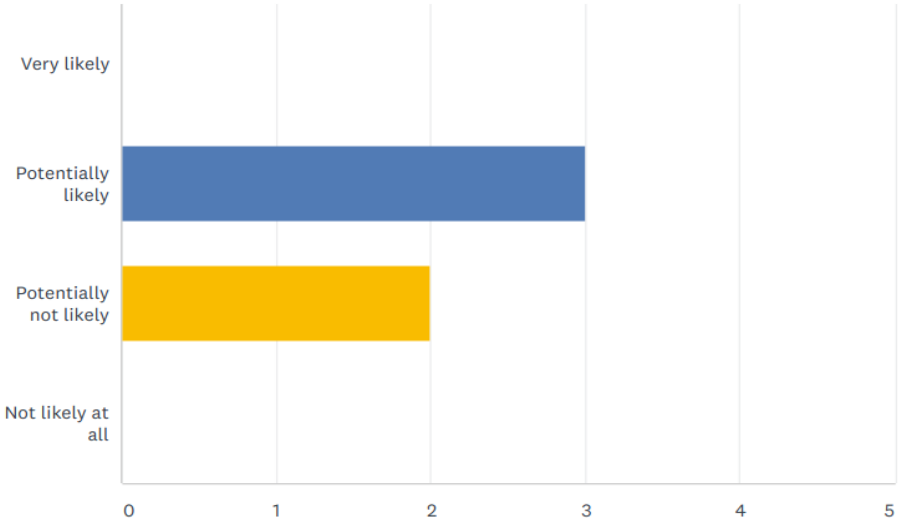

Figure 15: The likelihood of the EHR becoming compromised during the transfer from the MSP infrastructure to the HWISC infrastructure.

The **fourth question** is related to business asset 4:

- How likely will the EHR become compromised before it is digitally signed in the MSP infrastructure prior to transfer to the HWISC infrastructure?

Medical service providers use their own ISs into which doctors insert the data contained in EHRs provided by them. Before the EHRs are sent to the NHIS, they are digitally signed in the MSP's IS using the MSP's e-seal. According to one expert the possibility that the EHR becomes compromised is very likely, three experts considered it potentially likely and one expert answered that it was potentially not likely (Figure 16).

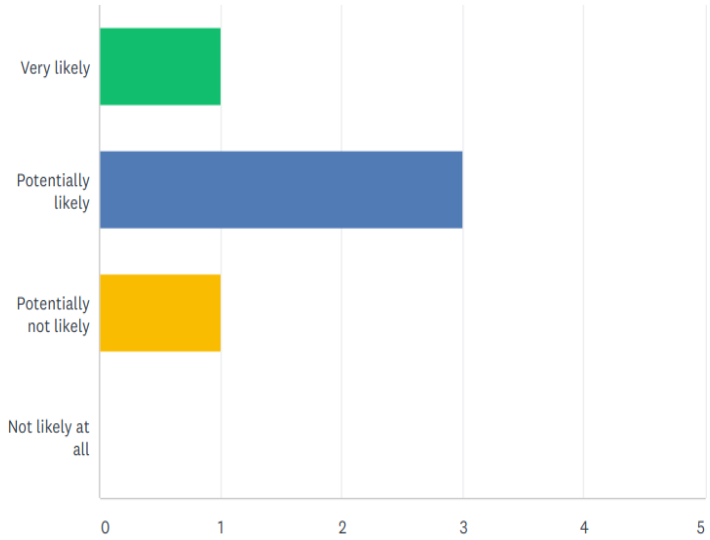

Figure 16: The likelihood that the EHR becomes compromised before it is digitally signed in the MSP infrastructure prior to transfer to the HWISC infrastructure.

The aim of the **fifth question** was to find out which is the best means of ensuring the integrity of EHRs – the personal digital signature of the GP or the organization's e-seal of the HWISC.

- Where should the digital signature be put on the EHR?

In my opinion the digital signature must be added to an EHR as close to its source as possible. I got three almost similar results: two experts answered that the GP must add the digital signature to the EHR, one expert said that the MSP could put the organization's e-seal on the EHR and two experts answered that the timestamp added by the IS of the GP was good as well (Figure 17).

