TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Health Technologies

MICHAEL ANYWAR YVEM165572

ESTONIAN HOSPITAL CYBER THREAT VULNERABILITY:

Evaluation of Cyber security standards deployed at Hospitals to deter cyber threats

Master's thesis

Supervisor: Liisa Parv

Academic degree: Msc

Co-supervisor: John Walker

Academic degree: Professor

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tervisetehnoloogiate instituut

MICHAEL ANYWAR YVEM165572

EESTI HAIGLATE KÜBEROHU VÕIMALIKKUS:

Haiglates kasutusel olevate küberjulgeoleku standardite hindamine, tõkestamak küberohtude.

Magistritöö

Juhendaja: Liisa Parv

Teaduskraad: Msc

Kaasjuhendaja: John Walker

Teaduskraad: Professor

Deklaratsioon;

Tõendan, et see magistritöö koostati ja see on tingitud minu sõltumatutest jõupingutustest ja et siin sisalduv töö on minu enda, välja arvatud juhul, kui tekstis on selgesõnaliselt teisiti sätestatud. Seda tööd ei ole esitatud mingil muul määral ega kutsekvalifikatsioonil, välja arvatud juhul, kui see on täpsustatud; samuti pole seda avaldatud.

Michael Anywar
Üliõpilase kood*:* YVEM165572

Juhendaja*: Liisa Parv*

Töö vastab magistritööle esitatavatele nõuetele.

Kaitsmiskomisjoni esimees*:*
Lubatud kaitsmisele

.....

(nimi, allkiri, kuupäev)

Master's Programme in Health Care Technology, 2016: Degree Thesis; 30 Credits.
Estonian Hospital Cyber Threat Vulnerability: *Evaluation of Cyber security standards deployed at Hospitals to deter cyber threats.*

Abstract

Background: *The years 2016-2017 saw a high number of hospitals falling victims to cyberattacks, majority of which were victims to ransomware. This has increased the concern for protecting sensitive hospital assets from breach be it; medical devices, patients or patient data. Authorities and bodies such as the European Commission have defined cyberattacks as an increasing concern to the health sector, hence regulations like GDPR have been framed to increase security requirements and enforce compliance.*

Objectives: *The study was set to identify and explore cyber security flaws in the security measures and standards already implemented at Estonian Hospitals, and to map and qualify vulnerabilities associated to these flaws.*

Methods: *Qualitative study design was used to evaluate the flaws associated to the security measures and standards implemented at the hospitals to help avert cyber threats. In-depth interviews guided by semi-structured interview guide were held as the data collection tool. The study evaluated the measures and standards deployed at the various participant hospitals of Estonia, as a scope for vulnerability evaluation.*

Results: *The study revealed the efforts being undertaken by the various hospitals to secure sensitive assets, but also the weakness in the measures they deploy to achieve cybersecurity compliance. The major flaw identified was the lack of cyber security standard in all the hospitals. Besides, limited human capital in respect to cyber security skill set, limited cyber security audits, over dependency and trust of private vendors were some of the major vulnerabilities identified with the measures aimed at averting cyber threats at the hospitals.*

Conclusion: *Hospitals do require and need to have standardised health sector cyber security standards that harmoniously match and sync with health sector needs; However, this would require both health sector and IT security professionals to form and design these standards basing on the health sector needs and not just generic IT system's needs.*

Keywords: *Cybersecurity, Cyber threat, Standards, Vulnerability, Hospitals*

Magistriprogramm Tervishoiutehnoloogia, 2016: Magistritöö; 30 ainepunkti.

Eesti haiglate küberkuritegevuse haavatavus: *haiglates kasutatavate küberjulgeoleku standardite hindamine küberohtude ennetamiseks.*

Lühikokkuvõte

Taust: *Aastatel 2016-2017 sattus suur arv haiglaid küberrünnakute alla, millest enamus pidid maksma ka lunaraha. See on tekitanud haiglates suuremat tähelepanu tundlike varade - meditsiiniseadmete, patsientide ja patsiendi andmete - kaitse tagamisele. Organisatsioonid, nagu näiteks Euroopa Komisjon, on küberrünnakuid määratlenud kui üha suurenevat probleemi tervise valdkonnas, ning seetõttu on turvalisuse suurendamiseks ja turvanõuete vastavuse tagamiseks välja töötatud õigusaktid, sealhulgas ka GDPR.*

Eesmärgid: *Uuringu eesmärk on tuvastada ja uurida Eesti haiglates juba rakendatud küberturvalisuse meetmete ja –standardite puudujääke ning kaardistada ja kirjeldada nende puudustega seotud võimalik haavatavus.*

Meetod: *Uuringus kasutati kvalitatiivse uuringu mudelit haiglates rakendatud turvanõuete ja –standardite puudujääkide hindamiseks, ning seeläbi küberohtude ennetamiseks. Andmekogumisvahendina viidi läbi poolstruktureeritud intervjuu juhendi baasil põhjalikud intervjuud, ning küberturvalisuse haavatavuse hindamiseks hinnati uuringus mitmetes Eesti haiglates rakendatud meetmeid ja standardeid.*

Tulemused: *Uuringu tulemusena selgus, et vaatamata haiglate jõupingutustele tundlike varade kindlustamisel on küberjulgeoleku tagamiseks kasutusele võetud ebapiisavad meetmed. Leiti, et peamiseks puuduseks on küberjulgeoleku standardi puudumine kõikides haiglates. Lisaks sellele leiti peamiste haavatavustena, et haiglates on piiratud arv küberjulgeoleku teadmiste ja oskustega inimesi, viiakse läbi ebapiisavalt küberjulgeoleku auditeid, ning haiglatel on suur sõltuvus erasektori müüjatest. Nimetatud haavatavused tuvastati haiglates küberohu ennetamiseks rakendatud meetmetest.*

Kokkuvõte: *Haiglad vajavad tervisevaldkonna vajadustega kooskõlas olevaid standardiseeritud küberjulgeoleku standardeid. Standardite väljatöötamiseks ja kujundamiseks peavad tervishoiusektori kui ka infotehnoloogia turvaspetsialistid koostööd tegema, luues standardid arvestades mitte ainult IT süsteemide, vaid ka tervishoiusektori vajadusi.*

Table of Contents

List of abbreviations

RIA: Riigi Infosüsteemi Amet (Estonian Information Systems Authority).

ISKE: Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (Translates into: Information Systems three-way reference security system).

ENISA: European Union Agency for Network and Information Security.

ISO/IEC: International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

BSI: German Federal Office for Security in Information Technology.

IT-Grundschutz-Kataloge: IT Baseline Protection Catalogs.

HIPAA: Health Insurance Portability and Accountability Act.

EU: European Union.

GDPR: General Data Protection Regulation.

ISMS: Information Security Management System.

AICPA: American Institute of Certified Public Accountants

IT: Information Technology.

NCBI: National Center for Biotechnology Information

List of Figures and Tables

1. Introduction

The Estonian cyber security has had many developments in the past years with rapid development of information and communication technology infrastructure. This has improved the availability and security of e-services, enhance transparency and citizen participation in governance, and cut public as well as private sector administration costs.

This also means that the dependence on technology to offer services has increased and so has the significance of technology in people's daily livelihood. As more benefits are realized, the number of e-services offered also increase so as to tap on these significances offered by technology in the country by both private and public sector. This increased desire to adapt and use technology for e-services, provides hope and high expectation that technology can operate seamlessly. With the internet being increasingly accessible throughout the country, the user base of internet enabled technological solutions and services has also increased. However, cloud computing potential actors of attack also increases along the superiority of technology and so does the complication of the attack techniques deployed by these wrong internet elements hence affecting the seamless operation of internet-based services.

Developments in international cyberspace are increasingly complex and it is difficult to delimit the impact of cyber threats to clear areas or actors. 2016 will be remembered for a number of unprecedented cyber incidents around the world. Witnessed were also power outages caused by cyberattacks on electrical grids. We saw how the internet of things devices and home appliances connected to the net was exploited to attack fundamental services of the internet, the effects of which transcended national and continental borders(1).

On Friday, May 12, 2017 a large cyberattack was launched using WannaCry (or WannaCrypt). In a few days, this ransomware virus targeting Microsoft Windows systems infected more than 230,000 computers in 150 countries. Once activated, the virus demanded ransom payments in order to unlock the infected system(2). This entire situation highlights a critical need to re-examine how we maintain our health information systems. Equally important is a need to rethink how organizations sunset older, unsupported operating systems, to ensure that security risks are minimized. For example, in 2016, the National Health Service (NHS) England was reported to have thousands of computers still running Windows XP a version no longer supported or maintained by Microsoft.

Estonia is not immune to developments in the international environment and there is no reason to expect global trends in cyberspace to pass the country according to a report by Riigi Infosüsteemi Amet (RIA)(1) which is the state agency responsible for the smooth operation information systems and IT infrastructure in Estonia. According to the 2018 state report (3) a total of 4, 300 patients had access to their data denied, this ranged from prescribed prescriptions, medical certificates, digital health card. At the same time, Estonia has specific strengths, vulnerabilities and interests in the cyber environment that stem from the choices made in developing its digital state and from the role that information and communication technology plays in functioning of society(1).

Due to the fact that Estonia as a state, the economy and population heavily depend on ICT infrastructure and e-services, cyber security risks are high. In its annual Cyber security assessment report for 2017, RIA stated; *"Even though there were no incidents as dramatic in Estonia, the healthcare system in Estonia did not go unscathed by ransomware schemes. At one of Estonia's largest hospitals, ransomware from infected computers spread to the file server. While provision of medical services was not disrupted, there were serious problems in other operational processes. The incident did not remain a single occurrence, unfortunately.*"(1)

National cyber security is affected by vectors with different skills, motivations and targets. It is often difficult to distinguish between the vectors or determine their relationship to national or international organizations. The number of state actors in cyberspace that are involved in cyber espionage targeted at computers connected to the Internet as well as closed networks continue to grow, with their aim being to collect information on both national security as well as economic interests(4).

