Data Protection in the Pirkanmaa Hospital District Financial Services

Bachelor's thesis

Häme University of Applied Sciences, International Business

Spring 2020

Tuire Täyränen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Degree programme
Campus

Author Tuire Täyränen **Year** 2020

Title Data Protection in Pirkanmaa Hospital District Financial Services

Supervisor(s) Annaleena Kolehmainen

TIIVISTELMÄ

Opinnäytetyö käsittelee tietosuojan toteuttamista Pirkanmaan sairaanhoitopiirin talouspalveluissa. Opinnäytetyö on kirjoitettu PSHP:n talouspalveluiden toimistopäällikön pyynnöstä. Kirjoittaja on itse työskennellyt PSHP:n talouspalveluissa yli kymmenen vuotta, ja on tehnyt siellä monenlaisia potilaslaskutukseen liittyviä töitä. Aihepiiri oli vahvasti esillä vuonna 2017, kun uutiset toivat esiin EU:n uuden tietosuoja-asetuksen voimaan astumista vuonna 2018. Uutiset nostivat esiin kysymyksiä liittyen tietosuojaan potilaslaskutuksessa, eikä kysymyksiin saatu vastauksia PSHP:n tietosuojavastaavalta. Opinnäytetyössä käydään läpi tietosuojalainsäädäntöön liittyvää terminologiaa, sekä tärkeimpiä tietosuojaan vaikuttavia lakeja Suomen julkisessa terveydenhuollossa. Opinnäytetyö käsittelee siis pääasiassa kansallisia lakeja, ja kansallista julkista terveydenhuollon toimintaa. Työssä tutkitaan hieman myös, miten Helsingin kaupunki on toteuttanut vaadittavat uudistukset, koska julkisena toimijana Helsingin haasteet ovat samanlaisia kuin PSHP:n, ja käydään läpi PSHP:n talouspalveluiden työnkuvat niiltä osin, kuin ne ovat tekemisissä potilastietojen kanssa. Samassa yhteydessä käydään läpi myös yleisimpiä tietosuojasäännösten aiheuttamia ongelmia ja niihin keksittyjä ratkaisuja. Lopputuloksena on, että suurin osa esiin nousseista ongelmista on saatu ratkaistua, mutta joitakin ongelmia on jäljellä. Talouspalveluiden työntekijät kokevat tilanteen vaikeaksi, koska heillä ei ole työnantajalta ohjeistusta, miten toimia, ja he joutuvat itse päättämään lain noudattamisen, ja potilaan tilanteen ymmärtämisen ja inhimillisen kohtelun välillä. Opinnäytetyön tavoitteena on tuoda esiin pienen tukipalvelun merkitys potilaalle.

Avainsanat GDPR, tietosuoja, Pirkanmaan sairaanhoitopiiri, talouspalvelut, potilaslaskutus

Sivut 50 sivua, joista liitteitä 1 sivu

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Name of degree programme
Campus

Author Tuire Täyränen **Year** 2020

Subject Data Protection in Pirkanmaa Hospital District Financial Services

Supervisor(s) Annaleena Kolehmainen

ABSTRACT

This thesis focuses on to data protection in the Pirkanmaa Hospital District financial services. The thesis is written by the request of the Office Manager in PSHP financial services. The writer has worked in PSHP financial services for over 10 years and has done many jobs related to patient billing.

The subject of data protection was strongly presented in the news in 2017, because of the impending enforcement of the EU's data protection regulations in 2018. The news brought up questions about data protection in patient billing, but no answers were received from the PSHP data protection supervisor.

This thesis goes through the terminology used in data protection legislation and the most important Acts affecting the national public healthcare and the writer mainly focused on national legislation, and national public healthcare. This work studies briefly how the city of Helsinki has executed these necessary actions, because as a public operator, the challenges are similar in Helsinki, and the job descriptions in PSHP financial services in the parts which are in contact with patient information.

The findings conclude that most issues have been resolved, but some remain. The employees of the financial district find the situation difficult, and have not received guidelines from the employer, so therefore must decide between following the legislation and understanding the patient's situation, and what would be the humane thing to do. The goal of the thesis is to emphasize the importance of a supporting service to the patient.

Keywords GDPR, data protection, Pirkanmaa Hospital District, financial services,
Pages 50 pages including appendices 1 pages

CONTENTS

1 INTRODUCTION

The Pirkanmaa Hospital District is a public health care provider in Finland. The main purpose and function is to provide health care services, and this means that the most important role is played by doctors and nurses, and every decision is thought through the function of health care. However, running a hospital requires more than just medical staff. It requires all types of supporting services, such as cleaning, IT, and financial services. Data protection is a very important function in a hospital, since the medical data of the patients is highly confidential.

The Pirkanmaa Hospital District has information about data protection in their webpage only in Finnish. There is a short information page where there is general information, and then there is a link to a page about the rights of the registered and execution of the rights. Behind the link is information of the rights, and how they should be handled in the hospital. There are also links to new pages if a person would want to make requests to check their information. There is also the contact information for the Data Protection Officer in Finland. (PSHP n.d.)

This is all however very general information about how the data protection is handled in the Pirkanmaa Hospital District, hereinafter referred to as PSHP. According to the person in charge of data protection in PSHP, they have gone meticulously through the functions in PSHP, and examined what is done correctly, and what needs improving. However, as it often happens, the focus has been in the medical functions, since they are the main reason the hospital exists. Most of the supporting services do not handle any personal data and the only exceptions of this are part of the financial services, and of course human resources. It is unclear if the invoices sent to the patients can be counted as medical documents, but they do contain confidential information. It seems that when carrying out the investigation of data protection needs, that the small group of under 20 people in the financial services would also need education in the matter has been forgotten.

The issues were brought up for the first time in 2017 when the talk about GDPR began, and a meeting with the data protection personnel was set up. The concerns were talked about, but no answers received. In 2018 the office manager of financial services asked to make a thesis of the issue, since it seemed the only way to get any information of the subject.

During the time of writing the thesis, new contact with the data protection personnel was taken, and a new meeting set up. The person in charge had changed since the previous meeting. The questions were more defined at this point, as the subject had become more familiar while the writing

process went further. However, there has been no answers to the questions even now.

It is obvious there is a gap needing to be closed. How can the data protection in PSHP financial services be improved? This thesis will go through the most important legislation concerning the data protection on public healthcare and the main issues the billers face concerning the subject.

1.1 **Introduction to data protection**

In 1890 two lawyers wrote an article about a right to be left alone, meaning a right to privacy. In 1948 the right to privacy is included in the newly adopted Universal Declaration of Human Rights. An Increase in the use of computers had OECD, Organisation for Economic Co-operation and Development, issue guidelines for data protection in 1980, and from there on data protection issues have been taken in varying levels into a national legislation of different countries. (EuroCloud, 2018)

Data protection can mean many things. One of the things it means is the way data is protected, for example the software used to prevent hacking. It could be called information security, meaning the actions taken to keep data from getting into the wrong hands. Another meaning is to make sure the data collected is used for the purposes it is meant to, and nothing else. It also includes having data available when needed, and it being recoverable after a possible disastrous incident, but also the possibility of modification or destroying data that is no longer correct or needed. (TechTarget, n.d.)

Data protection has become increasingly important over the years as globalization and internet have taken over the world. Every bit of information can easily be spread throughout the whole planet in a matter of seconds. There are several reasons why data protection has become so important. Without the protection, it is possible to create even life-threatening situations for other persons (Njord Lawfirm 2018).

One of the fairly recent examples for the need of data protection is the case of Cambridge Analytica. Facebook had given Cambridge Analytica access to their user information, which was then used to modify people's voting behaviour to favour Donald Trump in the presidential election. This scandal is one of the greatest examples of how personal data can affect even the realization of democracy, and why data protection is increasingly important to us all. (Privacy International, 2019)

2 LEGISLATION

There are many different things that affect data protection in Finland. First of all, the EU has released the general data protection regulation (GDPR), and then we have national legislation as well. In the national legislation, there are several different laws which affect public healthcare, and the way documents and information is handled. (Krakau, 2019)

Figure 1. Data protection decree hierarchy (Krakau, 2019)

The right to data protection is not absolute. This right needs to be seen in respect of the function it has in society, and it has to be in correct relation to other basic rights. The data protection legislation respects all basic rights, and it considers the basic principles of the Charter of Fundamental Rights of the European Union. Especially it considers the following:

- The right to have their private- and family life, home, and messages respected
- The right to have personal information protected
- Freedom of thought, conscience, and religion
- Freedom of speech and communication
- Freedom of livelihood
- The right for effective legal protection and fair judicial proceedings
- The right to cultural, religious, and linguistic diversity. (Krakau, 2019)

2.1 Terminology

In legislation there is important terminology that has to be understood correctly. In this chapter, the most important terminology is explained. There are some terms, which might have more than one, slightly different meanings depending on the situation.

2.1.1 Personal data

In GDPR personal data is considered as all information associated to identified or identifiable natural person. A person is identifiable if he can be identified directly or indirectly especially from identifier. Such identifiers are name, social security number, location, network identification information, and one or more physical, physiological, genetic, psychical, economic, cultural, or social factor. (Krakau 2019)

National legislation is a bit simpler. It considers as personal data all kinds of entries which describe a natural person, his features, or living conditions, that can be identified to regard him, his family, or anyone living in the same household. (Krakau, 2019)

Direct personal data is for example name, social security number, address, e-mail address, or profession. Indirect personal data is any information that can be used to identify a person, for example a car licence plate, or a detailed description; red haired, young female cashier in Koskikatu R-kioski. (Krakau, 2019)

2.1.2 Handling personal data

In terms of data protection legislation, handling means any actions that target personal data, or collections of personal data. Handling can be done manually or using automated data processing. Actions are all kinds of collecting, saving, changing, organizing, searching, using, deleting, destroying, combining, or handing over information. Handler of personal data means natural person, legal person, official, office, or any other body, which handles personal data for a registry keeper. (Krakau, 2019)

2.1.3 Person registry

According to the GDPR, a person register means any parsed group of information, from which an information can be found by certain basis, whether the group of information is concentrated, distributed, or divided by functional or geographical basis. (Krakau, 2019)

In national data protection legislation, a person register is a bit more specified. It includes mentions about a group of information which consists of cohesive entries according to purpose. It also specifies that entries are organized in a way that the information of a certain person can be found easily and without unreasonable expenses. (Krakau, 2019)

The registry keeper is obligated to prove they have followed legislation.

Figure 2. The objects for indication of obligation in practise (Krakau, 2019)

2.1.4 Registry keeper

Registry keeper is one or more persons, community, facility, organization, or association, who set up a person registry to be used in their actions. They also have a right to rule about a usage of the registry, or they are legally obligated to keep the registry. Registry keeper is responsible for legal handling of the information. (Riikonen, n.d.)

2.1.5 Registered

Registered is a person of whom the data is about. Registered can be for example a client, or an employee. In legislation a patient is someone who uses medical services or is a target of medical services. (Riikonen, n.d.)

2.1.6 Rights of a registered

The central rights of a registered are:

- A right to be informed
- A right to receive a notification of information security violations
- A right the access information
- A right to correct the information
- A right to be forgotten, meaning the right to have all information deleted or destroyed
- A right to limit the handling of information
- A right to move the information from one system to another
- A right to oppose

Basically it means that the registered has a right to know that his information is being handled, and to know what information is included, why it is being handled, to whom the information is being released to, how the information is being protected, how long the information is being stored, and the registered can also oppose handling of the information. (Lehti, 2019)

To be able to access their information, the registered must be identified. There are no decrees for the form of a request to see the information, and legislation does not have any specification on how the identification should happen, and the identification process should be in respect to the content and risks of the information. Information can be denied, if the registered cannot be identified properly. (Lehti, 2019)

The registry keeper has to inform the registered of the actions taken to fulfil his request without any unnecessary delay, and within a month of receiving the request. The deadline can be prolonged for two months if needed, considering the amount and complexity of the requests. The registry keeper has to inform the registered about the prolonging and the reasons for it, within a month from receiving the request. If the request cannot be fulfilled, the registry keeper must inform the registered without delay and within a month of receiving the request. They also must inform why the request could not be fulfilled, and about a possibility to make a complaint to a supervising authority. They must also inform the registered about other means of legal protection the registered has. (Lehti, 2019)

Figure 3. Execution of the right to check information (Lehti, 2019)

2.1.7 Limitation to a right to check information

Section 15 of the Data Protection Act gives rights to see own information, but in section 34 there are given some limitations to this right. These limitations are if

- "Providing the access to data would compromise national security, defence, or public order and safety, or hamper the prevention or investigation of offences
- Providing access to data could seriously endanger the health or medical treatment of the data subject or the rights of some other person
- The personal data are used in performance of supervisory and inspection tasks and the refusal to provide access to the data is necessary to safeguard an important economic or financial interest of Finland or European Union." (Data Protection Act 1050/2018)

In general, a patient has a right to see his own medical records. However, the right is not absolute, as is given to understand in section 34 of Data Protection Act. Treating doctors make decisions whether the patient's health or treatment will be endangered. Because of this, it is forbidden for an employee of PSHP to go and look at their own medical information, though they would have access to it because of their job.

