LUND UNIVERSITY
School of Economics and Management

Department of Informatics

The application of data security management in healthcare organizations

A qualitative study on healthcare organizations data security management in relation to data leakage

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: Amanda Javidi Agheli
Josefin Boström

Supervisor: Odd Steen

Grading Teachers: Miranda Kajtazi
Asif Akram

The application of data security management in healthcare organizations: A qualitative study on healthcare organizations data security management in relation to data leakage

AUTHORS: Josefin Boström and Amanda Javidi Agheli

PUBLISHER: Department of Informatics, Lund School of Economics and Management, Lund University

PRESENTED: June, 2021

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Christina Keller, Professor

NUMBER OF PAGES: 96

KEY WORDS: data security management, data leakage, healthcare organizations, organizational activities, data security policies

ABSTRACT (MAX. 200 WORDS):
Healthcare organizations manage, transfer, and store large amounts of private and sensitive data about their patients over digital solutions, which puts them in a vulnerable situation as intruders try to access and leak this data. However, the risk of data leakage is just as great to occur by the exchange of information made by an inattentive employee. To manage and protect data from unauthorized parties receiving data that was not intended for them, it is important to apply appropriate means. Technical solutions have earlier been considered valuable, but it is not enough to only manage the technical solutions. For this reason, this study aimed to examine organizational activities and security policies that healthcare organizations apply for ensuring that the data is managed and protected in relation to the risk of data leakage. This study concluded that healthcare organizations can manage their data by controlling the

distribution of access and encouraging education and awareness of laws, policies, and risks. While technical solutions may indicate a favourable outcome, organizational activities are equally important to include in the data security management.

Content

Figures

Tables

1 Introduction

At this very moment, a current pandemic is spread all around the world which has affected the society as a whole, in various ways (Sjödin et al, 2020). Healthcare organizations is one kind of organization that has been affected and been required to adapt to the use of more digital tools. The increased employment of these tools has not only been established from the digital society itself, but also developed due to the current situation with restrictions and recommendations of staying in quarantine (Sjödin et al, 2020). Healthcare processes that were not carried out digitally before are now increasing the scope of sensitive data (Bini et al, 2020). This means that an even larger amount of data is now being collected, containing information about patients and their conditions, appointments, medicine prescriptions etc., which puts them in a vulnerable situation (Islam et al, 2017).

One common solution for maintaining this data is over cloud solutions (Smys, Senjyu & Lafata, 2019). While this is an appropriate and efficient way to store data for organizations, it is also important that the data is not exposed to any risk (Soomro, Shah & Ahmed, 2016; Stewart & Jürjens, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016; Smys, Senjyu & Lafata, 2019). There are various known risks, in general, to store and manage data on the cloud, including attacks from hackers, a temporary connection loss allowing data to become inaccessible for a while, but also issues concerning data leakage (Soomro, Shah & Ahmed, 2016; Werlinger, Hawkey & Beznosov 2009; Stewart & Jürjens, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016).

Data leakage is an act of data being leaked from an organization and thus no longer secured from unauthorized parties getting access to the data (Shabtai, Elovici & Rokach; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016; Manmadhan & Achuthan, 2014). This type of risk can be considered critical for organizations to avoid, especially in regard to sensitive data, as it can create major consequences, such as violations of the GDPR, but also misdemeanor to other similar regulations and laws (Abouelmehdi et al, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016).

For organizations to be able to protect their data and prevent any illegal actions from occurring, more healthcare organizations are now beginning to develop as "smart" hospitals, where the use of automated and digitized tools is increasing (Zhang et al, 2018). As a result of this development, organizations are integrating technical solutions as useful methods for preventing data from getting leaked (Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). However, technical solutions cannot alone care for the security of data, rather it is important to include managerial activities as well (Soomro, Shah & Ahmed, 2016; Wall & Palvia, 2021; McLeod & Dolezel, 2018; van der Kleij, Wijn & Hof, 2020). Managerial activities, including policies, regulations, and guidelines, can be considered equally important, since security issues and violations are also likely to occur as a result of an action made by an inattentive employee (Wall & Palvia, 2021).