There is no question that these vectors will continue acting and breaches will continue to happen. However, health organizations can mitigate future risk by ensuring best security practices are adhered to. Hence, this study focused on evaluating the effectiveness of standards used in Estonian hospitals against cyberattacks.

Cyberattacks range from ransomware, medical device hi-jacking, unauthorized access to patient data which sometimes can cause physical harm to patients, interruptions to smooth operation of care provision work flow in hospitals, etc.(5).

1.1. Background

The year 2016-2017, saw a great rise in hospitals experiencing cyberattacks ranging from ransomware to infrastructure destruction (6). In 2016, over 12 hospitals reported their data having been breached, 3 of which came from Europe, that is Klinikum Arnsberg hospital and Lukas Hospitals of Germany, in which surgery operations were delayed, as hackers had held systems at ransom, while the majority of the affected hospitals of 2016, were US based, with over $5m worth of ransom demanded and over 1000s of patient data lost(7) and a Estonian primary care center paid at least 1.3 worth of bitcoins in order to salvage encrypted patient data(3).

In order to advance and make health care provision more personalized, in addition to the legacy hospital assets, many pervasive systems have been proposed, some adopted into the general hospital care system. Given the fact that these systems need to interoperate with the traditional systems in order to support the core functions of the hospital, focus is then put on Infrastructure and interoperability.
This interconnectivity of medical devices has left many hospital assets vulnerable to security breaches and threats that they were once guarded against, in the same way just like any other networked computing systems of current technological era.
However, unlike other networked computing systems, there is an increasing concern that the connectivity of these hospital assets will directly affect clinical care and patient safety(8).

Collaboration among various stakeholders, numerous interconnected assets and high flexibility requirements do not only lead to complexity and dynamics but also to blurred organisational boundaries. Due to the great number of significant assets at stake for example patient life, sensitive personal information and financial resources hence information security becomes a key issue for hospitals(9). Since attackers are never resting, hospitals are called upon to be proactive and not comfortable with the already existing defense mechanisms.

While it should be acknowledged and noted that the security standards implemented in Estonia; Infosüsteemide Kolmeastmelise Etalonturbe Süsteemi (ISKE), adopted most of its policies from the Germany Standards, IT Grundschutz which was last updated in 2013. In Chapter 2, different IT systems security standards that are relevant to the health care sector are discussed.

1.2. Problem Statement

With the continued intrusion of information systems of various organization using various methods and tactics, hospitals of recent specifically the year 2016-2017 have been among the top exploited with some experiencing disruptions in their normal operations. And when this happens, patient's/client's lives are at stake and are at jeopardy, not forgetting the vast amount of data that hospitals hold. Such tactics range from social engineering to exploitation of vulnerabilities that exist within medical devices.

One of the major reasons hospitals have been so vulnerable to cyberattacks has been due to the failure of the implemented standards being effective enough or poorly implemented. Reports show lack of compliance and also failure to implement standards hence. Coupled with advances and development in technology(10), new vulnerabilities that are not addressed by current standards have been exposed, hence with such a continued trend; there is need and call to action for continued evaluation of standards and frameworks implemented at hospitals to ensure continued resilience against cyber threats.

1.3. Aim

This study is set to explore and identify possible vulnerabilities that could exist and also suggest possible measures and recommendations necessary to Estonian hospitals on their cyber security policies and/ or on already implemented standards and frameworks in order to effectively protect both clients (patients) and hospital assets against cyberattacks. This shall be achieved through evaluating the already implemented security measures.

1.4. Objectives of the Study

- Identify any possible flaws in the cyber security standards and frameworks implemented by carrying out interviews with Heads of IT Security systems in the various identified hospitals.
- Map and qualify the vulnerabilities associated with flaws identified in implemented standards to recommendations made by the various reviewed Cyber Security Standards and Frameworks;

1.5. Research Question

With the continued ransom cyberattacks against hospitals, the researcher is prompted raise a research question of whether the current standards and frameworks deployed in hospitals against cyber threat are effective enough to stop hospital cyberattacks or malicious intrusion? Basing on this question, then the researcher shall be able to come up with possible reasons and solutions where needed.

2. Literature Review

The period 2016-2017 was a busy year for most cybersecurity professionals especially in the healthcare sector as many hospitals reported to have been victims of cyberattacks or have been maliciously accessed. This has called many to rethink their strategies, while for other this was an opportunity to evaluate their standards since the attacks were continuous.

Several independent evaluators performed independent finding into the preparedness and of hospitals towards cyberattacks(11).

Evaluation of Cybersecurity standards enable the identification, quantifying and prioritizing of vulnerabilities in a healthcare setting in order to effectively identify defence mechanism that are effective in protecting against attacks and also revealing vulnerabilities before being exploited by an attack agent(12). According to ENISA(European Union Agency for Network and Information Security) (2012, 11) evaluation can inform about policy changes and the framing of issues in the long term; allow learning from past experience, evidence of effectiveness or learning can support the accountability of political action, evidence base can give credibility towards general public and international partners. Evaluation can support outreach and enhance public image as transparent organisation.

In development of this paper, theoretical input from different literature is reviewed in order to seek answers to what standards are being deployed in hospitals, their level of effectiveness (how they are assessed); what frameworks exist that can effectively defend the healthcare ecosystem from cyberattacks so that both patients and hospital assets like patient information(data), are not accessed by the wrong agents.

To further re-iterate this concern, between 2016-2017, Thycotic (2017, (13)) carried out a ground breaking security measurement index benchmark survey to determine the cybersecurity metrics worldwide. This ranged from different industries and the report was alarming. The evaluation was based on internationally accepted cybersecurity evaluation framework of ISO/IEC 27001:2013 and best practices from experts and professional cybersecurity associations. The result of this report showed that many organisations were failing to evaluate the effectiveness of their cybersecurity standards, in which health care service providers were also participants.

The need to evaluate cybersecurity standards is an important aspect of keeping the healthcare sector secure by answering such as “why” certain attacks still keep on occurring and hospitals falling victims to ransoms attacks often. Evaluation refers to making a judgment or determination concerning the quality of a performance, work product, or use of skills against a set of standards(14). Hence in evaluating standards, organisations aim at finding strengths and weakness and also finding future improvement possibilities.
However, it should be noted that despite the fact that the healthcare industry is heavily adopting IT systems, few standards are really meant for healthcare, but rather are generic in nature; general purpose IT systems.

2.1. Method and Criterion of Choosing Literature

While determining what materials of literature to review, the research was mainly performed on materials from governmental cyber security bodies, in the European Union(EU) and the USA government portal, Google Scholar databases, both private and public independent Security evaluator portals and Cyber security company portals were visited. Academic portals from which materials were sought included NCBI, ResearchGate, IEEE, PubMed and security system companies.

While searching for literature to review in relation to this study, literature published between 2012-2017 was considered, 3 main keywords in English were used for searching materials. These were: “Securing Hospitals, Cyber Security Standards, Evaluation of methods in Cyber security and Hospital Cyber security.”
Since less studies have been carried out in Estonia, studies that were performed in the United States of America (USA) were preferred, with ENISA having studies in Europe.
Researcher independently reviewed, assessed and validated the quality of the materials before having them included in the literature review.

2.2. Reviewed Materials

Since this study was based and carried out in Estonia, it was only fitting to first recognise the fact that cyber security evaluation research studies on hospitals are not common, since trust is highly entrusted in the State machinery, and this sees the state and its public-private run agencies release annual security reports (15).

With respect to this the researcher used study materials and literature review from various academic database and source in order to broadly understanding the various standards and approaches in evaluating cybersecurity.

With focus on Estonia in specific, the state of design, development, best practices and principles used in the cybersecurity domain largely focus on compliance of standards and policies set by the state. It can therefore be urged that the state spends more on research in the field of security and the people believe and trust that the state knows best what is best for the industries, hence they apply security measures while trying to comply to the requirements set out by the state. While well-intentioned, the tendency to rely on open standards which are non-organisation specific can be a daunting especially for the health care sector.

Some organizations however, supplement these practices by incorporating traditional information security concepts and principles, and attempt to build in-house security measures in to the development of IT systems they implement (16).

However, in primarily focusing only on compliance model of evaluation of standards, a number of issues arise for example, certain of aspects of the society, like culture, behaviours are less focused on and instead excessive resource are allocated in following and implementing compliance requirements.

Contemporary cyber security evaluation practices on the other hand also do exist and these are largely driven by compliance requirements, which force organizations to focus on security controls and vulnerabilities(16). Multiple areas are focused on while using this approach. These areas range from vulnerabilities, assets, threats and controls which are evaluated collectively with variables of probability and impact.

Security controls are implemented to prevent attacks executed by threat actors that exploit vulnerabilities that are exposed. Usually an unbalanced focus on evaluating controls and identification of vulnerabilities prevents organizations from identifying and combating the most serious element which is the threats.

2.3. Relevant Evaluation Approaches.

The researcher in this section gives overview of relevant cybersecurity evaluation standards used and their relevant to assessment of cybersecurity of the Healthcare ecosystem with some having regulatory and legal backing, while some standards are industry led, voluntary, and sector specific.

One of the agenda of ENISA which is enabling and associating with strategic programmes for national cyber security strategies and standards of member countries of the EU fits into a much bigger picture of boosting member states and EU institutions to include evidence-based approaches in their cyber security strategies(2012, (12)). Given that Estonia is a permanent member of the EU, reports are submitted from progress reports on cyber security compliance with the relevant actions on annual basis.

