AALTO UNIVERSITY SCHOOL OF ELECTRICAL ENGINEERING

Anna Torvinen

DEVELOPMENT OF INFORMATION SECURITY SERVICES FOR FINNISH HEALTHCARE ORGANIZATIONS

Thesis for Master of Science degree has been submitted for approval on October 10th 2011 in Espoo, Finland

Supervisor

Professor Raimo Sepponen

Instructor

MSc. Ari Mikkola

Abstract of the Master's Thesis

AALTO UNIVERSITY SCHOOL OF ELECTRICAL ENGINEERING
Author: Anna Torvinen

Name of the thesis: Development of information security services for Finnish healthcare organizations
Date 10.10.2011
Number of pages: 55+32

Department: Electronics
Professorship: Applied electronics

Supervisor: Professor Raimo Sepponen
Instructor: MSc. Ari Mikkola

In healthcare information has to stay confidential and unchanged, but when needed it must be available in a short notice.

The purpose of this study is to get familiar with the current and prospective state of information security in healthcare. Based on the findings, we define what kind of information security needs healthcare has, and how Fujitsu could best respond to these needs and develop its information security services. In this research we also take a look at the information security services of one hospital district which is a customer of Fujitsu.

To reach the goals we have taken a literature research, during which we learned about legislation of health information, KanTa project and information security methods. We also interviewed specialists of information security, healthcare and sales about the current situation and future visions of healthcare information security.

Based on these findings we presented solutions on how Fujitsu could enhance the information security of healthcare overall, and how it could develop its own services and practices.

Solutions could be, for example, a tighter cooperation with healthcare organizations, finalizing of information security services, highlighting the financial benefits of information security, development of internal information security, and creation of healthcare information security concept.

Keywords: Information security, privacy, healthcare, KanTa projects, electrical prescription, electrical patient information archive, legislation, East Savo hospital district, Fujitsu Finland Oy, information security services, healthcare information systems

Diplomityön tiivistelmä

AALTO-YLIOPISTO SÄHKÖTEKNIIKAN KORKEAKOULU
Tekijä: Anna Torvinen
Työn nimi: Suomen terveydenhuollon organisaatioille suunnattujen tietoturvapalvelujen kehittäminen
Päivämäärä: 10.10.2011
Sivumäärä: 55+32

Laitos: Elektroniikan laitos
Professuuri: Sovellettu elektroniikka

Työn valvoja: Professori Raimo Sepponen
Työn ohjaaja: DI Ari Mikkola

Terveydenhuollossa tietojen on pysyttävä luottamuksellisina ja yhtenäisinä mutta tarvittaessa niiden on oltava nopeastikin saatavilla.

Tämän työn tarkoituksena on tutustua terveydenhuollon tietoturvan nykytilaan ja tulevaisuuden suuntauksiin. Näiden pohjalta arvioidaan, millaisia tarpeita terveydenhuollolla on tietoturvan suhteen ja miten Fujitsu voisi kaikkein parhaiten vastata näihin tarpeisiin ja kehittää omia tietoturvapalveluitaan. Tutkimuksessa perehdytään myös erään Fujitsun asiakkaan, suomalaisen sairaanhoitopiirin, tietoturvaratkaisuihin.

Tavoitteiden saavuttamiseksi on tehty kirjallisuustutkimus, jossa on perehdytty muun muassa terveystietoja koskevaan lainsäädäntöön, KanTa-hankkeeseen ja tietoturvamenetelmiin, sekä haastateltu tietoturvan, terveydenhuollon ja myynnin asiantuntijoita terveydenhuollon tietoturvan nykytilasta ja tulevaisuuden näkymistä.

Näiden tietojen pohjalta on esitetty ratkaisuehdotuksia siihen, miten Fujitsu voisi osaltaan parantaa terveydenhuollon tietoturvaa ylipäätään, sekä miten se voisi parantaa omia palveluita ja käytäntöjään.

Ratkaisuina voisi olla esimerkiksi tiiviimpi yhteistyö terveydenhuollon organisaatioiden kanssa, tietoturvapalveluiden viimeistely ja hyötyjen taloudellinen korostaminen, organisaation oman tietoturvan kehitys sekä terveydenhuollon tietoturvan kokonaiskonseptin luominen.

Hakusanat: Tietoturva, tietosuoja, terveydenhuolto, KanTa-hanke, sähköinen resepti, sähköinen potilastietoarkisto, lainsäädäntö, Itä-Savon sairaanhoitopiiri, Fujitsu Finland Oy, tietoturvapalvelut, terveydenhuollon tietojärjestelmät

Preface

This master's thesis project was carried out at Fujitsu Finland Oy in Helsinki, and was part of Master of Science degree at Aalto University School of Electrical Engineering.

First of all, I want to thank Fujitsu for offering this great opportunity to take a deeper look at information security of healthcare sector. Learning of new things, which were not so familiar to me in advance, was fascinating.

Thank you, Ari Mikkola, for encouragement, patience and comments which showed deep understanding of the field.

Thank you, Raimo Sepponen, for interesting meetings and good advices.

Thank you, Petri Heinälä, my superior, for support and trust.

Thank you, all the experts I interviewed during my research. Each interview opened my eyes to see the field from different point of view.

Anna, your peer support and pressure have been priceless. The lunches during the days in silent library have been a pleasure. For Katri and Anna, thank you for the sauna evenings when the topics of discussions were not related to studying at all.

Uku, dear, thank you for being so understanding and listening my long thesis related monologues at home. And thank you for all the support during the making of this thesis, and during all my university studies.

My dear family, thank you for all the support you have given me during my long career of studying and life. Without your support, I wouldn't be here.

In Espoo, 10th October 2011

Anna Torvinen

Contents

Pictures

Abbreviations and symbols

ATM	Automatic Teller Machine
Carea	Kymenlaakson sairaanhoito- ja sosiaalipalvelujen kuntayhtymä, Kymeenlaakso Social and Health Services
CIA	Confidentiality, integrity and availability – basic terms of information security
CMM	Capability Maturity Model
Eksote	Etelä-Karjalan sosiaali- ja terveyspiiri, South Karelia District of Social and Health Services
epSOS	Smart Open Services for European Patients - the European eHealth Project
ERR	equal error rate
FAR	false acceptance rate
FRR	false rejection rate
GPS	Global Positioning System
HL7	An organization involved in development of international healthcare informatics interoperability standards
h1-h10	Refers to the number of an interview
IAM	Identity and Access Management
ICT, IT	Information and communications technology, Information technology
IdM	Identity Management
ISSHP	Itä-Savon sairaanhoitopiiri, Hospital district of Itä-Savo
KanTa	Kansallinen Terveysarkisto, National archive of health information
PACS	Picture archiving and communication system
PC	Personal Computer
PIN	Personal Identification Number
R-Bay	eMarketplace for radiology
RFID	Radio-frequency identification
ROI	Return On Investment
SHQS	Social and Health Quality Service quality recognition
SSO	Single Sign-On
VPN	Virtual Private Networks
WLAN	Wireless Local Area Networks

“- - Whatever I see or hear in the lives of my patients,
whether in connection with my professional practice or not,
which ought not to be spoken of outside,
I will keep secret,
as considering all such things to be private. - -”

(The Hippocratic Oath) (1)

1. Introduction

1.1. Background and motivation

Confidentiality is one of the backbones of physicist's ethics. If patient cannot feel comfortable to tell his doctor even the most sensitive facts of his health, the quality of the treatment can suffer. A main rule of the relationship between the doctor and a patient is that the doctor cannot, without consent, forward any information related to his patients and their treatments to outsiders. Physicist's obligation to confidentiality continues even after the duty or occupation ends. (2) This is one of the reasons why information security is so vital in healthcare.

For most of the people information security is just a bunch of passwords, and a firewall and antivirus software in their computer. But for people working with information security, it is much more – overall safety, technical solutions, quality, minimizing risks, processes, psychological issue and state of mind.

If we had to explain information security using just three words, those would be confidentiality, integrity and availability. These words mean that only right persons can have access to information which is kept unchanged and is available when needed. (3) (4)

In healthcare information security is noticed especially when it's missing. At the present time information security in healthcare organizations has stimulated a lot of discussion. Following headlines are recent examples: "Power cut in Mikkeli central hospital caused extensive damage to property" (5), "Extensive patient data phishing was revealed in Helsinki" (6). Both incidents might have been able to prevent with better risk assessment.

At the moment, KanTa (Kansallinen Terveysarkisto – National archive of health information) projects are implementing electronic prescription in to our society. National patient information archive and a portal, where patients can view their own information, are coming soon. These projects bring additional requirements for the information security of healthcare and patient data privacy. Patient has to be able to trust his doctor and the whole healthcare infrastructure all the time. Many organizations haven't got as much sensitive customer information as healthcare has. (7)

Information security isn't the only motivator for organizations to invest for information security services. For example, identity management system enhances information security in the organization, but also makes the work more cost-effective (8). Especially now, when the world economics isn’t flourishing, money and cost-efficiency are big motivators.

In the near future of Finland, the percentage of pensioners will get bigger and the percentage of tax payers smaller (9). This will create challenges for the healthcare as the personnel-patient-ratio will decrease. Luckily, information technologies (IT) can be utilized to make the work more effective. On the other hand, the role of information security will become more important as information is moved to electronic form.

Healthcare organizations are one of the customer sectors of Fujitsu. The services in this sector are mainly related to IT infrastructure and support services, like information security services. However, these information security services are not tailored particularly to respond to the needs of healthcare organizations. Also the selling of the information security services is perceived as challenging.

The purpose of this thesis is to find out how Fujitsu should develop the information security services to better respond to the needs of healthcare, and how to market the services in an effective, healthcare oriented way. An additional question is how the processes, practices and marketing of Fujitsu could be developed? That is why we explore the current situation and the future prospects of the healthcare to see what kind of needs of information security healthcare has. We use one healthcare district as a good example of well managed information security concept. Later, we will take a deeper look at their information security solutions.

1.2. Structure of the thesis

To obtain our goal, we need first to get familiar with what kind of organization Fujitsu is. Then we take a peak to the hospital district of East-Savo (later referred as ISSHP, Itä-Savon sairaanhoitopiiri), whose information security is one of the best managed among all Finnish healthcare organizations.

Then we describe the basic idea and the most important concepts and terms of information security. What do confidentiality, integrity and availability mean? Which are the methods of identification and authentication? How are identities and access managed? How access can be controlled?

After this we know the idea of information security generally and it’s time to get familiar with the current status of healthcare IT in Finland. First, we summon up how the healthcare field is changing at the moment, and give some forecasts how it will change in the near future. Because healthcare is strictly regulated, we take a look at the Finnish legislation about health information, specially its security aspects. We also take a glance to information security management process in healthcare organizations.

Since national KanTa project is causing big changes in Finnish healthcare, we want to know what it covers, and what kind of affects does it have to healthcare in general and healthcare information security in particular. We also need to know what are the main features and the biggest problems in healthcare information security.

At this point, we understand the aspects of both information security and information security in healthcare. Then we learn what kind of information security concept ISSHP has, and are then able to move from theory to practice, the research part of this thesis.

The research is performed with interviews of ten specialists of information security and/or healthcare IT. The questions are related to the current problem areas of healthcare information security. What makes the information security concept of ISSHP so successful? Why the selling of information security services is so hard? And what are the future needs of information security in healthcare?

Then we can pull all the results together, and see the most problematic areas and reasons for those. Then we suggest what could be done to make the services and activities of Fujitsu better and more suitable for healthcare organizations now and in the near future.

1.3. Target Company: Fujitsu Finland Oy

Fujitsu is an international ICT-based (Information and communications technology) business solution provider with circa 170 000 employees in 70 countries. For its customers Fujitsu offers different kind of computing and communications systems and advanced microelectronics. Fujitsu was based on 1935 and its headquarters is located in Tokyo. Fujitsu gets about two thirds of its net sales from Japan and 15 % from Europe. (10)

In Finland Fujitsu is one of the leading ICT service and hardware suppliers employing 2900 people. In Finland Fujitsu is concentrated mainly on business ICT services. Patja ICT infrastructure services and Sohva application services are two main products. These services cover the whole spectrum of computers from laptops to data center solutions. (10)

Patja is an operations model, in which Fujitsu takes care of customers ICT infrastructure covering all customers work stations, servers, printers and mobile phones. Patja consists of different services from which the customer can choose those ones he needs. The service guarantees that the processes and information security are all up to date and well sized. By optimizing the needed hardware and services, the costs of ICT are reduced. (10)

Sohva is an application partnership, in which customer's applications are taken care by Fujitsu. Fujitsu is responsible for developing, managing and supporting the application. (10)

"Would half give you more" is a vision for optimizing customer's ICT. With optimization the areas, in which quality and efficiency can be enhanced, are found. Optimization areas are for example devices, data centers and service models. The ways to do the optimization are for instance cloud services, virtualization, printing management, modern communication solutions and self-service of end users. (10)

With several services Fujitsu has different purchase models for customer to choose the way for buying the service. With Customer solution model the customer purchases and owns the licenses and hardware by himself. With Hosting model the environment along with the licenses is owned by the customer or Fujitsu. Costs are based on monthly charge. With Full service model the customer pays to Fujitsu for using the service. Fujitsu maintains and manages the service. (10)

1.3.1. Information security services

Fujitsu has a wide range of information security services from consulting services to anti-virus services. Here is presented some of them to get a view of the variety.

Examples of consulting services (10):

- **Risk analysis and management** analyses the risks in customer's organization and plans how those could be managed.
- **Information security survey** finds out the customer's current state of information security.
- **Information security policy development** covers the whole organization and has a view, approved by the management, about information security objectives, principles and implementation.
- **Security auditing** determines customer's information security level.
- **Trim-service** educates customer's personnel to use work practices, which don't jeopardize information security.
- **Preparing for certification consulting** aims to remove the obstacles for certification by comparing customer's security practices to standards.
- **Disposal of electronical information** is necessary for example when the user of a workstation changes. After programmed information disposal the computer is fully operational again.

Examples of other information security services (10):

- **Enterprise Single-Sign-On Service** helps to log on to applications without typing username and password every time, because it stores users' credentials.
- **Identity Management Service** provides the means for centralized management of user identities, the information that different systems need of them and role-based management of access rights and enforcement of authorization policies. It collects all the information to one place and helps to keep that information up to date automatically.
- **mPollux Authentication Services** add strong authentication and control of access control to different information systems and services. For example with CallSign technique user identifies himself with his mobile phone.
- **Workstation Encryption Service and Anti-Virus service** are centrally managed solutions which include the licenses for workstation encryption software and anti-virus software.
- **Certificate Service** implements and manages the certificates used by asymmetric encryption methods.

1.4. Target Organization: ISSHP

ISSHP is the smallest hospital district in Finland. It consists of one hospital and six healthcare centers. The district belongs to the tertiary care group of Kuopio University Hospital. The population of Itä-Savo area is about 46 000. ISSHP has 750 employees and it is an IT pioneer among all the hospital districts of Finland. (11)

ISSHP has gained Social and Health Quality Service (SHQS) quality recognition for several times since the year 2001 (12). This recognition requires that certain structural and process criteria are met. Also risk management and security has to be ensured. For example, risk management has to be coordinated, risks have to be recognized and analyzed, accidents have to be reported, and employees' health has to be taken care of. (13)

ISSHP fulfills the high level of information security (14) defined by the Ministry of Finance. The scale contains five levels – open level, basic level, elevated level, high level and special level. In high level, information security processes are documented and measured. (15) The information security concept of ISSHP will be described in detail in chapter 3.6 Information security concept of ISSHP.

2. Information security

2.1. What is information security?

Our information society has moved to internet. Electronic services, e-services, make our life much easier. You don’t have to queue to a bank to pay a bill or wait for ages to get a response to your letter. You just go to web bank or send an e-mail. But the coin has two sides, because along comes a higher possibility for information ending up in wrong hands. Consequences can be unpleasant. (3) What if that information were your health records? You wouldn’t be the first one having that experience. We need information security!

Information security is a wide field of science the main task being to prevent risks related to the confidentiality, integrity and usability of information, information systems and telecommunication (3). Information privacy, on the other hand, means that the private and personal information of the people is protected from unauthorized use (4).

Usually, information security can be quite hard to ensure perfectly, because the defender has to find and analyze all weaknesses in the system, and prepare for all possible risks (4). One weakness can make all the other protections useless because the information security level of the organization is as strong as its weakest part (3).

Information security isn’t just technical solutions which can be found from stores. It forms also from internal confidence, right procedures, training and caution. It is said that information security is only 20 percent of technology, and the rest 80 percent is psychology. (4)

To help you to understand the variety of information security we have divided different security methods to own categories. This categorization makes security planning, implementation and controlling easier. Here is one way to categorize: (16)

1. **Administrative and organizational security** – activities related to security management
2. **Personnel security** – minimizing risks related to personnel
3. **Data security** – securing data of different formats
4. **Software security** – management of security features in operating systems and applications
5. **Hardware security** – managing security features in equipment
6. **Telecommunications security** – maintaining confidentiality, integrity and availability during and after the transfer of information

7. **Operations security** – affecting users' behavior to assure good quality of work and minimize incidents
8. **Physical and facilities security** – securing the work environment from physical threats and accidents

In a healthcare organization all these categories are very important, but data and telecommunications security are maybe the most essential ones concerning the privacy of information.

2.2. Information security terms

To understand the concept of information security thoroughly we should be familiar with the basic terms of information security. Information security can be divided into three different main concepts – confidentiality, integrity and availability. This is sometimes referred as a CIA concept. These and other important terms of information security are underlined in this chapter.

Confidentiality means that the information is available for only those who have the right to read and edit the information (4). Those persons have to have an authorization. We have to define who is authorized to read each piece of information. Thus we need to classify the information into public or secret information. Secret information can be divided again for example to top-secret, secret and confidential information. In addition, we need to identify and authenticate the users and manage privileges. (3) A separate chapter will discuss more about the methods of identification and authentication.

Integrity of information requires that the information doesn’t change due to the defects in the programs and systems, or due to corruption. Information shouldn’t either be exposed to manipulation. To detect the changes it’s important to attach the name of the author and the time stamp of creation to the information. (3) The stamps give undeniable evidence that the action has been done, and the principle of non-repudiation is obeyed. Technically non-repudiation is proved by using digital signature. If the changes are done by the system, the right term is system or organization signature. (3)

Availability means that the information is available when needed and where needed. Information systems must work properly, and the accessibility has to be ensured. Possible malfunctions have to be taken care of by building security mechanisms. For example hospital information systems have to be up all the time, but regular office systems are needed only during the office hours (4). Usability is a synonym both to availability and utility, which means that the information is saved in a readable and understandable format. For example the information shouldn’t be saved in a format, which is no more used. With physical access control the entrance to the place, where information can be accessed, is either allowed or blocked. (3)

Logging, auditability and accountability refer all to logging the actions done in information systems, following the use of systems and information, and controlling it. Every action has to leave a trail, what has been done, who has done, and when it is done, to be used later in tracking. (3)

2.3. Methods of Identification and Authentication

Confidentiality requires users' identification and authentication, by which the users can be first recognized (identified) and then verified (authenticated). In addition to human user, the user can be also a device, an internet service, or a program. (4)

We use authentication processes many times a day even without noticing. We authenticate our friends based on their appearance or voice, when we see or speak with them. In email authentication is based on the sender's address, but this method is very unsecure, because it's easy to fake. If digital signature is added to e-mail, the sender information becomes more reliable. (4)

Authentication requires that the object has some unique features. Generally we use three different feature sets. (4)

1. Something we are
2. Something we have
3. Something we know

Finnish law about "Strong digital identification and signatures" (17) requires that for the identification to be strong, at least two of the methods above are used.

Next three chapters are dedicated to explain those methods above in more detail, but there are also other minor methods existing. We present two of those minor ones shortly, before heading to the three main ones.

What we do refers to some mechanical task, which we perform in a way that is both repeatable and specific to us. For example handwritten signatures have been used for ages in banking to confirm the identity of people signing cheques and credit card payment slips. Handwritten signature is relatively easy to fake. To increase the security of written signature we can use special pads, which measure the pressure and speed we use in writing. Speed measure and intervals can be also used, when writing password with a keyboard. (18)

Where we are means that when we log in the system takes into account our location, like the terminal we log on from. For example a system manager could only log on into a system from an operator console. With mobile devices and GPS (Global Positioning System) users' location can be used to resolve later disputes about the true identity of that user. (18)

2.3.1. Something we are

Something we are refers to our physical characteristics, like our appearance, voice, fingerprint, iris patterns, hand geometry or even DNA (4) (18). If that feature is authenticated by using a technology, we discuss about biometric identification. (4)

Biometrical methods must have at least following properties (19):

1. Universality - Every person should have the characteristic
2. Uniqueness - No two or more persons should be the same in terms of characteristic
3. Permanence - Characteristic should be invariant in time
4. Collectability - Characteristic should be quantitatively measurable

Let's use fingerprint as an example from how biometrical authentication works. At first, we need samples of the user's fingerprint to form reference template. To get higher accuracy, we can record multiple templates from several fingers. Templates are stored into a database. This process is called enrollment. When we want to log on using our fingerprint, new reading of our fingerprint is taken and compared to reference templates in the database. (18)

There are two purposes for which biometric schemes are used (18):

1. In identification the user is compared to database of multiple persons.
2. In verification the user is matched to templates of the person, he says he is.