Applying and acting in accordance with policies and rules are especially important for healthcare organizations, in consideration of the sensitive data they maintain and put into practice (Abouelmehdi, Beni-Hessane & Khaloufi, 2018). By managing and transmitting large amounts of data for supporting proper care within and for partnering organizations, and more importantly, maintaining the data about their patients, employees, and the organization,

healthcare organizations can be considered susceptible to data breaches (Abouelmehdi, Beni-Hessane & Khaloufi, 2018; McLeod & Dolezel, 2018). Thus, it is of great importance to manage and protect the data in an appropriate way (Abouelmehdi, Beni-Hessane & Khaloufi, 2018). However, since it is not solely hackers carrying out these actions, rather the breach can be caused by the exchange of data across various devices, healthcare organizations must also account for their employees (McLeod & Dolezel, 2018). With this growing concern where healthcare organization's data becomes an objective for data breaches, acorganizationing technical protection measures failing to care for the data, this study will focus on the organizational aspect of solutions, such as managerial activities and security policies, that healthcare organizations adapt to and employ for ensuring that the data is protected and managed accurately in relation to risk of data leakage.

1.1 Problem

As digital solutions are developing and becoming increasingly beneficial for healthcare organizations to integrate for accessing, managing, transferring and storing data, security is still a concern in regard to preserving confidentiality, integrity and availability (Chinnasamy & Deepalakshmi, 2018; Chinnasamy et al, 2021). The data collected within healthcare organizations about patients is known as sensitive information and requires a great need of confidentiality and security (Shabtai, Elovici & Rokach, 2012; Abouelmehdi et al, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). Data that is stored and managed digitally, on the other hand, is known to have challenges with security and privacy, especially on account for the tools used to manage and store the data (Shabtai, Elovici & Rokach, 2012; Abouelmehdi et al, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). By applying digital solutions, like cloud solutions, there are various concerns, where one common issue is the risk of data leakage (Galetsia, Katsaliakia & Kumarb, 2019).

The use of digital solutions is so well integrated in the society and healthcare processes that it creates no other option than to face the general risk of data leakage (Abouelmehdi et al, 2017: Van Velthoven et al, 2019). In consideration of this, it becomes even more urgent to ensure that data is stored safely. This is especially important to recognize with various laws and regulations that influence the storage and maintenance of data, created by sources and authorities like the General Data Protection Regulation (Abouelmehdi et al, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). For this reason, it creates a desire for healthcare organizations to apply and secure routines and means, where risk and security management is considered, not only influenced by technical solutions but on a managerial level as well (Soomro, Shah & Ahmed, 2016; Wall & Palvia, 2021; McLeod & Dolezel, 2018). This study thus intends to investigate how healthcare organizations manage the issue with data leakage and how their data is protected, concentrating on the organizational activities that are put into practice.

1.2 Purpose

The purpose of this study is to achieve an overview of the most important organizational factors that healthcare organizations apply to manage and protect their data, while tackling the risk of data leakage. Prior research has mainly focused on the technical solutions as the

major source for managing and protecting data towards any possible breach and violation. As a consequence, managerial activities have not been considered as crucial as them. If they are not recognized as important factors nor given a sufficient amount of attention, the security of the data may be at risk. Based on this, this study is concentrating on organizational activities in relation to data security management.

1.3 Research Question

To be able to provide an overview of how healthcare organizations structure their data security management in relation to the identified data leakage issues, we are aiming to answer the following research question:

> How do healthcare organizations structure their data security management in relation to the risk of data leakage?

1.4 Research Aim and Motivation

Based on the identified issues and challenges with data leakage in relation to the management of data over digital solutions, it becomes interesting to achieve an overview of its impact on the data security management used within the healthcare organizations routines. By taking this into consideration, as well as recognising that the use of digital solutions will most likely increase as an option for storing and managing data, the means for attaining the data in a safe way becomes even more crucial. There is no doubt that well developed data security management routines, with consideration for security and policies, are of a great demand within healthcare organizations, in particular the importance of protecting the sensitive data that is stored.

The research aim for this study is thus to examine how healthcare organizations structure their data security management in relation to the challenges and issues with managing and storing data digitally while tackling the risk of data leakage. The aim focuses on the structure of the healthcare organizations data security management that is implemented within the organization business processes and activities. By examining the structure of the data security management, we aim to provide an overview of what concrete actions and routines the healthcare organizations use in their daily processes to manage the risk of data leakage.