The most specific guidance on evaluation of strategies on nation cyber security standards comes from ENISA's good practice guide on formulating cyber security strategies. In developing cyber security standards, different evaluation approaches are used in order to match the type and relevancy of assets to be protected. Since this study aimed at the healthcare sector specifically hospitals, the researcher identified specific cyber security standards and regulations that were useful in evaluating Estonian hospitals cyber security.

The most recent guideline being the GDPR (General Data Protection Regulation), which becomes effective come May 2018, was made and released by the EU. GDPR define how organizations, businesses or the government can use an individual's personal information hence, the mishandling of an individual's healthcare data can have long-term effects. Disturbingly, the highest figures so far of data security incidences have been reported most among in the healthcare sector. Regulations exist to guarantee healthcare data is not vulnerable to attack, misuse, or misappropriation(17).

The GDPR's objectives also aim at guaranteeing that there is privacy by default, denoting that data protection measures are implemented across all data-processing activities. These changes that the GDPR brings on board on data protection rules are however not new, the key principles, concepts, and themes of the current data protection regime remain in place. Instead, the new rules build on what is already there, but they do differ significantly with many new requirements(18).

The health care sector just like anyone else in the EU, that controls data or performs data processing, falls under the GDPR. Data controllers and processors have extended responsibilities and obligations under the GDPR. Hence hospitals are required to put in place both technical and organizational *evidence-based* measures to ensure that processing personal data fully complies with GDPR requirements, which means the way hospitals implement data protection standards and policies is very significant.

Hospitals who according to GDPR are processors will now have to maintain records of all of their processing activities, ready for disclosure in order to show compliance. In addition, processing on behalf of a controller must be set out in a contract according to certain criteria laid down under the GDPR. The healthcare sector thus, will have to accept and implement a more general methodology to data governance and administration, of which if done accordingly, hospitals are expected to reap the reward of knowing where data is and where it goes to, hence permitting good compliance practice and reduced risk.

With the manner in which security is managed in hospitals, that is with a lot of secrecy, GDPR brings in an important change which requires organization by default to report data breaches. Breaches must be reported to a data protection regulator for which in Estonia, that regulator is RIS, and this reporting has to be made within 72 hours and those affected by the breach must also be informed. The healthcare sector will therefore have to put in place clear, practical and effective procedures that can be acted upon immediately this should be at the top of the GDPR compliance checklist(19).

ISO/IEC 27001:2013 is an information systems security standard that covers all types of organizations e.g. commercial enterprises, government agencies, not-for profit organizations. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System(ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof(16).

Note is also taken that ISO 27001 gives evaluators a certain degree of freedom, in order to ensure effective and efficient assessment of an ISMS according to the specific information security requirements of the organization under question. An ISMS is a systematic approach to

managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. With healthcare being sector of focus, the controls discussed in the International standards are only those identified to be appropriate in providing confidentiality, integrity and availability of personal health information and to warrant that access to such information can be assessed and accounted for. These controls help to avoid faults in medical practice that might result from failure to maintain the integrity of health information. In addition, they help to ensure that the continuity of medical services is maintained. ISO(20) lists a number of considerations to be taken into account when implementing healthcare security, these include;

a) honoring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care is right to privacy;

b) maintaining established privacy and security best practices in health informatics;

c) maintaining individual and organizational accountability among health organizations and health professionals;

d) supporting the implementation of systematic risk management within health organizations;

e) meeting the security needs identified in common healthcare situations;

f) reducing operating costs by facilitating the increased use of technology in a safe, secure, and well managed manner that supports, but does not constrain current health activities;

g) maintaining public trust in health organizations and the information systems these organizations rely upon;

h) maintaining professional standards and ethics as established by health-related professional organizations (insofar as information security maintains the confidentiality and integrity of health information);

i) operating electronic health information systems in an environment appropriately secured against threats;

j) facilitating interoperability among health systems, since health information increasingly flows among organizations and across jurisdictional boundaries (especially as such interoperability enhances the proper handling of health information to ensure its continued confidentiality, integrity and availability).

The next IT systems Security evaluation standard is the BSI framework (IT-Grundschutz). This standard aims at establishing and maintaining an appropriate level of protection for all

information assets in an organisation through providing a methodology for evaluating and management of information security. Hence any cyber security strategy implemented, must be able to guarantee the protection of hospital assets(21).

The BSI evaluation model involves evaluating of measures deployed by information security management system as well as auditing of the specific information security measures on the basis of IT-Grundschutz. The aim of IT-Grundschutz is to achieve an appropriate level of security threshold for all types of information of an organization.
IT-Grundschutz focuses on the protection of business-related information, which has a standard security requirement. IT-Grundschutz may be useful also for IT systems and applications with high security requirements(21).
The IT Grundschutz utilises a cataloguing mechanism to offer a synopsis and a grouping of different threats. The catalogues describes the standard security measures in detail by including standard security procedures and details for typical IT systems with ordinary protection requirements, description of the threat scenario which is globally assumed, detailed descriptions of measures to assist with their implementation, a description of the process involved in attaining and maintaining an appropriate level of IT security and simple methodology for ascertaining the level of IT security attained by comparing the target with the actual system status(21). It is from this that the ISKE framework adopted by Estonia was developed(22).
The main reasons IT Grundschutz was because RIA needed a standard that was regularly updated; did not require any risk assessments which were considered time consuming; had enough set of safeguards; and enabled a common understanding of the security level needed in public sector information systems.

Given the fact that Estonia heavily relies on e-Service; the use of internet to deliver services of which include e-prescription(23), another framework for evaluation of cyber security standards that can be used is Trust Services. This is a framework that addresses security and privacy risks mainly focussed on online service providers(24). The criteria and principles underlying Trust Services are set by American Institute of Certified Public Accountants (AICPA). These criteria are used by auditors providing attestation services on systems in the subject matters of security, availability, processing integrity, privacy, confidentiality, and certification authorities.

The Trust Services framework has three types of assurances: examination, review, and agreed-upon procedures engagements. In examination and review engagements, the evaluator expresses an opinion, for example, about whether there exist controls of a system and that they operate effectively to meet the criteria for systems reliability. In an agreed-upon procedures engagement, the practitioner does not express an opinion but rather performs an audit following agreed-up-on procedures and then reports the findings.

Another standard widely used in the USA, which the researcher found helpful and could be adopted in Estonia is the Health Insurance Portability and Accountability Act (HIPAA) framework. HIPAA has two (two) major goals, Healthcare Privacy and Data Security, of which the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and wellbeing(25). This is achieved through establishment of national standards for the protection of certain health information especially individually identifiable health information.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed(26).

The Security Rule, establish a national set of security standards for protecting of certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations must put in place to secure individuals' electronic protected health information(27).

Hence, while evaluating any methods used in cyber defence of the healthcare sector, HIPAA enables focus on identification of strengths or weakness on protecting an individual's health data both electronic and non-electronic.

The HIPAA strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the HIPAA is designed to be flexible and broad to cover the variety of uses and disclosures that need to be addressed.

Whereas these approaches to evaluation of cyber security standards can be used individually since they vary in complexity and rigour, for effectiveness of studies certain organisations or evaluation entities like Deloitte, KPMG, HIMSS or Thycotic combine(13) two or more of the Cyber security standards in order to achieve maximum results and coverage. Hence according to the researcher, in order to achieve maximum input and goal aim of the study, a combination of the standards had to be used while evaluating Estonian Hospitals.

The Researcher combines ISKE, HIPAA, GDPR, ISO/IEC 27001 in order to raise some appropriate evaluation criteria in so as to achieve maximum results and coverage which in the end will make the study more relevant to the organisations being evaluated and Estonia in general.

Understanding the standards and Compliance regulations chosen in relation to health care.

Compliance Rules	HIPAA	For, a health facility to be HIPAA compliant, there are two sets of rules that are adopted as standards for the electronic health care transactions and code sets, unique identifiers, and security. A. HIPAA Privacy Rule: This rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. The Privacy Rule standards address the use and disclosure of individuals' health information called "protected health information" by organizations subject to the Privacy Rule called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used(26).

		B. HIPAA Security Rule: This rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI)(28).
	GDPR	GDPR contains precautions that seeks to ensure that healthcare data is not vulnerable to attack, misuse or misappropriation. This is to be achieved by enforcing privacy by design or default, meaning data protection measures must be implemented across all data processing activities, for example, from patient registration to discharged of a patient(29). GDPR stipulates the consequences that any organisation (healthcare facility) is likely to face if they misuse an individual's healthcare data or they do not properly following regulation guidelines(19).
Security Standards	BSI- IT-Grundschutz Catalogues	The Standards and Catalogues are a set of recommendations designed to assist an organization in achieving an appropriate security level for information throughout an organization(21). The Federal Office for Information Security (BSI) in Germany develops and maintains the BSI Standards, of which IT-Grundschutz is a part, with the providing methods, processes, procedures, and approaches to information security management, risk analysis, and business continuity management(30). The aim of IT-Grundschutz is to achieve an appropriate security level for all types of information of an organisation. IT-Grundschutz uses a holistic approach to this process.

		Through proper application of well-proven technical, organisational, personnel, and infrastructural safeguards, a security level is reached that is suitable and adequate to protect business-related information having normal protection requirements(31).
	ISO/IEC 27001	ISO 27001 standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)(20). The security requirements within ISO/IEC 27001 are general and proposed to be appropriate to all entities, irrespective of size, nature and type. The standard encourages the classification or risk assessment methodology that allows organizations to ascertain, investigate and treat security risks(32). Through specific framework that organisations must adhere to, the standard provides mandatory list of requirements that are tested and audited(33).
	ISKE	ISKE(Infosüsteemide Kolmeastmeline Etalonturbe Süsteem), also known as the Informations systems security Catalogue for Estonia, is basically an adoption of the Germany BIS- IT-Grundshcutz to suit the Estonian IT infrastructure by the State Information systems agency. The purpose of the ISKE implementation is to ensure an adequate level of security in the information systems processed. The system is designed primarily for security of information systems used for the maintenance of state and local government databases and related information assets. ISKE can also be used by businesses to secure their IT assets.