Biometric identification isn't as clear method as e.g. password. There are no simple yes-or-no-answers. The stored reference template will hardly ever match precisely to the current measurement. That is why we need a matching algorithm to count the similarity between the two templates, and check if they are above a predefined threshold. Threshold setting will lead us to new problems: false positives and false negatives. Thus we can calculate *false acceptance rate* (FAR, a person is identified as another person) and *false rejection rate* (FRR, a legitimate user is rejected) to each algorithm. The threshold setting is always a tradeoff between FAR and FRR. The optimal threshold value is obtained in the point where FAR and FRR are equal. This is referred as e*qual error rate* (ERR). With ERR we can compare different biometrical methods. For example the ERR of iris pattern recognition is smaller than the ERR of fingerprint, thus iris pattern recognition is more reliable method. (18)

2.3.2. Something we have

Something we have refers to a physical token like a key, an identity card, or a debit card. (4) The greatest weakness of tokens is that they are easy to lose or steal. Anyone, who has the token, has the same rights as the legitimate owner. Therefore, we usually use “something we know” in combination with the token, to increase security. For example bank cards need often a PIN-code (Personal Identification Number) to work. (18)

2.3.3. Something we know

Something we know is a secret which you know, like a password or a PIN-code. But anybody who obtains this secret is “you”. If someone else was using your username and password to make some harm, how could you prove that it wasn’t truly you? (18)

In fact, having a username and a password, to access to your computer, is quite a weak way to identify yourself. Both username and password are “things you know”, so only one method of identification is used. It’s like drawing money from ATM (*Automatic Teller Machine*) by using just your credit card. (3)

User has an important role to play in password protection. User can easily tell his password to someone, or write it down. Someone might even leave a written password in to a place where others can see it. And probably you too have some experiences about forgotten passwords. (18)

There are two basic guessing strategies an attacker may use if he wants to pretend to be “you”. With brute force strategy the attacker tries all possible combinations of valid symbols. To prevent that, it’s better to have long passwords which contain upper- and lower-case letters, numbers, and symbols. Another technique is called intelligent search. In this technique the attacker tries obvious passwords related to user’s life (like relatives’ names, pets’ names, car registration number, phone number etc.), or just some generally popular passwords. (18)

How to improve password security? One way is to make users to use good enough passwords. A password checker can prevent user to choose too easy passwords, and a password generator can be used to produce right kind of passwords for the user. Passwords can have expiration dates, by which the user has to pick a new one. (18)

Another method is to limit login attempts. The system counts failed login attempts, and locks itself after certain amount of failed attempts. But using of these methods has side effects. If passwords are often changing, and are too long and complicated, the user might end up choosing easy passwords, or writing those down. (18)

Single Sign-On (SSO) technology solves the problem of multiple and hard to remember passwords. With SSO user has to log in to a network just once and system remembers this password and passes it on to a password management system, which knows user's other passwords, when the user wants to log in to other services, applications, databases etc. But using SSO generates new problems. How the stored passwords can be protected? (18)

2.4. Access control

Access control ensures that only authorized people can have an access to the information. To control the access properly we need to define answers to the following three questions: (3)

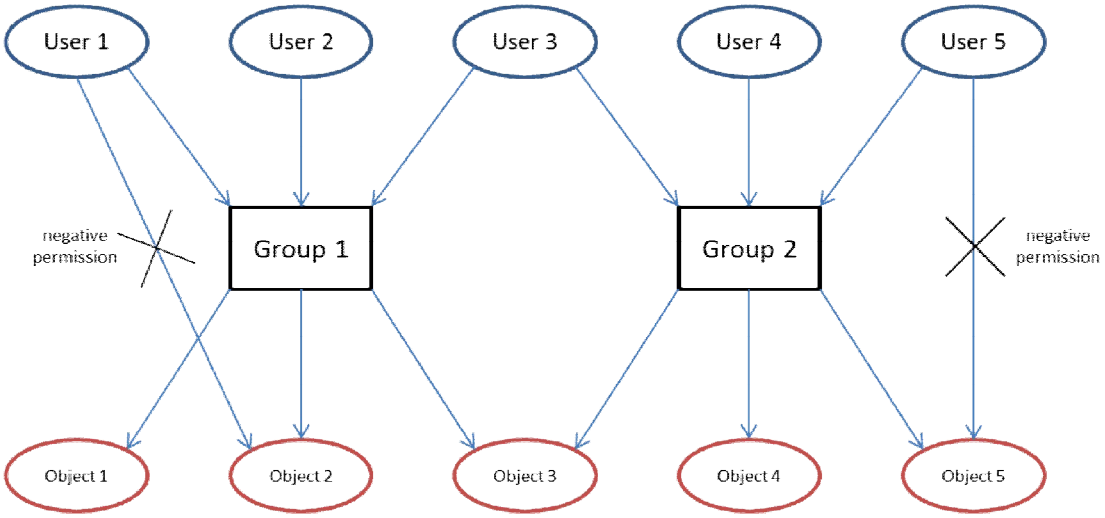
1. How we define the use and the users of an information system and its content?
2. How we manage the access and user rights?
3. With which methods the users are identified and authenticated?

Access control is usually combined with audit. The system keeps track on the users who have read and edited the data. Audit is very useful especially when abnormalities are traced afterwards. (4)

But who is in charge of the setting of the security policies, and who decides what others can and cannot do? Two fundamental options exist. First one is to let the owner of a resource (e.g. information) to decree who is allowed to have an access to that resource. This policy may be called discretionary, because access control is at the discretion of the owner. Another option is that a system-wide policy decrees, who is allowed to have an access. (18)

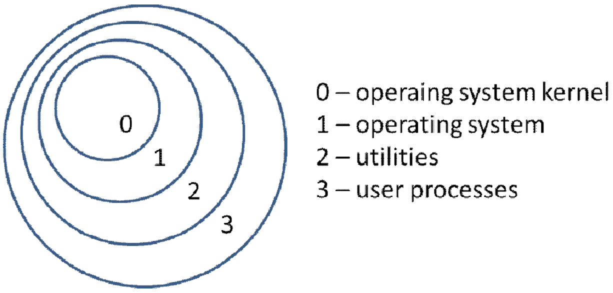
Intermediate layers between users and objects make policies more manageable. Here we represent three different layers. Groups are used to make access control policies simpler. If some users have similar access rights, they are collected in to groups and the groups are given access permissions. In some security policies a user can be a member of one group only. Other policies allow multiple memberships. In some special cases users can be given or denied an access right that normally follows from membership of some group. A negative permission is a record in an access control structure that defines the access operations which the user is not allowed to perform. Picture 1 'Access control with groups and negative permissions' gives a graphical explanation of these policies. (18)

Additional intermediate layer is role-based access control where a collection of application specific operations is called a role. Here subjects inherit their access rights from the role they are performing. Users can have more than one role and the same role can be given to multiple users. (18)



Picture 1 'Access control with groups and negative permissions' (18)

With protection ring, which is the last layer to be represented, each subject and object is assigned a number depending on their importance. An access control decision is made by comparing the numbers of subject and objects (Picture 2 'Protection ring'). For example a normal office worker (specified as number 4) cannot access to operating system kernel (specified as number 0). (18)



Picture 2 'Protection ring' (18)

2.5. Identity and access management

Identity and access management (IAM) manages the identities and access rights of the users. IAM is causing similar kind of problems in many organizations. Users are equipped with unnecessary access rights “just in case”, or the access rights of the personnel, who have left the organization or switched to other tasks, are still pending. One of the reasons for these both problems is that the management processes or surveillance of the access rights is insufficient. (20)

In everyday life these defects might lead to the increase of abuse. In addition, the traditional IAM requires lot of work and is exposed to errors since most of the actions are made by hand by multiple system operators. Solving of the access right problems is also hard to do because the name of the initiator of the change or the name of the approver is not recorded to any document. (20)

In one example improper identity management of a company led to huge costs in the form of licenses. The company checked the amount of usernames from their database and found over 4600 users. Employees they had less than 1000. When licenses were purchased by looking the amount of usernames the costs were over four times greater than they could have been, and money was wasted for no reason. And if we take in to account also the amount of applications which needed licenses, the costs are enormous. (21)

Designing of a proper IAM system for an organization requires a lot of specifications. The project is not easy. Questions needing answers are for example (20):

1. Who has the right to use each system?
2. What do the rights contain?
3. When will the right end?
4. Who will grant the right?
5. Who is responsible for updating the rights?

It is useful to specify the rights for one organization at a time. Granting of the rights could be the job of the human resources because the rights are usually linked to employment relationship and job description. Proper coordination is extremely important to avoid dangerous loopholes. (20)

When specifying access rights it’s not practical, or even rational to regard users on individual level. Traditionally access rights are managed with different combinations of single right and called those combinations as the user roles of a system. Single users are then scattered to those roles. When the needs have been changing it has been easier to increase the amount of roles and thus the work loads of administrators have also been increasing. (20)

Specification of access rights is mostly just connecting functional roles with different access rights. When it is done, the most of the work is over. Maintenance is needed just in those situations when the content of some functional role changes, or new roles are established. Changes in some person’s job description lead only to the updating of his functional roles. (20)

One person can have multiple roles. He can for example be a member of organization ‘A’, a member of an executive team of group ‘A1’, and a member of project ‘P’. Thus he has three functional roles which all contain different needs of information, and mandate for action. (20)

Each role has to have an owner as well as each piece of information and each system has. The owner specifies the role, maintains the content of it, and keeps track of the members. (20)

Federation is a useful method for IAM. When we want to cross the organization borders of two or more organizations and combine the identities between organizations we use federation. Federation requires common “trust circle” where all parties have specified common principles, approved each other’s processes (e.g. user registration and identification), and written a formal contract in which they agree to follow common processes. (20)

3. Information security in healthcare

What is the relationship between information security and healthcare? Confidentiality, integrity, and availability are all essential in health information. Health information must be available only for those who have the right to see it (confidentiality). You wouldn't want for example your insurance company to see that you have a high risk for some disease.

It's also important that the health information is correct, and doesn't change by any chance (integrity). What if a surgeon would remove the healthy kidney instead of the faulty one because of an error in the health information software?

Health information must be available when needed (availability). It would have dangerous consequences if a physician wasn't able to see that you are hypersensitive to penicillin when you are brought unconscious to an emergency department after an accident.

As health information is changing to electrical form, information security is becoming more and more important. But what concrete changes has happened during this health information transition and what is yet to come?

3.1. Healthcare IT is changing

During the past ten years, healthcare has experienced big changes as the patient information has been moved from paper archives to electrical ones. Also medical images are nowadays managed in electrical form with Picture archiving and communication system (PACS). Electrical referral and consultation systems are widely used. All these changes give possibilities to analyze and share information more extensively. (22)

The change to electrical handling of patient information generates new challenges to development and management of information security. It's quite likely that the role of information security and the importance of security risk management will increase. (23)

New patient information systems have already caused a lot of criticism, especially the lack of usability and functionality. A study (24) made by Winblad et al. showed that all patient information systems in Finland have had some defects and room for improvement. Doctors have had experiences of system crashes, outages, slowness of functions, and data losses. Systems haven't supported the cooperation of doctors and other personnel. Malfunctioning and other defects may, in worst case, cause risks in patients' treatment. Also the time which doctor has to spend with the computer is away from the time for the patient.

The compatibility problem of patient information systems is also a current issue. The vendors of the patient information systems are said to force healthcare organizations to buy all the services from the same vendor due to closed application interfaces (25). The aim of the Finnish HL7 organization, which is a member of the international HL7 organization, is to promote open standards for the interfaces of healthcare systems. Several hospital districts and IT vendors have their representatives in the Finnish HL7 organization. (26)

The development of the information systems of healthcare is currently in progress and the amount of different systems is huge. Several systems are expiring and needing renewal. The outcomes of national development projects have been modest when compared to the objectives and the demand. Projects are done with the emphasis on IT, and the projects are managed inadequately. Legislative reforms are based on the existing organizations, meaning that the old methods and rigid structures are directing the development of legislation. (27)

At the moment, Finland is implementing new KanTa services (eArchive and ePrescription) which make the patient information available in every part of Finland. Architecture is based on databases which are available for authorized organizations through open interfaces. Same kind of project (epSOS) is going on also between European countries. epSOS is meant to transfer patients' essential information inside Europe. (28)

Between 2010 and 2020 the amount of aging population will grow in Finland faster than in any other European countries (9). This change of age structure will lead to a situation where the amount of pensioners grows and the amount of people paying taxes decreases. Also the amount of medical staff decreases as nurses and doctors retire. With current arrangement of work Finland will get in to troubles.

As the population ages it's beneficial that people can live in their own homes as long as possible. Elderly people need support to be able to live independent life. This increases the need of supporting technologies such as information and communications technology. This requires new methods and technologies for health and nursery services and home appliances. (28)

In the parliament of Finland the Committee for the Future has brought forward peoples' need of taking care of their own health and the prevention of diseases (29). The healthcare services and technologies have to be organized in such a way that preventive actions are possible and easy to do. It's not just professionals' work to take care of the health of Finnish people. For normal citizens the internet is a common place to look for medical information. Question is how to make sure that the information in the internet is true?

To prevent small diseases from growing to bigger problems, the healthcare has to come close to the people. For example the city of Lahti is offering Health kiosk services in a mall. These open and free services are meant for everybody without appointment. Going to ask a question or two about your health has been made easy. (30)

New Taltioni project is going to form a database where Finnish people can store all their health and wellbeing information. With Taltioni citizens can manage, use, and produce the information related to their health through the internet and mobile technologies. The use of information doesn't depend on location, time or organization. Enterprises can develop new innovative applications based on this database. (31)

As the personnel resources get smaller, the need of telemedicine grows. In the future telemedicine will be integrated to be a part of normal activities in healthcare organizations nationwide, and telemedicine activities will be just normal videoconferencing. A try-out of telemedicine was done between the years 2007 and 2009 when EU funded an R-Bay project. The task of R-Bay was to offer a channel, eMarketplace, for buying and selling imaging related eHealth services (32).

3.2. Finnish legislation about health information

The actions of healthcare organization must obey the law, and take into account different standards and rules. Obeying the law, in addition to that it's ethically and morally right, also protects the organization from possible juridical acts and reimbursements. (3)

Numerous acts and degrees govern the activities of healthcare organizations in Finland. In this chapter we will present five of those. Those five, in writer's opinion, are the ones related most closely to health information and information security.

Client data act is about how electrical documents should be handled in health care. Act on ePrescriptions prescribes the legislation of electrical prescriptions. Decree on Patient Documents tells how patient related documents ought to be dealt with. Personal Data Act is about regulating personal information, and who is allowed to handle it and how. And finally, new Healthcare Act is a comprehensive reform to healthcare.

3.2.1. Client data act 159/2007

Electrical documents enhance the availability and usability of healthcare documents. As with all health related information it is extremely important that the information is kept intact and non-changeable. Only one document should thus be labeled as the original and others as a copy of it. (33)

Log files are also essential when dealt with electrical documents. Log register of use contains information on who has used the document, when and why. Delivery log register on the other hand tells if the document is shared to other parties. Also users and user rights has to be registered. An adult patient has a right to view his information, and know who has used it, or to whom it is shared to and why, but the patient cannot share the log files for other uses. (33)

Patient information can be shared for health and medical care purposes only. Before sharing the relationship between the requestor and the patient must be confirmed. The patient can deny the sharing of his information based on the service event or service provider. The denial and consent are in effect until further notice, and the patient can change his mind when ever. If a patient has denied the access to his information, this information couldn't be used even if it were relevant for the ongoing treatments. (33)

These decrees, mentioned above, impose some requirements for the whole system as well. The system has to enable using, transferring, storing, and securing of patient documents. Integrity, constancy, and non-repudiation of the documents are certified with a digital signature. That is why the users have to be able to be identified and verified reliably. Each user has to be electronically identified using the strong methods of identification. Organizations and devices must have an identifying method equally credible. To ensure a good quality of health care, the patient data has to be available all the time. Collecting statistics from the patient documents has to be possible also. (33)

3.2.2. Act on ePrescriptions 61/2007

The purpose of the act on ePrescriptions is to improve patient and drug safety, and ease and intensify the prescribing and delivery processes of medicines. With electronic prescriptions physicians can easily check which other medications the patient is having, and take it into account when prescribing other drugs. Also other healthcare authorities can make use of prescription data. (34)

Prescriptions are archived in the Prescription Center for the first 30 months, and then in Prescription Archive for 10 years. Viewing, saving, and other activities require strong identification. Data transfers from and to Prescription Center has to be encrypted and signed electronically. (34)

When a patient needs some medication a physician writes him an electronic prescription, unless the patient denies it. The patient can ask to make the prescription secret. The physician treating the patient can view patient’s previous prescriptions on patient’s consent. The physician has to give the patient a separate report about the prescription, unless the patient doesn’t want it. The physician can sign all of the prescriptions of one visit on the same time with a digital signature. The signature must be implemented so that the physician’s right to order the medicines is checked before the signature is sign. (34)

A pharmacist has to give a report for the patient about the purchased medicine. If someone other than the patient is picking the medicines, the report is given only against a signed consent. The buyer has to prove that he has the right to receive the medicine. The pharmacist can make corrections to the prescription against the prescriber’s verbal consent. The correction has to be signed digitally. The pharmacist has a right to get patient’s information from the Prescription Center against patient’s verbal consent. (34)

The prescription can be cancelled against patient’s verbal consent by the prescriber or a supplier. A nurse can cancel only those medicines which she has also a right to prescribe. Cancellation can be done by the prescriber without patient’s consent if the patient has given false information on purpose. Electronic prescriptions can be renewed by writing a new prescription. The patient can ask the pharmacist to request for a renewal. (34)

The patient has right to check his information from Prescription Center or Prescription Archive. He has also right to know who has been dealing with his information and why. (34)

3.2.3. Decree on Patient Documents 298/2009

A patient document can be a patient report and other related information, a medical cause of death information, other documents related to organizing and implementing treatment, or documents received from other instances. (35)

Electrical documents, which are saved to archives, should form an intact entity with identified service events. When a document is deleted from the archives, a stamp of the action should be left to the archive. (35)

Patient documents should be created and stored in such a way that the integrity and usability can be secured during the storage. Log files related to using and sharing of the patient documents should be kept intact and unchanged at least for 12 years after the creation. If patient information is given through the national archiving service to the patient himself via viewing access, the patient should be identified in a reliable way. (35)

Only those users, who relate to patient's treatment, can handle the patient documents, but only in that extent as their work and responsibilities require. Access management system, where each user can get specified rights, should be implemented to the electrical patient information system. Users should be identified and verified unambiguously. (35)

3.2.4. Personal Data Act 523/1999

Every time when personal data is being processed the purpose of the processing must be defined. The controller of the personal data register must ensure that all data is correct, complete, and up to date. (36)

Personal data should be used only when it's needed. In healthcare it's acceptable to handle sensitive information about patient's medical condition, illness, disability, treatment procedures, or other essential information. Nevertheless, a person, who has obtained some personal information about someone else while processing it, is forbidden to express the information to any third party. (36)

The controller of the register must ensure that patient's identification code isn't written unnecessarily on any printed documents. The controller has a responsibility to correct, eliminate, or add incorrect, incomplete, or outdated personal data. The controller has to prevent the sharing of such information which might jeopardize the subject or his privacy rights. Appropriate technical and organizational procedures must be implemented to protect personal data to prevent unauthorized access, accidental or unlawful destruction, alteration, disclosure, transfer, or any other illegal processing. (36)

Everyone has a right to know what information the register contains about himself. However, there is no right of inspection if the data might cause risk to patient's health or treatment. If the patient wants to know, what information the registers contain about him, he can make a request to a doctor or other healthcare professional who is responsible for obtaining the data and giving the information in the registry entries. (36)

3.2.5. Healthcare Act 1326/2010

The new healthcare act is a comprehensive reform to healthcare. The purpose of the act is to enhance the cooperation between healthcare organizations, make services equally available, enhance quality, and guarantee patients' safety (37). For the patients the act brings a freedom to choose their place of treatment and the person who treats them. The treatment pathway becomes more agile when patient information can be easily transferred between organizations using common register of patient information. (38)

The information in the register can be used without patient's consent also in other units than in the one where the information was collected. Patient can however deny the use of his information in other units. That is why the patient has to receive a statement about the patient information register and his possibility to deny the information transfer. A note about the given statement has to be marked to patient's records. To ensure privacy the use of patient information has to be followed, and the treatment relationship between the requestor and the patient has to be proved. (37)

3.3. Information security management process

The purpose of information security management is to enhance the ability of an organization to keep the used information safe from threats. That is why the information needing protection must be recognized and defined. Also the reasons of, why it must be protected and from what, help in identifying and preventing the risks. (3)

Today healthcare organizations lack a proper information security management process quite often. The reason might be cost-cutting, urge to business efficiency, or the lack of skills, understanding, or resources. Typically the responsibility from information security is divided to multiple persons, and thus the entirety is not being managed. In the future healthcare organizations are probably required to have an information security certificate. For that, a proper information security management process is needed. (23)

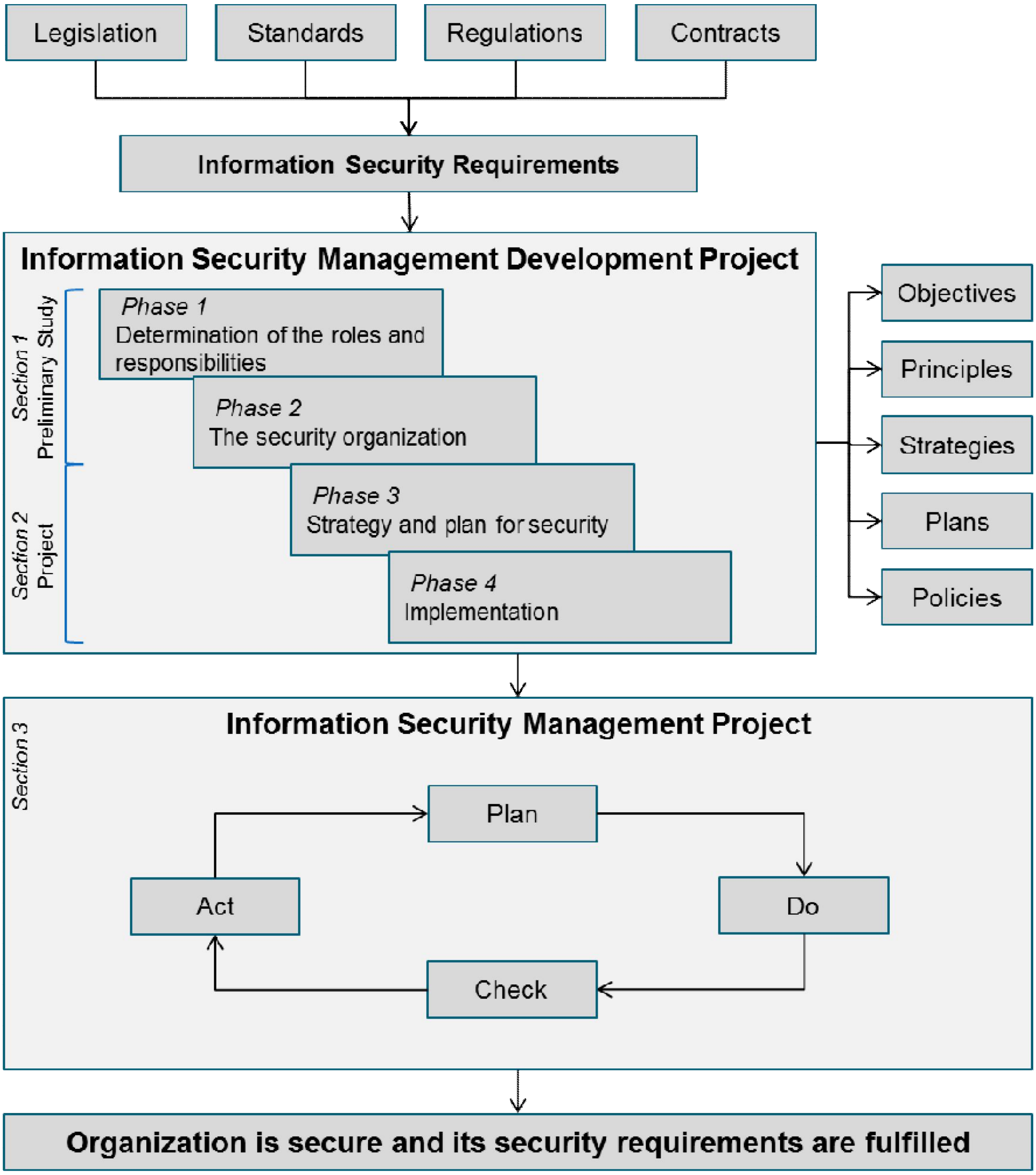
There are different kinds of models about how an organization could create its own information security management process. For example standard ISO/IEC 27799 about "Health informatics – Information security management in health using ISO/IEC 27002" gives one model for that (39). It's especially about information security in healthcare organizations.