If only some of the data is such, that it falls under section 34 of Data Protection Act, the registered has a right to receive the rest of the information. The registered should be told the reasons for the restrictions, unless it endangers the meaning of the restriction. However, if the registered does not have a right to receive the data, the data should be given to the Data Protection Officer if the registered so wishes. (Lehti, 2019)

All actions done to fulfil the requests of the registered, and the information given are usually free of charge. If the request is groundless, unreasonable, or they are made frequently, a registry keeper can demand a reasonable

payment based on administrative costs, or decline fulfilling the request. (Lehti, 2019)

If a request is made electronically, the information has to be delivered in a commonly used electronic form, unless the registered otherwise asks for. When data is sent electronically, confidentiality has to be considered. If a registered wishes the information can be given orally. (Lehti, 2019)

If the registered requests correction to his medical data, the correction must be made according section 20 of the Social- and Health Ministry's Decree of Medical Records 298/2009. The Decree instructs, that corrections should be made so, that the original and corrected data can be read later. Name and rank of the person who made the correction, and date and reasons for the correction must be noted in the medical records. (Lehti, 2019)

2.1.8 Party's right to receive data

A party has a right to receive information that can affect or have affected processing of a case. This right includes public and confidential documents from an official, meaning in principle all documents related to processing of the case. The right can extend to data of another person, if it has affected the case. It does not include transcribed notes and drafts. The party has an extensive right to receive and use also confidential information in his own case, for that part as it is needed in the case to which an access to information has been based on. (Lehti, 2019)

A party is a someone whose right, benefit, or obligation is being processed in the administration. In some cases, the party can be for example a guardian, or an appellant, as prescribed by law. For example, a foster care falls under this definition. Special legislation can complete and specify the definitions. (Lehti, 2019)

A party, his representative, or assistant has no right to receive a document, if the release of the data is against public interest, child's interest, or some other very important private interest. The Act on the Openness of Government Activities section 11 includes some other restrictions as well, for example data related to public procurement (trade secrets), official's position in legal proceedings, and preparation documents when the preparation is incomplete. (Lehti, 2019)

2.1.9 Outsider

Outsider is a person, community, facility, organization, or association which is not the registered, registry keeper, personal data handler, or someone handling the personal data for a registry keeper. Whatever information is obtained by handling personal data, has to be kept secret

from outsiders. In a hospital an outsider is someone who might work in the treating unit but is not involved in the medical treatment of the patient or otherwise taking care of his affairs. (Riikonen, n.d.)

2.1.10 Consent

Consent or permission means voluntary, distinctive, and conscious expression of will, with which a registered accepts a handling of personal data. A registered must have a real possibility to deny giving a consent. A registered must be informed of what kind of personal data handling he is giving his consent to. (Riikonen, n.d.)

3 INTRODUCTION TO GENERAL DATA PROTECTION REGULATION

EU's General Data Protection Legislation, hereinafter known as GDPR, is very general legislation. It is meant as minimum rules which have to be followed, but each EU nation has their own laws to specify a regulation of how in that country data protection should be handled. National legislation cannot be contradictory to GDPR. GDPR obligates every organization which either keep person registries, or handles personal data, in both, private and public sectors. A scale in which personal data is handled, the nature of the personal information, or technology used to handle the information does not matter. (Krakau, 2019)

GDPR was created because the residents of different countries in the world lacked a trust for how their personal information is handled. The lack of trust has hindered a development of digital economy and business. Globalization has increased challenges in data protection, and the goal of GDPR is to increase openness of personal data handling, and to secure free movement of information within the EU borders, while increasing a person's right to monitor handling of their personal information.
GDPR is supposed to increase a growth of the businesses by creating convergent rules to all companies in the EU area, and by making business easier and fairer. (Krakau, 2019)

GDPR has to be dispensed, even if register keeper would not be located in the EU area, if it provides products or services within the EU. The legislation must be dispensed also, if a company acts in the EU, even if their data handling does not happen within the EU borders. An example could be a North American company selling products online to the EU area and having outsourced their customer service to India. In that case neither the company nor data handling would happen in the EU, but because they sell to the EU area, they must follow GDPR. (Krakau, 2019)

The GDPR does not concern handling of personal data which is done privately and is not bound to any professional or commercial actions. It also does not concern competent officials, when they handle personal data related to crimes and criminal activity. Data handling for these purposes is covered in special legislation. (Krakau, 2019)

3.1 General principles for personal data collecting and handling

There are several basic principles to guide personal data collecting and handling. Collecting and handling should be legal, reasonable and transparent. A registered should be informed of what data is collected, why, and how it is used. The data should also be bound to the purpose of use, and both parties should be aware of for what purpose the data is collected for. The amount of data should be kept at minimum, so no irrelevant information regarding the purpose is collected. Information should be correct, and all incorrect and imprecise entries should be removed. The collected information also needs to be protected by all necessary technical and organizational means and storing of information is limited by time and relevance. (Krakau, 2019)

Binding the information to a purposed use means that the information needs to be collected for a specific, legal use. It cannot be used or handled later against these purposes. The deviation to these rules is allowed, if handling of information is for public interest, such as scientific or historical research purposes, or statistical purpose. (Krakau, 2019)

According to the GDPR, a personal data can be handled only if a registered has given a permission, handling is required to fulfil a contract, where registered is a party, handling is required to fulfil a legal obligation of a registry keeper, handling is necessary to secure crucial benefits of a registered or another natural person, handling is required to complete a task concerning public interest, or to use a public authority given to a registry keeper, or if handling is needed to execute a rightful interest of a registry keeper or a third party, unless basic rights require data protection of a registered, especially if registered is a child. (Krakau, 2019)

3.2 Summary of changes the GDPR brought

With the GDPR residents the EU area now have a built in and default data protection. The registered got new rights, and legislation now requires analysis of risks related to the collected data. Companies are also required to appoint a data protection supervisor. It emphasizes the responsibility to train the personnel who handle the data, and it separates the personal responsibility of a handler from the responsibility of a company. The GDPR also specified the consequences of a violation of data protection legislation, and obligated companies to report data protection violations.

4 INTRODUCTION TO NATIONAL DATA PROTECTION LEGISLATION

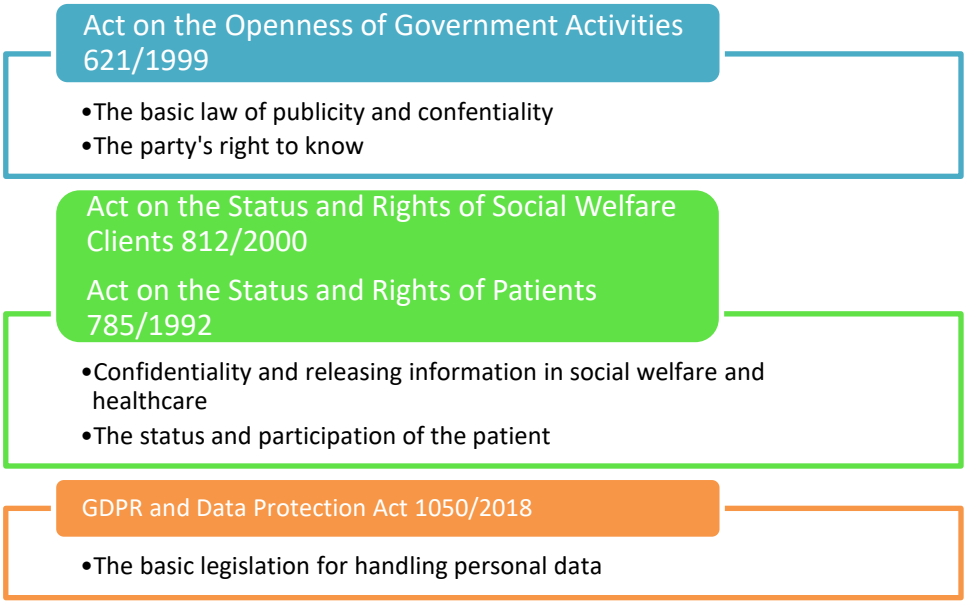

Figure 1. The structure of legislation (Lehti, 2019)

4.1 Data Protection Act 1050/2018

The National Data Protection Act 1050/2018 came into effect 1.1.2019. It replaced the old Personal Information Act. It defines, completes, and expands the GDPR, and they must be used side by side. (Krakau, 2019)

Combined with this National Data Protection Act Finland has over 700 special laws, which affect data protection. (Krakau, 2019)

Personal information is divided into categories, some of the information is basic information, and some is special information. Earlier, older legislation referred to the special information as sensitive information, and the special or sensitive information requires higher level of secrecy than basic information. (Krakau, 2019)

There are some exceptions when Data Protection Act gives a possibility to deviate from some of the rights of a registered, when making statistics is in question. Those exceptions require that the statistics cannot be made without handling personal information, creating the statistics has a proper connection to a registry keeper's operations, and that the information is not made available so that a certain person can be identified, unless the information is given for public statistics. (Krakau, 2019)

4.1.1 Public interest as basis for handling personal information

According to the GDPR article 6, there are several reasons for handling personal data legally. One of the reasons can be public interest:

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (GDPR Directive 95/46/EC, article 6, point 1, subpoint e)

Basically, it means that if the information processed regards the position or duties, and managing them in public corporation, business, association, or similar. It can also mean that the processing is required to execute a task for public interest, or that the processing is necessary for scientific or historical research. Lastly the processing is allowed with this basis for archiving research and cultural heritage material. In each case the processing has to be in relation to the pursued goal, and the goal has to be for public interest. (Krakau, 2019)

4.1.2 Special personal information (sensitive information)

According to the Data protection Act, the basic rule about handling a special personal information is, that it is forbidden. Special personal information, aka sensitive information is for example race and ethnicity, religion, belonging to a labour union, criminal activity related issues, health issues and everything related to it, sexuality or sexual behaviour, or a need or use of social services. The GDPR adds to the list also genetic and biometric information. (Data Protection Act 1050/2018. Krakau, 2019)

However, though the law generally forbids a handling and collecting sensitive information, there is a list of exceptions to it. The first and most important exception is permission from a registered. Permission is not a guarantee though, because there are places in legislation where it is forbidden to give a permission. (Krakau, 2019)

Other reasons why sensitive information can be collected and handled are to follow special obligations and rights of a registered and registry keeper in labour justice, social security, and social protection.
The information can be handled also if vital rights of a registered or another natural person need to be preserved, and a registered is unable to give permission. Registered can also specifically bring some special information into public, and handling that information is allowed. Lastly handling of special information is allowed for court of law, and an organization when they are conducting their legally obligated actions. For organizations and associations, the handling is restricted to only members, and it requires protective measures. As an example, employer is allowed to handle information about employees labour union affiliations, to be able to deduct the membership fee from a salary and to account it to a union. Insurance business also allows handling special information, as well

as archiving research and cultural heritage material, with an exception of genetic material. (Krakau, 2019)

PSHP is conducting its' legally obligated actions when handling sensitive information of its' patients. There is no question of whether they have a right to collect and handle the information according to legislation.
In PSHP the changes with the GDPR and the new Data Protection Act have not been very big. The information that is being handled in there has been considered sensitive even in earlier legislation. Safety of data has been a crucial part of the operation for a long time before new legislation became effective.