3. METHODOLOGY

While determining what research method to use, it is relevant to consider the fact that associated tasks and researcher's views have an impact and can influence the nature and course that the research is to take.

These associated tasks also end up influencing the research question, data collection method and their analysis.

Hence, with this in mind, the study took an explorative approach in order to have an in-depth understanding of the cyber security standards and measures deployed at Estonian Hospitals.

3.1. Approach.

In tackle the research question, this study followed semi-structured qualitative study approach, mainly because the field of study had been categorized as sensitive and complex area, that is; a national concern, in which data collection would prove complex; that is to say, virtually any subject matter could turn out to raise sensitivities, depending on circumstance and experience of the participants.

In order to fully overcome the anticipated obstacles, in-depth face to face interviews and email interviews assisted by interview guide were the researcher's choice of data collection technique.

With the two methods; in-depth face to face interviews and email interviews, the researcher was able to capture rich data which combined both social cues like voice(34), intonation and body language to gauge how comfortable a respondent is on speaking about the subject; and enabled a wide coverage through emails to areas that were inaccessible but were relevant to the study.

In the end, the semi-structured interviews provided the researcher with;

- The opportunity to generate data that carries several aspects of one's insights into the phenomenon such as complexities and richness involved in the study.
- Insights into participants perceptions and values while considering language as an essential aspect of the respondents.
- Contextual and relational aspects were seen as significant to understanding participants' perceptions and experiences with cyber security in hospitals;
- The data generated could be analyzed in different ways

Having considered an approach that integrates secondary data in different aspects of the study, a broader understanding of the subject can be yielded hence providing a stronger foundation for this study.

By definition, qualitative study enables researchers to obtain significant insights into contextual and relational aspects of respondents perceptions of general phenomenon as it occurs(35), thus enabled the easy understanding of the current standards of cyber security and frameworks implemented in Estonian hospitals along with the various measures undertaken. With this, the researcher was able to reach tentative understanding of the situation under investigation.

3.2. Study Area Setting.

Estonia consists of several hospitals which are located and named basing in their locality and level of Advancement.

The study was conducted at the offices of the various hospital Information Systems Managers in environments that they had preselected and deemed suitable for the study to be conducted.

List of Estonian Hospitals and individual duties/roles played by the participants at the various hospitals that in which the study was conducted. These participants were specifically identified as the top most source of information and data that would be necessary for this study.

Table 1:Anonymized Participants and their Roles at hospitals

Hospital	Roles
1	IT Systems Manager
2	IT Systems Manager
3	IT Systems Administrator
4	Chief Security Officer

3.3. Participant Selection

The selection of participants into the study was based on snowball sampling which followed a set of inclusion - exclusion criteria. The participants had to actively be involved with IT systems administration and decision making at the hospital and also willing to openly discuss the issues surrounding the cyber security environment in their work environment. Besides, they were the top most source of information that I could access basing on hierarchy and superiority at the management level at the IT departments at the various participating hospitals. Hence interviewing with the elite proved to be the only way to access certain information on cyber security in the hospitals.

Language of communication considered as a criterion for inclusion was English. Since the study was conducted in an environment where English is not the official language of communication, participants had to be able to communicate and feel free with use, understanding and speaking in English.

3.4. Data Collection Tools.

In-depth interview was used as a data collection tool for the understanding of hospital cyber security standards. The interviews were steered with a set of semi-structured interview guide questionnaires (See appendix A).

The interview questions were asked in English which is not a native language of the participants.

One interview was held via email, due to the time constraint and distance between the interviewer and participant. This one interview did not have significant effects on the results of the study as it ended up that this specific hospital was using an information system provided by the same vendor as another participating hospital, hence researcher draw a conclusion, that this could have been one of the reasons the responses did not vary so much after the analysis of the collected data.

3.5. Processing of Collected Data

During the interviews, audio recording of each interview was made, and notes taken, after which the audio recording were transcribed and compiled together with the notes. The researcher categorized the respondents accounts in ways that could be summarized thematically.

These interviews were held in silent rooms in which the participants could easily express their minds and discuss openly about the study area. During the interview sessions, there were no other persons present in the room but just the researcher and the respondent

Processing of the transcribed data was accomplished thematically, following elementary stages;

i. Sorting and rearranging of the transcribed audio recording.
ii. Generation of notes and thorough reading of the transcripts.
iii. Segmenting and labeling of the text.
iv. Thematically rearranging and categorizing of the data text.
v. Interpretation of the themed data in accordance to the research question.

By using themes, the researcher found this to be much more useful and understanding and answering the research question and issues identified by the various participants.

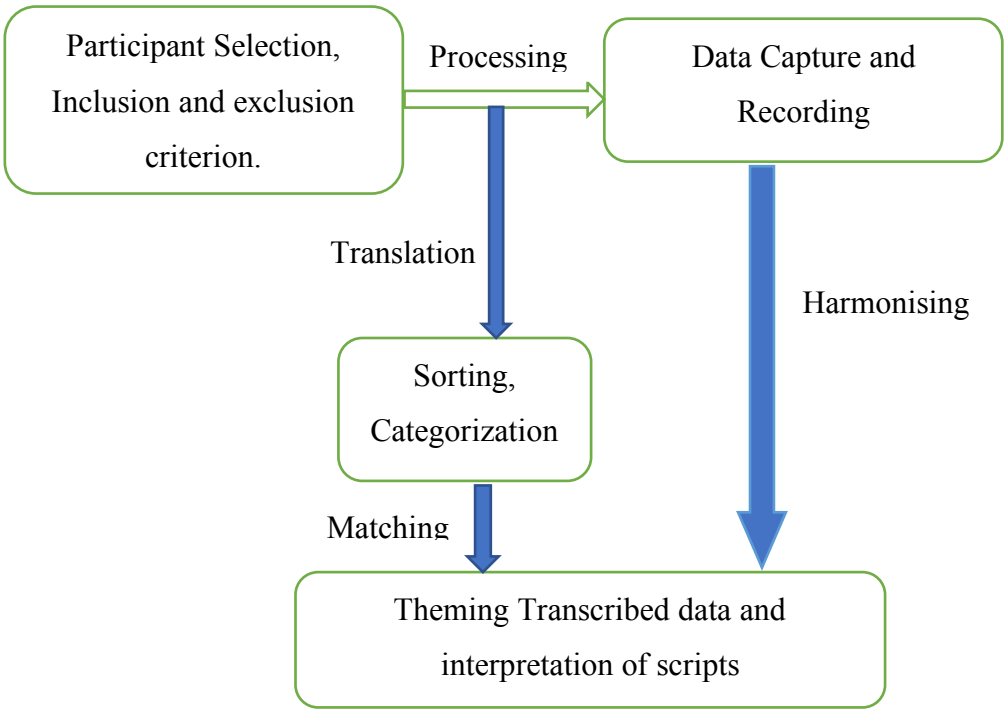

Figure 1: Translation, Processing and Matching of Data for evaluation of Standards in Hospitals

3.6. Validity and Reliability

The importance of measuring the accuracy and consistency of research instruments (especially questionnaires) known as validity and reliability, respectively, have been documented in several studies, but their measure is not commonly carried out among health and social science researchers in developing countries(36). To ensure that the study was and is valid, the interview question guide was developed from validated questionnaires from studies already conducted in the same field cyber security vulnerability evaluation.

3.7. Ethical considerations

Detailed information and privacy disclaimers were sent out to all possible participants before the actual interview. This clarified the magnitudes, consequences and benefits of the study and what would be shared and censored. This was meant to gain trust of the participants and to assure them that the study is meant for the good of the hospital and the healthcare sector.

Contribution and participation to the study was free to retract from any time. Confidentiality and anonymity of participants was maintained throughout the phase of data analysis and

presentation of the study results. Before the interviews, permission to carry out the actual interviews were obtained to ensure that all activities were in accordance to the regulations and did not break any regulations.

Furthermore, to maximize reliability of the data and the report in general, the report findings had to be shared with the participants to ensure that they agree with the findings and to confirm that accounts of both the researcher and participants tally.

4. Results

The results of the in-depth interviews that were carried by the researcher are presented in this chapter together with the research question that answers were being sought.

The data generated out of the responses to the interviews held by both email and interview physically on location inside the hospitals was been analysed thematically and aggregated under 6 main themes, which were identified as shown in the table below.

Table 2: In-depth interview resultant theme

Research Question	Interview Question Category	Resulting theme from analysed interview Response
• Are the current standards and frameworks deployed in hospitals against cyber threat effective enough to stop hospital cyberattacks or malicious intrusion? • What measures can be undertaken to improve or enhance these standards?	➢ General knowledge and awareness of Cyber security standards ➢ Organizational ➢ Technical implementation ➢ Needs & Requirements ➢ Compliance ➢ Preparedness and Plans	❖ Availability of Standards ❖ Awareness, training and Compitence ❖ Assets Protection ❖ Management Responsibilities ❖ Challenges ❖ Attitude of users of IT systems. ❖ Plans for continuity and future preparedness.

4.1. Availability of standards.

During the analysis of the field work, the first resultant findings theme was in relation to standards awareness. In regard to availability of standards in managing of Cyber vulnerabilities, all informants have expressed the use and their knowledge of Infosüsteemide Kolmeastmelise Etalonturbe Süsteemi (ISKE), which is the security standard adopted by the state primarily for securing local government databases.