A report (23) written by Tero Tammisalo presents another principles and methods for information security management in a healthcare organization. Of course there are other good models about information security management existing, in addition to these two mentioned. But because the latter document is tailored especially for Finnish healthcare organizations, we'll take a deeper look in to that.

Picture 3 'Information security management process' presents Tammisalo's diagram of development of information security management. The development project is a one-time project consisting two sections (sections 1 and 2 in the Picture 3). Managing of the information security is a continuous process (section 3 in the Picture 3). (23)

The input for the development project must contain requirements for information security. These requirements can be collected from legislation, standards, regulations, and contracts which are related to the field of the organization.

Section 1 is a preliminary study during which the needed roles and responsibilities are defined, and the security organization is formed. Section 2 is the main part of the project where the strategy and the plan for the security are created, and the implementation is done. During these two sections a bunch of documents, including objectives, principles, strategies, plans, and policies of the organization, are written. (23)


Legislation
Standards
Regulations
Contracts
Information Security Requirements
Information Security Management Development Project
Section 1
Preliminary Study
Phase 1
Determination of the roles and responsibilities
Phase 2
The security organization
Section 2
Project
Phase 3
Strategy and plan for security
Phase 4
Implementation
Objectives
Principles
Strategies
Plans
Policies
Section 3
Information Security Management Project
Plan
Do
Check
Act
Organization is secure and its security requirements are fulfilled

Picture 3 'Information security management process' (23)

Section 3 is the continuous process aiming to maintain a proper level of information security. In the Plan phase the framework and rules for maintaining the security level are created. The chosen principles are executed in Do phase, and followed and checked in the Check phase. The needs for changes in the maintaining process are evaluated and planned in the Act phase. (23)

What is a proper security level then? Capability maturity model (CMM) measures, how the organizations has reached its objectives. The model includes 6 levels of security – the greater the level, the better the security. (23)

- Level 0 – Problem hasn't been identified
- Level 1 – Handling of the problem is occasional
- Level 2 – Some processes are used
- Level 3 – Procedures are standardized and documented
- Level 4 – Risks are managed and measures are used
- Level 5 – Activities are optimized

Two of the most important aspects in information security process are the commitment of the management and the education of the personnel, which both have an effect on how well the information security processes are being adopted.

Management owns the information security processes so if the owner doesn't care about the security it's very hard for the personnel to care. Security policies are statements of the management on how the organization can stay secure. That is why the management has to show example and motivate people. It's also important that the management gives feedback to the personnel even if any security breaches were not noticed. (3)

One of the greatest risks related to security is the attitude and knowledge of the personnel – how the instructions are taken, and how well the right ways of acting are known. Education is maybe the easiest way to lift up the level of security. (23)

3.4. KanTa project

KanTa (Kansallinen Terveysarkisto – National archive of health information) is a common name for four national projects developing health information services in the Finnish healthcare. Electronic prescription project replaces old paper prescriptions with electronic ones. National medicine database gathers information about the medicines sold in Finland. Electronic archive of patient records facilitates the sharing of patient information between different healthcare organizations. One upcoming project also gives patients an access to view to their own prescription and patient data over the internet. (7)

Smartcard, digital signature, and certification are concepts which enhance KanTa projects although they don't directly relate to it. Smartcard and digital signatures can be used in many purposes in healthcare. Certificates are needed to make sure that the services are of good quality. The last sections of this chapter will tell a bit more about those too.

3.4.1. Electronic prescription

The purpose of the electronic prescription is to enhance the safety and effectiveness of medical treatment. ePrescription project has gone a long way already since the first prescriptions were written in Turku in May 2010 when the pilot use started. The project will be widening as the information systems between the pharmacist's and prescription center are being unified. According the Act on ePrescriptions, ePrescriptions will be in use all over the Finland on March 2014 at latest. (7)

ePrescriptions can be written by physicians and dentists. Also medical and dental students are allowed to write prescriptions on some level. That is why patient information systems and pharmacy systems has to have identity and access management system with which each user can get just those rights which he needs to fulfill his tasks. (40)

Electrical identification and digital signatures can ensure that the person, who prescribes and delivers the medicine, has a right to do so. Smartcards are used as a platform for these procedures. Smartcards are connected to PIN-codes to get the certificates situated on the card to readable form. (40)

If necessary, prescriptions and deliveries can be corrected. However, the fixed version forms just a new version and the old one stays in the version history. So the original prescription and delivery is not changed. (40)

As the law prescribes, only those physicians and nurses, who are responsible on patient's treatment, are allowed to see the prescriptions. That is why, every time when information is retrieved from the prescription center the reason and the existence of consent have to be given. This information is saved to the files of prescription center to be used in the surveillances of patient's privacy. (40)

3.4.2. Electronic archive of patient records

According the law electronic archives will be in active use all over the Finland at September 2015 at latest. (7) The meaning of the electronic archive project is to develop healthcare processes to use completely electronic data processing and archiving. Current archiving methods are based on printing the data on paper or on microfilm. Sharing information in paper form isn’t as effective as it could be digitally. (41)

KanTa services give better tools for sharing information inside and between organizations. Services ease and speed up practical work and enhance patient’s safety when patient uses different service providers. Information from prior treatments is available fast and easily. (41)

Patient information is saved to provider’s patient information system which is able to compile a document of the information, and pass it on to national archive. From the national archive other healthcare providers can get a copy of the document. (41)

Information security requirements demand that operational processes pay attention to security and privacy more systematically. This may cause changes to current practices of security, like how the documents are signed, how the user management is done in patient information systems, and how to control the consents of treatment. (41)

When the user is retrieving patient’s documents from the patient information system the system has to consider if it is going to be for the use in the own organization or a delivery to outside of the organization. If the information is going to be used inside of the organization, all the information is available. If the information is going to be delivered outside, the system has to check if the recipient has patient’s consent, or if the delivery is based on law. (41)

3.4.3. Patient’s view access to own data

View access to patient’s own data is a service with which citizens can see their own patient, prescription and log information. (16)

A citizen can log into view service through Tunnistus.fi service with his bank access codes or with an electronic identity card. Each authentication event will create a log entry. Also every search will generate a log entry to the log files of the Prescription Center and the electrical patient information system. (16)

Now is going on a phase where the citizens can through a view access see the basic information of their service events, and who has asked to see their information. In the future, the citizens are able to manage their consent and appointment information through the view access, and by other ways take part in producing and managing their own health information. (41)

3.4.4. Digital signature

By handwriting his signature one attaches himself to a document, and approves the content of it. Digital signature corresponds to handwritten signature entirely. It can be used also for the identification and ensuring of non-repudiation. All of these concepts are widely used in KanTa projects. (41)

During the ePrescription pilot users recognized the need to write multiple signatures at one time both in the patient information and pharmacy systems. According the Act on ePrescriptions all prescriptions related to one patient visit can be signed at the same time. (40) User just selects those documents he wants to sign and then does it by inserting his PIN-code. (41)

3.4.5. Smartcard in healthcare

In patient information systems all actions require that the user has logged in to the system. When the user isn't sitting in the front of his computer, the workstation must be logged off. All users have to have a unique username, and the use of common usernames is forbidden. The users have to be identified reliably. (41)

Because the personnel in many healthcare organizations write digital signatures, for example to ePrescriptions, and thus need a smartcard for that, the smartcard is an ideal option for other identifications too. As smartcards can be used to other identification methods why not to combine the existing one to the other methods, and take care of only one smartcard. (41)

3.4.6. Certification

Certification is a great way to build trust towards the information systems. Certification is a process which ensures that the product, function, or service passes the needed requirements or standards. In the past the customer information systems in healthcare didn't need certifications. Only medical devices needed to be certified. Recently the European Union and the United States have proposed that the certifications should be required from healthcare information systems too to assure the fulfillment of requirements, trustworthiness, and information security of the systems. (42)

The implementation of the national healthcare information systems has created a need for certifying this kind of systems. KanTa services require functional cooperation and minimum level of security from electronic archives, local and regional patient information systems, and centralized national information services. The functionalities of the systems have to support both flexible and seamless care process. To achieve these goals nationally on the same time KanTa related information systems should be certified. (42)

3.5. Main features of healthcare information security

This far we have discussed about the requirements and needs of healthcare information systems and processes. But what are the most problematic areas of healthcare information security. What information security issues cause most problems? Which are the most essential ones?

3.5.1. Identity and access management

Identity and access management (IAM) is struggling with the similar problems in healthcare as in other organizations: “Just in case” access rights, access rights for persons who don’t work in the organization anymore, manual work leads to errors and so on. (20)

In addition to user and system roles we could use functional roles which are connected to realizations of action, like caring doctor, attending nurse or member of diagnostic team (43). In other words, we try to find groups of users with similar work tasks. Therefore, they have similar needs of information and mandate for action. (20)

In healthcare it is important to take care that only personnel related to treatment can handle patient’s information. Because in the most cases it’s impossible to define in advance who will be taking part to the treatment of particular patient, we can use organizational and specialty divisions. In a hospital we could assume that if patient has been registered to a ward, the personnel of that ward could see his information, but the personnel of the next ward couldn’t. In addition, information can be restricted according specialties. In an emergency all limitations can be overridden and those situations are dealt afterwards. (41)

Finnish healthcare field is also known for high staff turnover, which is characteristic for periodic and predominantly female workforce (44). Also retirements of old, experienced people and young professionals, who are still looking for their own field, increase the turnover (45). That is why new workforce has to be registered and old ones unregistered more often than in regular office work.

3.5.2. Log data

Information security is implemented with different kind of control methods. Those methods can be either proactive (e.g. preventing the use of data) or reactive (e.g. investigation starts if someone has viewed confidential data without permissions) (3).

The nature of healthcare requires that in emergency situations the needed information is available without any technical obstacles. That is why the most effective control method is to monitor afterwards. This method also brings deterrence against possible abuses. Thus the method is to use access rights to take care of most of the use cases, and with the log files explain the exceptions. (41) The problem is though, how to control all the logs if the amount of systems generating those is huge.

To be able to use log files as trustworthy evidence the saved information has to be diverse. (41) Who did what? When and where? Where to, where from and on what? Who gave the authority?

3.5.3. Continuity planning

In healthcare the lack of continuity planning can lead to devastating consequences. For example intensive care unit without electricity would be a nightmare.

With continuity planning possible crisis and the consequences are prevented as well as possible. On the other hand, if the risk actualizes, the normal status is achieved as soon as possible. Thus, healthcare organizations have to have sufficient capacity to react in serious crises. (3)

3.6. Information security concept of ISSHP

The concept generation of ISSHP started from defining all (on some extent) possible risks of the organization. After that all risks were scanned and decided how the risks would be minimized. During that phase the development plan was done. Then started the organization of the activities mentioned in the development plan. Information security and risk management processes were created as well as the tools supporting the processes. In the last phase the processes were implemented to everyday work practices. (14) Below we present you the most important solutions of the ISSHP concept.

3.6.1. Identity management

Identity management was causing the most risks in ISSHP when the risk assessment was done in the beginning of the development project seven years ago (14). On that time there was 1500 unused user accounts since the information about employees' departures hasn't reached the IT management. Everyone could ask for user rights, and the rights were given one system at a time. The users had too much access rights, and temporary employees had enormous amounts of rights since their work place was changing all the time. In the beginning the process for applying the rights varied according to the system. Managing of the access rights required lots of work. (46)

Nowadays the processes are renewed. The roles and rights are defined, and the amount of roles is reduced from 200 to 90. When a new employee is recruited, the supervisor assigns him a role. If the job is temporary, the end date is given. The implementation of new processes included a lot of training of the supervisors since the supervisors rarely knew what role to give for a new employee. After the supervisor has selected a role for a new employee, the personnel department checks it and the needed right is given. The user interface of the system needed to be user friendly and simple enough compared to the old system. (46)

Now, when the roles are given by the supervisors, the amount of excessive rights has reduced, and the rights are within the requirements. Old, unused rights don't exist anymore. The work load related to identity management tasks has decreased. There's no more default usernames or general usernames with which the systems could be used. The implementation process hasn't been easy, but very profitable. (46)

3.6.2. SSO and smart card

In ISSHP Single-Sign-On (SSO) service and smartcard have an important role in the information security. The IT management wanted to have a strong authentication to everywhere, not just to workstations. Thus, all essential daily activities are connected to a smart card, RFID-chip (Radio-frequency identification) in the smart card, and a PIN-code. Nowadays, the personnel uses their smartcards when writing digital signature, passing through doors, monitoring working hours, paying lunch in canteen, and logging in to applications and workstations. On some day, also the patients will get their own smart cards to walk in the hospital premises. (46)

The demand for SSO solution was significant. After the vacation period the use of helpdesk increased when personnel had forgotten their passwords. All in all, the amount of usernames and password was huge as every application had its own. (46)

Experience has taught that the personnel take care of their smartcards. The amount of lost cards is small. Sometimes a person, who has forgotten his card at home, has been forced to fetch it because without the card the person couldn't do his work. (46)

In the implementation phase several challenges were faced. The use of substitutes' smartcards required an exact operating model since the cards might have been needed in a short notice. Another question was how to make the system secure enough because the use of information systems depended on the card system? The procedures for situations when everything crashes had to be up to date. The users had to be also trained and motivated to use the card. Calculations have showed that the SSO investment paid for itself in four months. (46)

3.6.3. Standardization and virtualization

ISSHP has over 500 different applications and systems in use. If each one of those had an icon in a computer desktop, finding the right icon would be very difficult. With desktop standardization user gets his personal role based view from each workstation. Thus the user doesn't have to pay attention to which workstation he is using. (46)

When a user logs on to a workstation, he sees an empty desktop. In a window he can see a menu with icons of the applications he has an access to. The desktop is the same on each workstation, and the user cannot change anything on the desktop. The user can save his documents only to a network drive. (46)

Standardization project has been quite challenging in ISSHP, because operating environments differ from each other. For example operating theater has different requirements for IT than laboratory. Also the variety of special equipment sets its own requirements. For example some systems can't be used with certain operating system. In ISSHP the amount of workstation models has been reduced to three. There's one PC (Personal Computer) model, one laptop model and one virtual terminal model. (46)

After all, for an organization standardization is better than letting all flowers to bloom. The advantages of standardization are great. Every user sees own desktop in every workstation inside the hospital district, even from mobile terminals. The problems related to the use of workstations have decreased significantly when the changes, made by users, have stopped. Also the abnormal behavior of the workstations, caused by the changes, has disappeared. Re-installations of the workstations have almost vanished. Even the users have been satisfied with this solution because of the improved usability. Maintaining and developing the systems has become easier, and the hardware investments are more scattered to a longer periods. Also the costs are thus easier to forecast. (46)

Virtualization of the workstations has made the logging in and using easier. Changing of the user, one logs out and another logs in, is fast. Also the implementation of new services has become easier. And when the user changes computer, he doesn't have to open all the applications again, because the system remembers his previous session. And because of both standardization and virtualization, the saved time can be used for core tasks, like taking care of the patients. (46)

3.6.4. Mobile work

In mobile work the user has more responsibility for his device. Without properly secured device the risk of losing also private information, when the device is lost, grows. Secure mobile devices bring also security, but usability too, especially to the work of home care nurses.

The mobile device has to be small enough, so that it's easy to carry with. It has to be absolutely safe too. It cannot contain any information. In ISSHP mobile device is just a screen and a keyboard with which the applications, locating in the intranet of the hospital, are used. The use of memory stick is prevented. Only smartcard, point-of-care testing devices, and mobile printer (to print e.g. prescriptions) are allowed. (46)

In the past the basic day of 160 home care nurses' was as following. In the morning a nurse arrives to her office. She browses patients' information from a workstation and writes notes to her notebook. She takes medical supplies and patients' keys with her and travels to the first destination. She opens her own notebook and looks at the other notebook locating in the destination. Then she performs treatments and writes those down on both notebooks. After that she delivers possible measurement results to laboratory. Then she travels to the next destination and after the last destination travels back to the office and writes the information from her notebook to the patient information system. (46)

When nurses were given a mobile terminal, the process became simpler. Now the nurses don't need to go to the office in the morning if they have all the medical supplies and keys with them. In the destination nurses take mobile connection to the patient information system from where they can see patient's treatment history. The results are written directly to the patient information system, and the specimens are delivered directly to the laboratory. In principle, nurses don't have to go to the office in the end of the day either. (46)

The advantages are unquestionable. More time can be used to take care of the patients, information and patient security is better, actions are not tied to offices (the number of the offices can be decreased), traveling expenses are smaller, and the mobile devices can be used as reserve and be taken to the field in crisis. (46)

4. Interview research

4.1. Research method

The purpose of this study is to find out how Fujitsu should develop its information security services to better respond to the needs of healthcare, how the processes and practices of Fujitsu could be developed, and how Fujitsu could formulate its marketing message to be appealing to the operational planners and purchase decision makers in the healthcare? That is why we have now explored the current situation and the future prospects of the healthcare to see what kind of needs of information security healthcare has.

As a method of research we use semi-structured interviewing in which the interview has a framework, but new questions can be brought up during the interview depending on what the interviewee says. This way we might end up getting results we didn’t even though before. (47)

When comparing semi-structured method to for example a questionnaire, we obtain a clear advantage. We are able to change the order of the questions, ask for clarifications on both sides, and get some real-life examples. On the other hand, interviewing is quite challenging method and requires a lot from the interviewer and the interviewee. Also the amount of opinions we get is smaller compared to the amount we could get with questionnaires, but we have decided to concentrate on quality over the quantity. (47)

4.1.1. Interview questions

Instead of starting to think questions for each interviewee group especially (like what we would like to ask from a sales person of Fujitsu) we began from reasoning what we truly need to know to develop information security services, processes and practices. After that we can consider who could give the required answers.

We deal the whole interview to three separate sections:

1. Motivation
   - Why secure IT is so important to healthcare organizations and what motivates them to purchase information security services? Who has an effect on information security in healthcare?
2. Solution
   - How the information security concept of ISSHP was formed?
   - What advantages and disadvantages the concept has?

  - How we could sell the concept and information security services overall better?
3. Future
   - What kind of development needs we have in the future to solve the current problems and also the coming problems?
   - What kind of visions the interviewees have about the future of healthcare IT? Can we prepare ourselves for that?

The interview questions can be found from Appendix A: Interview questions. As the interviews were semi-structured, all of the questions were not asked from everyone and some additional questions were asked during the interviews to clarify the answers. In the end of the interview we also asked if the interviewee wanted to add or highlight something, to make sure he/she was able to say everything he/she wanted.

4.1.2. Interviewees

After we had the needed questions formed we could start to consider who could give us the answers. Of course we wanted to include the persons, who have been developing the ISSHP concept both in Fujitsu and ISSHP, to hear their reasoning for the concept being what it now is.

An information security specialist of Fujitsu, not too familiar with ISSHP concept, could give a bit more objective opinion about the advantages and disadvantages of the concept. The personnel of ISSHP would tell the users' story about the concept, and how they are coping with it in everyday work.