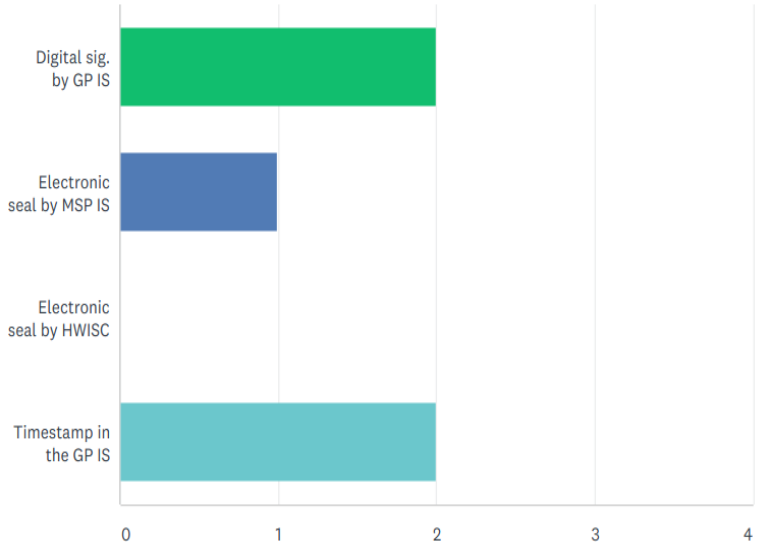

Figure 17: Places of adding the digital signature to the EHR.

6.6 Threats to Validity

When validating the accuracy of the results, I used my best knowledge and technologies. Validation by some other approach or by using different technologies, however, may give a different outcome. My conclusions were mainly based on the survey performed by me and potentially I could miss some concepts from the comparison of the answers. The Estonian e-health infrastructure must guarantee the integrity and confidentiality of EHRs, by taking many security requirements into account. A major problem is that persons who are responsible for the security are changing very often.

6.7 Summary

In this chapter I found answers to the five questions contained in my questionnaire. The interviewees are highly experienced in e-health industry, whereas the majority of them have also good educational background.

The **first question** was: How likely will the confidentiality of registered patient information be compromised by the hacker in the IS of the MSP? One expert answered that very likely the EHR could be modified, one expert considered this possibility potentially likely and three experts said it was potentially not likely.

The **second question** was: How likely will the EHR be compromised inside the IS of the MSP by another MSP worker? One of the experts considered such a possibility potentially likely and four experts thought it was potentially not likely. In order to make such attack, the hacker must have very high know-how and excellent technical equipment.

The **third question** was: How likely will the EHR become compromised during the transfer from the MSP infrastructure to the HWISC infrastructure? Three experts considered it potentially likely and two experts thought it was potentially not likely.

The **fourth question** was: How likely will the EHR become compromised before it is digitally signed in the MSP infrastructure prior to transfer to the HWISC infrastructure? One expert considered such a possibility very likely, three experts potentially likely and one expert potentially not likely.

The **fifth question** was: Where should the digital signature be put on the EHR? In my opinion it should be done as close to the source of the EHR as possible. The answers of the experts were quite similar: two experts answered that the GP must digitally sign the EHR, one expert thinks that the MSP can put the organization's e-seal on the EHR and two experts think that the timestamp added by the IS of the GP can also be used.

7 Concluding Remarks

In this master's thesis the security issues affecting the Estonian e-health infrastructure are analysed. The Estonian e-health infrastructure is a very good example about different organizations trying to collaborate and keep the integrity and confidentiality of patient medical data on a high level. The analysis performed in this study shows that adding an e-seal to EHRs by the NHIS poses great security risks. Due to the adoption of such a decision, the EHR integrity is not ensured on the highest level and the data in thousands of EHRs are of very low credibility.