ISKE was adopted from the Germany BSI, which offers a certain level of threshold of security for Information Technology Systems. All interviewees expressed how they have at least

implemented a certain level of ISKE or have started to implement it, although before they had just implemented some required level of security basing on intuition and necessity and not following any standards.

RIA being the regulatory body of public information system in Estonia, does require all hospitals to use and implement ISKE in their daily operations while implementing the required security standards,

".. on the issues of standards and Framework, we are implementing ISKE, this is basically Estonian made Standard, and RIA recommends it to us and all the databases we use have to be ISKE compliant…." [1-3]

"*We use ISKE as a standard, I have been working here since June 2017, there have been some attempts to implement ISKE before, but now this year is when the management decided that it is ISKE we will implement, and the reasons have been reasonable enough…" [4-4]*

Whether or not ISKE is implemented alone in order to meet a high-level security threshold that can be realized alongside combination of various standards such as HIPAA, ISO, informants stated that ISKE's implementation mainly covers infrastructural settings and ignores organizational culture and people's behaviour.

"…We are implementing ISKE, however it is mainly focused on protection if network Infrastructure, servers, data centers, backups and such, no much details, like for software and development or bug fixes and identification. However, we have the obligation to use ISKE, it is mandatory for databases that are having delicate information." [1-4].

One further mentioned despite being obligated to use ISKE as a standard, ISKE itself is in an out-dated form and is biased in a way due to its concentration on the infrastructure setting. Also mentioned was that it is up to the IT specialist to determine what section of ISKE to implement, depending on suitability and level of relevancy.

"Well what I can say about ISKE, is that it has the bias, as it mainly focuses on infrastructure but not so much on clients, or patients or even devices especially in our field of operation, medical devices or any other devices. But also, the other issue is that ISKE is outdated; which means we take it as a template, so we try to interpret the security measures in a way that it becomes different from that of either some ministry or hence ends up in a way that its out own

framework. So, we customize in it and decide whether something is important to us or no." [1-1]

"Currently we are evaluating how deep we should implement this ISKE. It is a very large standard. If you open the ISKE standard catalogue you will see that it is a very large standard, so we just implemented a specific section of it, or just what we believe is relevant to us." [3-3]

Mention was the lack of a wide spread Hospital (Healthcare facility) cyber security standard that would cover up the healthcare sector looking at its vulnerability and the amount of assets it has.

"*A lot of the guidelines that are implemented are based in common knowledge though, and not necessarily on a specific standard." [1-1], [4-4]*

"This can be attributed to by the lack of vigilance from RIA which gives the hospitals the leeway to manage themselves without regular supervision and checks. And only waiting for events to happen." [4-4]

4.2. Awareness, training and competence

While carrying out the field study, the informants consented and agreed that there is shortage of skills and know-how in the field of cyber security especially that can operate in hospital settings. Interviewees attributed this to the fact that hospitals do not have enough money to pay highly skilled cyber security professionals, despite the high price paid when breaches occur.

Further stated was that most of the hospital cyber security work is handled by less cyber security centric IT professionals with basic IT knowledge and not necessarily professionals who would be appropriate to manage and monitor cyber security system of the hospital.

"I myself, I do know we do not have enough people in the Team to address every issue as fast as it should be... " [2-2]

".. we sure should have some specialized skilled personnel, but at the moment, all our security is just under people like Systems administrators, which should not especially with a hospital…" [1-1]

On the issue of awareness, informants reported that most of the users are aware of security concerns within the hospital setting but are just reluctant to act or follow cyber security hygiene procedures. For example, most medics were reported not to be having time when it came to

issues to do with cyber hygiene education, and they continue to assume that the IT department will cover everything by itself.

"…Our main worry is user awareness because we have not been focusing on the user in the past, so the culture has been embedded into the users the IT department does everything. We have been concentrating on the procurement of new security inputs and devices, building infrastructure, new software, but the users have not been a concern to invest in…"[3-4].

"…We still have nurses who continuously write notes in MS word and the share among themselves and other medics via email despite the fact that we have systems in place to write notes.." [4-4].

4.3. Asset Protection.

When it comes to assets, the informants asserted that, their main area of focus has been infrastructure protection. Which involved procurement of various high-tech IT equipment's and rather leave securing of assets like medical devices to the manufacturers.

"It is not our responsibility to fix the vulnerability in these medical devices that might end up causing a threat to our assets. We tend to leave such issues to the vendors themselves to manage and handle. However, we know that these large companies that manufacture these devices do not care a lot, they do not take security seriously." [3-3].

The researcher was informed that the level of trust placed in these vendors is high so at times the hospitals are blinded by this trust and just keep absorbing and trusting whatever the vendor provides without necessarily routine checking that is required.

"From the vendor side, we do not have any real measures to ensure our assets are protected. We just have to trust them and take the risks. Hopefully in the near future while renewing contracts, we can include clauses that are provide for more regulation and also certify software codes that we purchase from these vendors as our assets." [1-1].

Confirmed by some of the interviewees was that not all IT related equipment and software do go through a national filter, hence just rely on the words of the vendor for its trust worthiness and vigilance of the IT team or Medical equipment department, who in most cases do not have the necessary Cyber security knowledge but just basic IT knowledge.

" ...Not sure every medical device or hospital input is going thought the filter of the Estonian Health Fund.(No information to support the claim.) In other words, I don't know that this is happening." [4-4].

But also acknowledged that it is their role to ensure that these devices are checked for any vulnerabilities before being put to use.

"Yes, basically it is our role to ensure those vulnerabilities are taken care of these vulnerabilities. Probably some standards on security of medical devices should be put up in place so that all manufacturers meet up these standards."

However, even though software used are acquired from competent companies, the informants did not rule out the fact that nobody has ever bothered to check the software products that are being used for any malware or any defects. This comes from the fact that research has it that over 80% of java-built applications have bugs in them, and these applications are continuously used(38).

"Currently nobody checks the codes of software that is provided to us by these vendors. This is something that the department could consider in the near future, especially given the nature of data that is processed using these software" [3-4].

Also indicated by some of the informers was the high level of trust bestowed on the software company providers that one pointed out how great the provider is and the high level of effort the software provider puts in securing the software they do provide for the hospital.

"...Our main partner (Software provider) has quite a good priority and reputation on securing user layer. However, ourselves we do not have an application architect by name that we can boldly say e's role is to ensure that all applications we use are safe and do not provide harm to other assets that we have. But there is such a department, head of ID services and development but I do not know how they do it …. [3-3]"

One issue that disturbed the information security officers was the fact that at the moment they do not have a contingency plan towards any incidences of disk encryptions.

"One event towards which we do not have any contingency plan due to its low occurrence probability but with high impact in case it happens is when our hard disk space area is encrypted probably due to some firmware update that goes wrong….[4-4]."

4.4. Management.

On the issue of management, the informants however were pleased that their employers show interest in improving the cyber security status of the hospitals, however, it has been a challenge to get the management of the hospitals to support the security departments continuously, the behaviours are only on a reaction after an action basis.

"Currently my superiors have shown great endeavour towards improving the status-quo, and I can say this is mainly because of the recent hacks and ransomware that hospitals have been experiencing. We also meet up once in a month to have updates on current states cyber security state of the hospital. This encourages my office to always keep things in check..."[4-4]

"With the current state of affairs as regards to hospital hacking, we have been receiving a budget that is average to cater for 80% of our requirements. I can confirm that on a scale of 5, we receive 4 of our needs are met by our budget ..."[4-4]."

4.5. Challenges

Being an environment where everyone is busy, the researcher was informed that one major challenge faced is limited time on the side of the end users. Most physicians and nurses say they busy, so it becomes for the cyber security administrators to carry out continuous awareness campaigns.

"Being one of the major hospital in Estonia, our medical staff use the excuse of patient influx to avoid participating in any cyber security awareness campaigns. Most doctors who are the main user of computers especially in the hospital say they don't have time.. *[1-1]*

"*I am particularly disturbed by the people who ignore awareness campaigns. I prefer somebody who gives me wrong response then ignoring. However, I do understand that at times they are busy working on patients….*" *[2-4]*

Another challenge that the informants indicated was the isolation of the IT department in procurement procedures that included medical devises that required access to the network or that utilized the hospital networks. The informants reported that most of them have a medical devices department which includes medical devices engineers with little or no IT background. So, purchases of devices are made without much consideration of the effects it would have on the on the IT infrastructure.

"My biggest problem since then is that the hospital has IT department and medical devices Department, of which a lot of the medical device have their own servers. For a long period, the IT department maintained its own servers and I noticed the servers managed by IT are well managed, while those managed my medical devices guys have been poorly managed." [4-4]

But optimism for improvements have been shown as some hospitals are working towards involving the IT department in most decisions that require acquisition of devices or changes to the IT infrastructure.

"Well that can be improved to say, lately we have medical engineers asking for approvals from us, from example they will call and ask for approval to add something to the network. Am hoping to get to the point where Medical device engineers can call and say we are planning to purchase something and we need your input." [2-2]

"So, I have been trying my best to get those two departments to work together and agree and how the IT team can give the medical devices server administration tasks to IT team. But now since then, we are seeing progress and we have some projects where the two departments are cooperating together so that we can do away with medical devices engineers managing servers…" [4-4]

4.6. Attitude of users of IT systems.

During the investigations, the researcher was informed that in the current settings, the attitude and behaviour of system users was paramount and some of the informants had taken action towards changing user's mindset in line with good cyber hygiene practices.
This however has not been an easy task for some.
"Most of user, specifically medics, are a little much older, and hence they tend to think that they know everything and end up brushing off cyber security recommendations that we suggest to them…"As some point they prefer to remain analog, yet the main purpose is to make their

operations much smoother yet secure so that hospital assets do not end up on the dark web..." [1-1].