As Fujitsu has had some challenges with the selling of information security services to healthcare organizations, we interview also the sales representatives of Fujitsu to hear, why they find it hard to sell information security services to healthcare organizations.

As we don't yet have a truly objective view about the concept, we will interview also some specialists of healthcare and/or information security, who are not related to the ISSHP concept.

Interviewees were first contacted via e-mail. From the contacted 15 persons 10 were interviewed. Four of the interviews were made as a phone interview and others were done as a face-to-face discussion. All interviews were done in Finnish between the 21st June and 9th September 2011. The background information (organization and specialty) of the interviewees can be found from Appendix B: Backgrounds of the interviewees.

4.2. Results of the interviews

During each interview the interviewer wrote notes under the question she was at that moment asking. In unclear situations the interviewer explained what the interviewee had said in own words, and asked it was understood correctly. First two interviews were also taped after the permission for taping was asked from the interviewees, but after those two interviews taping was noticed not to give any extra benefit, so in the later interviews it wasn't used. The interviewer read through the notes right after the interview and write it to whole sentences. Thus the notes from the interviews aren't official citations, but the content corresponds to what the interviewees were saying. The points from the notes were sorted to six categories. Here below we go through the results one category at a time. All detailed points can be found from Appendix C: Detailed results of the interviews.

4.2.1. Overview of the information security in healthcare

Healthcare organizations are characterized by the fact that their customer information, healthcare information, is protected with law. Patients have to give their consent if their information can be used.

In healthcare, there are a lot of different types of work contracts. Personnel who make occasional work shifts and on call personnel are characteristic examples of the workers of healthcare. A healthcare professional might have different roles in his job. He might have treatment relationships to patients, he might be a researcher, and he might be even a supervisor – all at the same time.

In healthcare, information security has to have high priority, and the needs grow continuously. But because information security is hard to justify economically, it is often seen just as a cost and as a thing that hampers other actions.

Several interviewees stated that information security doesn't get enough attention in healthcare. Its priority is too low, and often it is experienced as a thing that just has to be done, and the responsibility of it is easily delegated for someone else. Information security is a hot topic in healthcare, but the words don't turn to actions. Sometimes information security is too easy to forget and think "why would something happen now if it hasn't happened before". Investments are big, and hurry is a good excuse not to do anything. Two interviewees admitted that usually our society assumes that in healthcare information security is managed better than it really is.

Few interviewees, on the other hand, had more positive view about the state of information security in healthcare. They agreed that information security is getting attention, but admitted that in everyday life it's sometimes forgotten. For example work issues are discussed in lunch restaurant, or in phone in public places. One interviewee stated that the professional staff is more conscious about information security than other workers of healthcare.

Today, all information is available inside a healthcare organization, and it cannot be restricted with access rights too much because in emergency situations the information must be available. Monitoring has to be done afterwards, and the user has to take the responsibility of what information he uses.

Legislation is one of the biggest motivators, in addition to economical motivator, when developing information security in healthcare. Some interviewees said that legislation is the only way to motivate healthcare organizations to develop their information security. One interviewee pointed out that all organizations have same kind of problems, but they all try to solve those in their own ways. “If I were to decide, I would order a national information security policy, which everyone would have to obey. Current recommendations are too loose.”

Other good motivators are information security accidents. Those wake up the management to act. The costs of accidents can be huge. For example if important systems are down, information might not be available, and the appointments have to be cancelled. One interviewee pointed out that in healthcare even minor privacy offences are noticed in media, but with business organizations the threshold is rarely exceeded.

Often the management of healthcare organizations doesn’t have enough information about the drivers and implications of information security. They don’t understand that it’s not just technical solutions which you can buy. Information security management processes must be implemented too. The budget for information security is often too small, and the management might not even be aware about the situation of their information security. They don’t know if it’s good or bad. Or if the management has paid attention to information security, they have not done it in a long run. The results of the current fiscals are more important than the results of the next years. There are neither enough personnel resources for example to make the log reports, and the budget for information security consulting isn’t big enough compared to the need of it.

The current patient information and other healthcare systems cause difficulties for implementation of information security. One problem is that the systems aren’t as secure as the legislation requires. Also the number of different patient information systems makes the implementation hard. Building of the national health information systems hasn’t made the implementation any easier. For IT vendors the information security needs of healthcare would be easiest to evaluate if they were close to their customers.

The critical need of few information security solutions were also brought forward by the interviewees. SSO is very important tool in healthcare since no one can remember all of his usernames and passwords. SSO is one of those rare things that also ease the work. Especially SSO supporting the use of shared workstations is the best, because in that case SSO can be used in every desktop of the organization, not just on user's own desktop where the password list is saved to.

During the past years, identity management has become more complex in healthcare since the work relationships have changed to more unstable. If IAM is done manually, costly mistakes can occur. Implementation of IAM can be hard with big organizations, but when it is well done the correct and suitable rights are guaranteed. One interviewee suggested that the access rights could be based on the treatment periods. When the period ends the right to access patient's data ends too.

Virtual desktop is a good solution especially when a nurse, treating a patient in his home, can have an access to patient's information. On the other hand, any traces of data cannot be left to the device with which the information was viewed, so an image of the data is a good solution.

Log reports have to be made automatic. The probability of getting caught, after looking irrelevant information, must be high. The log investigations could be implemented with data mining. Log information could be scanned through and looked after special use profiles, which of the log events are relevant and which are not.

4.2.2. Who effects on the information security of healthcare

According to the interviews, legislation has the greatest impact to information security of healthcare, but it's not the only one. Fear of losing reputation is also a big factor; especially in private sector this can have devastating effects on business.

The vendors of patient information and other systems have quite a big effect on information security. The vendors might not see the overall benefits of its customers. That can be seen as non-functioning interfaces. The vendors are not open for changes to the old systems. The systems cannot be integrated, and they don't support information security requirements. Because of the old systems log keeping is difficult and bad. And how to implement information security processes if the systems doesn't support those.

In addition to vendors there are also other stakeholders, like pharmacies and social services, who have their say about information security. International stakeholders, like EU and its decrees, have to be taken care of too.

KanTa project has made healthcare organizations to think about information security. Through the access to their own data patient gets an ability to see who has used his information, and patients can easily announce about privacy offences. And when the new generations become independent customers of healthcare, they might want to do things in the internet same way as we now deal with banks. This creates pressure for information security.

Thrive for better usability and more efficient work is one motivator. Especially in authentication instant wins can be obtained, when right solutions are implemented.

Society and its changes, like criminality, development (also technological), and new ways of hacking, have an effect too. The discussions about the quality of healthcare information systems, and the requests for more effective healthcare, direct both healthcare and its information security.

4.2.3. Implementation of information security to healthcare organization

Information security is an attitude which creates the possibilities for actions. When the way of approaching is right, a good way wins the easiest way. It's important to implement information security to be part of normal activities, processes, and culture in an organization. At its best information security isn't even noticed.

When implementing information security, it's very important that the management is committed in to the processes, and that it understands clearly the meaning of information security. The whole organization should be motivated too. Planning and organizing in a long run is also significant. If the attitude of the management is neglectful, the information security is probably too.

As many purchases in public services are done through bidding competitions, there are some pitfalls one should be careful of. If the requirements are written improperly, the organization may have to purchase a system it doesn't want to take. And as the competitions might take long, the danger might be that when it's finally ready, it's already an old technology. Current acquisition act forbids considering the references of the vendor. An organization cannot purchase a system directly from a vendor who it knows to be a reliable one. Thus also smaller and newer competitors get a possibility.

One interviewee emphasized how important it is to design information systems for its users. In acceptance of information security user satisfaction is the most important thing, and through that the authentication, user management, and information security overall has to be developed.

When a new system is brought to an organization, the users must be trained to use it. Training process is challenging and expensive, but vital. In healthcare organizations the personnel has to also keep up their professional level with trainings. When the trainings of the tools, like software and applications, are added, trainings all together might take a lot of time. Training is truly needed since some healthcare professionals have not even got any computer training in their basic education. Nevertheless they should be able to use technologies so well that they can take also patients into account. When the information systems are in use and can be used effectively, costs are lower.

When any kinds of changes are done in any organization, resistance of change exists and it cannot ever get rid of. But it can be reduced by marketing the changes better to the users. The message should be that the new solutions will ease their work, and those are not done just for someone else's profit.

4.2.4. The experiences of ISSHP

The success behind the ISSHP concept lies in a long run planning, commitment of the management, and a holistic view. In 2002 ISSHP defined what society and they require from their information security, and then set objectives for it. Then they defined what steps should be taken to meet the objectives, and took those. Since that they have planned information security in three year cycles, and defined what the most critical development targets are.

ISSHP has seen that the information security and privacy are important, and they have wanted to be forerunners in it. They have searched new approaches and cost-efficiency. The experiences have shown that preparing for the future in advance pays off. All the glory of ISSHP concept goes to their active IT manager.

ISSHP was first hospital districts who fulfilled the high level of information security. Their personnel are proud of how well the information security has been handled in their organization, and they can truly trust that everything has been taken care of. Their concept takes care of the users' opinion.

In ISSHP the benefits of information security were viewed through their core business – healthcare. They decided not to do e.g. IT services, and especially information security services, by themselves. Instead they outsourced it to those who do it better. The development of the concept started from their needs. Even though the running and managing of the services is outsourced, the development of the IT is still the responsibility of IT personnel of ISSHP.

As a small healthcare district, the possibilities of the existence of ISSHP depend on how well their IT works. Moreover, when IT is well taken care of the amount of personnel doesn't have to be that large. The principle of ISSHP is that they cannot strive for perfection of information security, but they can do breaking in so hard that anyone wouldn't found it interesting to do.

When compared to the other healthcare organizations, ISSHP has a lot of IT personnel developing IT. As a relatively small organization, managing of ISSHP might be easier. ISSHP is an exception to the other healthcare organizations, because they have taken care of the information security on a large scale. “In some other organizations information security consists of log information system and an advice ‘keep your computer locked’”, one interviewee said.

ISSHP concept could be copied to other organizations as well, although different patient information systems and technical environments make the copying of technological solutions challenging. In fact copying has been already done to Carea (Kymenlaakso Social and Health Services) and Eksote (South Karelia District of Social and Health Services).

Implementation of information security has been challenging in ISSHP. Multiple projects has been planned and implemented in the same time, and personnel have had to adapt to changes. A lot of work has been done to motivate the personnel, and there’s still a lot to do. Utilization of the resources, like personnel, has been difficult. Information systems had to be unified with other parties (like pharmacies during the implementation of ePrescription), and sometimes vendors of the information systems haven’t been able to reach the required level. The development of information security has to be continuous because the world is changing continuously.

According to personnel representative, working with smart cards has been challenging. Pressure and sloppiness are causes why the card is easily forgotten to take with when a person walks away from the computer.

But the implementation could have been more difficult. Without good partnership with Fujitsu and ISSHP, and well done planning it would have been much harder. For personnel learning to use the new systems and tools can be hard or easy. For someone a new application is easy to use and for someone else it’s hard. Afterwards difficult things can reveal to be easy after all. Restrictions related to internet surfing and modifications of the desktop, like downloading of own software, have caused some dissatisfaction. But after all it has just forced everybody to obey the laws and policies of the organization.

Luckily, technical solutions have made the information security much better, and some of those have even made the work easier to do. Usability of the systems has been important with the new solutions. Single-sign-on system was first of the new solutions implemented in ISSHP, and it has made logging in a lot easier. The personnel don’t have to remember multiple passwords, just one PIN-code. Using it also saves time.

Even though the use of smart cards is sometimes challenging, it has also made the work easier, and no one would give it away anymore. If the biometric identification had added, it would be even easier. With virtualization, sessions now follow from one place to another. Response times have also become shorter.

When systems communicate with each other, the information is available from one single place. And when information has to be written only once, time is saved. Time is saved also with videoconferencing systems. When there's no need to travel to attend to the meetings.

Although information security is said to be just wasting money, there are also some solutions which save money. In ISSHP, ROI (Return on investment) is calculated for all big investments, and decisions are based on that. Identity management system reduces the manual work and the amount of errors, and thus saves money. All solutions which make the work easier and faster save money. For example the use of SSO, virtualization, mobile work (reports can be made in the location) and remotely produced services save money. For example SSO system paid the investment back just in four months (46). It's also important to remember that when an organization has already invested for example on helpdesk service, it will be more expensive to not use it than use it.

Actually, when the interviewees were asked what causes the highest costs in information security? The answer was mostly development, as ISSHP is developing their systems continuously. But in the long run the investments will pay it back. During the years 2008 to 2010 the costs of IT management have raised 21 %, but really the raise has been 2 % because the savings of previous investments have covered most of the costs (46).

The personnel are truly proud about their information security level. Just small practical enhancements should be done. On the field people would need protector shields, which would block the view from outsiders, on their devices. Also the locations of computers in the departments should be properly planned. Now it's easy for the customer to see to the monitor, and sometimes the computer, instead of true person, is the first one to welcome new customers.

Seven years ago ISSHP started to arrange pure information security trainings. Now every worker is obliged to attend on one two hour long training once a year. If the trainings are not attended, the person will soon have a non-working smart card. The information security knowledge has not been truly tested in ISSHP, but in auditions the knowhow has been noted and progress is seen. Information security is brought near the personnel, and no one could say that he hasn't got the information.

In ISSHP information security portal is used to pass security information. Risk-reporting is done through the portal and for users it's easy to find information from just one place. Possible security breaches are always reported and discussed. Personnel know that ISSHP has a monitoring system and that the use is followed.

From all of their information security services the IT manager of ISSHP values most the strong identification, the SSO system, virtualization, and the information security technologies of the intranet (firewall etc.).

4.2.5. Fujitsu and the information security of healthcare

To be a trustworthy vendor of information security services Fujitsu has to have its own information security in good condition. Information security cannot be just one entity, but a part of other actions to.

In the interviews, the representatives of Fujitsu were asked why it is so hard to sell information security services. One of the reasons given was that Fujitsu doesn't have a long view strategy for selling the information security services. Information security services are hard to sell also because the descriptions of the services and commercialization are not clear enough for salespersons to understand. In Fujitsu information security knowhow is too related to certain persons. ISSHP case has pushed things to right direction and made Fujitsu to tailor its services for a specific business instead of using the standardized model.

Fujitsu would need an overall concept of information security services for healthcare. It shouldn't be just separate blocks packed together, but a continuous management model with management, processes, and proper resources. The concept should be simple enough that the salespersons can understand its basics easily and feel comfortable to describe it to the customers. It could be a story to tell regarding the special features of healthcare.

For salespersons it's important to know and understand what they are selling. Currently they feel that information security is difficult and complex, and if they have had negative experiences about selling the information security services, the threshold to sell those again is higher. According to the interviews, salespersons would need more training, support, and right attitude. They should be able to modify the services to better respond to the needs of healthcare.

Also customers' attitudes and understanding of information security might be poor. Information security is not seen as an important part of healthcare IT. Customers might want to take shortcuts and choose the easiest way. Salespersons should make it clearer to customers how they can benefit, also economically, from information security.

Interviewees were asked what factors affect to the purchasing decision. Money and costs were the most important ones, after that the requirements of legislation. Also resources, attitudes, quality, compatibility with current systems, vendor's trustworthiness, solvency and expertise, customer's benefits, in what schedule the service can be implemented, national solutions, and their own reputation (the customer don’t want to get bad publicity) effect.

Fujitsu is seen as a good partner in basic IT. With more innovative projects, the ideas have been harder to push through, because the business idea of Fujitsu is to standardize its services. According to the representatives of Fujitsu, Fujitsu has knowledge about healthcare.

4.2.6. Future visions

In the future the society will undergo several changes. The amount of organized global hackings will increase though the probability of those to happen in Finland is small. ePrescriptions will be usual targets for forgers, and improper uses of patient information will expand when information of every Finnish person can be found from the same database. These will put on pressure for increased control.

Aging and retiring of people will lead to personnel crisis, and the costs of healthcare will grow. Especially investments for development and acquirement of information technology will take a lot of money, but in the long run will pay it back. The problem is, though, how to rationalize the advantages of ICT to the ones who pay for it.

Electronic and internet services will spread also to healthcare. The challenge is whether the legislation allows the changes or not. Resistance of the change will exist.

From technological solutions for example virtualization, web applications, mobile technologies, and cloud services will become more common, but work has to be done since e.g. cloud services will create challenges with privacy. One interviewee was pondering whether the legislation actually already allows using cloud services or not.

In the future work overall will be less location-specific. The amount of mobile work rises. This generates needs both for privacy and information security and for information being available when needed. Wireless Local Area Networks (WLAN) might become more open, as the speed of WLANs grows. Thus the organizational intranets might be restricted with Virtual Private Networks (VPN).

Future will bring more standards along. According to the interviews, interfaces will open and systems will be integrated. This enables the multi-vendor environment. As the standards might be international, also the applications can become international.

One growing trend is usability. This has to be noticed also in the services of Fujitsu. Services have to be easy to use. For example biometrical identification will come more common and make identification process more usable. Also information security needs usability boost. The role of information security grows and will be important. Information cannot be left unprotected in any circumstances.

In the future people and organizations buy services instead of hardware. Outsourcing will grow, and organizations will be responsible only for organization of the activities and development.

In healthcare national information systems help to spread the information between healthcare organizations. Hospital districts will merge, and the information systems have to be integrated and developed too. These changes will put pressure on development of information security and especially to identity and access management services.

Self-service, self-care, and self-control of the patients will save personnel resources. For example self-check-in devices will welcome the patients on the hospital door. Also the automatic measurement devices will generate more information about patient's condition.

In the future, instead of curing the illnesses the focus will move more to promoting of the health. People might execute health tests in the internet, and based on the results get recommendations. "You eat too much fat. You should consult your dietician."

4.3. Development proposals based on the results

In the previous chapter, we presented the results of the interviews. In this chapter we ask: what could and should Fujitsu do?

4.3.1. Increasing the commitment and understanding of the management

For ISSHP the commitment of its management and development of information security on a long run were essential success factors. How could Fujitsu influence to other healthcare organizations so that they would understand this too?

Could we collect information from ISSHP to get a better view of their budget development on a long run? Could these numbers give us financial backup? Could we find examples from other kind of development cases where the long run development has truly paid off?

4.3.2. Security level analyzing service

One problem mentioned in the interviews was that the healthcare organizations don't know their information security level. They haven't done benchmarking. They don't know if their information security technologies and processes are sufficient or not. Could Fujitsu offer them some analyzing service which would scan the information security level of the organization? The service could be just a few day long consultation service and be quite superficial. The service could give some indication of the information security level according to CMM (described in chapter 3.3 Information security management process).

4.3.3. Visualizing the benefits of information security

To help the healthcare organizations to understand the benefits of information security, the advantages should be visualized as well as possible. Those should be presented clearly and especially in a numerical form because the costs and savings caused by the information security effect on the decision very much. We would need a way to tell that the development of information security doesn't cost much when compared to the savings which it will bring.

This far the benefits have been presented usually as sentences like "this saves money, because…" and "this makes the work more effective, because…" Numerical factors should be given too. "This investment will pay itself back in four months", would give more information. Even though the numbers wouldn't be completely accurate, it would be better than nothing. Could the savings of multiple services be visualized into one curve or picture? Will the savings of multiple services be greater than the savings of each service summed up together?

On the other hand, we could also define the costs of security breaches. On personal level we could define what it costs for IT manager personally if his work contract were terminated because of security failure, and how this incident will effect on his later work opportunities. On organizational level we could define what it costs for a municipality if the current IT manager of health center were replaced with a new one. Golden handshake, recruitment costs, and orientation of the new one might be quite expensive. A great incident could also effect on the work motivation of the personnel and the customers' loyalty, especially in private healthcare organizations. What would the financial costs of that be?

In addition to financial costs and benefits, we should also present the benefits of good usability. When the personnel can use IT systems effectively, the saved time can be used for serving the customers better or doing other essential tasks. This will certainly raise employee and customer satisfaction. Could we compare the satisfaction rates of healthcare professionals in different organizations? Would this ease the recruiting of new personnel? Would the personnel of "better ICT" organization be happier?

4.3.4. Improvement of mutual understanding

For customers, it's not always easy to describe what they need, especially when the needs are related to the future or non-familiar technologies. Customers might not be able to see the situations which need expertise and the problems and needs related to those situations. (48) Those are one of the reasons why the close cooperation with the customers is vital. Fujitsu is already close to some of the customers, but could it be even closer.

Could the understanding between Fujitsu and healthcare organizations be increased by organizing workshops in which the problems and possible solutions are discussed thoroughly? As one interviewee presented, often each organization is solving common problems by itself instead of solving it with other similar organizations. That is why the participants of the workshops could be from multiple organizations. Thus, the problems would be seen from many angles, and the amount of possible solutions would be greater. If the services are thus far tailored for one customer at a time, with workshops like this Fujitsu could hit several birds with one stone. Sponsoring for this kind of even could be asked from Finland's Ministry of Social Affairs and Health or other same kind of organizations.

4.3.5. Creation of overall concept

Some interviewees wanted to create an overall concept of information security for healthcare in which the needs of healthcare are taken care of. The challenge in this is that usually the organizations cannot afford to invest to all these services at the same time. Thus the concept should be able to cut into small packages.

According to the interviews, the most valuable information security services for the healthcare organizations would be these six services: SSO, smart card, virtualization, solutions for mobile work, IdM (Identity Management), and automated log alarms and reports. Also regular information security trainings and information security portal should be included.

The benefits of SSO service are phenomenal. Having only one password or PIN code, and being able to log in to multiple applications and systems quickly, ease the work of healthcare professionals quite a lot. When a smart card is connected with SSO and other systems needing authentication, the benefits are high. The practice of combining the non-functioning of the smart card and the absence of information security trainings motivates the personnel of ISSHP to attend to the trainings.