Social security number can be handled by permission from the registered, or if it is decreed in law. It can also be handled if it is important to unequivocally identify a registered for an operation provided by law, to execute the rights or obligations of a registered or a registry keeper, or for historical or scientific research and statistics. Basically, it can be handled for giving credit, debt collecting, insurance-, renting-, employment related actions, and so forth. Using social security number in regular e-mail should be avoided, and without the previous reasons there is no reason to give up the social security number. (Krakau, 2019)

4.1.3 Distributing confidential information

Official can distribute confidential information for a couple of reasons. The most pressing reasons are by law, or by consent of a protected. Information can be given also for performing an official duty, or for a task performed by an official. (Lehti, 2019)

Only data necessary for completing the specific task can be distributed. Other confidential data can be distributed if it is not reasonable to remove them because of the quantity of them, or similar reason. (Lehti, 2019)

When data is distributed, it is necessary to ensure in advance, that the protection and security of the data is taken care of. (Lehti, 2019)

The basic principles guiding the interpretation of legislation are the principles of good administration.
According to the principle of proportionality, publicity should not be restricted more than what is necessary for the interests of a protected.
The principle for objectivity demands objective and proper reasons to deny data distribution.
The principle of purpose requires data protection legislation to be used only for the purpose they were made for – to protect the privacy while allowing necessary exchange of information. (Lehti, 2019)

4.1.4 Distributing medical information in healthcare

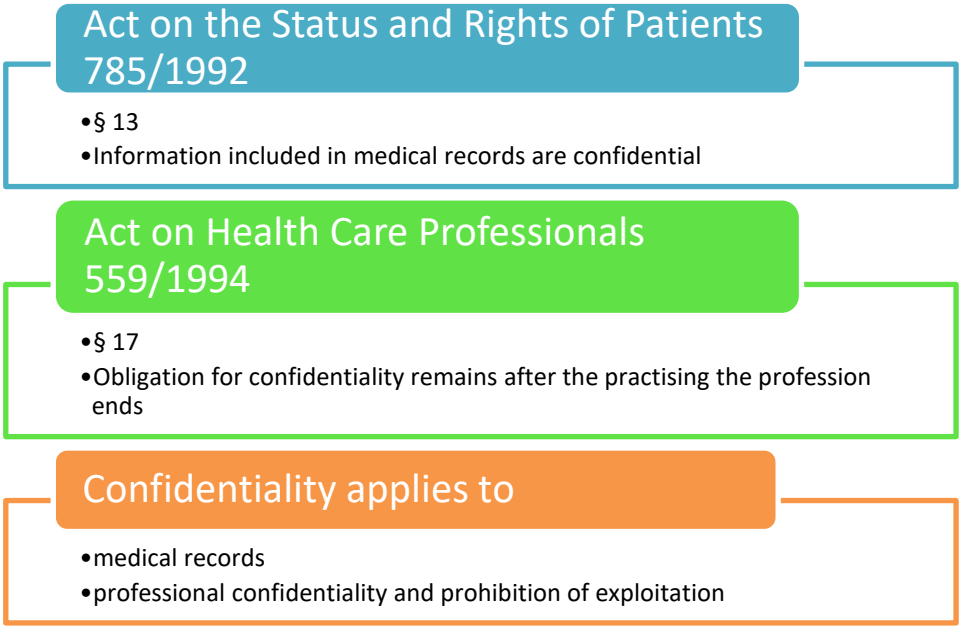

Figure 2. Grounds for confidentiality in healthcare (Lehti, 2019)

Medical data can be handled only by employees taking part in treatment or treatment related actions. The right is also restricted to include only the treating unit, or by the assignment of the treating unit. The data can be handled only in the extent of what is necessary to the assignment and responsibilities. (Lehti, 2019)

Outsider in healthcare means others than the personnel directly related to a treatment of the patient, or the personnel taking care of tasks related to a treatment of the patient. As an example, a doctor is directly treating the patient, and a radiographer is related to the treatment. This means that outsiders are healthcare personnel who are not taking part in treatment of the patient, family and loved ones of the patient, unless they are helping to find out the will of the patient regarding his treatment, and personnel working in other healthcare branches. (Lehti, 2019)

Consent to hand over the necessary medical information can be given. In general, the consent must be written, but the consent can become apparent from the context as well. The consent received from the context is other than written or oral consent, and it must be voluntary, and the giver has to be aware of

- a distribution of the information
- to whom the data is given to
- what data is distributed
- the purpose of distribution
- the consequence of the distribution (Lehti, 2019)

The disclosure of information can be done without a consent, if the patient is not in a condition to give a consent because of a mental disorder, retardation, or other similar reason. The disclosure is limited to another branch of healthcare in the purpose of arranging the treatment. Knowledge of an identity and state of patient's health can also be given to a family or loved one of an unconscious patient, unless there is a reason to assume the patient would forbid it. Data about a health and healthcare of a deceased person can be given to someone who needs it to research or achieve important rights or benefits for themselves. Only necessary information can be disclosed, and it requires a written application. (Lehti, 2019)

If a consent cannot be received from the patient or a legal guardian, disclosing information to an outsider requires regulation in legislation concerning the receiver. By this basis necessary data can be given to

- Social welfare official
- Statement to child welfare official
- Child welfare, police, student welfare, based on statutory reporting
- Compulsory education provider
- Identification and contact information of a young person to outreach youth work
- Supervising official such as The Social Insurance Institution (Kela), patient injury committee etc.
- According the laws of statutory insurances and pensions (Lehti, 2019)

4.1.5 Minor as patient

If a minor's level of development allows him to make decisions regarding his medical treatment and care, the treatment must be given in agreement with him. Decisions are made together with the minor, if he is mature enough. In those cases, a medical professional has made an evaluation on the maturity level of the minor. (Lehti, 2019)

If the minor does not hold sufficient level of understanding, the treatment is given in agreement with the legal guardian, but the extent of the interference with personal inviolability determines the level required for the maturity of the minor. The right to self-determination has to be evaluated for each time a treatment is given, considering the type of the matter. Legislation does not give any certain age-limit, but the evaluation has to be done for each minor patient and situation individually. (Lehti, 2019)

When it comes to minors, family and loved ones are considered outsiders just as they are with adults. In general, disclosing information about the treatment or care of a minor requires consent from the patient, even if the patient is minor and under legal care of parents or other guardians. The situation with minors is comparable to a situation when an adult is unable to make decisions regarding his treatment and care because of a psychiatric issue, retardation, or other similar reason. According to the Act on the Status and Rights of Patients, in cases when the will of a patient cannot be found out, the legal representative must be consulted and a consent for treatment and care must be received from him. The legal representative is obligated to consider the wishes of the patient if they have been made known earlier, but if the wishes are not known, the legal representative must consider a personal benefit of the patient. If certain form or treatment is denied by the patient or the legal representative, the patient must be treated with some other medically approved way, if possible. If the patient has several people who may have opinions on the treatment and care, the patient must be treated the way that can be considered beneficial to his personal interests. (Laki potilaan asemasta ja oikeuksista 785/1992)

Data about an incompetent person can be disclosed to an outsider with a consent from legal representative. Legal representative can be a guardian as a parent or a caretaker, or a trustee. Trustees and caretakers must have a right to receive information to be able to give the consent. A parent with a non-caretaker status might have a right to receive information, but they do not have a right to give consent to disclose information to outsiders. (Lehti, 2019)

Trustees are for people who are for some reason unable to take care of their own financial affairs, though an interest of a person can be looked after in other areas as well. Incompetent people can make decisions regarding their own affairs, if they are able to understand the meaning of the decision. Those decisions the person is not able to understand, will fall to the trustee. The incompetent person means someone under 18 years old (minor), or someone who is over 18 years old, but is declared as incompetent. The official has a right to make decisions on what information will be disclosed to a trustee. (Lehti, 2019)

4.1.6 Child’s right to prohibit, and information exchange

Minor can prohibit a disclosure of information to a parent or a caretaker with certain conditions. A right to prohibit is decreed in legislation concerning social welfare, healthcare, and student welfare. The prohibition right is decreed a bit differently in different laws. A decision of prohibition is not made in general but is evaluated by the situation and the matter at hand. The evaluation is affected by the age of the child, nature of the situation, circumstances, and other similar matters. The right to prohibit has to be documented. (Lehti, 2019)

When a medical professional evaluates a minor to be able to prohibit the right to disclose information to caretakers, the child must be informed of the right. The decision whether the child allows the disclosure of information or not is recorded in the medical records. (Lehti, 2019)

5 SPECIAL LEGISLATION

There are over 30 essential Acts which affect public healthcare in Finland. Only some of them are meaningful when it comes to the functions of PSHP financial services. They are all used together with GDPR and Data Protection Act, and they specify and complete them.

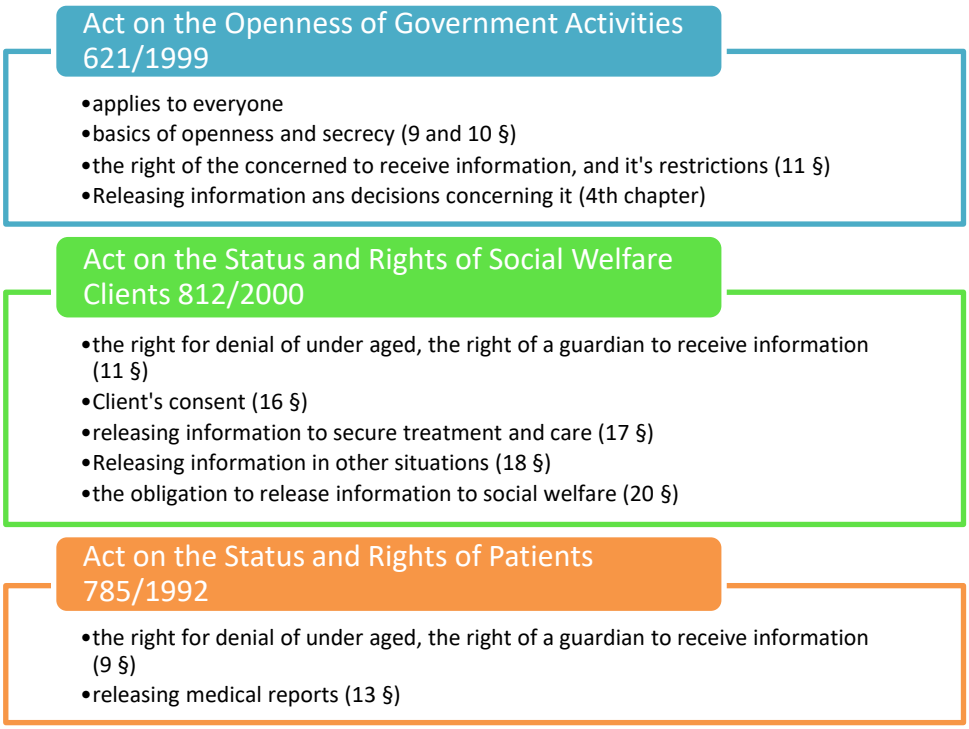

Figure 1. The central regulation of other legislation concerning information exchange. (Lehti, 2019)

5.1 **Other central legislation**

Figure 2. Other central legislation (Lehti, 2019)

5.1.1 The Constitution of Finland 731/1999

In section 10 of The Constitution is about a right to privacy.

"Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.
The secrecy of correspondence, telephone and other confidential communications is inviolable." (The Constitution of Finland 731/1999)

Later in the same section there are given some exceptions to the right to privacy, if the purpose is to guarantee basic rights or investigate a crime. Especially the restrictions to the secrecy of communication are listed. Communication might be imposed for criminal investigation, securing the security of an individual or a society, at trials or security checks, or to obtain information about activities that might be a threat to national security. (The Constitution of Finland 731/1999)

The fact that a right to privacy is written in The Constitution shows that it is seen as a basic right in Finland. The most important content of the right to privacy is:

- A right to be evaluated by correct and necessary information
- A right to decide about the handling of own personal information, unless this right is restricted by legislation
- A right to know about handling of own information, and the purpose of it
- A right to arrange personal life without unwarranted intervention from outsiders

5.1.2 Act on the Openness of Government Activities 621/1999

While a right for privacy is a basic right, so is publicity and openness of the government activities. In section 12 of The Constitution is decreed that documents and records possessed by authorities are public, unless restricted in an Act. Confidentiality is an exception, and it has to be based on law. When a basis for secrecy is considered, the consideration should be favourable to the basic rights, meaning that the publicity could actualize as widely as possible. However, some other basic rights can act as opposing force for a publicity. The basis for consideration has to be a strength of the interest in secrecy, and a significance of the guarded information. In general, the Act on the Openness of Government Activities, or the "Publicity Act" gives more information about the publicity of the documents held by authorities. (Lehti, 2019. Act on the Openness of Government Activities 621/1999)

"An official document shall be secret if it has been so provided in this Act or another Act, or if it has been declared secret by an authority on the basis of an Act, or if it contains information covered by the duty of non-disclosure, as provided in an Act." (Act on Openness of Government Activities 621/1999)

A confidential document, or a copy, or a print of a document is not allowed to be shown or given to an outsider, including showing or allowing usage through technical connection. Section 24 of the Publicity Act includes a list of confidential official documents. The list includes documents which include information of the state of health of a person, or medical care, or treatment given. (Lehti, 2019, Act on the Openness of Government Activities 621/1999)

The confidentiality obligation in healthcare does not end when employment ends. The obligation applies also to trainees and other personnel, who have obtained confidential information through legal actions. (Act on the Openness of Government Activities 621/1999)