"Our system users, have been easy to deal with though especially with the current state of cyberattacks that hospitals have been experiencing. So they are really following up the guidelines that our department posts." [3-4].

4.7. Plans for Continuity and Future Preparedness.

As part of a continuity plan, some of the informants indicated a certain level of effort in pushing forward for the inclusion of facility employees into cyber hygiene awareness campaigns, though has not yet fully been effective due to the methods being used. They also showed their high level of trust in X-Road, the IT systems infrastructure of Estonia.

"...In the recent months, I have been pushing much on employees to be aware of what to do and continuously to do it so that their behaviours change so that security hygiene becomes a habit and part of life and not just only after some incident ..."[2-4].

"As I have come to learn that the technical side of security can easily be solved but when it comes to people, that is another level of its own hence, we will focus a lot of focus on that in the time to come" [3-3].

As regards to the data protection regulation (GDPR) a directive by the European Commission, the informants informed the researcher of how they are doing all that they can in order to be ready by May 25 2018 when GDPR comes into force, however there is also lack of confidence in their current status in relation to what is required by GDPR.

"...I have been waiting to see if the state data protection agency publishes some information, but yeah there is a lot of job to be done yet in order to achieve GDPR requirements..., but lately they have been actively publishing information out. So, I hope by then we will have enough information on which we can base to." [2-2]

"As the dates for GDPR comes closer, our lawyer has taken on the issue of personal identifiable data, who and how to communicate with people including data that include patient identifiable data. So, people know the risks and what to and not to communicate. This am sure will help us at some point in securing data as GDPR requires."[1-1]

"Part of our main plan is to continue working closely with RIA, and other partners." [1-4]

"A lot of data exchange from our side is performed with encryption and using ID cards and most of our communication and data exchange is through X-Road, so we can consider that as safe. So yes, we are confident on that. [1-4].

During the study, the researcher was informed of routine audits, however these audits are carried out on yearly basis.

"*As part of my plan for the hospital's security, we have tried to carry out yearly audits, as before I came, this was done depending on the moods within the departments and depending on how management feels*." *[4-4]*. While another respondent mentioned that their audits are basically done once every two years.

5. Discussions of main findings

Following the exploratory study and content analysis of the conducted interviews, assessed was the implementation of cyber security standard and measures undertaken by information security officers of various hospitals to safe guard Estonian Hospitals from cyberattacks. The core results of the study revealed awareness and competence levels among the various cyber security standards implementers, challenges in implementing cyber security standards in hospitals, management issues, attitude of general hospital employees towards cyber security and preparedness to cyber threats by the hospital information security departments.

All the information security departments of the various hospitals agree to the existence and use of ISKE as an information systems implementation standard at the hospitals. However, they also did acknowledge that the standards being implemented are generic, and basic, which means they do not entirely cover the health care sector which in its own setting is a much broad and complex ecosystem that involves different sectors and departments. Because of this complexity, the sector would greatly require implementation and integration of several standards, or the creation of specific standard unanimously covers the entire health sector as an integral system.

However, some informants indicated that implementation of ISKE is not mandatory, as they just identify only the measures they think are useful to them. This in the process, ignores the fact that partial implementing a security standard may render it less effective or weaken the measure as its dependency on another measure can be broken. ISKE as a standard is already outdated and the latest version was updated in 2017 January, of which during the year 2017, several cyberattacks were witnessed and some Estonian hospitals experienced interruptions to their daily operations due to these events.
The literature review regarding cyber security standards reveal that various security standards exist, however not all standards are suitable for the environments they are being implemented in. However, literature further reveals that standards are more effective if combined with other standards, hence this would be an opportunity for IT security personals to put into consideration.

Unlike some cases where specific standards like HIPAA have been implemented in hospitals to enable the protection of patient data from unauthorized access, the hospital IT teams agreed

that there is none like such being implemented but rather a mix of ideas and measures that one would think might be necessary basing on intuition and basic knowledge. Hence, need for the creation of specific Health cyber security standards that would deeply take into account the entire hospital ecosystem.

Just like health professionals have associations in which they share ideas and discuss polices that affect them, cyber security in hospitals require the same. Not just an electronic group mail on which notifications on attacks are received but rather a platform on which policies and revisions to security standards can be made as well as sharing ideas on from which even the most remote hospital can benefit from.
For example, instead of just implementing security standards made by individuals who have no connection at all with the health sector, from these associations would the best standards and security measures originate. This would also be an encouragement for the government regulatory body, RIA to get these groups together and come up with a healthcare sector leaning standards. This will not only be benefitable for the Estonian health sector, but also a form of revenue generating avenue. Instead healthcare organisations going to other countries to get certified, they would rather get certified in Estonia, using the Estonian healthcare cyber security standards.

Pertaining to the awareness of cyber threats and competence towards implementation of cyber security measures in hospitals, all the informants have shown high awareness and acknowledgment towards need for high technical skills in combating cyber threats.
The heads of the departments pointed out to the limited knowledge and manpower channelled towards cyber security at the hospitals. This is mainly attributed by the high salary scale needed to maintain inhouse cyber security professionals who are on high demand from different sectors hence, this leaves hospitals with less skilled cyber experts. Hence this would require management to specifically set a side specific funds just to cater for the procurement of specialist cyber security skillset either from individuals or specialized organizations.
The IT department heads further pointed out their concern on system users within the hospitals who of much of the time had been ignored and more emphasis was put on infrastructure. Acknowledged was that of recent most cyber vulnerabilities have been through the users, hence they would try to close that gap.

One major game changer suggested was regular cyber security drills and mock ups with employees to get them acquainted with cyber threats and how to avert them in their daily work environment.

Pertaining assets protection, a structural weak point within the hospitals was pointed out, and this concerned the separation of the medical devices departments from IT teams. This in some hospitals created conflicts in situations where medical devices departments managed their own servers yet needed to have access to resources on the networks being managed by the IT teams. Some of the hospitals however reported a move towards involvement of the IT teams on all procurement procedures of medical devices that required access to network within and out of the hospitals.

Hospital management needs to understand that spending alone does not always result into value, hence in the circumstances that prevention and remediation ever fails, they face unexpected costs beyond known values for not having been efficient in their cyber security mechanisms and frameworks. Eloquently understanding which assets must be protected, and what the repercussion will be for the hospital if protection fails, requires an intelligent security policy that builds resilience from within the IT department and outside the IT a hospital specific strategy that protects the entire healthcare sector.

Similarly, the more regular audits are in the hospitals, rather than the of once a year audits, the easier it will be to identify and report to concerned bodies before as cyberattacks now can occur any time.

Having input from several vendors, the Hospital information officers acknowledge that they do not have the necessary skill set to perform compliance checks on all products ranging from software to devices that are procured. Rather they put their trust solemnly into these private vendors. However, it is to be taken into consideration that these vendors themselves cannot fully certify that their products are fully compliant to cyber security requirements as stated by various standards that are implemented at the hospitals. Of course, this is a concern to them as well as there has already evidence of software code been misused by the vending companies to foster a cyberattack on victims though not in the healthcare sector for this matter.

As is the norm, hospitals are generally busy places and so are the personnel, specifically physicians, hence this makes it hard for the information security department to carry out trainings and cyber security campaigns to help promote cyber hygiene and awareness among physicians. This henceforth calls for more intuitive methods and ways to pass on awareness

skills without necessarily infringing on work, which in the end will change system users' mindset towards cyber security and taking it as more serious issue.

The fact that X-road already provides a high-level security as a platform on which data can be exchanged is a great achievement, however, this does not mean that hospitals should solemnly let down their guards. As this has been proved that a vulnerability can exist looking at the previously discovered flaw in the ID card security system of Estonia.

The study further revealed the need for openness about cyber security in general in the health sector as in any other sectors. Because the sector holds sensitive data on patients, issues to do with cyber security in hospitals is regarded as a secret in the hospitals that the study was carried, yet the more open hospitals are on this, more likely their weaknesses are to be discovered and fixed, than rather trying to cover it up and then discovered by a wrong party or hacker.

This was further witnessed during the recruitment process of participants. As much as resistance was met due to the limited communication capabilities, some would be potential participants cited concern about exposure of their weakness and possible exploitation, yet the study is meant to identify the loopholes for possible corrective measures.

Cyberattacks are evolving at a high speed with the execution modes varying frequently. It is sad to learn that most of the respondents have yearly audits despite the fact that cyberattacks have increase to more than 45 percent (39). Hence it would right and fitting for Estonian hospitals to create much more efficient audit routines that can easily identify any beaches while the effects of any such attacks are still minimal and can be contained.

To sum this up, the core of successful cyber security mechanism is to be able to point out and increase effort levels required to launch an attack on the higher-value assets of a hospital or any other organisation. Given the fact that regulations such as GDPR comes into effect May 2018, such assets carry mission critical value to the operations of a hospital for example patient data, medical devices, patient registrations general hospital operations and management of which some could be liable to the most strict and tough regulatory penalties once they fall victims of cyberattack. Hence, increasing the attack efforts on these assets makes it as difficult and costly as possible for attack vectors to achieve their motive, and minimize the resultant effects of their actions and vandalism if they do gain access.

5.1. Limitations of the study

Reflecting on the methods of the study and results, it is only right and fitting to consider the fact that there were also limitations and challenges that hindered the smooth flow and directing of the study.

Acknowledging from the numbers, the primary constraint to the study was the number of participants that took part in the study. This was a result of several factors, ranging cultural to individual factors. Some participants had very tight schedules hence they could not participate in the study. The number of informants in the study was limited to only four (4) out of planned (six) 6 and this could have greatly affected the outcome of the study as the more participants, the better the outcome. This could also have been attributed to the fact that there are not very many hospitals in Estonia, and the participating hospitals were considered the major hospitals. Adding to time constraints, the interview and interview invite were designed in English which is not a native language of both the researcher and the informants and hence, in a way this could have hindered participation of certain would have been informants.