Virtualization of the workstations and sessions has removed the possibility for personal changes by the personnel. Because of that ISSHP has avoided malwares and re-installations which followed from changes users made. Some of the changes also affected on the functioning of information systems. In addition to security, this solution brings also cost savings.

The solutions for mobile work have enhanced above all the work of homecare nurses and enhanced information security when the information systems are used from external networks. Even though the laptop would end up to wrong hands, the losses would be just hardware, not the information itself. Mobile work is also increasing in the future when the amount of for example home care and electronic consultation increases.

IdM service brings, in addition to security, also cost savings because the amount of manual work decreases. Users are equipped with proper rights, not too little or too much, according to their roles.

The idea of automatic log reports, which are created by investigating use profiles, sounds very interesting. Thus the probability of getting caught from looking irrelevant information would increase. But first we should test can we truly see the misuse through use profiles. It would be interesting to see if the misuse cases can be revealed in real-time.

The implementation process should be part of the overall concept. It should describe what the implementation requires from the customer. The overall concept could include a proposal of the order in which the separate services could be implemented if they were not implemented all at the same time.

4.3.6. Segmenting marketing materials

Marketing materials should be segmented to better take into account the needs of healthcare. Thus the customer could see that the problems of his sector are taken truly care of and the solutions are tailored to fulfill his needs.

Marketing materials could include case stories of other healthcare customers and how they have experienced information security services. If the writing of the case stories can be outsourced to some objective party, the message of the stories would be even more credible. In addition, the stories could be presented in a video. Thus the stories would be more personal, and the solutions could be described by other means than just words. The videos could be available in the internet or be just short clips which a salesperson can show to support his speech.

4.3.7. Increasing the information security knowledge of salespersons

One of the challenges in the selling of information security services has been that the salespersons don’t know enough about information security. On the other hand, the problem is that the information security services aren’t productized so far that those would be easy to sell. One interviewee mentioned that information security is related to specific persons.

Even though the information security specialists would know how the unfinished services could be finalized into a proper service, for salespersons it could be impossible because they don't have enough understanding about information security. In addition to finalizing of the services, a small training of information security for salespersons wouldn't make things worse. For example the information security specialists of Fujitsu could give them a training session. The session could be filmed, in which case it could be watched also later.

The salespersons should know about information security that much that they could spot, and on some level even analyze the problems, in customers' organizations. Even though the salespersons couldn't be able to present a proper technical solution for the problem, they could tell the customer that Fujitsu can solve the need and pass the message to some information security specialist.

4.3.8. Improving security awareness in Fujitsu

One of the interviewees highlighted the importance of management leading by example. Why couldn't Fujitsu show example to the customers too? When information security is in good shape in Fujitsu, the message is better passed to customers.

When information security is properly recognized from own actions, one can better notice the possibilities for enhancements from his own organization and also from other organizations. That is why information security should be even more highlighted in Fujitsu. Every person, who is in a relation to customers, could be able to spot the possible problems.

In addition to annual trainings, could the personnel do also an annual self-assessment test about their own information security practices? In the self-assessment test the user could give realistic answers because the detailed results could be private and showed only to the person himself. The person could compare the results of different years and see if his actions have changed. The averages of the self-assessment tests could be visible for the management who could react to unexceptional trends. The training and self-assessment concept could be commercialized also to customers. The self-assessments could be tied to be a part of the trainings and the questions could be like

> "I look that the persons, to whom I open the door, have an access card with them."
> Always – usually – often – sometimes – never
>
> "I don't use the same password to my home computer and for the information systems of my employer."
> Always – usually – often – sometimes – never

Another way to bring information security more forward could be different kind of theme weeks during which the information security could be presented in a playful ways. There could be competitions like who spotted unlocked computers from the office the most. The events could generate also nice stories to amuse the customers. Why not to have fun with information security?

4.3.9. View to the future

Since one of the key elements in ISSHP concept has been the planning for the future, it would be essential for Fujitsu too to help other healthcare organizations to prepare for the future in early phase. The workshops, mentioned earlier, could also take into account the future visions, not just current problems. Also services of Fujitsu should be developed with a vision about the future in mind.

5. Conclusions

The purpose of this study was to find out, how Fujitsu should develop the information security services to better respond the needs of healthcare, and how to market the services in an effective, healthcare oriented way. An additional question was how the processes, practices, and marketing of Fujitsu could be developed? These were all answered in some way.

During this study, we familiarized with the state of information security in healthcare, and what is required from it. We started from getting familiar with information security terms and the legislation related to health information. We took a look at the national centralized healthcare services, KanTa services, and what kinds of information security solutions are essential for healthcare.

We interviewed ten specialists of information security, healthcare, and/or sales, and pulled together the main points of the interviews. The interviews were very fruitful and gave a great view to the industry through the eyes of professionals. By analyzing the results we were able to recommend solutions with which the challenges could be overcome.

The main idea behind the recommended solutions was better communication. Better communication inside Fujitsu overall, between sales and the information security specialist, and between Fujitsu and customers. Also a recommendation for healthcare information security service concept was given.

This study was tried to do in an objective way, but as in all qualitative research, some subjective factors cannot be left without notice. The results of this study might be on some level biased due the great percentage of Fujitsu representatives. Most of the interviewees had also some ties to ISSHP. That might have made ISSHP look so much better than other healthcare organizations. Each interviewee was also found through Fujitsu contacts.

Also the interview questions and the interpretations of the interviewees' opinions might have been biased because of the interviewer. What the interviewer has valued important or interesting and what doesn't? As the author of this study didn't have very much experience about information security before, she might have had not that much perspective of the field.

The competence of the development suggestions might have been more sophisticate, with a longer familiarization to Fujitsu and also to ISSHP. When the organization is more familiar, more appropriate solution models can be given.

Some minor changes could have been done now when we look back the journey travelled. For example all of the questions were not asked from all of the interviewees. Some more information could have been obtained if those all would have been asked. And instead of asking what effects on purchasing decision, we could have asked which factors effect on the attitude towards information security and the development of information security concept during the development process. For salespersons it's better to think of the whole process than just purchasing situation.

The method of this research, interviewing, requires a lot from the interviewer. In this study the interviewer was quite inexperienced with the method. Some additional information could have been available, if the interviewer was more experienced.

How to continue after this study? For Fujitsu, it could be valuable to evaluate the suggested solutions through the eyes of the organization and to think if there is another ways to solve the problems than the ones presented. On the other hand the solutions of one researcher, not too familiar with the organization, might seem a bit unqualified, but after all be the ones no one else in the organization could have seen.

As in all development projects, also in this coming implementation project of these suggested solutions, the first thing is to find out a common scope for different parties. In this implementation process many specialties are needed and communication is a big issue. Common goal should be defined. What do we truly want to do? How to ensure that every one, taking part to the implementation, has the same interoperable goal?

This same question is important also to the whole healthcare sector of Finland. How the processes and technologies should be implemented that those serve the common goal – healthier people. The results of this will be left seen.

6. Bibliography

1. The Hippocratic Oath. *U.S. National Library of Medicine.* [Online] June 24, 2010. [Cited: September 05, 2011.] http://www.nlm.nih.gov/hmd/greek/greek_oath.html.

2. **Suomen Lääkäriliitto - Finnish Medical Association.** *Lääkärin etiikka - Physician´s Ethics.* 6th. Joensuu : PunaMusta Oy, 2005.

3. **Tammisalo, Tero.** *Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt.* Helsinki : Stakes, 2005.

4. **Järvinen, Petteri.** *Tietoturva & yksityisyys.* Porvoo : Docendo Finland Oy, 2002.

5. Sähkökatko sekoitti sairaalan Mikkelissä. *Itä-Savo.* [Online] June 16, 2011. [Cited: September 8, 2011.] http://www.ita-savo.fi/Uutiset/11339124.html.

6. Laaja potilastietojen urkinta paljastunut Helsingissä. *YLE.* [Online] July 12, 2011. [Cited: September 8, 2011.] http://www.yle.fi/uutiset/kotimaa/2011/07/laaja_potilastietojen_urkinta_paljastunut_helsingissa_2720182.html.

7. *Kansallinen Terveysarkisto - National Archive of Health Information.* [Online] Kela - The Social Insurance Institution of Finland. [Cited: March 31, 2011.] http://www.kanta.fi.

8. **Fujitsu.** Datasheet - Identity Management. [Online] [Cited: September 15, 2011.] http://www.fujitsu.com/downloads/EU/fi/pdf/services/idm08.pdf.

9. **Hämäläinen, P, Reponen, J and Winblad, I.** *eHealth of Finland - Check point 2008.* Jyväskylä : Gummerus Printing, 2009.

10. **Fujitsu.** Fujitsu Finland. [Online] [Cited: May 09, 2011.] www.fujitsu.com/fi.

11. **Itä-Savon sairaanhoitopiirin kuntayhtymä.** Itä-Savon sairaanhoitopiiri. [Online] [Cited: May 09, 2011.] http://www.isshp.fi/.

12. **Savon sanomat.** Laatutunnustus Itä-Savon sairaanhoitopiirille. [Online] September 30, 2008. [Cited: May 10, 2011.] http://www.savonsanomat.fi/uutiset/savo/laatutunnustus-it%C3%A4-savon-sairaanhoitopiirille/247610.

13. **SHQuality.** Laaduntunnustuksen edellytykset. [Online] June 14, 2007. [Cited: May 10, 2011.] http://www.labquality.org/LQ/(S(anzrcpzrs4git055fvbkdoyy))/pdf.aspx?dir=3&path=SHQuality/5.2_Laaduntunnustuksen_edellytykset.pdf.

14. **Kansikas, Aarno (Information security consultant in Fujitsu).** *Discussion about information security in ISSHP.* April 15, 2011.

15. **Ministry of Finance.** Tietoturvatasot. [Online] April 22, 2009. [Cited: May 11, 2011.] http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/08_muut_julkaisut/TTT_esite_low.pdf.

16. **KanTa - National Archive of Health Information.** Tietoturvallisuus - Information security. *Information security policy of KanTa-services.* [Online] January 1, 2011. [Cited: March 8, 2011.] https://www.kanta.fi/c/document_library/get_file?uuid=25efb0ee-fd88-4d8d-870a-ae8a40ef10af&groupId=10206.

17. **Parliament of Finland.** Act on Electronic Signatures 617/2009. *FINLEX.* [Online] August 7, 2009. [Cited: February 24, 2011.] http://www.finlex.fi/fi/laki/ajantasa/2009/20090617.

18. **Gollmann, Dieter.** *Computer Security.* Chichester : John Wiley & Sons, Ltd, 2006.

19. **Jain, A.K, Bolle, R and S, Pankanti.** Introduction to biometrics. *Biometrics - Personal Identification in Networked Society.* New York : Kluwer Academic Publishers, 2002.

20. **Valtionhallinnon tietoturvallisuuden johtoryhmä.** Käyttövaltuushallinnon periaatteet ja hyvät käytännöt - VAHTI 9/2006. *Valtiovarainministeriö.* [Online] November 22, 2006. [Cited: May 03, 2011.] http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf.

21. **Salovuori, Jarno.** Haamukäyttäjä on riski. *Kauppalehti.* 23th May, 2011.

22. **Winblad, I, et al.** *Informaatio- ja kommunikaatioteknologian käyttö Suomen terveydenhuollossa vuonna 2007 - Tilanne ja kehityksen seuranta.* Helsinki : Stakes, 2008.

23. **Tammisalo, Tero.** *Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi - Periaatteet ja menetelmät.* Helsinki : Stakes, 2007.

24. *Potilastietojärjestelmät tuotemerkeittäin arvioitu - Kaikissa on kehitettävää.* **Winblad, I, et al.** 50-52, s.l. : Suomen Lääkärilehti, 2010, Vol. 65.

25. Kiristys rajapinnoilla kaatoi palkitun ohjelmistoyhtiön. *Tietoviikko.* [Online] October 29, 2008. [Cited: September 8, 2011.] http://www.tietoviikko.fi/kaikki_uutiset/kiristys+rajapinnoilla+kaatoi+palkitun+ohjelmistoyhtion/a151346.

26. *HL7 Finland Ry.* [Online] [Cited: September 10, 2011.] http://www.hl7.fi/.

27. **Valtiontalouden tarkastusvirasto.** *Sosiaali- ja terveydenhuollon valtakunnallisten IT-hankkeiden toteuttaminen.* Helsinki : Edita Prima Oy, 2011.

28. **Ministry of Transport and Communications.** *Tuotteva ja uudistuva Suomi - Digitaalinen agenda vuosille 2011-2020.* Vantaa : s.n., 2010.

29. **Parliament of Finland - Committee for the Future.** *The Future of Health Care - The Position of the Committee for the Future on Health Care in the Year 2015.* 2006.

30. **City of Lahti.** Terveyskioski. *Lahden kaupunki.* [Online] [Cited: September 14, 2011.] http://www.lahti.fi/www/cms.nsf/pages/77EA625C07037671C22576E1004B36DF.

31. Taltioni. [Online] Sitra. [Cited: September 14, 2011.] http://www.taltioni.fi/.

32. R-Bay. [Online] [Cited: September 14, 2011.] http://www.r-bay.org/.

33. **Parliament of Finland.** Client data act 159/2007. *FINLEX.* [Online] February 9, 2007. [Cited: March 11, 2011.] http://www.finlex.fi/fi/laki/ajantasa/2007/20070159.

34. **Parliament of Finland.** Act on ePrescriptions 61/2007. *FINLEX.* [Online] February 2, 2007. [Cited: March 11, 2011.] http://www.finlex.fi/fi/laki/ajantasa/2007/20070061.

35. **Ministry of Social Affairs and Health.** Decree on Patient Documents 298/2009. *FINLEX.* [Online] March 30, 2009. [Cited: March 11, 2011.] http://www.finlex.fi/fi/laki/alkup/2009/20090298.

36. **Parliament of Finland.** Personal Data Act 523/1999. *FINLEX.* [Online] April 22, 2009. [Cited: March 11, 2011.] http://www.finlex.fi/fi/laki/ajantasa/1999/19990523.

37. **Parliament of Finland.** Health Care Act 1326/2010. *FINLEX.* [Online] December 30, 2010. [Cited: March 31, 2011.] http://www.finlex.fi/fi/laki/ajantasa/2010/20101326.

38. **Ministry of Social Affairs and Health.** Terveydenhuoltolaki - usein kysyttyjä kysymyksiä (Healthcare Act FAQ). *Ministry of Social Affairs and Health.* [Online] January 26, 2011. [Cited: April 07, 2011.] http://www.stm.fi/vireilla/lainsaadantohankkeet/sosiaali_ja_terveydenhuolto/terveydenhuoltolaki/10.

39. **ISO - International Organization for Standardization.** *ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002.* Brussels : s.n., 2008.

40. **Kela – The Social Insurance Institution of Finland.** Sähköinen lääkemääräys vaatimusmäärittely - Yleiskuvaus. *Kansallinen Terveysarkisto.* [Online] January 26, 2011. [Cited: April 12, 2011.]

https://www.kanta.fi/c/document_library/get_file?uuid=008f6ef1-2fab-479c-8bfe-5c63ae240b63&groupId=10206.

41. **Kela - The Social Insurance Institution of Finland.** Määrittelyt eArkistolle - KanTa-jatkomäärittely - Yleiskuvaus. *Kansallinen Terveysarkisto.* [Online] November 02, 2007. [Cited: April 27, 2011.] https://www.kanta.fi/c/document_library/get_file?uuid=70e2e46a-1431-44e6-9dc1-a4de2ac39e0d&groupId=10206.

42. **Ruotsalainen, P and Mykkänen, J.** *Menetelmä sosiaali- ja terveydenhuollon tietojärjestelmien sertifiointivaatimusten tuottamiselle.* Helsinki : Stakes, 2008.

43. *Authorisation and access control for electronic health record systems.* **Blobel, Bernd.** Magdeburg, Germany : s.n., 2004, International Journal of Medical Informatics, Vol. 73/3, pp. 251-257.

44. **Miettinen, Anneli.** Pätkätyön tulevaisuus. [Online] 2007. [Cited: June 15, 2011.] http://vaestoliitto-fi-bin.directo.fi/@Bin/572b0a277037b06260cc39a9a3d82a27/1308133883/application/pdf/386606/P%C3%A4tk%C3%A4ty%C3%B6n%20tulevaisuus.pdf.

45. **Sarvimäki, Pirjo.** Sosiaalialan ammattihenkilöiden foorumin lausunto Kaste II valmistelua varten. *Sosiaaliportti.* [Online] March 28, 2011. [Cited: June 15, 2011.] http://www.sosiaaliportti.fi/File/6786e277-af48-4777-a891-5a5a2f0de962/SOSIAALIALAN_FOORUMIN_LAUSUNTO_KASTE_II_OHJELMAAN_2011.pdf.

46. **Fujitsu.** Itä-Savon sairaanhoitopiiri 9.11.2010. *Teemat: Vakiointi, Tunnushallinta, Kertakirjautuminen, Office Communicator, Mobiili kotihoito, Toimiva leikkaussali.* [Video recording]. Savonlinna : s.n., November 9, 2010. Speakers: Hemmo Pirhonen, Ari Pätsi, Antti Kaipainen, Ari-Pekka Salo.

47. **Hirsijärvi, Sirkka and Hurme, Helena.** *Teemahaastattelu.* Helsinki : Gaudeamus, 1982.

48. **Koivisto, Mikko.** Mitä on palvelumuotoilu? [Online] 2007. [Cited: September 26, 2011.] http://www.muova.fi/documents/key20110926152126/Raportit%20ja%20julkaisut/Lopputyo_TaM_MikkoKoivisto_2007.pdf.

7. Appendices

7.1. Appendix A: Interview questions

Questions were asked in Finnish, but are here also translated in English.

General questions / Yleiset kysymykset

What does information security mean to you? How is it shown in your daily life?
Mitä tietoturva sinulle merkitsee? Miten se näkyy arjessasi?

What encourages healthcare organizations to develop identification, identity management, and information security over all?
Mikä kannustaa terveydenhuollon organisaatiota kehittämään tunnistusta, käyttäjätietojen hallintaa ja tietoturvallisuutta yleensä?

What kind of problems and needs do healthcare organizations have with identity management, user identification, and information security over all?
Millaisia ongelmia ja tarpeita terveydenhuollossa on käyttäjätietojen hallinnassa, käyttäjien tunnistamisessa ja tietoturvallisuudessa yleensä?

How does third parties effect on the information security of healthcare organization?
Miten ulkopuoliset tahot vaikuttavat terveydenhuollon organisaation tietoturvaan? Miten hyvin olet perillä ulkoisista vaatimuksista?

Does information security get enough attention in healthcare?
Saako tietoturva ansaitsemansa huomion terveydenhuollossa? Kiinnitetäänkö tietoturvaan tarpeeksi huomiota?

For persons knowing ISSHP / ISSHP:n tuntevat

What was the process that led to the current ISSHP concept?
Miten ISSHP:n konseptiin päädyttiin?

What is good about the concept? What needs to be developed?
Mitä siinä on hyvää? Mitä kehitettävää?

Compared to other healthcare organizations, what is better / worse in ISSHP concept? Why?
Verrattuna muihin terveydenhuollon organisaatioihin, mikä ISSHP:n konseptissa on paremmin / huonommin? Miksi?

What has been easy / difficult during the implementation process? Why?
Mikä on ollut helppoa / hankalaa käyttöönottoprosessin aikana? Miksi?

What brings savings / costs in the concept? Why?
Mikä konseptissa tuo säästöjä / kuluja? Miksi?

How are the benefits / results of the concept being measured? How are those being utilized?
Miten konseptin hyötyä / tuloksia mitataan? Miten niitä on hyödynnetty?

Has the everyday life of an employee become easier / harder? How?
Onko työntekijän arki helpottunut / vaikeutunut? Miten?

Which technological solutions of ISSHP are particularly beneficial according to your experiences?
Mitkä ISSHP:lla käytössä olevat tekniset ratkaisut ovat erityisen hyödyllisiä kokemustesi perusteella?

Can the concept be copied to other hospital districts like it is now?
Voiko konseptia monistaa tällaisenaan muihin sairaanhoitopiireihin?

What kind of vendor Fujitsu is? What is your opinion about the cooperation with Fujitsu? Good? Bad? How does Fujitsu differ from others?
Millainen Fujitsu on toimittajana? Millaista on ollut yhteistyö Fujitsun kanssa? Hyvää? Huonoa? Miten Fujitsu erottuu muista?

For persons not familiar with ISSHP / Ei ISSHP:tä tuntevat

Are you familiar with ISSHP concept? In which kind of situations you have heard about it? What kind of impression have you got? What kind of concept ISSHP has compared to other organizations?
Oletko tietoinen ISSHP:n konseptista? Missä yhteydessä olet törmännyt siihen? Millainen kuva sinulle on konseptista muodostunut? Millainen ISSHP:n konsepti on verrattuna muihin organisaatioihin?

What does generate costs in the information security of healthcare? What should be developed to get the greatest savings?
Mikä terveydenhuollon tietoturvassa yleensä aiheuttaa kuluja? Mitä kehittämällä saadaan suurimmat säästöt?

Can the work of the personnel be made easier with some specific solutions? Are there some solutions which enhance the information security, but make the work itself harder?
Voidaanko joillain tietoturvaratkaisuilla helpottaa henkilökunnan työtä erityisesti? Onko jotain ratkaisuja jotka parantavat tietoturvaa, mutta vaikeuttavat työtä?

What kind of impression you have about Fujitsu as a vendor? Good? Bad? How does Fujitsu differ from others?

Millainen on mielikuvasi Fujitsusta toimittajana? Hyvää? Huonoa? Miten Fujitsu erottuu muista?