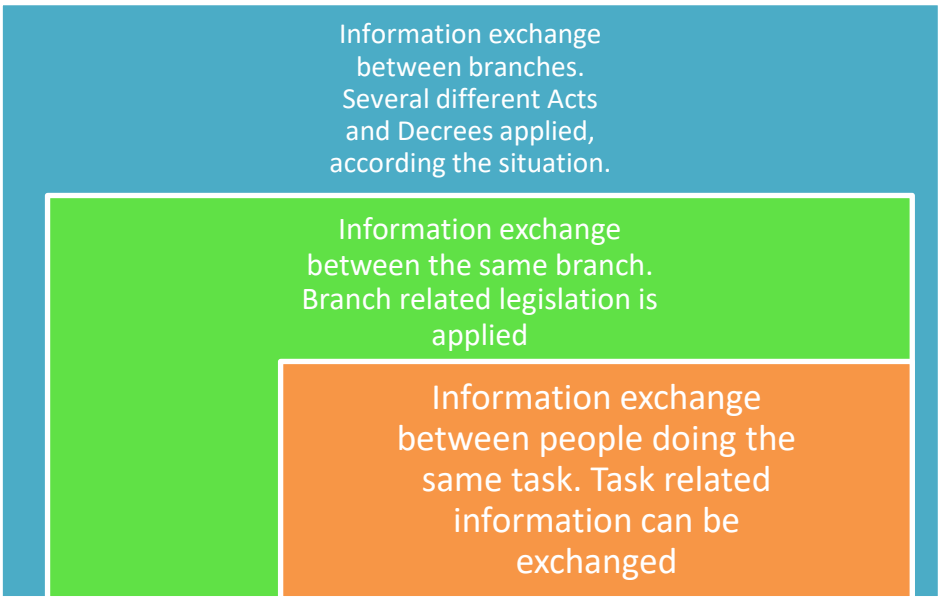

Figure 3. Different levels of information exchange (Lehti, 2019)

Confidential information cannot be released to an outsider. Different units and persons of an official which perform a same or a similar task are not outsiders in respect of each other. Outsider can be a person who works in the same occupational community, but who does not take care of the client's affairs. Confidentiality does not prevent consultation, if an identity is not revealed. (Lehti, 2019)

In the GDPR article 86 is decreed that it is possible to create national legislation to fit together the principle of openness and a personal data protection. (Lehti, 2019)

5.2 Act on the Openness of Government Activities or Data Protection Act?

The registered can be made requests based on either the "Publicity Act" or the Data Protection Act. If it is unclear to which Act the request is based, the official has the obligation to instruct the registered. When needed, the official must explain the regulation concerning the right to receive data to clarify the basis on which the request has been made of. In the upcoming charts the main differences are cleared. (Lehti, 2019)

5.2.1 Using the right – making a request

There are some differences of requirements to a request depending whether the request is done according the Publicity Act or the Data Protection Act.

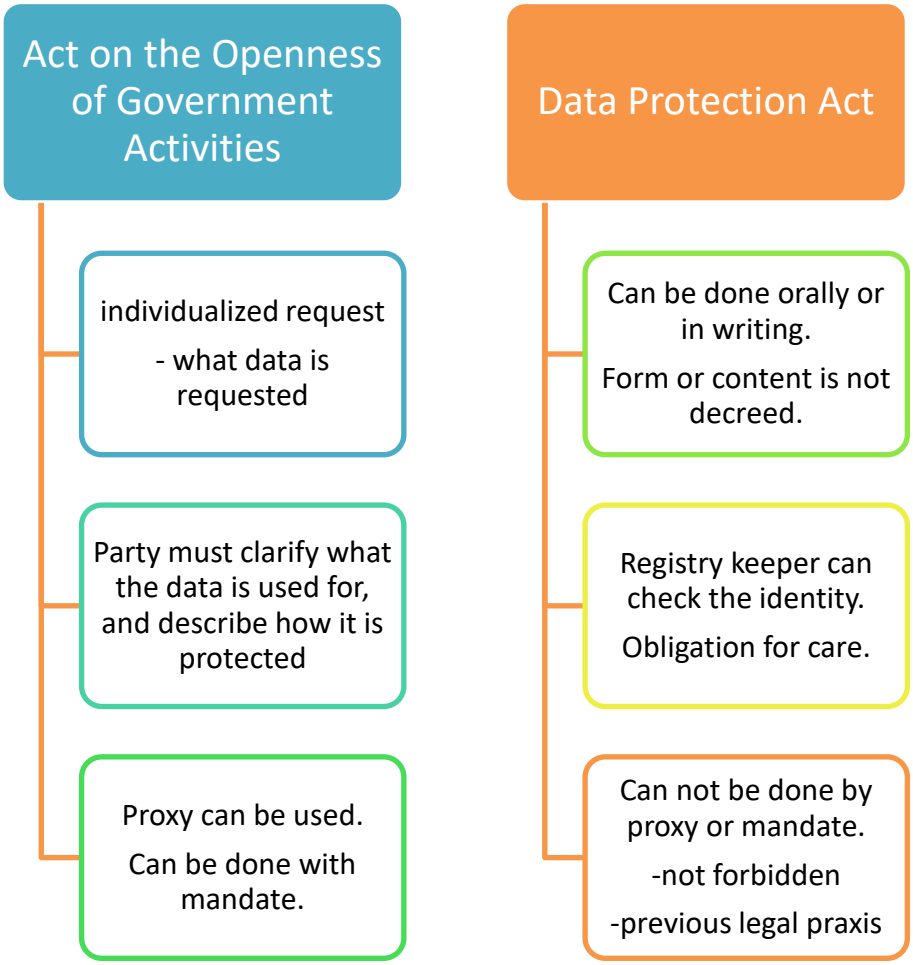

Figure 4. Using the right. Comparison in making the request according to the Publicity Act vs Data Protection Act. (Lehti, 2019)

5.2.2 The right to check own data

The information the registered has a right to receive varies depending on to which Act the request is based on.

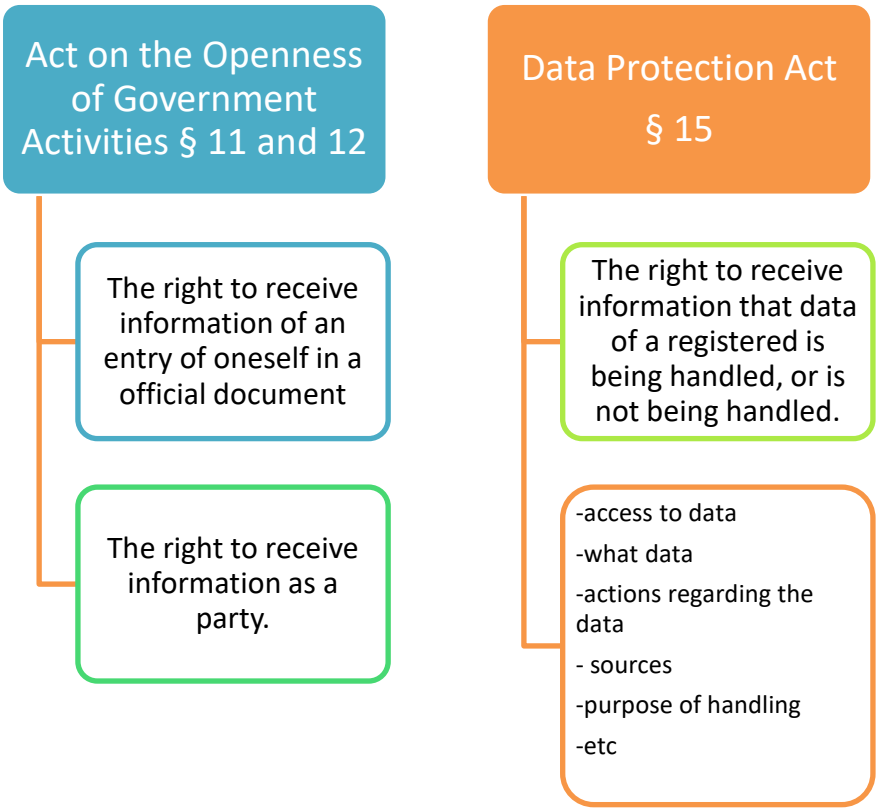

Figure 5. The right. What information the registered has a right to receive. (Lehti, 2019)

5.2.3 Limitations to the right to check own data

There can be certain limitations to a right to check own data depending on the applied Act.

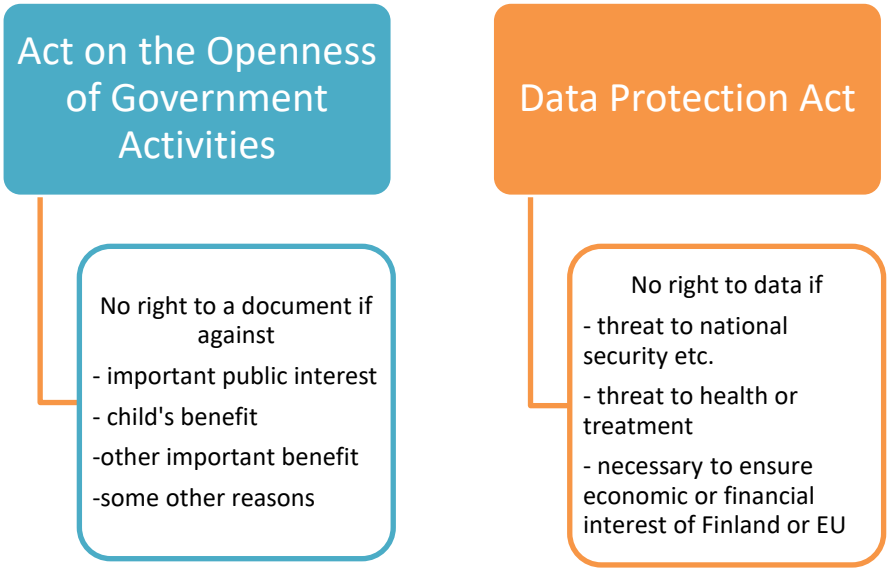

Figure 6. Limitations. What are the limitations to the rights? (Lehti, 2019)

5.2.4 Making the decision

The decision-making process whether the information can be released or not is a bit different depending on which Act the request is based on.

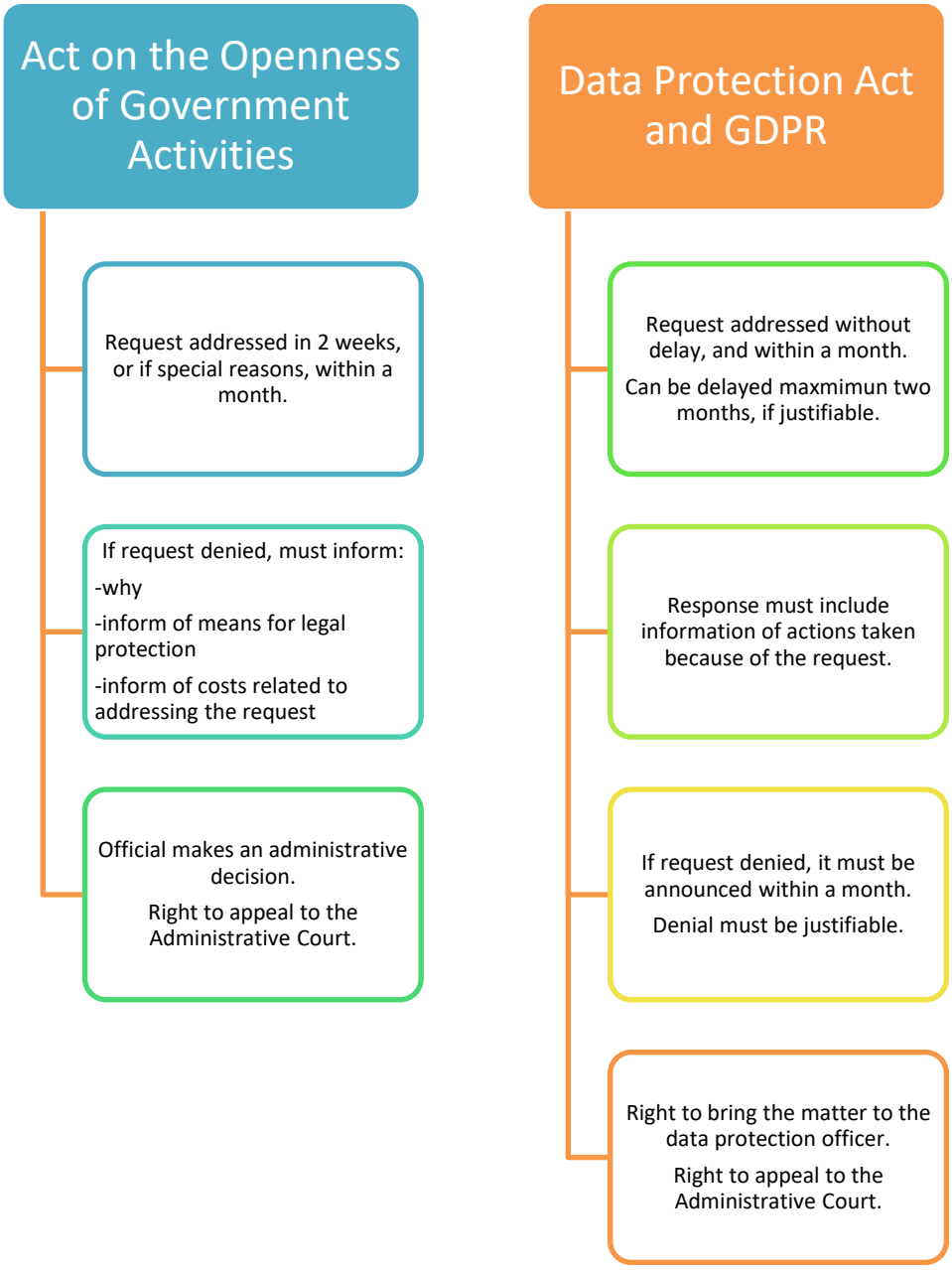

Figure 7. Decision process. What kind of a process is making the decision? (Lehti, 2019)

5.3 **Act and Decree of Client Charges in Healthcare or Social Welfare (734/1992)**

Most important part of special legislation affecting the work done in PSHP financial services, is the Act and Decree of Client Charges in Healthcare or Social Welfare.