Besides having an effect on the number of participants, the language of conducting the interviews could have had an effect on the responses as well as the informants could have responded in different ways for example by providing more information to the researcher if they were to express themselves in a language they were more comfortable with.

The other limitation to the study is in connection with recruitment of study participants. The study employed snowball sampling in enlistment of informants for both face-to-face interviews and email interviews. This however is believed to have created a selection and volunteering bias which limits the validity and quality of the sample, and this is one of the major concerns of snowball sampling research(40). The issue of bias has been the general problem in all epidemiological sampling designs as much as random sampling designs have the advantage of being grounded in a probabilistic theory, which provides a formal model of selection and selection bias, and with the practical tools to infer from sample to population (41).

From the participants involved, the study is believed to have been small scale and hence the qualitative data gathered is only recognized to be to be indicative of the vulnerability of certain hospitals and not Estonia in its entirety. Hence, not all areas of vulnerability were covered. Probably if a wider and more diverse population was covered, and not including only the heads

of the Information systems departments but other IT workers as well, probably more issues that require improvements as far as cyber security of hospitals would have been identified.
Besides conducting the study among the main hospitals, the results of the study could have been shaped differently if all hospitals both small regional participated in the study.

Naturally, resistance to the researcher was deemed to be met, given the fact that the researcher was I non-native carrying out a study on sensitive state matter. The informants were not used to being interviewed by a foreigner on such sensitive subject matter and hence those who ended up participating in the study, could have provided responses differently probably in case the researcher was not considered a foreigner.

5.2. Future Research

Considering the fact that hospitals hold massive and sensitive data on patients and/ citizens, cyber security of hospitals is paramount and firm action plan that covers all hospitals and their responsible parties need to be considered. Despite this study having been conducted in a less broad setting, it can be considered as a stepping stone in the formation of an all-inclusive public healthcare cyber security standards.
Basing on the findings of the study, the researcher recommends the next study that could be a follow up of this study, is one that aims at achieving a cyber security standard that wholly covers the hospital ecosystem while being easy to implement and fitting to the healthcare environment. This ecosystem would cover from patients, to hospital input vendors; these being software providers and medical devices.
An ideal standard that can be developed and adopted by these hospitals should at least cover three main areas:

- Ensure people, process and technology elements completely and comprehensively address information and cybersecurity risks consistent with their business objectives, including legislative, regulatory and best practice requirements
- Identify risks from the use of information by the hospital's business units and facilitate the avoidance, transfer, reduction or acceptance of risk
- Support policy definition, enforcement, measurement, monitoring and reporting for each component of the security program and ensure these components are adequately addressed

Another set of follow up research that could be adopted, is the development/design of a curriculum design that takes into account the need to impact cyber security skills and knowhow into healthcare facilities hence remove the burden or dependence on only IT cyber security professionals.

6. Conclusion

The aim of this study was to evaluate the cybersecurity vulnerability of Estonian hospitals. For this to be possible, the researcher had to analyse data collected from interview participants who were the "cream" of IT administration at the various participating hospitals.

The researcher would like to stress that the data collection was achieved through semi-structured interviews.

The results of the study revealed that that Estonian hospitals do not have specific standards but rather use generic information system security measures basing on intuition as mechanisms towards cyber threats, hence a high need for health-related cyber security standards that can be accepted and implemented broadly in these hospitals and in the wider spectrum of the healthcare sector.

The study revealed a high need to get cyber skillset into the healthcare sector. At the current situation, few cyber security specialists are interested with working at hospitals (health facilities) full time mainly due to less pay. However, hospital management needs to know that cyber security should not be treated as an IT issue/problem where by hospitals spend highly on governance, risk and compliance as a route to increase security, but rather a long-term hospital wide strategy that calls for spending that is appropriate to achieving the desired security potential and effectiveness which does not come in a short term, but rather long term. And the best way to achieve long term potential, is by investing in knowledge and skillset that can also be transferable. This in the long term will lead to a strong cyber security foundation in the hospitals.

Now that the healthcare sector health facilities in particular have proved to be soft cyberattack launch spot for attackers, the researcher calls upon the healthcare community at large not to only rely on compliance but enhance their cyber security portfolios which take into account extreme testing to single out vulnerabilities as government regulatory bodies alone cannot monitor or do all these kinds of work worse of all if these bodies themselves are just theoretical and not practical. For example, currently the state offers a Sandbox (42) where the health sector can easily engage into vigorous security testing before implementation of certain systems.

But for now, as long as hospitals do not invest where appropriate in brilliant cyber security basics, continue operating without specific cyber security standards, the chances of these loop holes being exploited by adversaries are still high and both patients and hospitals will continue paying the prices.

Appendix A. Invitation letter to participate in the study.

Request for participation in a study aimed at evaluating Cyber security standards deployed at Estonian Hospitals.

The vulnerability of hospitals to attacks of recent has been on the increase, which has called upon authorities to urge upon hospitals to strengthen their cyber security measures and frameworks. As a scholar of Healthcare Technology, I believe that cybersecurity is an important aspect of the hospital ecosystem and hence optimizing and re-enforcing this frequently is a high priority and a must by health/medical centers.

However, to ensure that this is achieved, monitoring and compliance checks have to be executed in order to evaluate the effectiveness of already implemented frameworks and standards.

As a Hospital Cyber security official, your expertise is sought, in order to find ways of enhancing the organization and compliance of cybersecurity of hospitals through sharing with your organizational procedures and experiences. Your opinion, suggestions, learned experience is of high value and so are your needs and preferences.

Your personality shall be provided unique number hence anonymized throughout the data coding and analysis process hence, your confidentiality is guaranteed. You will not be identified by name in any reports of the completed study. Audio recording will only be used to transcribe the interview. The researcher will be the only one retrieving and utilizing your data. The information acquired throughout this study will be available in a master's thesis research paper in reviewed and summarized form, however the data will be organized as summative data and your replies would be fully be private.

Hence, this letter is to solicit your willingness and consent to take part in this study, through participating in an interview that will last between 1-1:30 hours most preferably at your office, but also in case of any other hindrances, like distance and time, a skype call would also be convenient. Between the period of 21.11.2017- 15.10, in English language Please feel free to contact the principle investigator,

Contact Information:

Michael Anywar

Email: mianyw@ttu.ee Phone: +37253932917

Appendix B: Findings Analysis Table

Security Component	Overall Risk Rating	Analysis
Risk Level		
Remediation / Fix Level		
Assets Protection Level		
Assets Exposure Level		
Risk Monitoring Level		
Threat Monitoring Level		
Threat Analysis		
Incident Response and recommendations		

Appendix C. Interview Guide:

1) Do you believe that the cyber security standards and frameworks/policies that you implement at the hospital are effective enough.? (That incase there exists any)
2) Any specifics? Like In-house built, RIA or some other agencies or combined.?
3) Are there any specific points you consider more important in the policy?

Do you have any worries and concerns with the vulnerabilities and concerns that could be posed by the so-called assets you protect so much?

a) HIS
b) Medical Devices
c) Employees

- Amidst all the security concerns what are your priorities when carrying out your risk assessment and treatment process?

4) What is your contingency plan as per now to my colleague who just dropped a 10GB USB flash drive labelled Regionaal haigla in the hospital corridor?
5) Do you have any concerns about rogue employees employed by a company whose Software you deployed at the hospital? Any specific body that certifies these software (security wise) and apps before deployment in the hospital? (Static Code Checks)
6) Since the Hospital Uses software / apps developed by single vendors/ different, how do you ensure that the systems you use are up to date and are secure. Talk of the ID card certificates that were cancelled by RIA. How did you as the CIO of the hospital react to that.
7) How about a heavy duty medical device used inside the hospital that uses custom software that is based on XP for its User interactivity? Do you still have such in the hospital? If you do, aren't you worried about their safety?
8) When implementing your policies, do you have any specific targets or objectives? Or it is because the law requires the hospital to do so.
9) Are you comfortable taking about your Implementation strategy of these policy(ies).
10) How often do you as the CTO of the hospital meet up or communicate with the people that interface with the assets you protect(guard)?
11) Do you have a Special Budget from the Hospital allocated to Security? Resources? Are these resources (budget enough)? From Personnel to continuous knowledge update?
12) Do you carry out staff education/ awareness programs.? Mocks on security?
13) Have you got any improved capabilities (processes, tools and coordinating structures); Actions and emergency response plans out of these awareness, or it is business as usual.

14) How often do you communicate and make sure your Policy is received by all your targets and implemented?
15) Under what circumstances do you communicate? DO you document these communications?
16) How often do you document? Any trends in your documentation that shows probably action is required at some stage in your already implemented policies? Or only when everything is okay.
17) How often do you carry out risk assessments and Audits plus ensuring your measures remain effectiveness?
18) Is this performed Internally? Or some International independent organisation like RIA, Deloitte?
19) This year alone, 2017 do you have any rough figures of the number of perform corrective actions performed? e.g
20) What are the biggest barriers your organisation faces to remediating and mitigating cybersecurity indicants? (Please select all that apply)
21) You have an equipment's department that recommends hospital equipment to purchase, in doing these recommendations does the CTO/ CIO also sit on this panel especially when devices or equipment to be purchase are networked medical devices?
    Any bad past experience with these devices?
22) What is your contingency plan for such new devices that are acquired by the hospital to mitigate any risks and attacks.
23) What is your most feared risk? Any specific response plans?
24) Do you profile your targets by any assets/ vulnerabilities by any chance?
25) Am sure during your risk mapping you have controls that have been effective for you. What do you consider as your most effective control to manage the hospital's information security risks? Practices, policies, programs, tools. DO you think you can rely on the same in the next 2-3 months?
26) How often if you really do, assess the effectiveness of your policies, do you review them? What is the lifespan of an implemented policy.
27) Do you as a Hospital cooperate with other organizations to improve your security besides RIA and Cybernetica? Or none.
28) How often do you hold Management/department meeting and stand ups? Or these are only triggered by an event.