During the compilation of this thesis I studied alternative ways of digitally signing medical documents. The main conclusion is that everywhere documents are provided by an e-signature, e-seal or timestamp close to the GP who has created the respective medical document. Such an approach enables avoiding any external modifications to the documents containing confidential data of people. However, different approaches could be noticed as to who owns the medical data – the patient, the doctor or the state. Different views were also found concerning the measures, and their costs, that should be taken to ensure the initial integrity of an EHR and avoid compromising it during transfer from one institution to another. The essential issue to be resolved by implementing security measures is to avoid making false decisions about patient's treatment resulting from the modification of information during the exchange of health data from one MSP to another through the NHIS.

The analysis is based on processes in the Estonian e-health infrastructure. The business and information system assets involved in these processes were identified, including registered patient personal information, GP compiling patient health information, EHR information transfer to the NHIS and transfer of EHR information from the MSP to the NHIS.

The final chapter of the thesis provides a summary of this research. It presents limitations of the research, answers to the research questions and a discussion about future work.

7.1 Limitations

Electronic health records have been used for quite a long time, but it is difficult to find papers dealing with EHRs and security. Papers originating from the 1990s are available, but they are out of date today because technology is changing rapidly. For that reason I used lots of material from the Internet and white papers. The survey validation is based on the literature and technologies used in this thesis. Another validation approach, however, may give different results.

The **external validity** of the present research lies in its applicability in everyday e-health practice. The outcomes of the thesis are valid for the Estonian e-health infrastructure, but with respective changes according to the local context are usable also in other countries.

The **reliability** of materials used in the thesis adds to its quality. My thesis is validated by literary sources, previous studies in the same field and interviews with the experts. Some limitations arose from surveys because it appeared impossible to get answers from all participants and find literature coverage.

7.2 Answers to Research Questions

The main research question of this thesis was: How to guarantee the integrity of the EHR business process? In order to find an answer to this question, three sub-research questions concentrating on different aspects of the current situation in the Estonian e-health infrastructure were analysed.

First, the assets present in the Estonian e-health infrastructure were brought out. The business assets comprise registered patient personal information, patient health information and EHR information, which are suppplemented by different IS assets (e.g. patient, MSP network, infrastrusture, digital signature, sending patient health information). Seven organizations having different responsibilities were determined in the Estonian e-health infrastructure: patients, GP, doctor, MSP, MHIS, medical software developer and Ministry of Social Affairs. Medical services are provided by large hospitals as well as small centres of GPs which use different IT solutions and ISs: those developed by different companies, X-Road infrastructure, portals managed by the HWISC and the NHIS database managed by the HWISC. Medical service providers send data to the NHIS and also receive data via the data exchange layer X-Road. The EHRs compiled by doctors using the MSP's IS are sent over the X-Road infrastructure to the NHIS database, where all needed validation and controls are done.

Second, the assessment of risks of assets in the Estonian e-health infrastructure was analysed. Two possible threat agents, a hacker and another MSP worker were defined, who can use different attack methods. A hacker may access the network or MSP computers through the man-in-the-middle attack or by taking advantage of the weakness in the MSP's health IS and change the EHR or the EHR is changed before the MSP adds the e-seal to it. An MSP worker can either change patient health information and the diagnosisnor send changed patient health information to the NHIS. All this poses risks to the organizations involved: loss of the confidentiality of patient information or theft of patient information, loss of the integrity of patient health information, negation of the integrity of the EHR and loss of trust in the MSP.

Third, the ways of mitigating risks in the Estonian e-health infrastructure were discussed. Four types of risks (R1–R4) are present in the Estonian e-health infrastructure: R1 is related to the registered patient personal information asset, R2 to the patient health information asset, R3 to the EHR information asset (created by the GP), R4 to the EHR information asset (created by the MSP). Different security requirements apply to different risks: with R1 and R2 the activity in the MSP network and computers must be monitored and logged; with R3 and R4 the integrity of the EHR must be secured when it is created by the GP.

In order to fulfil these security requirements, various security controls can be implemented. For R1 secured connections and encryption of the database should be used for patient registration auditing database queries logs. For R2 stronger passwords or smart cards should be employed for authentication. In the case of R3 the digital signature, e-seal or KSI timestamp need to be used on compiling the EHR. In the case of R4 the received EHR must be verified with the previous original received, by using for example Blockchain cryptographic digest.