The Act sets basic rules about the prices for public healthcare, and which services are free. It also sets basic rules of what must be considered when making decisions on payments based on a patient's ability to pay. The Act makes a difference between the payments from a citizen of Finland, and a foreigner. It also sets an upper limit to the interest rate charged from payments not paid in time and allows for distraint without the decision from the court. Public healthcare and social welfare payments parallel with taxes and other similar-natured payments. (Laki ja asetus sosiaali- ja terveydenhuollon asiakasmaksuista 734/1992 ja 912/1992)

In 1999 the government made an Act for Changing the Act of Client Charges in Healthcare or Social Welfare. At that point they added § 6 a and 7 a. § 6 a is about the annual ceiling for client charges in public healthcare. At first it was decreed that the annual ceiling is calculated from the payments made within twelve months from the first visit. In 2000 the government made a new Act to change the calculation to begin from a beginning of a calendar year and ending at the end of a calendar year. At this point the government also added a part where they restrict the right to ask for corrections to the payments based on annual ceiling. In the 1999 version there was no mention for how long the corrections can be demanded for, but in the 2000 change it was restricted to current or previous year. The Act says that if the service user does not request refund within the next calendar year, they lose the right to a refund. An exception to this is the cases when the payment did not originally belong to the annual ceiling, but because of decisions made by officials or insurance companies it should have been calculated into the annual ceiling. In those cases, the service user has to make a request for a refund within a year from the date the decision was made. (Laki sosiaali- ja terveydenhuollon asiakasmaksuista annetun lain muuttamisesti 1308/1999. Laki sosiaali- ja terveydenhuollon asiakasmaksuista annetun lain 6a §:n muuttamisesta 1222/2000)

In the Decree of Client Charges in Healthcare or Social Welfare the first thing is to clear the terminology used. Then it goes on to list the actual sums of money that can be charged from different services from the patients. Every time the government checks and possibly changes the sums, which happens every two years, they make a new Decree for Changing the Decree of Client Charges in Healthcare or Social Welfare. (Laki sosiaali- ja terveydenhuollon asiakasmaksuista 734/1992)

All in all, there is over thirty Acts and Decrees which are considered most important when it comes to data protection in public healthcare. Quite many of them do not apply to the financial services but are more specific legislation about different actions or affiliations that take place in public healthcare.

6 CASE STUDY: DATA PROTECTION IN CITY OF HELSINKI

The city of Helsinki has about 38 000 employees, and most of them handle personal data. They have around 800 different information systems in use. (Karhula, 2019)

6.1 Organization of data protection

The first and foremost responsible body is the city government. Their job is to fulfil the obligations of data protection legislation, and to monitor the execution of them. One of the obligations is to have a data protection supervisor. The data protection supervisor works full time and has a team of three people to help. Duties of the data protection supervisor are set in the articles 38 and 39 of the GDPR, and she reports straight to the top of the city government. The data protection supervisor gets support in information security issues from the city office, and especially from the information security expert. (Karhula, 2019)

In each industry or public utility there is a person in charge of data protection. That person is the contact between the organization and the data protection supervisor. The duty of the person in charge is to inform and guide in data protection matters, participate in evaluating the effects of the data protection issues, and participate in procurement, if it involves processing of personal data in behalf of the city. Each industry, bureau, and public utility must also have a person in charge for information security issues. The data protection team has meetings with each industry, bureau, and public utility. (Karhula, 2019)

The city of Helsinki also has a city-level data protection working committee. They meet once a month to prepare actions related to the GDPR and national data protection legislation. They also share good practises from different industries and bureaus, and they can divide into subgroups, and use experts from outside of the group. The committee is composed of the data protection supervisor, data protection lawyer, representatives from each industry, bureau, and public utility, and the chief information security officers from each industry. (Karhula, 2019)

6.2 The beginning of data protection works in Helsinki

In 2017 Helsinki city government approved first data protection policies. The policies have been updated since then, in 2019. The policies were mainly principle policies. They also analysed registries and compared the list of information systems and existing registry descriptions. All industries, bureaus, and public utilities were required to fulfil a form about person registries they were using. The purpose of the analysis was to find out what

personal data Helsinki was using, what changes were required to information systems, and to collect information to make new registry descriptions. The analysis helped to create ten main questions:
Who is the main registry keeper considering the data in question?
In which information systems the registered data is used?
What is the legal purpose according the GDPR to handle the data?
What are the data groups and groups of registered in the registry?
Does the registry include sensitive information?
If it does, what are the grounds for handling the data in question?
Retention time of personal data
How the data is removed from the system after retention time is over?
Releasing the data according legislation
Is the information system collecting log entries about all usage?
How the data is protected technically?
What changes in contracts are needed? (Karhula, 2019)

6.3 **The obligations of data protection legislation determined by city of Helsinki**

The data protection committee determined the main duties of the city. (Karhula, 2019)

6.3.1 Guidance of rights, and a possibility to carry them out

Helsinki published in 2018 webpages in internet, which give information about the different data collected in different services of the city. It also gives information about rights of a registered and using those rights. The registry descriptions of different registries are also published in those pages. The descriptions give information about legal grounds for collecting and processing data, the information held in the registry, and the retention times of the data. (Karhula, 2019)

The request to get own data, and the request to correct own data can also be made online. The online request uses strong identification process. There is also a process to make the requests in paper, and the information of the rights of the registered is also in print, if needed. (Karhula, 2019)

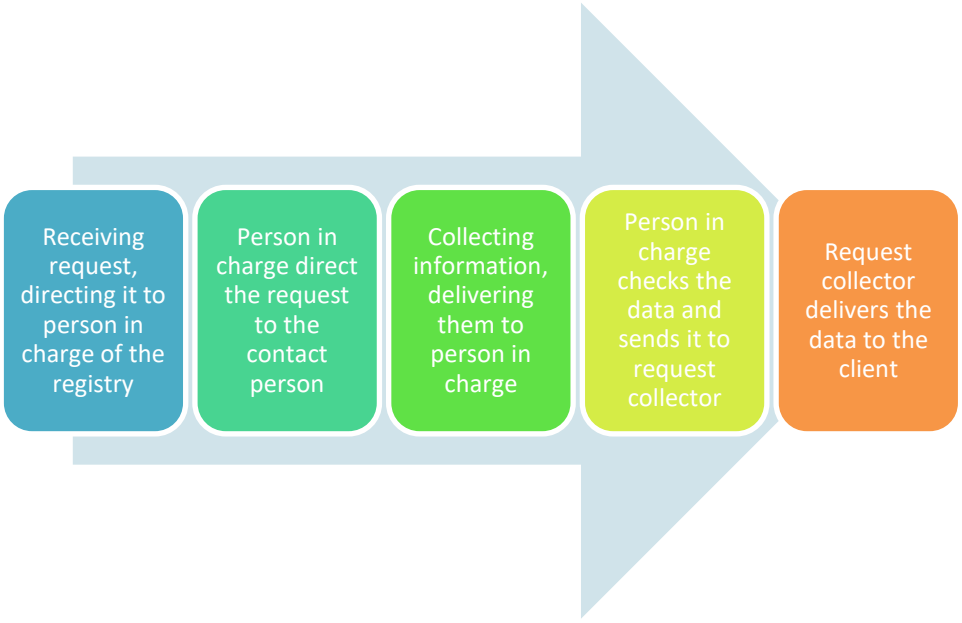

Figure 8. Electric request in practise (Karhula, 2019)

At the moment the flow of information within the city officials, and also delivering the answer to the client require some fine tuning. At the moment the channel used to make a request can be used to send small amount of data to a client, but larger quantities must be sent through encrypted e-mail. (Karhula, 2019)

The same process happens with requests for correcting data. With manual requests the record office checks the identity of the request maker, and the data is sent to the client with regular mail. (Karhula, 2019)

6.3.2 Updating contracts to fulfil the demands of the GDPR

When the city makes new contract, they add an addendum about the city's data protection and confidentiality. The addendum includes all terms about data protection and information security. With old contracts main way to go has been negotiating the data protection addendum into the contract, or in certain cases, some other addendum has been used, as long as it has fulfilled the requirements of the GDPR. (Karhula, 2019)

In practise the city has provided guidance and information, but the industries, bureaus, and public utilities have negotiated independently with suppliers. The data protection committee has a sub-committee for contracts, and they have organized targeted training for those who make procurements and contracts. (Karhula, 2019)

The main questions have been discussed in a city-level and centralized fashion with main suppliers of Helsinki. The results of the discussion can be used by different industries within the city. (Karhula, 2019)

The municipality sector has not had a data protection addendum, which could have been offered to all partners by all municipalities and industries. (Karhula, 2019)

6.3.3 Guidance to employees about data protection legislation

The city of Helsinki has created a video training and a ten questions long test for all personnel who handle personal data. The video lasts 30 minutes, and goes through basic data protection principles, such as responsibilities, grounds and legality, sensitive information, rights of a registered, publicity law, and reporting data protection violations. The managers document the completion. (Karhula, 2019)

More comprehensive training is arranged for key personnel. The trainers are the data protection supervisor, and the data protection lawyer. The key personnel then train employees in their bureau. Helsinki also has a data protection page in intranet, where anyone can find guidance, and also the training videos. For example, there is a video for 10 advices for working in multi-purpose offices in social and healthcare. In the intranet employees can also find a manual for data protection, where the most important principles, processing organization, and the most important processes have been explained. The manual has been created in the sub-committee of the data protection committee. (Karhula, 2019)

In practise the test for data protection was to be done in the end of 2018. Completing the test is built into the citywide work introduction of a new employee. Live training done by the data protection supervisor has been arranged when needed. The original data protection manual was done by seven lawyers in the data protection committee. It has been worked into an easier to read version later. During the spring and fall 2019 a targeted training has been arranged. For these targeted trainings the committee has analysed and recognised specific groups, such as human resources, procurement, and communications. (Karhula, 2019)

6.3.4 Executing built-in and default value data protection

The first step to create a default, built-in data protection within different city's functions is to spread knowledge and understanding of data protection. This is done through training, manual, and other instructions to employees. The data protection supervisor has also toured in different boards of the city and city's bureaus informing the boards of the requirements of the legislation. The default data protection is also included in all development of functions, processes, and procedures. It has been taken as one of the top projects of the city office. The documentation process is also under process to guide the actions and for the supervising officials. The preparation for final data accounts is in process. (Karhula, 2019)

6.3.5 Taking care of information security of person registries

The first thing to secure in the registries was data logging. The city started a project to map the information systems which had sensitive information and made plans how to continue with them. The information systems are being renewed in the bureaus according the plan, and the progression is reported to the data protection committee. Continuous plans for data protection are being made, and the collaboration with the data administration is a key part of them. (Karhula, 2019)

6.3.6 Other notable features

The city has made procedural guidelines for data protection violations. It was mainly focused on possible attacks against the information systems, but the processes including papers have been proven to be especially vulnerable, and in the future, they should be specifically focused on. The city is also planning to clarify instructions for data protection violations. A tool to assess the effects of data protection is being made. It started as a simple initial mapping in Word and continued to the creation of the tool in Excel. The tool will have three different models, for light, moderate, and heavy use.