Usability view / Käytettävyysnäkökulma

In the publicity, difficulties in the use of patient information systems have been discussed. What do you think about it?
Julkisuudessa on paljon puhuttu potilastietojärjestelmien vaikeakäyttöisyydestä. Mitä mieltä olet tästä?

Salespersons view / Myyjän näkökulma

How well are you familiar with the information security services of Fujitsu?
Kuinka hyvin olet perillä Fujitsun tarjoamista tietoturvapalveluista?

Why are the current information security services hard to sell?
Miksi nykyisiä tietoturvapalveluja on vaikeaa myydä?

What kind of concept would be easier to sell?
Millaista konseptia olisi helppo myydä?

Which are the 3 most important factors of the purchase decision?
Mitkä ovat 3 tärkeintä ostopäätökseen vaikuttavaa tekijää?

Future / Tulevaisuus

To what direction does the IT of healthcare develop?
Mihin suuntaan terveydenhuollon tietotekniikka kehittyy?

What kinds of challenges are coming? What are “the traditional problems” of the future?
Mitä haasteita tulossa? Mitkä ovat tulevaisuuden ”perinteisiä ongelmia”?

What kinds of development needs are coming? How the current or future needs could be solved?
Millaisia kehitystarpeita on tulossa? Eli miten ratkaistaan nykyiset tai tulevat haasteet?

How information security can adapt for the changes?
Miten tietoturvan sopeuduttava muutoksiin?

Final questions / Lopuksi

Do you have something in your mind what you would like to highlight or add?
Tuleeko mieleesi vielä jotain, jota haluaisit tuoda esille?

7.2. Appendix B: Backgrounds of the interviewees

Interview number	Date of interview	Phone interview	Speciality				Organization		
			Infromation security	Healthcare	Sales	Other	Fujitsu	ISSHP	Other
1	21.6.2011		x				x*		
2	28.6.2011		x				x*		
3	30.6.2011	x		x	x		x		
4	14.7.2011		x				x		
5	1.8.2011	x	x	x					x
6	19.8.2011		x				x*		
7	23.8.2011				x		x*		
8	25.8.2011	x	x	x				x	
9	6.9.2011		x		x		x		
10	9.9.2011	x		x		x		x	

* = involved with ISSHP

7.3. Appendix C: Detailed results of the interviews

Note: Marking (h1) after the sentence refers to interview number one, (h2) to interview number 2 and so on. Some sentences are mentioned multiple times, when the sentence is related to multiple topics. The relevant point is underlined.

C1. Overview of the information security in healthcare

Tietoturvaan tulisi kiinnittää huomiota

Terveydenhuollossa tietoturvan on oltava korkealla tasolla. Tietoturva on monimutkaista, haastavaa ja tarpeet kasvavat jatkuvasti. (h7)

Tietoturva on terveydenhuollossa tärkeintä tietohallinnon kannalta. (h8)

Tietoturvalla on usein liian matala prioriteetti sen tarpeellisuuteen nähden. (h3)

Tietoturvaan voitaisiin kiinnittää terveydenhuollossa enemmänkin huomiota. (h6)

Tietoturva ei saa ansaitsemaansa huomiota terveydenhuollossa. Monesti se koetaan välttämättömänä pahana ja harvassa paikassa se on kunnossa. Liian usein tietoturva delegoidaan "pois silmistä". (h7)

Tietoturva ei saa ansaitsemaansa huomiota terveydenhuollossa. Puhutaan paljon, mutta tekoja ei ole. Tässä esteenä on kentän monimuotoisuus ja perehtyneisyyden puute. Toisaalta myös välinpitämättömyys vaivaa, eli työnnetään pää pensaaseen ja ajatellaan "ei ole ennenkään tapahtunut mitään". Investoinnit ovat kalliita ja kiireeseen on myös helppo vedota. (h8)

Mielestäni tietoturva saa terveydenhuollossa aika hyvin ansaitsemansa huomion. Terveydenhuollon toimijat ovat kuitenkin isoja yksiköitä, joissa on pätevä IT-puoli, joka ymmärtää haasteet. Tosin IT-puoli ei välttämättä tunnista esimerkiksi käyttäjien tuskaa runsaasta salasanamäärästä. (h9)

Tietoturvaan kiinnitetään terveydenhuollossa kyllä tosi paljon huomiota, mutta käytännön tasolla, jokapäiväisessä työssä, ei mielletä mitä tietoturva tarkoittaa. Esimerkiksi työmatkalla, puhelimessa tai ruokalassa saatetaan puhua työasioista huomioimatta, kuinka monen sivullisen korvaan asia kantautuu. (h10)

Terveydenhuollon organisaatiot poikkeavat muista

Tietoturvan hyödyt nähdään parhaiten kun ollaan toimialassa (esimerkiksi terveydenhuollossa) paremmin sisällä (h7)

Terveydenhuollon erottaa muista organisaatioista erityisesti se että heillä tieto on erikseen suojattua lainsäädännöllä, henkilökunnalla saattaa olla paljonkin erilaisia rooleja (hoitosuhde potilaaseen, tutkia, esimies) ja erityyppisiä työsuhteita on paljon (keikkalääkärit, päivystäjät, lyhyet työsuhteet). (h9)

Terveydenhuollossa tietojen käytön tekee haastavaksi se, että potilaalta on erikseen kysyttävä, mihin tietoja saa käyttää ja mitä ei (h9)

Terveydenhuollossa on tärkeää, ettei myöskään puhuttu tieto kantaudu vääriin korviin. (h6)

Tietoturva nähdään haittana tai kuluna

Haasteena on, ettei tietoturvaan haluta satsata rahallisesti. (h1)

Tietoturvan taloudellinen perustelu ja ROI:n määritys on vaikeaa. (h1)

Pääsääntöisesti tietoturva aiheuttaa vain kuluja (pl. automaattinen tunnushallinta). (h1)

Asiakkaat [Fujitsun] kokevat tietoturvan kustannuksena (h4)

Tietoturvaa on vaikea perustella taloudellisesti. Laadulliset parannukset ja normien täyttämiset ovat yleensä perusteena hankinnoille. (h5)

Usein mielletään että tietoturva "haittaa toimintaa". (h5)

Tietoturvaan kiinnitetään kyllä huomiota, mutta se koetaan lähinnä pakkopullana, joka häiritsee muuta toimintaa. (h3)

Kansa ei ole perillä terveydenhuollon tietoturvan tasosta

Yhteiskunta olettaa tietoturvan olevan paremmassa kunnossa kuin se välttämättä onkaan. (h3)

Kansa ei ole tietoinen tietoturvan oikeasta tolasta terveydenhuollossa. (h4)

Henkilöstö on kuitenkin usein valveutunutta

Terveydenhuollon ammattihenkilöstö on varsin valveutunutta verrattuna muihin työntekijöihin. Tietosuoja-asiat ovat hyvin tunnettuja heidän keskuudessaan. (h5)

Käyttäjän otettava vastuuta

Nykyään kaikki tieto on saatavilla ja tietojen saatavuutta ei myöskään voida rajata käyttöoikeuksilla liikaa. Käyttäjän itsensä on otettava vastuu siitä, mitä tietoja hän saa käyttää. (h6)

Terveydenhuollossa saattaa potilaan tietoja tarvita kiireellisestikin, joten pääsyoikeuksia ei voida paljoa rajoittaa. Tämän takia jälkiseurannan on oltava tehokasta. Jälkiseuranta voitaisiin toteuttaa esimerkiksi tiedon louhinnan (data mining) avulla. (h9)

Lainsäädäntö pakottaa tietoturvan kehittämiseen

Parannuksia tietoturvaan saadaan vain lainsäädännön avulla. (h1)

Säädökset sanelevat pitkälti terveydenhuollon tietoturvatason (h3)

Kaikilla toimijoilla on samat ongelmat, joita kaikki yrittävät ratkaista kukin omalla tavallaan. (h7)

"Jos saisin itse päättää, määräisin kansallisen tietoturvapolitiikan, jota kaikkien on pakko noudattaa. Nykyiset suositukset ovat liian löysiä." (h7)

Vahinkoja sattuu

Eniten kuluja aiheuttaa teknisen tietoturvan asiat (laaja kokonaisuus). Myös vahingot saattavat olla massiivisen kalliita. Esimerkiksi jos järjestelmät eivät käytössä, aikoja joudutaan perumaan. (h5)

Tietoturvaan tajutaan satsata vasta kun jotain sattuu (h1)

Terveydenhuollon tietosuojarikkeet huomioidaan kyllä. Bisnespuolella uutiskynnys harvoin ylittyy, mutta potilaiden tietosuojan yksityisyydenloukkaukset, myös yksittäistapaukset, saavat paljon huomiota erityisesti lehdistössä. (h5)

Kehityskohteita ovat: oikeat valtuudet oikeilla ihmisillä, tiedon käytön seurattavuus, tiedon saatavuuden varmistaminen, helppokäyttöisyys (h4)

Tietoturvaymmärrys puuttuu

Viime aikoina tietoturvaymmärrys on parantunut. (h2)

[Fujitsun] asiakkailla tietoturvan johtaminen ei ole aina kunnossa. (h3)

Haasteena on se että ei löydy tarpeeksi ymmärrystä siitä, että tietoturva ei hoidu pelkästään teknisiä ratkaisuja ostamalla. (h3)

Kaikki organisaatiot eivät ymmärrä, että heillä ei ole niin hyvät käytännöt kuin voisi ja tarvitsisi olla. (h3)

Tietoturvaan ei budjetoida tarpeeksi eikä käyttäjäorganisaatio kiinnitä siihen tarpeeksi huomiota. IT-organisaation puolelta huomiota kyllä heruisi. (h4)

Suurin ongelma ja tarve terveydenhuollossa on tietoturvan merkityksen korostaminen. Ei ymmärretä että tietoturva on jatkuva prosessi. (h7)

Terveydenhuollossa tietoturva-asiat saattavat olla kunnossa, vaikkei tietoturvaa olekaan suoranaisesti huomioitu tai tunnistettu. Organisointi saattaa olla heikolla tolalla, mutta asiat silti kunnossa. (h5)

Pitkäjänteistä kehittämistä ei ole

Haasteena on että asiakas ei ajattele pitkän aikavälin tapahtumia. Eletään tässä fiskaalissa/kvartaalissa. (h1)

Haasteena on, että pitkäjänteinen kehittäminen puuttuu. (h3)

Moninaiset tietojärjestelmät aiheuttavat haasteita

Potilastietojärjestelmien lukumäärä tuottaa haasteita. (h6)

Terveydenhuollossa on ongelmana, että järjestelmät eivät ole tietoturvamielessä lain vaatimalla tasolla, kaukana siitä. (h8)

Terveydenhuollon haasteena on valtava määrä järjestelmiä ja potilastietoja monissa eri järjestelmissä. Myös järjestelmätoimittajat haluavat pitää kiinni asemistaan, eivätkä halua avata rajapintoja. (h9)

Tekniikka asettaa haasteita

Tekniikka, ja sen jatkuvuus erityisesti, asettaa omat haasteensa. (h2)

Tietotekniikka kahlitsee liian paljon työaikaa. (h10)

Kehityskohteita saatetaan löytää, kun tyytymättömyydet puretaan osiin. (h5)

Ei ole tarpeeksi resursseja

Mitä enemmän lokitetaan, sitä vähemmän saadaan selville, koska aikaa lokiselvitysten tekemiselle ei ole. Henkilökunta erityisesti IT-puolella on kiireistä. (h5)

Terveydenhuollossa on konsultoinnin tarvetta, mutta ei välttämättä rahaa siihen (h5)

Kansallinen yhdistäminen

Kansallinen yhdistäminen on haastavaa. (h6)

Terveydenhuollon keskitetyt järjestelmät ovat vaikeita rakentaa. Muun muassa Kanta-hanke on osoittanut tämän. Asiakkaalla on harvoin tietoa, miten tällainen järjestelmä pitäisi rakentaa. (h9)

Tietoturvaratkaisu SSO

Kertakirjautuminen on harvoja asioita, jotka helpottavat käyttöä. (h9)

SSO on myös tärkeä työkalu terveydenhuollossa, sillä kukaan ei pysty muistamaan tunnuksiaan. Erityisesti verkossa oleva SSO on joustavampi terveydenhuollon ympäristöön, sillä tällöin SSO:sta voi hyötyä jokaisella päätteellä, ei ainoastaan sillä, jonne salasanalista on tallennettu. (h9)

Tietoturvaratkaisu IdM

Vuosien saatossa käyttöoikeushallinta on muuttunut terveydenhuollossa vaikeammaksi, koska työsuhteet ovat muuttuneet epästabiilimmiksi. (h9)

Käyttöoikeushallinta asettaa haasteita terveydenhuollolle: kuka saa oikeudet ja miten asianmukainen käyttö selvitetään jälkikäteen. (h9)

Eniten kuluja terveydenhuollossa aiheutuu käyttöoikeuksien ja tunnusten manuaalisesta hallinnasta. Käyttäjiä ja järjestelmiä on paljon, käyttäjät ovat epästabiileja. Tämä altistaa virheille. (h9)

Kun IdM on hyvin toteutettu, oikeat ja sopivat oikeudet ovat taattuja. (h9)

Käyttöoikeuksia tietoihin voitaisiin myöntää hoitojaksokohtaisesti, eli kun hoitojakso päättyy, poistuvat käyttöoikeudet. (h9)

Käyttäjätietojen hallintaa tarvitaan, mutta sen toteuttaminen on hankalaa. Organisaatiot ovat suuria ja toteutusta varten on liian vähän osaajia ja rahaa. "Arvaisin, että koska käytössä huomattavan rikas määrä sovelluksia, käyttäjähallinnan integrointi on hyvin haastavaa." (h5)

Kehityskohteita ovat: oikeat valtuudet oikeilla ihmisillä, tiedon käytön seurattavuus, tiedon saatavuuden varmistaminen, helppokäyttöisyys (h4)

Tietoturvaratkaisu virtualisointi

Terveydenhuollossa on tärkeä miettiä, missä dataa voidaan tallentaa ja katsoa. Esimerkiksi kotisairaanhoidossa olisi hyvä, että hoitaja pääsee käsiksi potilastietoihin ja pystyy tallentamaan tietoja suoraan potilaan luona. Kuitenkaan datasta ei saisi jäädä mitään talteen puhelimeen/päätteeseen, jolla dataa on käsitelty. Mahtaakohan lainsäädännössä olla jopa pykälä, joka kieltää potilastietojen siirtämisen sairaalan ulkopuolelle. Tähän ongelmaan tuo ratkaisun esimerkiksi virtuaalityöpöytä. Tällöin käyttäjä näkee datasta ainoastaan kuvan. (h9)

Tietoturvaratkaisu automaattinen lokien tarkistus

Lokijälkien tarkistusta on kehitettävä automaattiseksi. Todennäköisyyden sille, että jää kiinni epäolennaisten tietojen katselusta, on oltava suuri. Tarkistuksen pitäisi olla reaaliaikaista toimintaa. Sen voisi toteuttaa esimerkiksi tiedonlouhinnan (data mining) avulla. Lokitiedoista voitaisiin etsiä esimerkiksi käyttöprofiileja, jotka eivät ole tarkoituksenmukaisia. (h9)

Kehityskohteita ovat: oikeat valtuudet oikeilla ihmisillä, tiedon käytön seurattavuus, tiedon saatavuuden varmistaminen, helppokäyttöisyys (h4)

C2. Who effects on the information security of healthcare

Lainsäädäntö

Lait asettavat myös vaatimuksia. Käytön seurannan on oltava järjestelmällistä. (h6)

Lainsäädännön lisäksi terveydenhuollon organisaation tietoturvaan vaikuttaa kentän laajuus aina apteekeista sosiaalihuoltoon. (h9)

Terveydenhuollon tietoturvaan vaikuttaa erityisesti valtio lainsäädännön kautta. Myös yhteistyökumppanit, sekä heidän mahdollisuudet ja mahdottomuudet. Lisäksi yhteiskunnassa tapahtuvat muutokset vaikuttavat, kuten rikollisuus, kehitys, uudet tavat murtautua… Näissä on pysyttävä ajan tasalla (h8)

Vaikuttajat: lainsäädäntö, yhteiskunta, kansainvälisyys (h2)

Vaikuttajat: pakko (lait, asetukset, sanktiot laiminlyönneistä, maineen menetys) (h3)

Tietoturvallisuuden kehittäminen lähtee liikkeelle lainsäädännöstä. Myös tekniikka vaikuttaa. (h6)

Tietoturvaan kannustaa: lainsäädäntö eniten (tietosuoja mielessä), yksityisellä puolella bisnes ja maine, tunnistautumisessa voidaan saada "pikavoittoja", kun valitaan oikeita tekniikoita, erityisesti ratkaisuja jotka hyödyttävät käyttäjää, käytettävyys ja saatavuus (h5)

Vaikuttajat: lainsäädäntö, Yleinen hektisyys (Moititaan terveydenhuollon tietojärjestelmien laatua, mutta samaan aikaan vaaditaan kuitenkin tehostamista), E-toiminta yksi muutoksen kohta (verkkoasiointi lisääntyy, Kun uusi sukupolvi asiakkaaksi, se luo paineita, että asioita on pystyttävä hoitamaan kuten pankissakin, eli verkossa) (h5)

Toimittajat

Vaikuttajat: Toimittajakenttä vaikuttaa tietoturvaan. Esimerkiksi toimialajärjestelmien toimittajat eivät katso kokonaisetua asiakkaan silmin. Tämä aiheuttaa ristiriitoja ja toimimattomia rajapintoja. Kokonaisarkkitehtuurin näkemys puuttuu. (h4)

Haasteiden syynä ovat muun muassa vanhat järjestelmät, joiden muuttaminen on jäykkää. Näiden järjestelmien toimittajat eivät ole kovin joustavia muutoksille. (h4)

Terveydenhuollossa on hajanainen järjestelmäkokonaisuus ja paljon toimittajia välissä. Järjestelmiä on hankala saada yhdistettyä. (h8)

Terveydenhuollossa on vaikea toteuttaa tietoturvavaatimuksia, kun ei ole järjestelmiä, joilla niitä voitaisiin toteuttaa. (h8)

Haasteena on tietosuojan problematiikka: vanhojen järjestelmien takia lokitus on hankalaa ja huonoa, käyttöoikeuksilla voitaisiin tietosuojaloukkauksia ehkäistä, mutta potilaan hoito ei saa keskeytyä. Tästä syystä järjestelmiin on taattava suhteellisen vapaa pääsy. (h5)

Vaikuttajat: sidosryhmät (federointi), asiakkaat, järjestelmien myyjät ja ylläpitäjät (h1)

Lisäksi terveydenhuollossa on haasteena, että kaikkien järjestelmien on sovittava työprosesseihin ja organisaation omiin vaatimuksiin. (h8)

E-ratkaisut

E-jutut lisäävät tietoturvatietoisuutta. (h5)

E-resepti ja e-arkisto kannustavat julkista puolta kehittämään tietoturvaa. (h5)

E-ratkaisut vaikuttavat myös organisaation tietoturvaan. Sekä ammattilaiset että kansalaiset pääsevät käsiksi tietoihin ja kansalaiset voivat myös valvoa omien tietojensa käyttöä. (h6)

Kansalliset e-ratkaisut pakottavat miettimään asioita uudestaan. (h7)

Vaikuttajat: lainsäädäntö, Yleinen hektisyys (Moititaan terveydenhuollon tietojärjestelmien laatua, mutta samaan aikaan vaaditaan kuitenkin tehostamista), E-toiminta yksi muutoksen kohta (verkkoasiointi lisääntyy, Kun uusi sukupolvi asiakkaaksi, se luo paineita, että asioita on pystyttävä hoitamaan kuten pankissakin, eli verkossa) (h5)

Muut sidosryhmät

Lainsäädännön lisäksi terveydenhuollon organisaation tietoturvaan vaikuttaa kentän laajuus aina apteekeista sosiaalihuoltoon. (h9)

Terveydenhuollon tietoturvaan vaikuttaa erityisesti valtio lainsäädännön kautta. Myös yhteistyökumppanit, sekä heidän mahdollisuudet ja mahdottomuudet. Lisäksi yhteiskunnassa tapahtuvat muutokset vaikuttavat, kuten rikollisuus, kehitys, uudet tavat murtautua... Näissä on pysyttävä ajan tasalla (h8)

Vaikuttajat: sidosryhmät (federointi), asiakkaat, järjestelmien myyjät ja ylläpitäjät (h1)

Alan toimijat vaikuttavat tietoturvaan. Muun muassa sosiaalitoimen yhdistäminen ja organisaatiorakenteen muuttuminen vaikuttaa. (h6)

Pelko maineen menetyksestä

Tietoturvan kehittämiseen terveydenhuoltoa kannustaa julki tulleet tapaukset, joissa tietoturva on pettänyt sekä pelko maineen menetyksestä. (h7)

Vaikuttajat: pakko (lait, asetukset, sanktiot laiminlyönneistä, maineen menetys) (h3)

Tietoturvaan kannustaa: lainsäädäntö eniten (tietosuoja mielessä), yksityisellä puolella bisnes ja maine, tunnistautumisessa voidaan saada "pikavoittoja", kun valitaan oikeita tekniikoita, erityisesti ratkaisuja jotka hyödyttävät käyttäjää, käytettävyys ja saatavuus (h5)

Pyrkimys parempaan käytettävyyteen

Tietoturvaan kannustaa: lainsäädäntö eniten (tietosuoja mielessä), yksityisellä puolella bisnes ja maine, tunnistautumisessa voidaan saada "pikavoittoja", kun valitaan oikeita tekniikoita, erityisesti ratkaisuja jotka hyödyttävät käyttäjää, käytettävyys ja saatavuus (h5)