To meet the security requirements for integrity, availability and confidentiality set on the NHIS by the law the following security controls should be applied. It is necessary to use secured connections and encryption of the database for patient registration auditing database queries logs. The MSP workers should use stronger passwords or smart cards for authentication. The digital signature, digital seal or KSI time stamp should be employed when the EHR is compiled. The received EHR should be verified with the original received (for example with Blockchain cryptographic digest).

7.3 Future Work and Author's Proposals

This research is based on the organization of the work at the Estonian e-health infrastructure. The aim of the analysis was to find out in which point of the infrastructure the integrity of the EHR must

be ensured. This case develops very rapidly with time: the technologies that are on a high level today may not be so secure in near future. I expect that this work opens up more studies in the integrity in e-health. There are many different opinions concerning the ways of ensuring the integrity of data and hopefully there will be more works on how to use them in the e-health infrastructure.

In my work I analysed security threats occurring in the Estonian e-health infrastructure. At present more cloud infrastructure is increasingly added to the e-health infrastructure and organizations over Europe are (and will be) changing cross-border e-health information. Therefore I suggest that ISSRM Domain Models should be applied in analysing security threats in hybrid environments that are laid over borders.

References

1. Luo, J.S. Electronic Medical Records. *Prim. Psychiatry*, 2006, 13(2), 20–23.

2. Weed, L.I. Medical records that guide and teach. *New Engl. J. Med.*, 1968, 278(11), 593–600; 278(12), 652–657.

3. *State of the Union*. Address of William J. Clinton USA (January 19, 1999), https://clinton4.nara.gov/WH/New/html/19990119-2656.html (accessed 30 March 2018).

4. ENISA. *Security and Resilience in eHealth Annex A: Countries' Report.* European Union Agency For Network And Information Security, 2015, https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-annex-a-countries2019-report (accessed 30 March 2018).

5. Stroetmann, K.A., Artmann, J. and Stroetmann, V.N. *European Countries on their Journey Towards National eHealth Infrastructures – Evidence on Progress and Recommendations for Cooperative Actions – Final European Progress Report.* January 20, http://es.esacproject.net/sites/intranet.esacproject.net/files/ehstrategies_final_report.pdf (accessed 30 March 2018).

6. Lekkas, D. and Gritzalis, D. Long-term verifiability of healthcare records authenticity. In *IMIA Working Conference on Security in Health Information Systems, Dijon, France (April 2006)*, https://pdfs.semanticscholar.org/a030/719b3503a62e659a02b6360df43d768f6d45.pdf (accessed 30 March 2018).

7. Katt, B., Trojer, T., Breu, R., Schabetsberger, T. and Wozak, F. *Meeting EHR Security Requirements: Authentication as a Security Service*. 2010, http://subs.emis.de/LNI/Proceedings/Proceedings174/103.pdf (accessed 30 March 2018).

8. Object Management Group. *Business Process Model and Notation*, http://www.bpmn.org/ (accessed 30 March 2018).

9. Häyrinen, K., Saranto, K. and Nykanen, P. Definition, structure, content, use and impacts of electronic health records: review of the research literature. *Int. J. Med. Inform.*, 2008, 77(5) 291–304.

10. International Organization for Standardization. ISO/TR 20514:2005: *Health Informatics – Electronic Health Record – Definition, Scope, and Context*, 2005.

11. Almutairi, B. *A Strategic Roadmap for Achieving the Potential Benefits of Electronic Health Record System in the State of Kuwait*. PhD thesis, University College, London, 2011.

12. The National Alliance for Health Information Technology. *Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms.* April 28, 2008, http://www.hitechanswers.net/wp-content/uploads/2013/05/NAHIT-Definitions2008.pdf (accessed 30 March 2018).

13. Enterprise Systems Steering Committee and the Global Enterprise Task Force. *Electronic Health Records: A Global Perspective*. Second Edition, Part I. 2010, http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/Globalpt1-edited%20final.pdf (accessed 30 March 2018).

14. Ajami, S. and Bagheri-Tad, T. Barriers for adopting electronic health records (EHRs) by physicians. *Acta Inform. Med.*, 2013, 21(2), 129–134.