29) In the process of performing all the activities mentioned, do you think these have been effective enough to secure the hospital?
30) What would you do better than what you have been doing now. Or would you continue operating the same way?

Picks:

How confident are you that the security protocols or architecture built inside your hospital's devices adequately protects clinician users and patients?

Is your hospital ready to implement GDPR?

What cyber threat intelligence sources do you rely on most to get information about the issues facing your organization?

Are you in position to quantify your level of effort in securing the Application layer at the hospital?

Michael Anywar
HealthCare Technology
Tallinn University of Technology Thesis Interview Questions. Autumn Semester 2017.

Reference:

1. Annual Cyber Security Assessment 2017 Estonian Information System Authority. [cited 2017 Oct 6]; Available from: https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF
2. Ehrenfeld JM. WannaCry, Cybersecurity and Health Information Technology: A Time to Act. Vol. 41, Journal of Medical Systems. 2017.
3. Infosüsteemi R. RIA kuberturvalisus -2018. Annu Rep [Internet]. 2018 [cited 2018 Apr 25]; Available from: https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf
4. Ministry of Economic Affairs and Communication. Cyber Security Strategy 2014-2017. 2014 [cited 2017 Oct 6];13. Available from: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
5. Le Bris A, Asri W El. STATE OF CYBERSECURITY &; CYBER THREATS IN HEALTHCARE ORGANIZATIONS Applied Cybersecurity Strategy for Managers. ESSEC Bus Sch [Internet]. 2017 [cited 2017 Oct 5];13. Available from: http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf
6. Check Point Research. MID-YEAR REPORT. Check Point Res [Internet]. 2017 [cited 2017 Oct 6];19. Available from: http://fr.security.westcon.com/documents/56775/2017-cyber-attack-trendswp.pdf
7. Erin Dietsche HI& CR. 12 Healthcare Ransomware Attacks of 2016 [Internet]. 2016 [cited 2017 Oct 19]. Available from: https://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html
8. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: A Complex Environment and Multifaceted Problem. Med Devices (Auckl) [Internet]. 2015 [cited 2017 Sep 24];8:305–16. Available from: http://www.ncbi.nlm.nih.gov/pubmed/26229513
9. Elinor Keshet. SMART Hospitals [Internet]. 2013. Available from: https://www.encorewiki.org/display/KMDI2003/SMART+Hospitals
10. SANS GSEC Practical Assignment Version 1.4b Option 2 Administrivia version 2.7 Pre-Approval Submission. 2003 [cited 2017 Dec 13]; Available from:

https://www.sans.org/reading-room/whitepapers/hipaa/developing-implementing-information-security-policy-standard-framework-1401

11. SOPHOS. Why cybercriminals attack healthcare more than any other industry – Naked Security [Internet]. 2016 [cited 2017 Oct 19]. Available from: https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry/
12. Falessi N, Gavrila R, Klejnstrup M, Moulinos K. National Cyber Security Strategies. Practical Guide on Development and Execution [Internet]. European Network and Information Security Agency (ENISA). 2012. 15 p. Available from: http://www.enisa.europa.eu
13. Thycotic. The 2017 State of Cybersecurity Metrics: Annual Report. Most companies failing at cybersecurity metrics. 2017 [cited 2017 Oct 6];(1). Available from: https://thycotic.com/wp-content/uploads/2013/03/2017-Cyber-Security-Strategy-Metrics-Report.pdf
14. Starr S. Moving from evaluation to assessment. J Med Libr Assoc [Internet]. 2014 Oct [cited 2017 Oct 7];102(4):227–9. Available from: http://www.ncbi.nlm.nih.gov/pubmed/25349539
15. UK Governement Inter-Ministerial Committee for Cyber Security. National Cyber Security Strategy; 2016-2021. 2016;
16. Muckin M, Fitch SC. A Threat-Driven Approach to Cyber Security. Lockheed Martin Corp [Internet]. 2016 [cited 2017 Oct 7]; Available from: http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven Approach whitepaper.pdf
17. 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 (Gen. EU [Internet]. 2017 [cited 2017 Dec 8];88. Available from: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
18. ICO. Guide to the General Data Protection Regulation (GDPR). 2017 [cited 2017 Dec 14]; Available from: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
19. Nima Baiati. How does GDPR impact the healthcare sector? | The Horizons Tracker [Internet]. 2017 [cited 2017 Dec 14]. Available from: http://adigaskell.org/2017/02/04/how-does-gdpr-impact-the-healthcare-sector/

20. ISO. ISO 27799:2016(en), Health informatics — Information security management in health using ISO/IEC 27002 [Internet]. 2016 [cited 2017 Dec 14]. Available from: https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en
21. Für Sicherheit in der Informationstechnik B. BSI-Standard 100-2 - IT-Grundschutz Methodology. 2008 [cited 2017 Oct 7]; Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1
22. Estonian Security System Overview. [cited 2017 Dec 14]; Available from: https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf
23. Eesti Haigekassa. Digital Prescription | Eesti Haigekassa [Internet]. 2015 [cited 2017 Oct 7]. Available from: https://www.haigekassa.ee/en/digital-prescription/
24. Ttust Service Principles, Criteria, and Illustrations TSP Section 100 Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. [cited 2017 Oct 7]; Available from: http://www.webtrust.org/principles-and-criteria/item27818.pdf
25. USA Health & Human Services. Compliance Assistance O C R Privacy Brief: Summary of the HIPAA Privacy Rule. 2012 [cited 2017 Oct 7];19. Available from: https://www.hhs.gov/sites/default/files/privacysummary.pdf
26. United Sates Department of Health & Human Services. Summary of the HIPAA Privacy Rule; HIPAA Compliance Assistance. [cited 2018 May 7]; Available from: https://www.hhs.gov/sites/default/files/privacysummary.pdf
27. HSS. Gov. Summary of the HIPAA Security Rule | HHS.gov [Internet]. [cited 2017 Dec 16]. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
28. Department of Health and Human Services UG. Health Insurance Reform: Security Standards; Final RUle. VerDate Jan<31>2003 [Internet]. 2003 [cited 2018 May 7];17(19). Available from: http://
29. Absolute Healthcare Whitepaper. What Healthcare Organizations should Know about the GDPR. ABSOLUTE [Internet]. 2018 [cited 2018 May 7]; Available from: https://www.whitepapers.em360tech.com/wp-content/uploads/GDPR-Implications-of-the-GDPR-in-Healthcare-042717-d1.pdf
30. BSI. BSI-Standard 100-3. Bundesamt für Sicherheit der Informationstechnik [Internet]. 2013 [cited 2018 May 7];2.5. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/s

tandard_100-3_e_pdf.pdf?__blob=publicationFile
31. Bundesamt für Sicherheit in der Informationstechnik. BSI: IT-Grundschutz catalogues - 13th version 2013 [Internet]. [cited 2018 May 7]. Available from: http://enos.itcollege.ee/~valdo/bsieng/en/gstoolhtml/allgemein/einstieg/01001.html
32. Framework for Improving Critical Infrastructure Cybersecurity. 2017 [cited 2017 Oct 7]; Available from: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf
33. ISO. ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements [Internet]. 2013 [cited 2017 Oct 7]. Available from: https://www.iso.org/standard/42103.html
34. Newton N. Exploring Qualitative Methods: The use of semi-structured interviews. Explor Qual Methods [Internet]. 2010;1–11. Available from: http://www.academia.edu/1561689/The_use_of_semi-structured_interviews_in_qualitative_research_strengths_and_weaknesses
35. Ritchie J, Lewis J. QUALITATIVE RESEARCH PRACTICE A Guide for Social Science Students and Researchers. [cited 2018 Apr 12]; Available from: https://mthoyibi.files.wordpress.com/2011/10/qualitative-research-practice_a-guide-for-social-science-students-and-researchers_jane-ritchie-and-jane-lewis-eds_20031.pdf
36. Bolarinwa O. Principles and methods of validity and reliability testing of questionnaires used in social and health science researches. Niger Postgrad Med J [Internet]. 2015;22(4):195. Available from: http://www.npmj.org/text.asp?2015/22/4/195/173959
37. Judith Green & Nicki Thorogood. Qualitative Methods for Health Research. Igarss 2014. 2014;(1):1–279.
38. Serious bug in widely used Java app library patched | InfoWorld [Internet]. [cited 2018 Apr 9]. Available from: https://www.infoworld.com/article/3005577/security/serious-bug-in-widely-used-java-app-library-patched.html
39. Ponemon Institute and Accenture. 2017 Cost of Cyber Crime Study. 2017 [cited 2018 Apr 24];56. Available from: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
40. Atkinson R. Accessing Hidden and Hard-to-Reach Populations: Snowball Research Strategies. Soc Surrey [Internet]. [cited 2017 Oct 20];(33). Available from: http://sru.soc.surrey.ac.uk/SRU33.pdf

41. Hendriks VM, Blanken P, Nico Adriaans PF. SNOWBALL SAMPLING: A PILOT STUDY ON COCAINE USE. [cited 2018 Apr 24]; Available from: https://www.researchgate.net/profile/Peter_Blanken2/publication/284700725_Snowball_sampling_Theoretical_and_practical_considerations/links/57a5b76a08ae3f45293198af/Snowball-sampling-Theoretical-and-practical-considerations.pdf
42. Riigi Infosüsteemi Amet. Cuckoo Sandbox [Internet]. 2018 [cited 2018 Apr 25]. Available from: http://cuckoo.cert.ee/