Kehityskohteita ovat: oikeat valtuudet oikeilla ihmisillä, tiedon käytön seurattavuus, tiedon saatavuuden varmistaminen, helppokäyttöisyys (h4)

Potilaat

Se että potilaat osaavat vaatia tietoonsa, kuka heidän tietojaan on katsonut ja onko tietoja käytetty oikein, luo paineita tietoturvaan panostamiselle. (h7)

Vaikuttajat: sidosryhmät (federointi), asiakkaat, järjestelmien myyjät ja ylläpitäjät (h1)

Yhteiskunta ja sen muutokset

Terveydenhuollon tietoturvaan vaikuttaa erityisesti valtio lainsäädännön kautta. Myös yhteistyökumppanit, sekä heidän mahdollisuudet ja mahdottomuudet. Lisäksi yhteiskunnassa tapahtuvat muutokset vaikuttavat, kuten rikollisuus, kehitys, uudet tavat murtautua... Näissä on pysyttävä ajan tasalla (h8)

Vaikuttajat: lainsäädäntö, yhteiskunta, kansainvälisyys (h2)

Vaikuttajat: lainsäädäntö, Yleinen hektisyys (Moititaan terveydenhuollon tietojärjestelmien laatua, mutta samaan aikaan vaaditaan kuitenkin tehostamista), E-toiminta yksi muutoksen kohta (verkkoasiointi lisääntyy, Kun uusi sukupolvi asiakkaaksi, se luo paineita, että asioita on pystyttävä hoitamaan kuten pankissakin, eli verkossa) (h5)

Kansainvälisyys

Vaikuttajat: lainsäädäntö, yhteiskunta, kansainvälisyys (h2)

Tekniikka

Tietoturvallisuuden kehittäminen lähtee liikkeelle lainsäädännöstä. Myös tekniikka vaikuttaa. (h6)

C3. Implementation of information security of healthcare organization

Asennejuttu

Parhaimmillaan tietoturvaa ei edes huomata. (h2)

Tietosuoja on pyhää. (h2)

Asenne luo mahdollisuudet toimia, ei aidan matalinta kohtaa. (h2)

Tietoturva tulisi saada osaksi normaalia toimintaa. (h2)

Tietoturva pitäisi saada osaksi toimintakulttuuria. (h2)

Tietoturva on asennejuttu. (h4)

Terveydenhuollossa on kaikissa toimissa huomioitava tietoturva ja tietosuoja. (h8)

Implementointi

Tietoturva on ennen kaikkea prosessi. (h5)

Tammisalon raportit (23) (3) ovat ehkä hiukan huonosti markkinoituja. Ne eivät ole täydellisiä, mutta hyviä kenkälusikoita. (h5)

Johdon sitoutuminen ja ymmärrys

Tärkeää on asiakkaan oma aktiivisuus sekä johdon sitoutuminen. (h1)

Tärkeää on, että asiakas ymmärtää tietoturvan merkityksen ja organisaatio on motivoitunut. (h2)

Tärkeää on, että hallinto on mukana kehittämisessä ja ymmärtää tietoturvan tärkeyden, muutoin on tehtävä suuri työ perusteltaessa tietoturvan tärkeyttä. (h2)

Pitkäjänteinen suunnittelu ja panostus ovat tärkeitä. (h4)

Haasteena on että ei mielletä tietojärjestelmien käyttöönoton olevan suuri projekti. Saatetaan sanoa, että puolen vuoden päästä on uusi järjestelmä käytössä, vaikkei edes määrittelyä ole tehty. Ostajapuolen osaamattomuus. Aikataulut kohtuuttomia. (h5)

Erityisesti haluan korostaa, että toiminnan on oltava suunniteltua, prosessinomaista ja organisoitua. Johdon sitoutuminen on erittäin tärkeää. (h8)

Haluan korostaa, että kaikessa on tärkeää, että johto sitoutuu ja näyttää mallia. Jos johto suhtautuu tietoturvaan retuperäisesti, on tuloksena "sitä saat mitä niität". (h10)

Käyttäjälähtöisyys

On lähdettävä liikkeelle siitä, että tietojärjestelmiä tehdään käyttäjille. Käyttäjätyytyväisyys on ensimmäinen asia ja sen kautta kehitetään tunnistusta ja käyttäjätietojen hallintaa sekä tietoturvaa ylipäätään. (h8)

Kilpailutus

Julkiset kilpailutukset ovat haastavia. Jos kilpailutus tehdään löysin rantein, on pakko ottaa järjestelmä jota ei haluta. Kilpailutusten pitkät kestot tuovat myös haasteita. (h4)

Uusi hankintalaki kieltää huomioimista valintakriteerinä toimittajan referenssit. Laki antaa uusille tulijoille mahdollisuuden. (h5)

Koulutus

Koulutus on haastavaa ja kallista, mutta erittäin tärkeää. (h1)

Kaikki henkilöstö ei ole saanut koulutuksensa ohessa tietoteknistä opetusta. (h6)

Tekniikan käyttö luo omat haasteensa. Työntekijöiden on opeteltava koko ajan uutta tekniikkaa. Samaan aikaan on pidettävä myös oman alan tietämys ajan tasalla. (h6)

Tärkeää on, että tekniikkaa osataan käyttää niin hyvin, että asiakasvuorovaikutus säilyy. Myös potilasta on kyettävä huomioimaan. (h6)

Kun tietojärjestelmät ovat käytössä ja niitä osataan käyttää, saadaan säästöjä. (h6)

Kuluja aiheuttaa

Kuluja tuottaa teknisen ympäristön rakentaminen sekä koulutus. Pitkässä juoksussa nämä tuovat todennäköisemmin kuitenkin säästöjä. (h6)

Muutosvastarinta

Uusien käytäntöjen käyttöön otossa muutosvastarinta on aina suurin vastustaja ja tästä tuskin koskaan päästään täysin eroon. Sitä voitaisiin kuitenkin mahdollisesti vähentää markkinoimalla muutokset käyttäjäkunnalle hyvin. Tulisi viestiä, että uudella käytännöllä halutaan helpottaa myös työntekijän työtä, eikä niitä tehdä pelkästään jonkin toisen tahon hyväksi. (h10)

C4. The experiences of ISSHP

Suunnittelu pitkällä tähtäimellä, johdon sitoutuminen, kokonaisvaltaisuus ja työntekijöiden ylpeys

ISSHP:ssä on visioitu 3-5 vuoden jaksoissa. (h7)

ISSHP:ssä on oltu e-jutuissa mukana ja huomattu, että ajoissa varautuminen kannattaa. (h7)

ISSHP:ssä katsottiin vuonna 2002 yhteiskunnan asettamat vaatimukset. Määriteltiin myös, mitä itse odotetaan tietoturvalta ja laadittiin tavoitteet tietoturvalle. Määritettiin toimenpiteet suunnitelman toteuttamiseksi ja toteutettiin ne askel askeleelta. (h8)

ISSHP:ssä on suunniteltu tietoturvaa 3 vuoden jaksoissa ja määritelty, mitkä ovat kriittisiä kehityskohteita. (h8)

ISSHP:n konsepti on pitkälti Pätsin [tietohallintopäällikkö] ansiota. Kun tulossa olevat muutokset, kuten uudet potilastietojärjestelmät, kansallinen muutos sekä sähköiset ratkaisut, on tiedetty, on voitu tehdä kehitystä pitkällä (5 ja 10 vuotta) tähtäimellä eikä vasta sitten kun on pakko. (h6)

ISSHP:llä on nähty tietoturva ja tietosuoja tärkeänä, on haluttu olla edelläkävijöitä ja etsitty uusia toimintatapoja ja kustannustehokkuutta. (h6)

Muista organisaatioista ISSHP eroaa siinä, että siellä on mietitty kokonaisuutta, oltu suunnitelmallisia ja organisoitu. (h8)

ISSHP sai ensimmäisenä ylimmän tietoturvaluokituksen. (h7)

ISSHP:n konseptissa hyvää on kokonaisvaltaisuus. (h8)

On kiva, että ISSHP:llä ollaan edelläkävijöitä tässä asiassa. Olen siitä ylpeä. (h10)

ISSHP:n tietoturvakonsepti kestää arvostelun. Työntekijät ovat ylpeitä työpaikkansa tietoturvasta ja he voivat luottaa siihen, että asiat ovat kunnossa (h7)

ISSHP:ssä tietoturvasta on luotu jatkuva toimintatapa; sen hallintoa ja johtamista on tuettu ja se on hyvin jalkautettu (h3)

ISSHP:ssä hyödyt katsottiin ydinliiketoiminnan kautta. (h7)

ISSHP:ssä johto keskustelee keskenään, eikä kuilua esimerkiksi IT-johdon ja ylimmän johdon välillä ole. (h7)

ISSHP:n malli on pitkälle optimoitu ja monia asioita on testattu käytännössä ja havaittu joko hyviksi tai huonoiksi. (h6)

ISSHP:n konseptissa on erityisen hyvää se, että se ottaa käyttäjät huomioon. (h6)

Ulkoistus

ISSHP:ssä päätettiin, ettei tehdä asioita itse vaan haetaan parhaat toimijat. (h7)

Ulkoistamisen hyödyt on ISSHP:ssä nähty. (h1)

ISSHP:ssä omalla tietohallinnalla on ollut kehitysvastuu ja kaikki, mikä on voitu ulkoista, on ulkoistettu. (h6)

Yleistä

ISSHP:n elinmahdollisuudet riippuvat tietotekniikan toimivuudesta. Kun tietotekniikka toimii, henkilökuntaa ei tarvita niin paljon. (h7)

ISSHP:n tietoturvaa ohjaa periaate: "Ei voida pyrkiä täydellisyyteen tietoturvassa, mutta pyritään tekemään murtautuminen niin hankalaksi, ettei mielenkiintoa siihen löydy". (h8)

ISSHP:ssä huomattiin, että käyttöoikeuksien hallinta on suurin riskitekijä ja fyysinen turva seuraava. (h1)

ISSHP:n teknisistä ratkaisuista "autiosaarelle" ottaisin mukaan vahvan tunnistautumisen, kertakirjautumisen, virtualisoinnin sekä sisäverkon tietoturvateknologian (palomuurit yms.). (h8)

Vertailu muihin

Verrattuna muihin terveydenhuollon organisaatioihin, Itä-Savossa on paljon omaa tietohallinnon väkeä. Lisäksi heillä johto on hyvin sitoutunut ja systemaattinen organisointi on aloitettu aikaisin. (h6)

Verrattuna muihin organisaatioihin, ISSHP:ssä on kokonaisuus kunnossa. Muilla tietoturvana on yleensä vain lokitietojärjestelmä ja "lukitse koneesi"-kehotus. (h7)

Verrattuna muihin organisaatioihin, ISSHP:llä tietoturvaan on erityisesti panostettu. (h10)

Mielikuva ISSHP:stä

Olen saanut positiivisen kuvan ISSHP:n ratkaisusta. Etuna heillä on tosin pienikokoinen organisaatio, joka on helpompi hallita. (h5)

Monistaminen muualle

ISSHP:n konseptia voi pitkälti monistaa tällaisenaan muihin sairaanhoitopiireihin. Tosin erilaiset potilastietojärjestelmät ja tekniset ympäristöt tuovat haasteita. (h6)

ISSHP:n konseptia on monistettu jo Careaan ja Etelä-Karjalaan. (h7)

Haastavaa

Haasteena on ollut erityisesti, että henkilökunta joutuu mukautumaan muutoksiin sekä se, että järjestelmiä on pitänyt yhtenäistää toimijoiden (kuten e-reseptin myötä apteekkien) kanssa. (h6)

Kehitysprosessissa on ollut haastavaa se, että tehdään paljon asioita, prosessien vieminen kentälle, sekä Fujitsun kannalta on jouduttu miettimään palveluita toimialan kannalta eikä tehdä kaikkea samalla muotilla. (h6)

ISSHP:n konseptin haasteena on, etteivät järjestelmien toimittajat kykene vaadittavaan tasoon. (h8)

Jatkuvan kehityksen oravanpyörän mukana pysyminen on haastavaa. (h8)

Käyttöönottoprosessissa hankalaa on ollut resurssien hyödyntäminen ja henkilökunnan motivointi. Henkilökunnan motivoimisen eteen on tehty paljon työtä ja tekemistä riittää edelleen. Se ei lopu ikinä. (h8)

Toimikorttien kanssa toimiminen on haastavaa. Kiire ja huolimattomuus vaivaavat ja kortti saattaa helposti unohtua koneeseen. Tarvittaisiin ehkä jämäkämpi ohjeistus siitä, ettei toimikorttia jätetä koneeseen. (h10)

Helppoa on ollut

Kehitysprosessin aikana helppoa on ollut erityisesti hyvät kumppanuussuhteet Fujitsun ja ISSHP:n välillä. (h6)

Käyttöönottoprosessi on ollut helppo sen jälkeen kun organisaatio ja prosessit on mietitty kunnolla ja yhteinen politiikka, linja, suunnitelmat ja tavoitteet löytyvät. Yksittäiset osa-alueet eivät ole olleet helppoja, koska paljon on pitänyt luoda tyhjästä. (h8)

Käyttöönottoprosessissa joillekin käyttäjille jotkut asiat ovat helppoa ja toisille samat asiat vaikeita. On siis vaikea sanoa, että jokin tietty asia olisi prosessissa ollut helppo. Ehkä perästäpäin voidaan todeta, että olihan tämä sittenkin helppoa. (h10)

Työtä helpottaa

Ensimmäinen juttu ISSHP:ssä oli kertakirjautuminen, joka helpotti työntekoa paljon. (h7)

Kortin käyttö ja virtuaalisuus helpottaa työtä. (h2)

Korttikirjautuminen monipuolisesti on hyvä juttu. (h1)

Työtä helpottaa järjestelmien keskinäinen kommunikaatio. Tieto on luettavissa yhdestä paikasta. (h4)

Virtuaalityöasemat helpottavat työtä. Istunto seuraa paikasta toiseen. (h4)

Työtä helpottaa yksikköjen välinen tiedon siirto. (h4)

Työtä helpottavat muun muassa kertakirjautuminen (koska terveydenhuollon järjestelmät ovat sirpaloituneita), vasteaikojen parantuminen (järjestelmiä muutettava ja kirjautumistekniikoita parannettava) sekä saatavuuteen ja käytettävyyteen liittyvät ratkaisut. (h5)

Työntekijän arki on jossain määrin helpottunut. Kaikki tieto on saatavilla järjestelmien kautta, korttikirjautuminen, videoneuvottelu, keskitetyt ratkaisut jne. (h6)

Erityisesti SSO on ISSHP:ssä helpottanut työntekijöiden arkea. (h7)

Kun tunnistaminen on helppoa ja kirjautuminen nopeaa, on järjestelmien käyttö helppoa ja säästää aikaa. (h8)

Työntekijän arki on helpottunut, koska tunnistautuminen on helppoa ja nopeaa, salasanoja on vähemmän, toiminta on nopeutunut, vahvan tunnistautumisen myötä on vain yksi kortti ja yksi PIN-koodi. (h8)

Erityisesti SSO helpottaa henkilökunnan työtä, koska tunnuksia ei tarvitse muistaa. Myös biometrinen tunnistaminen ja HSD- ja PKI-korttien käyttö työpöydän esiin saamiseksi helpottaa/helpottaisi työtä. (h9)

Uusien käytäntöjen ansiosta työntekijän arki on päivänselvästi helpottunut. Jo se helpottaa, että tieto viedään järjestelmään vain yhden kerran. Samasta asiakirjasta ei myöskään ole useita versioita (tähän suuntaan on ainakin pyrkimys). Tekniikassa on panostettu helppokäyttöisyyteen ja osattu ajatella käyttäjäystävällisesti. (h10)

Työntekijän arki on vaikeutunut lähinnä, koska uudistukset ovat asettaneet rajoja (mm nettisurffailu, työaseman muutokset). Rajoitusten avulla on pakotettu noudattamaan lakeja ja organisaation omia säädöksiä. (h8)

Sirukortit helpottavat työtä, kun PIN-koodi riittää. Biometriikassa sitäkään ei tarvittaisi. (h4)

Toimikortti on saavuttanut suuren suosion ISSHP:ssä, eikä sitä kukaan antaisi enää pois. (h10)

Säästöjä

IdM, kertakirjautuminen ja muut käyttöä helpottavat ratkaisut tuovat säästöjä (h4)

Virtuaaliympäristö ja istunnon säilyminen tuovat säästöjä. (h6)

Kotipalvelupuolella säästöjä voidaan saavuttaa erityisesti sillä, että kirjaukset voidaan tehdä suoraan paikanpäältä. (h6)

Palvelujen tuottaminen etänä tuo säästöjä. (h6)

ISSHP:n konseptissa tuo säästöjä erityisesti kertakirjautuminen ("miljoonaluokkien säästöt"). (h7)

ISSHP:ssä kaikelle lasketaan ROI, jonka pohjalta päätökset tehdään. Esim. OCS tuo paljon säästöjä, kun terveydenhoitajien ei tarvitse matkustaa parin tunnin kokousta varten pitkiä matkoja, vaan kokoukset voidaan käydä OCS:n välityksellä. (h7)

Konsepti tuo säästöjä koska järjestelmissä ei ole häiriöitä, kuten haittaohjelmia. Tällöin vältytään uudelleen asennuksilta. (h8)

Kun tukipalvelut ovat selkeitä ja ne ymmärretään, palvelua on helppo hyödyntää, eikä jäädä omalle työpisteelle pohtimaan ratkaisua ongelmaan. Tämä tuo säästöjä. (h6)

Konseptin hyötyjä mitataan rahallisesti erityisesti isoimmissa hankinnoissa. Muu kuin rahallinen mittaus on ympäripyöreämpää. Kyselemällä ja katselemalla on kuitenkin hyötyjä nähty. (h8)

Kun sekä Fujitsulla että asiakkaalla osataan palvelukokonaisuus, on palveluja helppo hyödyntää. Näin saadaan säästöjä. (h6)

Säästöä tuo käyttäjien automaattinen hallinta sekä virtuaalityöasemat (investoinnit ja lisenssit). Toimintojen helppous tuo tehokkuutta. (h2)

Kuluja

Kuluja aiheuttavat tilakustannukset, kun palvelimet yms. ovat asiakkaan omissa tiloissa. Toisaalta yhteydet ovat tällöin halvemmat ja riskit pienemmät. (h2)

ISSHP:ssä kuluja aiheuttaa jatkuvat uudistuskustannukset, koska koko ajan mennään kauhealla vauhdilla eteenpäin. (h7)

Konseptissa kuluja tuottaa se, ettei kehitys lopu koskaan. Joka vuosi on investoitava. (h8)

Kehitettävää

Kentällä näytön eteen tarvittaisiin suojuksia, jotta sivullisten olisi vaikeampaa nähdä mitä näytöllä tapahtuu. (h10)

Kehitettävää ISSHP:ssä löytyy muun muassa päätteiden sijoittelusta yksiköissä. Huomiota tulisi kohdistaa siihen, ettei asiakas näkisi näytölle asioidessaan yksikössä. Monissa paikoissa sisään astuessaan asiakas kohtaa ensimmäisenä tietokoneen ja sitten vasta ihmisen. (h10)

Henkilökunnan tietoturvaosaaminen

Noin 7 vuotta sitten ISSHP:llä on aloitettu "puhtaat tietoturvakoulutukset". Jokainen työntekijä on velvoitettu käymään kerran vuodessa kahden tunnin mittainen tietoturvakoulutus. Toimikorttia hankittaessa on allekirjoitettava tietoturva ja tietosuojasitoumukset. (h6)

Tietoturvaosaamista ei ole ISSHP:llä säännönmukaisesti testattu, mutta mm. auditoinneissa on osaaminen huomioitu ja kehittymistä on selkeästi havaittu. Henkilökunta tiedostaa vaatimukset ja osaaminen havaitaan käytännössä. (h6)

ISSHP:n konseptissa on hyvää erityisesti se, että tietosuojaan on oikeasti panostettu henkilöstöresursseja. Kukaan ei voi sanoa ettei olisi saanut asioista tietoa. Tietoturva koulutukset ovat pakollisia, vaikkakin sisällössä on vielä kehitettävää. Ylipäätään tietoturva tuodaan lähelle henkilöstöä. (h10)

ISSHP:ssä SSO-kortti menee vanhaksi, ellei koulutuksissa ole käyty. (h7)

Tietoturvaportaali

Tietoturvaportaalissa tietoturvatieto on keskitetysti yhdessä paikassa, jossa voidaan tehdä myös riski-ilmoitukset. (h6)

Tietoturvaportaalista saatu palaute on ollut positiivista: kaikki aineisto on yhdessä paikassa ja tiedetään oikea väylä riski-ilmoituksiin. (h8)

ISSHP:llä on käytössä seurantajärjestelmä ja "pelotteena" toimii "käyttöä seurataan"-toteamus. Tietoturvaloukkaukset käsitellään aina ja jokainen palaute kirjataan. Kyseisten henkilöiden kanssa keskustellaan, mutta niistä ei ilmoiteta kuin lukumäärällisesti henkilökunnalle. (h6)

C5. Fujitsu and the information security of healthcare

Fujitsun tietoturvastrategia

Fujitsu tarvitsisi pitkäjänteisempiä strategioita tietoturvapalvelujen myyntiin. (h4)

Tietoturvapalveluja on vaikea myydä koska palveluja ei ole selkeästi kuvattu eikä tuotteistettu tarpeeksi pitkälle, niin että myyjät sen kunnolla ymmärtäisivät. Asiakkaiden parissa tietoturvaa ei ole mielletty tärkeänä osana ja Fujitsulla tietoturvaosaaminen on henkilösidonnaista. (h6)