6.4 **Conclusions of Helsinki's guidelines**

The beginning of the data protection work is in understanding the flows of personal data and organizing the data protection work well. Creating a default, built in data protection requires comprehensive training and instructing of the employees. Also implementing data protection in the processes and actions in advance plays a key role, and it includes creating contracts and contract layouts according to data protection regulation. Data protection cannot be efficient without good information security and understanding the legislation about confidentiality and publicity with the GDPR is essential. (Karhula, 2019)

7 **INTRODUCTION TO PUBLIC HEALTHCARE IN FINLAND**

At the moment public healthcare is a responsibility of municipalities, and it is financed mostly through taxes. In the beginning of each year, each municipality goes through negotiations with each area of responsibility in special healthcare. The goal of these negotiations is to estimate how much the residents of each municipality will use services of the particular area of responsibility, and how much it will cost in a year. The municipality will then pay monthly for the services provided. In the end of the year, the special healthcare provider will either return money to the municipality, if

services are used less than what was estimated and paid for, or send a surcharge, if services were used more than what was paid for.

Public healthcare is divided into two parts; to healthcare centres, and special healthcare providers. When someone needs medical help, the first step is to go to basic health care, which can be a local healthcare centre or for example an occupational health care. If the medical issue is such, that it requires special knowledge or special equipment, the patient receives a referral to a special healthcare unit, which has an area of specialization that is connected to his issue. The patient will receive an invitation to arrive to a doctor's appointment, and the process begins.

In 2018, Finland has budgeted nearly 287,5 million euros to public social and health care. (Valtiovarainministeriö, n.d.)

Legislation dictates certain rules of how public health care must be arranged. The duty to arrange it is on municipalities, to meet the needs of the population of the municipality. However, there is some freedom for municipalities to decide how they will arrange it, whether it is in their own healthcare centre, outsourced to private sector, or other ways. Special healthcare services are arranged as hospital districts, and each municipality belongs into a certain district. (Hoitopaikanvalinta.fi n.d.)

7.1 General information of the Pirkanmaa hospital district

Pirkanmaa hospital district, known as PSHP, is a public special healthcare provider located in Pirkanmaa area, in Finland. It consists of six hospitals; Tays Central hospital, Tays Hatanpää, Tays Sastamala, Tays Valkeakoski, Tays Pitkäniemi, and disabled care units. PSHP also owns limited liability companies, which provide services for the patients of PSHP as well. These limited liability companies are Hospital for Joint Replacement Coxa, Tays Heart Hospital, and Fimlab Laboratories. Tays Central hospital works also as a university hospital, meaning medical students of Tampere University do their training in the Tampere university hospital. (Pirkanmaa Hospital District 2017, 2018).

PSHP is owned by 23 municipalities, making it a joint municipal authority. All these municipalities combined, PSHP provides services for over half a million people. PSHP also provides services to other hospital districts, such as Southern Ostrobothnia, Kanta-Häme, and Päijät-Häme. When these areas are added, PSHP serves over a million Finns. The hospital district has approximately 7000 employees, from which about 79 percent are doctors and nursing staff, 13 percent is maintenance personnel, and the rest are office and research personnel (Pirkanmaa Hospital District 2018).

7.1.1 Data protection in the PSHP

In November 2019 PSHP released an education program in intranet concerning data protection. The whole staff is required to learn it and take a small test to see how well they understand it. It is yet unclear whether the training applies to the work in the financial services, since usually this kind of questionnaires and training has been aimed towards the medical personnel. It is however a step into the right direction, making it mandatory to familiarize oneself with data protection requirements. In the PSHP internet page open to everyone is also detailed information about making requests to receive data, and according to the data protection supervisor, they receive those requests frequently.

At the moment one of the questions is the protection of the employees of the PSHP. When a patient makes a request to see information about handling his data, they also receive the names of the employees who have done the handling. This includes the billers, while they are making the invoices to the patient or the municipality. This has created a situation where a financial services employee has become a target of stalking and other frightening behaviour by a patient who has seen the name in his papers. There are several employees with unique names, which makes their contact information easy to find.

8 THE PIRKANMAA HOSPITAL DISTRICT FINANCIAL SERVICES

PSHP financial services consists of billing, and financial planning. Financial planners have no contact with any information regarding patients, so their work is not addressed. The information and job descriptions in this chapter is information gained through years of working in the financial services, and it has been confirmed during the fall of 2019 by discussing and evaluating the information with one to five colleagues depending on the job description. Some of the jobs are done by eight people, and some by one or two.

8.1 **Billers**

Billers are the part of the personnel who have the most contact with patients, after medical treatment personnel. The job includes not only billing, but also customer service by phone and e-mail.

Client fees in public health care are heavily controlled by legislation. Act and Decree of Social and Healthcare Client Fees apply to everything charged from patients.

8.2 **Billing entries**

Billing is based on entries made by treating unit. Billers do not see any information regarding the treatment of patients. The entries that affect the billing are made by the treating unit.

8.2.1 Issues with incorrect entries

One of the main issues billers face is incorrect entries. The reasons for incorrect entries are many. Newest reason is a so-called self-entrance, meaning that when a time has been reserved for a patient, it has been made with the information available at the time of the reserving. In many cases the situation has changed so, that the entry should be modified once the patient arrives, but because the patient does the registration himself, he does not know of the need to modify the entry. In many cases no one checks the entries afterwards, and the incorrect information stays and affects the invoice.

An example of this situation is that a patient arrives to have a check-up. Before the check-up he has been admitted to a ward in a local healthcare centre. When the patient is in a ward, no other charges can be made from him, the in-ward charge covers everything. The patient was not in the ward when the time was booked, so the entries are made like he would be coming from home. In general, the patients do not know the entries are incorrect, they do not know of the rules and regulations in public healthcare billing, so they do not know to ask for a correction to the entries.

Another reason for an incorrect entry is that most of the entries are done by a ward secretary. They work normal office hours, so patients that come or leave outside of the office hours are registered by nurses. Most nurses are not interested in billing issues, their job is to look after the medical well-being of the patient, so they do not pay attention to the entries that affect invoices.

The most common example of this issue is when the patient leaves the hospital to be transferred to a different healthcare unit. In such cases only the receiving unit is allowed to bill the transfer day. When the exit entry is incorrect, also the sending unit will send an invoice from the transfer day, and the patient pays double for one day.

Third common reason for incorrect entries and invoices are occupational or traffic accidents. These accidents are legislated and should be billed from insurance companies instead of patients. Sometimes the entries are done without taking the accident into account. It can happen if the patient does not mention it, or if the accident has happened earlier and the treating unit is unaware of the cause of the injury. Some injuries are such

that they require treatment decades after the actual accident, so the accident information is easily lost in time.

The billers are sometimes able to see from the markings in the billing program if something is not right. In those cases, they contact the treating unit and ask for them to check the entries and correct them. In most cases however, the biller does now know something is wrong, as they have no right to see the treatment information. They do not see where the patient came from, where the patient went to, and what the visit was about.

There are several ways of how these mistakes could be avoided. One way is giving the billers the right to see relevant information about the treatment, however the problem then is the sheer mass of the entries to be checked. Another way is to have systematic checking of entries in each treatment unit, every day. Because of the volume of the patients, it would most likely require about 50 percent of the time of a single person in most units. The only realistic way is to have better introduction to the programs used, making entries, and highlighting the importance of the correct, billing related entries

8.3 **Annual ceiling for client fees**

The Act of Social and Healthcare Client Fees gives instructions for an annual ceiling for client fees. The purpose of this ceiling is to put a limit on how high the costs can get for a patient before they can receive easement. The annual ceiling is not same every year. Every two years government checks the client fees and annual ceiling according to the social insurance index. The client fees the government decides are maximum fees, and each public healthcare provider is free to decide their fees within the maximum limit. The annual ceiling will be the same in the whole country, it is not dependent whether the service provider charges maximum fees, or under. (Laki sosiaali- ja terveydenhuollon asiakasmaksuista 734/1992)

To calculate the annual ceiling, all the payments to all public healthcare service providers should be included, with certain exceptions. Service providers cannot see each other's payments, so the responsibility to keep track of the ceiling is given to the patient in the Act. The Act also limits the trading of information between the service providers;

"The service user's home municipality's healthcare centre can collect payment information from other public healthcare providers, to execute the annual ceiling. Handing over the payment information from other service providers requires permission from the service user." (Laki sosiaali- ja terveydenhuollon asiakasmaksuista 734/1992)

8.3.1 Issues with annual ceiling

The problem with the annual ceiling is that most of the service providers or the clients have no idea of the restriction in the law, concerning the trading of the payment information. It is usually considered just as good customer service, and looking after a benefit of a patient, to take care of the annual ceiling without a consent from the service user. PSHP billers have begun educating other service providers of this restriction, whenever needed. The Act does not specify what kind of permission is required, so the billers require at least some kind of consent. The crucial thing for PSHP billers is to know that anyone who asks for the information has been in contact with the service user, possible guardian, or in some cases a family member. Often the service user does not understand the concept of annual ceiling or is otherwise incapable of taking care of his or her finances, and in those cases, it has been enough to get the permission from someone who supposedly is handling such issues for the client.

8.4 **Payment time and payment plans**

PSHP service users often contact customer service in the financial services regarding payment time. They are unable to make the payment when the invoice is due, or the invoice is for such a large sum, that they cannot pay it all at once. There are general guidelines to making these payment agreements, but the billers have quite a lot of freedom, and the guidelines can be disregarded to a point. If a biller is unsure whether to make a certain agreement, they can guide the client to the credit controller of the client fees ledger. The credit controller has nearly unlimited right to make the payment agreements as seen fit, only the most complex cases will be discussed with the Assistant Officer Manager.

8.4.1 Issues in payment plans

One issue in payment plans is between the hospital guidelines of equal treatment of clients, and the fact that some of them pay their fees as agreed, and some do not. It is considered useless to make payment agreements with people who have never paid any invoices to the hospital, yet how can the hospital not make the agreements with them, if they make the agreements with others? Clients do not stand in the same line when their past behaviour is taken into consideration. However, it is thought that everyone has the same opportunity to pay their invoices, and therefore their behaviour is a factor to take into consideration. If the situation is more complicated, for example the client has not used the hospital's services in years, they deserve the benefit of the doubt, though the old invoices would still be unpaid. One major question is, if the knowledge of the paid or unpaid invoices can be used in making decision about payment plans. It is obvious PSHP has a registry of invoices and whether they are paid or unpaid, it is a fundamental necessity.

Other issue is that in many cases it is not the service user, patient, who contacts the billers to make a payment plan. They are often spouses or close relatives, social workers, or guardians. With social workers and guardians there is no issue, as they are either with the patient, or they have legal reasons to take care of the patient's affairs. However, the issue is not a serious one usually when it is a close relative taking contact. The billers ask for the invoice number. The invoices are most often sent to the official address of the service user, and therefore it is clear that if it is a close relative, and they know the invoice number, they have received the invoice from the service user. If the service user chooses to hand out the information to an outsider, there is no reason why the billers could not make the payment plans with the outsider.

8.5 **Changes in billing address**

In some cases, people wish for the invoices to be sent elsewhere than to the official address of the patient, for many reasons. Most common reasons are health issues, such as dementia or psychiatric problems. Then there are cases when the patient wants the invoices to be sent for example to a summer cottage, or other address where they spend a lot of time. Sometimes relatively healthy elderly people turn to their children to pay their bills in online bank, since they do not know how to use computers, and they hope the invoices to be sent straight to the child's address.

8.5.1 Issues in billing address changes

The problem arises with the patients who are unable to take care of their own affairs. Most of them are unable to give their consent to someone else receiving their invoices, since they do not understand the meaning of such consent. Many of these patients have official guardians or other official arrangements, but most of them are relying on their relatives to look after their finances. Sadly, they usually do not make a warrant in time, and the relatives just take over the finances once they realise the patient is not able to handle them anymore. Usually the dementia has already progressed so far, that it is impossible to get a warrant anymore, either because the patient does not want to give it, or because they do not understand the meaning of it anymore. The problem with hospital invoices comes from the fact, that even the knowledge that the patient has received treatment is special information which should not be released to outsiders. The invoice also includes information of when the treatment has taken place, and in which PSHP hospital.

8.6 **Requests to receive all billing information from a certain time period**

Sometime billers receive requests to send out listings of billing information of patients. Usually information is needed to apply for reimbursement from insurance company or some other association, like The Cancer

Society or a sick fund. Listings can also be requested for tax collector, or for other healthcare units for calculating the annual ceiling.

8.6.1 Issues in billing information listings

There are couple of different kinds of listings the billers can make. One of them lists only the invoice numbers, due dates, sums, and whether the invoice has been paid. The others include also information of the time of the treatment. All listings reveal that the patient has received treatment, which alone is enough for the information to become highly sensitive and confidential.

8.7 **Other information requests**

Sometimes the billers receive phone calls from other officials, such as Kela (Social Insurance Institution of Finland), or police. Police calls fairly rarely nowadays, but if they do, it is usually concerning invoices for forensic tests, such as blood tests for drunk drivers. In those cases, billers can give the information they see, since it is information the police do have a right to receive. It regards only information of the invoice, never of the patient. Earlier police sometimes called to ask whether a certain person is in the hospital, when they were looking for a missing person, but those calls have stopped.