15. *Benefits of EHRs*, https://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs#footnote-1 (accessed 30 March 2018).

16. Bowman, S. Impact of electronic health record systems on information integrity: Quality and safety implications. *Persp. Health Inf. Manag.*, 2013 Fall, 10(Fall), 1c, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3797550/ (accessed 30 March 2018).

17. The European Parliament and the Council. 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. *OJ L*, 23/11/1995, 281,

0031–0050, http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046 (accessed 30 March 2018).

18. The Council of the European Union. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter. *OJ L*, 30.12.2008, 350/60, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1414070625251&uri=CELEX%3A32008F0977 (accessed 30 March 2018).

19. The European Parliament and the Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *OJ L,* 4.5.2016, 119/1, http://eurlex.europa.eu/legalcontent/EN/TXT/uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC (accessed 30 March 2018).

20. The European Parliament and the Council. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *OJ L,* 4.5.2016, 119/89, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC (accessed 30 March 2018).

21. *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html?language=es (accessed 30 March 2018).

22. *Summary of the HIPAA Security Rule*, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (accessed 30 March 2018).

23. Alder, S., Kelleher, A. and Greene, S. HIPAA Compliance Guide. H ow to make your organization compliant with the Health Insurance Portability and Accountability Act Privacy, Security and Breach Notification Rules. *HIPAA Journal*,

http://www.hipaajournal.com/wp-content/uploads/2015/05/HIPAAJournal-com-HIPAA-Compliance-Guide.pdf (accessed 30 March 2018).

24. Lepasepp, K., Matjus, M. and Haamer, M. *Overview of the National Laws on Electronic Health Records in the EU Member States. National Report for the Republic of Estonia*. 13 May 2014, http://ec.europa.eu/health//sites/health/files/ehealth/docs/laws_estonia_en.pdf (accessed 30 March 2018).

25. European Commission. *Protection of Personal Data*, http://ec.europa.eu/justice/data-protection/ (accessed 30 March 2018).

26. *American Recovery and Reinvestment Act of 2009*, https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf (accessed 30 March 2018).

27. Mehndiratta, P., Sachdeva, S. and Kulshrestha, S. A model of privacy and security for electronic health records. In: Madaan, A., Kikuchi, S., Bhalla, S. (eds) *Databases in Networked Information Systems. DNIS 2014*. Lecture Notes in Computer Science, 2014, 8381. Springer, Cham.

28. Bishop, M. *Introduction to Computer Security*. 2004, http://nob.cs.ucdavis.edu/book/book-intro/slides/06.pdf (accessed 30 March 2018).

29. *Health Level Seven® International*, http://www.hl7.org/about/index.cfm?ref=common (accessed 30 March 2018).

30. *The openEHR Foundation*, http://www.openehr.org (accessed 30 March 2018).

31. *OpenEHR*, https://en.wikipedia.org/wiki/OpenEHR (accessed 30 March 2018).

32. International Organization for Standardization. ISO 18308:2011: *Health Informatics – Requirements for an Electronic Health Record Architecture*, 2011.

33. International Organization for Standardization. ISO/IEC JTC 1/SC 27: *IT Security Techniques*, 1989.

34. International Organization for Standardization. ISO/TC 215: *Health Informatics*, 1998.

35. Eichelberg, M., Aden, T., Riesmeier, J., Dogac, A. and Laleci, G.B. A survey and analysis of electronic healthcare record standards. *ACM Comput. Surv. (CSUR)*, 2005, 37(4), 277–315.

36. Matulevičius, R. *Fundamentals of Secure System Modelling*. Springer, 2017.

37. *FAQ: Information risk management*, http://www.iso27001security.com/html/risk_mgmt.html (accessed 30 March 2018).

38. International Organization for Standardization. ISO/IEC 27005:2011: *Information technology – Security techniques – Information security risk management*, 2011. https://www.iso.org/standard/56742.html (accessed 30 March 2018)

39. *NIST Cybersecurity Framework.* https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework (accessed 30 March 2018).

40. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0.* 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed 30 March 2018)

41. Mayer, N. *Model-based Management of Information System Security Risk*. Computer Science, University of Namur, 2009.

42. *BSI-Standards*, https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html (accessed 30 March 2018)

43. Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 100-1: Information Security Management Systems (ISMS)*, 2008 **https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf;jsessionid=A203BC9589EC4A7433DFD572BE065B07.2_cid351?__blob=publicationFile&v=1** (accessed 30 March 2018)

44. Dubois, E., Heymans, P., Mayer, N., and Matulevičius, R. *A Systematic Approach to Define the Domain of Information System Security Risk Management*. Springer, New York, 2010.

45. Khadraoui, D. (ed.). *Advances in Enterprise Information Technology Security.* Idea Group Inc (IGI), 2007.

46. CLUSIF. *MEHARI-2010-Risk-Analysis-and-Treatment-Guide.* 2010, http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf (accessed 30 March 2018)

47. Riigikogu. Health Services Organisation Act. Passed 9 May 2001, entered into force 1 January 2002. *RT 1 I*, 2001, 50, 284, https://www.haigekassa.ee/uploads/userfiles/Health_Services_Organisation_Act.pdf (accessed 30 March 2018).

48. Estonian E-Health Foundation. *Health Information System*, http://www.e-tervis.ee/index.php/en/health-information-system (accessed 30 March 2018).

49. Vabariigi Valitsus. Tervise infosüsteemi edastatavate dokumentide andmekoosseisud ning nende säilitamise tingimused ja kord. Määrus 53. *RT L*, 2008, 78, 1098, https://www.riigiteataja.ee/akt/13029628 (in Estonian; accessed 30 March 2018).

50. Government of the Republic. *Regulation: The System of Security Measures for Information Systems.* 2009, https://www.ria.ee/public/ISKE/Regulation-the-system-of-security-measures-for-information-systems-2007-12-20.pdf (accessed 30 March 2018).

51. Riigikogu. Digital Signatures Act. *RT I*, 2000, 26, 150, https://www.riigiteataja.ee/en/eli/530102013080/consolide (accessed 30 March 2018).

52. AS Sertifitseerimiskeskus. *The Estonian ID Card and Digital Signature Concept Principles and Solutions Ver 20030307*, http://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf (accessed 30 March 2018).

53. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley. R. and Polk, W. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *RFC*, 2008, 5280, https://tools.ietf.org/html/rfc5280 (accessed 30 March 2018).

54. Zeilenga, K. (ed.). Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map. *RFC*, 2006, 4510, https://tools.ietf.org/html/rfc4510 (accessed 30 March 2018).

55. Santesson, S., Myers, M., Ankney, R., Malpani, A., Galper, S. and Adams, C. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. *RFC*, 2013, 6960, https://tools.ietf.org/html/rfc6960 (accessed 30 March 2018).

56. IHE ITI Technical Committee. *IHE IT Infrastructure Technical Framework, Supplement 10, Document Digital Signature (DSG)*. 2016, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DSG.pdf (accessed 30 March 2018).

57. Riigi Infosüsteemide Arenduskeskus. *Infosüsteemide kolmeastmelise etalonturbe süsteem ISKE Rakendusjuhend. Versioon 8.00*. Jaanuar 2017 (in Estonian; accessed 30 March 2018).

58. Vabariigi Valitsus. Infosüsteemide turvameetmete süsteemi kehtestamine. Määrus 273. *RT I*, 2004, 63, 443, https://www.riigiteataja.ee/akt/791875 (in Estonian; accessed 30 March 2018).

59. Matulevičius, R., Norta, A., Udokwu, C. and Nõukas, R. Security risk management in the aviation turnaround sector. In: Dang, T., Wagner, R., Küng, J., Thoai, N., Takizawa, M. and Neuhold. E. (eds) *Future Data and Security Engineering*. FDSE 2016. Lecture Notes in Computer Science, vol 10018. Springer, Cham.

Non-exclusive licence to reproduce thesis and make thesis public

I, Alvar Ristikivi,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright

Ensuring the Integrity of Electronic Health Records

supervised by Jaan Priisalu and Raimundas Matulevičius,

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tallinn, 23.04.2018