ISSHP:n kehitysprosessissa on ollut haastavaa se, että tehdään paljon asioita, prosessien vieminen kentälle, sekä Fujitsun kannalta on jouduttu miettimään palveluita toimialan kannalta eikä tehdä kaikkea samalla muotilla. (h6)

Tietoturva Fujitsussa

Meillä Fujitsulla tietoturvan pitää olla kunnossa, jotta voidaan olla luotettava toimittaja. Laadun tae, sertifikaatit. (h7)

Tietoturva ei ole Fujitsussa erillinen kokonaisuus vaan osa toimintaa. (h7)

Konsepti

Terveydenhuollon tietoturvassa oleellista on kokonaisvaltainen ote, ei yksittäisratkaisuja, jatkuva hallintamalli, johtaminen, resurssit kunnossa sekä kokonaisuus. (h3)

Tietoturvapalveluja on vaikea myydä, koska palveluja ei ole selkeästi kuvattu eikä tuotteistettu tarpeeksi pitkälle, niin että myyjät sen kunnolla ymmärtäisivät. Asiakkaiden parissa tietoturvaa ei ole mielletty tärkeänä osana ja Fujitsulla tietoturvaosaaminen on henkilösidonnaista. (h6)

Nykyisiä tietoturvapalveluja on hankala myydä koska Fujitsulla ei ole kokonaisvaltaista konseptia vaan palikoita. (h7)

Nykyisiä tietoturvapalveluja on vaikea myydä, koska asiakkaille pitäisi pystyä kuvaamaan prosessi. (h9)

Myyntimateriaali pitäisi muokata sellaiseksi, että myyjä ymmärtää sen komponentit. Tällöin uskalletaan lähteä kertomaan asiakkaille juttuja, kun ymmärretään palveluiden sisältö ja sovelluskohteet. (h9)

Jotta tietoturvakonseptin myyminen olisi helpompaa, pitäisi ensin pystyä luomaan kuva koko terveydenhuollon kentästä ja sen tarpeista. Pitäisi luoda kokonaisvaltainen tarina ja tietoa, millä tavalla alan ongelmat ratkaistaan. (h9)

Myyjien tietoturvatietämys

Myytäessä on tärkeä mennä asenne edellä. Pitää tietää mitä myydään. (h2)

Myyjät kokevat tietoturvan hankalana ja monimutkaisena. (h4)

Myyjät tarvitsevat koulutusta, tukea ja asennekasvatusta. (h4)

Asennekasvatus on tärkeää sekä myyvässä että ostavassa organisaatiossa. (h4)

Tietoturvapalveluja on vaikea myydä, koska palveluja ei ole selkeästi kuvattu eikä tuotteistettu tarpeeksi pitkälle, niin että myyjät sen kunnolla ymmärtäisivät. Asiakkaiden parissa tietoturvaa ei ole mielletty tärkeänä osana ja Fujitsulla tietoturvaosaaminen on henkilösidonnaista. (h6)

Nykyisiä tietoturvapalveluja on hankala myydä, koska myyjät eivät ymmärrä mistä tietoturvassa on kysymys. (h7)

Myyjät saattavat olla hanakoita ottamaan uusia tietoturvaprojekteja käsiinsä, jos aiemmat toimitusprojektit ovat menneet huonosti. (h9)

Myyjille saattaa olla hankalaa löytää oikea, asiakkaalle sopiva, tuote tietoturvapaletista. He eivät osaa välttämättä soveltaa tietoturvapalveluja asiakkaan tarpeiden mukaiseksi. Myyjät ja asiakkaat eivät aina ymmärrä, että kaikkia palveluita ei tarvitse ottaa kerralla, vaan voidaan valita tällä hetkellä oleellisimmat. (h9)

Asiakkaiden tietoturvaymmärrys

Asennekasvatus on tärkeää sekä myyvässä että ostavassa organisaatiossa. (h4)

Tietoturvapalveluja on vaikea myydä, koska palveluja ei ole selkeästi kuvattu eikä tuotteistettu tarpeeksi pitkälle, niin että myyjät sen kunnolla ymmärtäisivät. Asiakkaiden parissa tietoturvaa ei olla mielletty tärkeänä osana ja Fujitsulla tietoturvaosaaminen on henkilösidonnaista. (h6)

Nykyisiä tietoturvapalveluja on hankala myydä, koska niitä ei arvosteta tarpeeksi. (h7)

Nykyisiä tietoturvapalveluja on hankala myydä, koska tietoturvaan ei haluta satsata, vaan mennään sieltä missä aita on matalin. (h7)

Nykyisiä tietoturvapalveluja on hankala myydä, koska tietoturvaa ei nähdä huipputärkeänä, kuten pitäisi. (h7)

Asiakkaiden saamat hyödyt esille

Asiakkaille on tehtävä selväksi, mitä hyötyjä he tietoturvasta saavat. (h4)

Ostopäätökseen vaikuttaa

Lainsäädäntö/vaatimustenmukaisuus tärkein ostopäätökseen vaikuttava tekijä (Valtionhallinnossa mitään ei tehdä, ellei siitä ole säädetty laissa). Myös raha vaikuttaa. Takaisinmaksuaikojen laskeminen on kuitenkin vaikeaa. (h1)

Ostopäätökseen vaikuttavat kustannukset (raha, tiukat budjettiraamit), resurssit (itse osaaminen) ja asenteet (hyötyä ei mitata, kustannushyötyihin ei uskota). (h2)

Ostopäätökseen vaikuttavat kustannukset, miten nopeasti palvelu saadaan käyttöön sekä miten palvelu asiakasta hyödyttää. (h4)

Ostopäätökseen vaikuttavat hinta (tärkein), laadulliset kriteerit sekä yhteensopivuus olemassa olevien tekniikoiden kanssa. (h5)

Ostopäätökseen vaikuttaa eniten hinta, sitten luottamus toimittajaan sekä toimittajan vakavaraisuus ja asiantuntemus. (h6)

Terveydenhuollossa kolme tärkeintä tietoturvan ostopäätökseen vaikuttavaa tekijää ovat kansalliset ratkaisut, se ettei haluta lehtien sivuille (maine) ja se mitä laki sanoo. (h7)

Fujitsussa hyvää

Yhteistyö Fujitsun kanssa on ollut hyvää perustietotekniikan suhteen. Hankalaa on ollut saada innovatiivisia projekteja läpi, koska suuressa firmassa pyritään pitkälti standardisoimaan palvelut ja tekemään kaikki asiat samalla tavalla kaikille asiakkaille. (h8)

Fujitsusta tekee hyvän se, että me tunnemme terveydenhuoltoalan. Toimintamme perustuu toimintaprojekteihin, joissa ollaan hyviä. (h9)

C6. Future visions

Yhteiskunta

Verkkorikollisuus

Tulevaisuuden haasteena on verkkorikollisuus. (h1)

KV-säädökset ja käyttäjien valvonta lisääntyy. Sähköinen resepti on kohteena väärentäjille. Tiedon välitys leviää (turvallisuus huomioitava). (h2)

Organisoidut globaalit tietomurrot lisääntyvät. Tosin on epätodennäköistä että niitä tapahtuisi Suomessa. (h3)

Tietämättömyydestä johtuvat väärinkäytöt laajenevat, kansallisten ratkaisujen myötä

Tulevaisuudessa pääosin tietämättömyydestä johtuvat väärinkäytöt laajenevat, kun samalla kertaa päästään ei vain oman sairaalan vaan lähes koko Suomen tietoihin. (h3)

Valvonta lisääntyy

KV-säädökset ja käyttäjien valvonta lisääntyy. Sähköinen resepti on kohteena väärentäjille. Tiedon välitys leviää (turvallisuus huomioitava). (h2)

Henkilöstökriisi

Pilvipalvelut ja e-hoidot luovat tietosuojahaasteita. Henkilöstökriisi väestön ikääntymisen myötä. (h5)

Väestön ikääntyminen

Pilvipalvelut ja e-hoidot luovat tietosuojahaasteita. Henkilöstökriisi väestön ikääntymisen myötä. (h5)

Resurssien määrä pienenee

Terveydenhuollon kustannusvaikutukset tulevat kasvamaan. Näitä kustannuksia pitäisi saada alenemaan. Kustannuksista paljon rahaa vie tietotekniikka, joka pitkälle vietynä vaatii suuria investointeja, mutta jotka tuovat suuria hyötyjä ja ajan kuluessa maksavat itsensä kyllä takaisin. Näitä muutoksia ei kuitenkaan tehdä yhdessä yössä. Haasteena on, miten maksavalle osapuolelle saadaan perusteltua hyötyjen korostuminen. (h10)

Tulevaisuudessa potilaan itsehoito ja -kontrolli lisääntyy. Järjestelmien sijaan ostetaan palveluita. Rahan ja IT-osaamisen vähyys sekä järjestelmien monimutkaisuus säilynevät samalla tasolla. (h5)

Tulevaisuudessakin on haasteena raha (miten tehdään kustannustehokkaasti), palveluiden helppokäyttöisyys, muutosvastarinta, puoltaako lainsäädäntö muutoksia ja onko riittävästi resursseja muutoksiin. (h6)

Sähköiset palvelut

Terveydenhuollon tietotekniikan suunta on selkeästi menossa sähköisen maailman, vailla rajoja, suuntaan. Jonain päivänä tullessani vastaanotolle, on minua vastaan ottamassa lukulaite, jolle ilmoitan saapumisestani. (h10)

Tulevaisuudessa palvelut siirtyvät yhä enemmän internetiin ja itsepalvelu lisääntyy niissä asioissa, jotka asiakas voi hoitaa itse (esim. ilmoittautuminen). Myös kansalliset ratkaisut tulevat. (h6)

Lainsäädännön mukauduttava

Tulevaisuuden haasteina ovat hajanainen kenttä, poliittinen tahto. (h7)

Tulevaisuudessakin on haasteena raha (miten tehdään kustannustehokkaasti), palveluiden helppokäyttöisyys, muutosvastarinta, puoltaako lainsäädäntö muutoksia ja onko riittävästi resursseja muutoksiin. (h6)

Muutosvastarinta

Tulevaisuudessakin on haasteena raha (miten tehdään kustannustehokkaasti), palveluiden helppokäyttöisyys, muutosvastarinta, puoltaako lainsäädäntö muutoksia ja onko riittävästi resursseja muutoksiin. (h6)

Tekniikka

Virtualisointi

Tulevaisuudessa virtualisointi, webbipohjaisuus, itsepalvelu ja helppokäyttöisyys lisääntyvät. Automaattiset mittauslaitteet tuottavat tietoa. (h4)

Tulevaisuuden terveydenhuollon tietotekniikka kehittyy virtualisoinnin ja mobiiliteknologian suuntaan. Jäljempänä tulevat myös pilvipalvelut. (h8)

Pilvipalvelut

Pilvipalvelut ja e-hoidot luovat tietosuojahaasteita. Henkilöstökriisi väestön ikääntymisen myötä. (h5)

Tulevaisuuden muutoksissa tietoturvan on kuljettava koko ajan mukana. Kyseenalaista on estääkö lainsäädäntö palvelujen tarjoamisen pilvestä. Tiedon on oltava suojattuna kaikissa olosuhteissa. (h6)

Tulevaisuuden terveydenhuollon tietotekniikka kehittyy virtualisoinnin ja mobiiliteknologian suuntaan. Jäljempänä tulevat myös pilvipalvelut. (h8)

Webpohjaisuus

Tulevaisuudessa virtualisointi, webbipohjaisuus, itsepalvelu ja helppokäyttöisyys lisääntyvät. Automaattiset mittauslaitteet tuottavat tietoa. (h4)

Tulevaisuudessa sovellukset muuttuvat selainpohjaisiksi. (h9)

Mobiiliteknologiat

Tulevaisuudessa erityisesti mobiilipäätteet tulevat kehittymään (kevyempiä, nopeampia). (h8)

Tulevaisuuden terveydenhuollon tietotekniikka kehittyy virtualisoinnin ja mobiiliteknologian suuntaan. Jäljempänä tulevat myös pilvipalvelut. (h8)

Liikkuva työntekijä

Tulevaisuuden haasteena on liikkuva työntekijä. Hänen tietosuojansa, tietoturvansa sekä toiminnan järjestäminen niin, että sama tieto on kaikkialla käytettävissä. (h8)

Avoimet verkot

Olettaisin myös että tulevaisuudessa, kun WLAN-yhteyden nopeutuvat, varsinaiset sisäverkot tulevat poistumaan ja verkot ”aukeavat”. Tällöin sisäverkkoon pääsyä kontrolloidaan VPN:n avulla. (h9)

Standardisoituminen

Tulevaisuudessa terveydenhuollon tietotekniikka standardisoituu. (h3)

Tulevaisuuden haasteena on perusjärjestelmien jäykkyys. Asiakkaiden tulisi vaatia parempaa, jotta kehitystä tapahtuisi. Helppokäyttöisyyden ja tietoturvan on mentävä rinnakkain. Monitoimittajaympäristö kehittyy. (h4)

Kansainväliset säädökset/ratkaisut

KV-säädökset ja käyttäjien valvonta lisääntyy. Sähköinen resepti on kohteena väärentäjille. Tiedon välitys leviää (turvallisuus huomioitava). (h2)

Tulevaisuutta ovat kansainväliset valmisjärjestelmäratkaisut, integroidut järjestelmät, yhtenäiset rajapinnat sekä konsolidoituminen toiminnallisesti ja tietoteknisesti. Tästä seuraa keskitetympää tietotekniikkaa. Myös tietoturvan rooli kasvaa. (h3)

Konsolidoituminen

Tulevaisuutta ovat kansainväliset valmisjärjestelmäratkaisut, integroidut järjestelmät, yhtenäiset rajapinnat sekä konsolidoituminen toiminnallisesti ja tietoteknisesti. Tästä seuraa keskitetympää tietotekniikkaa. Myös tietoturvan rooli kasvaa. (h3)

Tulevaisuudessa terveydenhuollon tietotekniikka konsolidoituu. (h7)

Tulevaisuudessa toimintoja konsolisoidaan isompiin syteemeihin. Esimerkiksi ennen kirurgian järjestelmään ovat päässeet vain kirurgit ja muu kirurgian henkilökunta. Kun kirurgian järjestelmä yhdistetään suurempaan ja kattavampaan järjestelmään, ei käyttöoikeuksia voida enää jakaa pelkästään tiettyyn järjestelmään, vaan on huomioitava mihin tietoihin käyttäjällä on oikeus päästä. Järjestelmien sisällä on alettava jakaa käyttöoikeuksia. (h9)

Yhtenäiset rajapinnat

Tulevaisuutta ovat kansainväliset valmisjärjestelmäratkaisut, integroidut järjestelmät, yhtenäiset rajapinnat sekä konsolidoituminen toiminnallisesti ja tietoteknisesti. Tästä seuraa keskitetympää tietotekniikkaa. Myös tietoturvan rooli kasvaa. (h3)

Tulevaisuudessa rajapintoja järjestelmien välille tullaan avaamaan ja järjestelmiä liitetään toisiinsa. (h9)

Integroidut järjestelmät

Tulevaisuutta ovat kansainväliset valmisjärjestelmäratkaisut, integroidut järjestelmät, yhtenäiset rajapinnat sekä konsolidoituminen toiminnallisesti ja tietoteknisesti. Tästä seuraa keskitetympää tietotekniikkaa. Myös tietoturvan rooli kasvaa. (h3)

Käytettävyyden korostuminen

Tulevaisuuden haasteena on perusjärjestelmien jäykkyys. Asiakkaiden tulisi vaatia parempaa, jotta kehitystä tapahtuisi. Helppokäyttöisyyden ja tietoturvan on mentävä rinnakkain. Monitoimittajaympäristö kehittyy. (h4)

Tulevaisuudessa virtualisointi, webbipohjaisuus, itsepalvelu ja helppokäyttöisyys lisääntyvät. Automaattiset mittauslaitteet tuottavat tietoa. (h4)

Tulevaisuudessa tietoturvan on sopeuduttava niin, että käytettävyys paranee ja turvallisuus säilyy, ollaan sitten kolmannen osapuolen tiloissa tai langattomissa verkoissa. (h8)

Tulevaisuus edellyttää, että Fujitsun on tehtävä palveluistaan selkeitä ja niin yksinkertaisia, että niitä on helppo käyttää. (h9)

Tulevaisuudessa tieto syötetään järjestelmään vain kerran. (h10)

Tulevaisuudessakin on haasteena raha (miten tehdään kustannustehokkaasti), palveluiden helppokäyttöisyys, muutosvastarinta, puoltaako lainsäädäntö muutoksia ja onko riittävästi resursseja muutoksiin. (h6)

Tietoturvan rooli kasvaa

Tulevaisuutta ovat kansainväliset valmisjärjestelmäratkaisut, integroidut järjestelmät, yhtenäiset rajapinnat sekä konsolidoituminen toiminnallisesti ja tietoteknisesti. Tästä seuraa keskitetympää tietotekniikkaa. Myös tietoturvan rooli kasvaa. (h3)

Tulevaisuudessa tietoturva tulee olemaan toptenissä. (h7)

Tietoturvan rooli tulee tulevaisuudessa kasvamaan. Painetta tulee muun muassa tekniseen suojaukseen (palomuuri yms.). Tieto ei saa livahtaa väärään paikkaan. (h10)

Tulevaisuuden muutoksissa tietoturvan on kuljettava koko ajan mukana. Kyseenalaista on estääkö lainsäädäntö palvelujen tarjoamisen pilvestä. Tiedon on oltava suojattuna kaikissa olosuhteissa. (h6)

Biometrinen tunnistautuminen

Olettaisin, että tulevaisuudessa biometriset tunnisteet tulevat terveydenhuoltoon. (h9)

Biometrinen tunnistaminen yleistyy tulevaisuudessa. (h9)

Ostetaan palveluja

Tulevaisuudessa potilaan itsehoito ja -kontrolli lisääntyy. Järjestelmien sijaan ostetaan palveluita. Rahan ja IT-osaamisen vähyys sekä järjestelmien monimutkaisuus säilynevät samalla tasolla. (h5)

Tulevaisuudessa prosesseja kehitetään edelleen, sairaanhoitopiirit yhdistyvät ja palveluja ulkoistetaan. Organisoiminen pysyy kuitenkin organisaatioilla itsellään. (h6)

Terveydenhuolto

Kansalliset ratkaisut

KV-säädökset ja käyttäjien valvonta lisääntyy. Sähköinen resepti on kohteena väärentäjille. Tiedon välitys leviää (turvallisuus huomioitava). (h2)

Lain antama mahdollisuus hoitopaikan valintaan, edellyttää, että minun perustietoni on oltava kaikkialla käytettävissä. Valtakunnallinen potilastietojärjestelmä on tulossa. Tämä tuonee kustannussäästöjä. (h10)

Tulevaisuudessa palvelut siirtyvät yhä enemmän internetiin ja itsepalvelu lisääntyy niissä asioissa, jotka asiakas voi hoitaa itse (esim. ilmoittautuminen). Myös kansalliset ratkaisut tulevat. (h6)

Sairaanhoitopiirien yhdistyminen

Tulevaisuudessa prosesseja kehitetään edelleen, sairaanhoitopiirit yhdistyvät ja palveluja ulkoistetaan. Organisoiminen pysyy kuitenkin organisaatioilla itsellään. (h6)

Tulevaisuudessa terveydenhuolto on suurempia kokonaisuuksia, koska piirien määrää vähenee. Tämän johdosta järjestelmiä tullaan yhdenmukaistamaan. (h7)

Terveydenhuollon tietojärjestelmien kehittäminen

Tulevaisuuden haasteena on perusjärjestelmien jäykkyys. Asiakkaiden tulisi vaatia parempaa, jotta kehitystä tapahtuisi. Helppokäyttöisyyden ja tietoturvan on mentävä rinnakkain. Monitoimittajaympäristö kehittyy. (h4)

Tulevaisuudessa terveydenhuolto on suurempia kokonaisuuksia, koska piirien määrää vähenee. Tämän johdosta järjestelmiä tullaan yhdenmukaistamaan. (h7)

Tulevaisuus edellyttää terveydenhuollon kannalta käyttöoikeuksien hallinnan käytäntöjen kehittämistä. (h9)

Potilaiden itsepalvelu

Tulevaisuudessa virtualisointi, webbipohjaisuus, itsepalvelu ja helppokäyttöisyys lisääntyvät. Automaattiset mittauslaitteet tuottavat tietoa. (h4)

Terveydenhuollon tietotekniikan suunta on selkeästi menossa sähköisen maailman, vailla rajoja, suuntaan. Jonain päivänä tullessani vastaanotolle, on minua vastaan ottamassa lukulaite, jolle ilmoitan saapumisestani. (h10)

Tulevaisuudessa potilaan itsehoito ja -kontrolli lisääntyy. Järjestelmien sijaan ostetaan palveluita. Rahan ja IT-osaamisen vähyys sekä järjestelmien monimutkaisuus säilynevät samalla tasolla. (h5)

Tulevaisuudessa palvelut siirtyvät yhä enemmän internetiin ja itsepalvelu lisääntyy niissä asioissa, jotka asiakas voi hoitaa itse (esim. ilmoittautuminen). Myös kansalliset ratkaisut tulevat. (h6)

Automaattiset mittauslaitteet

Tulevaisuudessa virtualisointi, webbipohjaisuus, itsepalvelu ja helppokäyttöisyys lisääntyvät. Automaattiset mittauslaitteet tuottavat tietoa. (h4)

Terveyden edistäminen

Tulevaisuudessa painopiste siirtynee terveyden edistämiseen. (h6)

Tulevaisuudessa terveydenhuolto painottuu sairauksien ennalta ehkäisyyn. Netissä saatetaan suorittaa terveystestejä, joiden perusteella "syöt liikaa rasvaa, käypäs ravintoterapeutin juttusilla". (h7)