Kela calls sometimes to confirm information a patient has given while applying for reimbursement of some kind. They never ask for information which would reveal details of the health of the patient, such as which policlinic or ward they have been in, they only need to know whether the patient has been or visited the hospital on the days they have made the reimbursement application for. Giving the information over is a bit problematic, as the fact that the patient has received treatment, and when it has happened is confidential information. However, the legislation provides the right of the official to receive information needed, and Kela phone calls are always made from a certain type of phone number which is easily recognizable. The phone number acts as a verification for the billers, that the call does in fact come from Kela.

8.8 **Credit controller in the client fees ledger**

Credit controller is a person who runs the payments to the system and handles everything concerning them. The credit controller also works as the line between the collection agency Intrum and the patients. About 50 percent of the job is to handle incorrect payments made by the patients. Most common incorrect payments are payments made in double, sometimes paying invoices that have been paid already years ago, sometimes there is a problem in the online bank and the payment is done twice at the same time. Other common incorrect payments are usually

wrong sum, or incorrect reference number. Credit controller takes care of making a list for payments to be returned to the patients. Payments will be returned if the patient has paid the invoice too many times, with too large sum, or if the billing is corrected because of the annual ceiling. Sometimes payments are also returned because of incorrect entries. Credit controller also handles estate inventory deeds and works together with distraint offices.

8.8.1 Returning payments

When the credit controller runs payments into the system, she will print out a program generated list of incorrect payments. The list consists of a reference number used, name and social security number of the patient to whose invoice the reference number refers to, sum and entry date of the payment, bank's archive number, and the reason the payment was incorrect.

Each item on the list will be checked, and since the list shows only the information of the patients the reference numbers refer to, the credit controller checks from the list received from bank through Monetra the name of the account holder. Often the name of the patient and the account holder is the same, but not always. Sometimes incorrect payments come from spouses, relatives, god parents, insurance companies, Kela, sick funds, or companies.

Problem with the bank list is that it has only limited space, one row per payment, and if the name of the payer is long, it shows only part of it. And even if the list would show the whole name, if it is a name of a person, it is highly likely there are other people with the same name in Finland. The job then is to find out who the payer really is. It begins with looking at the information of the patient available to the credit controller. If the payer is a close relative or a spouse, they are likely to be marked as contact persons to the patient. If they cannot be found from the contact persons, the credit controller has a right to see information from the civil registry. From there the controller can see spouses, children, and parents, unless the patient is fairly old, and the parents have not been entered to the system. Through parents, looking at their children, siblings can be found, and from there the spouses and children of the siblings, and the children's spouses and children and so on and so on, for every person. If the credit controller cannot find the name of the payer from the civil registry either, they will contact the bank. With the archive number and other available information of the payment, the bank can find the name and address of the payer. With the name and address the right person is easier to find. Then the credit controller will contact the payer and ask if they would give their account number. If they are not willing to give that information, the credit controller will send a remittance. With the remittance the payer can claim the money from the bank. Sadly, bank will charge 8 euros for claiming the money, and sometimes the money to be returned is as low as 9 euros.

There is not much problems with confidentiality in returning incorrect payments in general, but there are some fairly rare exceptions. Sometimes, especially with a payment of a child, the credit controller just wants to reach either of the parents, if it is obvious the payment is made by either of them. With the limited information the controller has available through the PSHP system, there is no chance to know if the parents have divorced, and the other parent thus receives information of the child's hospital visit. Same kind of problem occurs when Intrum sends notification invoices. They have a legal right to collect the payment from any of the child's guardians, as long as the guardianship is valid. So even if the other parent would not have been in the life of the child in years, they may receive a notification invoice and gain confidential information.

When contacting the payer, whether it is the patient or someone else, it is crucial to confirm the person to be who they are supposed to be before releasing any information to them. The first step taken is to not introduce yourself before becoming certain that the right person has been reached. According to the PSHP's Data Protection Supervisor, there are limits to how far the responsibility goes, as there is a responsibility on the person who has been called to as well. They are not allowed to pretend to be someone, and if they do, there can be consequences on them.

8.8.2 Estate inventory deeds

Once a person dies, in Finland it is required by law to make an estate inventory deed. If the estate does not have money, the heirs are required to deliver the deed to the PSHP financials office. First thing to check from the deed, is whether the deceased has a widow. If there is no widow, and the estate does not have money, the controller makes a credit loss recommendation, and the invoices will then be marked as credit loss. However, the situation is completely different, if there is a widow. Widow is not really part of the heirs' collective, as widow usually does not inherit. However, the widow owns part of the possessions which the couple has used during their marriage. In the estate inventory deed the possessions are divided to those owned by the deceased, and to those owned by the widow. If the property owned by the deceased is not enough to cover the debts of the deceased, the credit controller will then see the financial situation of the widow and decides whether to continue collecting the PSHP client fees of the deceased from the widow, or make the credit loss recommendation. The right to continue collecting the debt from the widow comes as a surprise to most, but it is not based on the code of inheritance, it is based on the Marriage Act.

"Each spouse shall participate in the common household of the family and the maintenance of the spouses to the best of his or her abilities. The maintenance of the spouses means the fulfilment of the common needs of

the spouses as well as the personal needs of each spouse." (Marriage Act 234/1929)

"Both spouses shall, however, be jointly and severally liable for a debt incurred by a spouse for the maintenance of the family." (Marriage Act 234/1929)

To the common needs and maintenance is included basic needs such as food and clothing, but also healthcare. Therefore, the healthcare bills can be collected from the widow. What happens then, if the spouses are estranged but not divorced? Another interesting case which has come up is a time when a person dies, they are not married, but they do have a child, but the child does not know the deceased at all. In those cases, basically a stranger receives confidential information about another person. Legislation is fairly clear though, as it is mandatory to find all the shareholders in the estate of the deceased. The shareholders can become responsible of the debts of the estate, so they do have the right to know of them.

8.9 **Billing of foreigners**

Foreigners who are in Finland and need to use the services of the hospital can be divided into two categories. First category is those who have the right to receive public health care with the same price as Finns. That category is billed exactly the same way as Finns. The second category are those who must pay the true costs, the costs which are usually covered by tax money. These people are billed separately from the others. Main issue with data protection is with people from certain countries, where the post is unreliable. Usually invoices sent through post will never reach the patients, and they often request them through e-mail. They often also have insurances, and the request for the invoices through e-mail can come from the insurance company as well. At the moment, as the general rule is that invoices should not be sent through e-mail to a recipient outside of the PSHP network, there is a big problem in getting the invoices to the recipient. Intrum and distraint offices cannot do anything to collect the debt from people living abroad, so the invoices will never be paid. This increases costs to the taxpayers.

8.10 **Assistant Office Manager**

Assistant Office Manager, who could also be described as a team leader for billers, has the most difficult job. All the cases the employees cannot solve will go to her. As a team leader she faces all the same issues as everyone else, but the cases can be far more complex. However, she can contact hospital's lawyers and other similar information resources the billers and the credit controller cannot.

8.11 **Denial to deliver contact information**

In Finland there is a system for people to apply for denial to deliver contact information. Basically, it means that the address of the person, and most often the whole family, will become classified information, only to be given forward by the person himself. Most often people applying for it are people who work in such professions that their personal safety might be compromised, such as police, or social workers. Some other common situations are people divorcing or otherwise escaping from an abusive relationship.

Magistrate gives an order that the contact information of a such person who has applied for this denial, will not be released from the population information system to anyone except public authorities, though in many cases the information will not be released to even them. Those public authorities who will get the contact information, will also receive information about the denial. The denial is valid for five years, and it can be extended for two years at a time. (Maistraatti n.d.)

PSHP get addresses for patients from the population information system, if the patient lives in Pirkanmaa area. If the patient lives outside of Pirkanmaa, the billers have a licence to look for the address from the population information system. However, if the patient has an active denial, the access to the system is more restricted. There are five employees in the whole PSHP who have the right to see the restricted information. Two of them work in the medical archives, and three in the billing. The general rule is that whatever information can be seen of these patients, it will only be used to send mail, such as invitations to doctor's appointments, or hospital bills. The employees with the right to see restricted information are not allowed to reveal any information which falls under the denial even to the medical staff or the hospital's own social workers.

Sometimes the patient with an active denial gives their address information during their hospital visit. It is forbidden to write this information anywhere in the hospital's programs. However, sometimes the instruction has been lacking, is forgotten, or for some other reason the address is written into the patient's contact information. It creates a problem with data protection, because then the information of the active denial is lost. While the hospital staff does not release the contact information to anyone except public authorities, the story is different with the automated billing system. When the invoice is created, and the information of the denial is lost, the invoice is sent to the Posti's printing service, with the contact information which should be classified. Later on, if the patient does not pay the invoice, the contact information will go forward to the collection agency as well. The material PSHP produces in terms of invoices is quite large, well over million invoices each year, so the number of invoices sent to the collection agency is usually several

hundreds to a bit over thousand each week. Because the amount of material is so big, it is impossible to go through each invoice manually to check from the population information system, if the information of the denial has been manually overwritten because of a human error.

8.12 **Outsourced services**

Pirkanmaa hospital district has outsourced certain functions related to the financial services. Montera Pirkanmaa handles accounting, purchase ledger, and the payment transactions. Intrum Oy handles notification invoices, debt collecting, and is a link between the PSHP and distraint office. Fujitsu is an IT support, and Posti together with their former subsidiary Opus Capita deliver all the mail sent from the PSHP, including invoices.

As PSHP is the registry keeper, they have a responsibility to take care that the companies they have outsourced their services to follow the needed data protection procedures. Combined with that, there is special legislation focusing on postal services as well as debt colleting, which the companies PSHP uses are required to follow.

9 **INTERVIEWS AND ANALYSIS**

To clarify the situation and feelings of the employees regarding data protection requirements in their work, interviews were conducted in the end of November 2019. The interviews were conducted through e-mail, the same questionnaire was sent to 8 employees in the billing team, and they all answered separately through e-mail without discussing their answers together. The selected staff were chosen based on different job descriptions and they all had long work history behind them. It became quickly obvious that about half of the people who answered the questions thought they knew enough of data protection, and half felt that they did not know enough. The information about data protection has been gained through media, training at work, and discussions with colleagues. The same half who thought they did not know enough hoped they would have received more information from the employer, especially specific information regarding their job, and they also felt unsure of what they can or cannot do while doing their job. Everyone felt that data protection requirements made doing their job more or less difficult, though there were situations when it also helped to make the client understand why they could not do certain things for them. Only one person did not think that data protection requirements made things more difficult for the client, the rest agreed that since most of the clients are old and sick, and

have difficulties understanding certain things, they would benefit if the employees could help them more.

During the research done for this thesis, it has become apparent that data protection requirements are so important, and so restricting, that it suggests that those employees who feel they know enough and understand enough do not fully understand the complete picture. While discussing their answers with them, it also became apparent that there is a strong conflict between the requirements of the legislation and understanding the difficult situation legislation creates for people who are unable to help themselves due to their health.

When conducting research for this thesis, the writer also arranged a meeting with all the employees and the PSHP data protection supervisor. Before that, there has been basically no information coming straight from the employer about the issues faced in the financial district. The employer has provided outside training as much as employees have asked for, but only few people have shown interest in them. The problem with outside training is also that it is quite general training, and it does not give answers to the specific questions that come up in the billing department. One of those questions being as simple as is the invoice comparable to a medical report? That would determine do the same rules apply to invoices that apply to medical records. Invoice does not tell anything about the health issues or treatment of the patient, but it does tell when the patient has been in the hospital. It also tells that the patient factually receives treatment in the hospital. However, already sending mail to the patient in an envelope where the sender can be identified discloses information that a certain person has a relationship to the hospital. On the other hand, the envelope must have the information of the sender, so Posti can return the letter to the sender if the recipient cannot be found. Already this creates a conflict in the confidentiality. Posti of course has a requirement of confidentiality through legislation, but accidents, such as delivering mail to the wrong mailbox happens frequently. Even if the owner of the wrong mailbox would not open the letter, they can see the name and address of the recipient and the information of the sender.

Another issue is that the unnecessary information should be removed when it has become obsolete. With the program used in the hospital, it is not possible. This is a concern especially in the billing department, where information regarding the annual ceiling is valid only for the current and the previous year. All information before that becomes obsolete, as the legislation determines the right to check the annual ceiling only to the current and previous year. At the moment there is a huge registry of the old payment information from other health care providers which has no use anymore but cannot be deleted. All these questions still go unanswered. Meeting with the PSHP data protection supervisor was held months ago, they wrote down our questions and promised to come back with the answer, but nothing has come from it. The chief of the area of

responsibility has also contacted the data protection department but has not received any answer either.

According to the employees, data protection requirements are considered mainly a nuisance, because it slows down the work, and makes it very difficult for the clients to get their issues resolved. Many clients get very frustrated and angry when they call but receive no help, as they do not know what to do and how to go forward. The employees have developed work arounds to help patients to get the service they need, but it does require more work and phone calls from the patients themselves. There are no work arounds for certain situations though, and those situations are the main concern for the employees who feel unsure of what they can or cannot do. At the moment biggest issue is the uncertainty of what to do when a relative, most often a child of an Alzheimer patient calls, and asks the invoices to be sent straight to their address instead of the patient's address. The simple answer is that it cannot be done, unless there is a signed permission from the patient. In most cases those permissions have not been made when the patient was able to understand their meaning, since no one thought that it would become an issue. Too often the relative just starts handling things when they realise the other one cannot do it themselves anymore. They take the online bank information from the patient and use it to pay the patient's bills, and so on. But then when the patient starts hiding the bills, or moves to a health care facility, the invoices are harder to get, and should be sent straight to the relative. A simple answer to the situation is that the patient should get a legal guardian. However, that is not a fast solution, as the process takes easily around six months, and during that time the invoices are already in the distraint.

In general, it seems that the data protection is taken into consideration in the financial district, but some issues remain. Some of the issues are things the employees have no power over, such as the inability to remove obsolete data from the billing program, but there are still couple of which create feelings of uncertainty and worry in those who seem to understand the importance of data protection. There is also always the question of personal responsibility if an issue or situation is not understood correctly, and the taken actions have violated confidentiality and data protection requirements.

It has become fairly clear that the financial district is nearly forgotten, or it is not understood what the work actually is, when it comes to hospital policies about data protection. The main focus is naturally in the main function, treating patients, but the complete lack of understanding the importance of the billing department to the patients is quite underwhelming. The well-being of people is not only treating or curing diseases, it also includes other aspects of their life. Though health care in Finland is mainly paid by tax money, people will receive invoices which can create difficult financial situations for them. Not having guidelines and

instructions, and helpful advice of what to do, is very stressful to the employees.

It seems that there is no solution to these issues unless the management starts paying attention to the work done in the billing department and works out guidelines of what to do. The employees have been very resourceful in generating ways they can make things as easy as possible to the patients, but the determination of the status of the invoices compared to medical records cannot be done by them. Neither they have an authority to make any decisions regarding what is required to be able to send the invoices to someone else than the patient or a legal guardian. They also cannot make decisions whether invoices can be sent through e-mail in situations when it is known the mail will not reach the destination in time, or at all. It all seems to boil down to the question of how confidential hospital invoices are. It creates a highly stressful environment to the employees when they feel the right and humane thing to do violates data protection legislation. The legislation seems to put people in unequal position according to their health. The most vulnerable have the weakest situation, and it pains not to be able to help them though it would be easy and not require much time or effort at all. It is of course understandable, legislation has to start from the assumption that the system works, and people have prepared for the time when they cannot do things themselves. Legislation cannot count the effects of human nature, or some misfortune, or accidents which create unforeseen problems for people. Legislation creates only general guidelines which do not account for every individual situation. Therefore, it becomes increasingly necessary to create those more detailed guidelines in the workplace, to account the most common situations where issues might arise. The guidelines provided by the employer also ease the stress from making decisions which might feel wrong or inhumane, as there is something to justify it with, to oneself and to the client. The guidelines would also remove the stress about personal responsibility; as long as the guidelines are followed, the responsibility is on the employer. When there are no guidelines, it is uncertain who will be held accountable for the mistakes made because of the lack of the guidelines.

10 **CONCLUSIONS**

There are over seven hundred different Acts in Finland alone which include regulations about data protection. They are mostly special legislation applying to certain fields, and only some of them apply to public healthcare. Some which do not have a straight relation to public healthcare can be related to it through services used by the healthcare provider, such as Posti, or debt collectors.

To understand the legislation, it is important to understand the terminology used. Especially, it is important to understand who the registry keeper is, and who is handling the data for the registry keeper. The division between the registry keeper and the handler of the data is important to determine the legal obligations and responsibilities of the parties towards the registered.

The most important legislation about data protection is the European Union regulation called GDPR. It gives guidelines which, at minimum, each country should meet. It applies not only to the EU countries, but also every company who is doing any kind of business within the EU borders. If a company is located in the USA, and their data is being handled in India but they sell to the EU, GDPR applies to them as well. Together with the GDPR all countries have their national legislation which gives more detailed guidelines. In Finland there is a Data Protection Act, and then those seven hundred plus special Acts.

After the GDPR and the national Data Protection Act, the most important Act to consider in public healthcare is a so-called Publicity Act. It determines in quite detailed way that all government activities should be as public as possible, as long as it does not compromise national or individual safety, or the national or the EU level financial interests. In the legislation all information regarding the state of health of a person is considered confidential information. The Constitution of Finland also has an effect on data protection, and so does the Act and Decree of the Client Charges of Healthcare or Social Welfare, and Act on the Status and Rights of the Patients. These latter Acts are the most used legislation affecting the work done in the financial services, though many others have details and elements which require attention while considering the correct actions by a healthcare provider.

To a registered it is important to receive information about the differences between the rights they have according to the Data Protection Act and the Publicity Act. The registered needs to know which Act they are basing their request on. When it comes to data within the public system, there are some differences on what information the registered can ask for, and what they can do if the request is denied. In general, requests based on Data Protection Act can be vaguer, and the information received might not be as detailed. There are also differences in whether a proxy or mandate can be used in making the requests. In general, all the information the client requires to understand the request and what he needs to base it on, should be received from the public operator they want to make the request from.

PSHP is a public healthcare provider, meaning that the funding comes mainly from tax money. It makes the hospital district a public operator meaning that the Publicity Act applies to them as well. PSHP provides the clients with information of how to make the data requests, as is determined in the legislation. PSHP has also taken steps to provide their

employees with necessary training about data protection requirements, but since the training program is only just released, there is no data of its effectiveness.

In the financial services the staff deals with patients who have received their invoices, and have financial concerns. It is never a straight forward road as every client has a different situation and the general rules are sometimes hard to apply without creating a very difficult situation to the patient. It has also become obvious that there is a lack of knowledge concerning the status of the invoices and the confidentiality level which should be applied to them. The requirement of equality can also sometimes be interpreted very differently, and there is no real consensus of how to apply the idea to the work, when there is no real equality in the situations of the patients. The general understanding of the importance and extent of the data protection seems to be quite thin as well. It is of course enough to know the restrictions applying to work, but it seems the reasons and general importance of the issue should be highlighted. In short, the seriousness of the subject is not fully understood. Partly it can be because Finland made a national decision to exclude public services from the financial sanctions if the data protection regulations are violated. There are of course other sanctions as well, but they seem quite difficult to apply to an organization executing their legal duties in the area of healthcare, unless the violations are heavy. The consequences of shutting down the operations for a time, as an example, would mostly fall on the citizens, as they would have no easy access to public special healthcare. This raises a question of an individual responsibility of each employee, is it higher because there can hardly be real consequences to the company? Who will be held accountable if violations happen? It is logical to exclude public services from the financial sanctions, because the sanctions would be paid by tax money, and the consequences would again fall on the citizens.

It seems there are no easy answers to get right away. It is understandable the concerns of less than twenty employees do not get high priority when the management has over seven thousand employees to think about. However, it seems the effects on the patients of the work done in financial services has also been forgotten, or not understood. As it often happens, only the main function is considered, and the complete picture is forgotten. The well-being of the patients does not come only from getting treatment to their health problems, but it includes other aspects of their life as well. The hospital cannot help with everything, but it would make a difference if the supporting services would get a closer look. The employees have done lots of work and come up with great solutions to most of the issues the legislation has created, but the few remaining problems still need to be solved.

REFERENCES

Asetus sosiaali- ja terveydenhuollon asiakasmaksuista 912/1992. Retrieved 23 October 2019 from https://www.finlex.fi/fi/laki/alkup/1992/19920912?search%5Btype%5D=pika&search%5Bpika%5D=asetus%20sosiaali-%20ja%20terveydenhuollon%20asiakasmaksuista

The Constitution of Finland 731/1999. Retrieved 23 October 2019 from https://www.finlex.fi/en/laki/kaannokset/1999/en19990731.pdf

Data Protection Act 1050/2018. Retrieved 22 October 2019 from https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf

EUR-Lex. (2016). REGULATIONS. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved 21 October 2016 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FI

EuroCloud (2018). A brief history of data protection: How did it all start? Retrieved 30 November 2019 from https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

Hoitopaikanvalinta.fi (n.d.) Julkinen terveydenhuolto. Retrieved 8 May 2019 from https://www.hoitopaikanvalinta.fi/terveyspalvelut-suomessa/suomen-terveydenhuoltojarjestelma/julkinen-terveydenhuolto/

Karhula P. Data protection officer in the city of Helsinki (2019). Henkilötietojen käsittelyn hallinnointi Helsingin kaupungilla. Training day by Association of Finnish Local and Regional Authorities (Kuntaliitto) for data protection officers 4 September 2019, Helsinki.

Krakau T. (2019). EU:n yleinen tietosuoja-asetus ja kansallinen tietosuojalaki. Training day by Association of Finnish Local and Regional Authorities (Kuntaliitto) for data protection officers 4 September 2019, Helsinki.

Laki potilaan asemasta ja oikeuksista 785/1992. Retrieved 25 October 2019from https://www.finlex.fi/fi/laki/ajantasa/1992/19920785

Laki sosiaali- ja terveydenhuollon asiakasmaksuista 734/1992. Retrieved 23 October 2019 from https://www.finlex.fi/fi/laki/alkup/1992/19920734?search%5Btype%5D=pika&search%5Bpika%5D=laki%20sosiaali-%20ja%20terveydenhuollon%20asiakasmaksuista

Laki sosiaali- ja terveydenhuollon asiakasmaksuista annetun lain muuttamisesta 1308/1999. Retrieved 23 October 2019 from https://www.finlex.fi/fi/laki/alkup/1999/19991308?search%5Btype%5D=pika&search%5Bpika%5D=laki%20sosiaali-%20ja%20terveydenhuollon%20asiakasmaksuista

Laki sosiaali- ja terveydenhuollon asiakasmaksuista annetun lain 6 a §:n muuttamisesta 1222/2000. Retrieved 23 October 2019 from https://www.finlex.fi/fi/laki/alkup/2000/20001222?search%5Btype%5D=pika&search%5Bpika%5D=laki%20sosiaali-%20ja%20terveydenhuollon%20asiakasmaksuista

Lehti S. (2019). FCG Koulutus Oy webinar. Asiakas- ja potilasasiakirjojen luovuttaminen. 5 September 2019, Tampere

Maistraatti (n.d.) Turvakielto. Retrieved 9 May 2019 from https://www.maistraatti.fi/fi/Palvelut/kotikunta_ja_vaestotiedot/Turvakielto/

Monetra (n.d.). Monetra. Retrieved 3 November 2019 from https://www.monetra.fi/

Njord Lawfirm (2018). Three reasons why we need strict data protection regulations. Retrieved 30 November 2019 from https://www.njordlaw.com/three-reasons-need-strict-data-protection-regulations/

Privacy International (2019). Cambridge Analytica, GDPR – 1 year on – a lot of words and some action. Retrieved 30 November 2019 from https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action

PSHP (n.d.) Tietosuoja. Retrieved 30 November 2019 from https://www.tays.fi/fi-FI/Sairaanhoitopiiri/Tietosuoja/Rekisteroidyn_oikeudet/Rekisteroidyn_oikeudet_ja_niiden_toteutt(87474)

Riikonen J. (n.d.). Henkilötietojen käsittely PSHP:n konsernissa. Pirkanmaa hospital district instructions.

TechTarget (n.d.) Data protection. Retrieved 30 November 2019 from https://searchdatabackup.techtarget.com/definition/data-protection

Valtiovarainministeriö (n.d.) Valtion talousarvioesitykset. Retrieved 8 May 2019 from http://budjetti.vm.fi/indox/sisalto.jsp;jsessionid=DF03ECB86C1CF01E9DFCAFBC3405F337?year=2018&lang=fi&maindoc=/2018/tae/hallituksenEsitys/hallituksenEsitys.xml&opennode=0:1:127:

Appendix 1

INTERVIEW QUESTIONS

1. Do you think you know enough of the data protection requirements?
2. Where have you received the information from?
3. Would you have wanted more training/instructions from the employer in the matter?
4. Do you feel uncertainty of what you can do in your work in regard of the data protection requirements?
5. Do you feel the data protection requirement helpful or as a difficulty in your work?
6. Do you think the data protection has negative effects to the clients in your work?