1.5 Delimitations

To make sure that the scope of our thesis is not too wide, some delimitations have been made. Since there are many different risks of managing data digitally, we limit our study to the risk of data leakage and the different responsible causes of that risk. Additionally, since technical solutions can be a sensitive subject for healthcare organizations to disclose, this study will concentrate on organizational solutions, such as policies and routines, that they work with and apply for protecting their data and thus delimit the technical part of security measures and

solutions. This study is also limited to Swedish healthcare organizations that are located in different regions of Sweden, with respect to achieving an equitable overview where all the selected healthcare organizations follow the same main laws.

2 Data Security

In this chapter all the collected literature will be presented as well as a description of how we collected the literature.

To be able to answer our research question, literature was collected about data security management, data leakage, policies and the GDPR. The literature that was collected were different journal articles and books. To find the most relevant literature for this study, we used keywords for previous research, via search engines such as Google Scholar and LubCat. The keywords we applied at first were mainly concentrated on data security management, sensitive data and data leakage, but we noticed that it was giving us too broad results, with over 4 million hits on Google Scholar.

To receive a more suiting result of literature from the search engines, considering the broad search results, we modified and filtered the chosen keywords to concentrate on data privacy and policies. The combination of data security management, healthcare, data leakage and policies provided more concentrated results from the search engines where more sources were focusing on the organizational perspective of data security management and the use of e.g., policies.

When carefully browsing through the different chapters within the articles and books, we noticed that many sources contained information about technical solutions in relation to data security management. A technical perspective and technical solutions within data security management could, as earlier described in our delimitations, be a sensitive subject to discuss with the interviewees. Therefore, we excluded literature with high focus on technical solutions.

For determining which sources to work with, we searched for books and journals with high quality and reliability, studied the presented evidence from each literature, its accuracy, as well as we thoughtfully and critically reviewed the abstracts, conclusions, and content to understand if it could be applicable for our study. After carefully filtering out fewer valuable sources, we choose a number of different articles and books that we thought would be useful and conform with our study.

2.1 Data and Sensitive Data

The concept “data” can be defined in different ways depending on the field and context that the concept is acknowledged in (Kitchin, 2014). From an informational perspective, data is information. The information can be stored and then used to analyse or process an activity or raw material (Kitchin, 2014). Data can be categorized into different categories such as quantitative or qualitative data, despite the presented definition. The quantitative data is usually presented in forms of numbers to describe area, length, and volume, while qualitative data is presented in different forms such as text, videos, and other art forms (Kitchin, 2014).

For healthcare organizations, data is mainly considered and referred to information about their patients, also known as patient data (Shakil et al, 2020). Healthcare organizations collect and

store data about practically every individual in society (Offner et al, 2020). This data can include patients' conditions, prescriptions, clinical trials, images, the safety and quality of care, patient experience, medical records, clinical and organizational processes, among others (Shakil et al, 2020; Abouelmehdi et al, 2017; Islam et al. 2017). While patient data may be treated as the most fragile information, healthcare organizations also maintain data about their organization, the employees, providers, and payers (Appari & Johnson, 2010). It can involve data about how to improve care, lower cost, increase efficiency and optimize treatment, but also personal and financial records, including health insurance and financial reports (Abouelmehdi et al, 2017; Shabtai, Elovici & Rokach, 2012). Data about patients and healthcare organizations are considered sensitive, as they are vital to the organization for improving activities and developing healthcare, but also since they could expose personal information (Offner et al, 2020; Abouelmedhi et al, 2017). This means that they can be targeted for data breaches, and it is therefore critical for healthcare to care for how their data is managed and protected (Offner et al, 2020; Abouelmedhi et al, 2017).

Sensitive data is a form of data that is characterised by intellectual property, financial records, patient records, but can also vary depending on the organization (Shabtai, Elovici & Rokach, 2012; Ohm, 2015). The data that healthcare organizations collect, store, and share amongst their medical staff, patients, and other organizations is considered sensitive, as it contains high levels of personal information (Offner et al, 2020). This personal data mainly consists of information such as names, identification numbers, email addresses, and phone numbers, but can also contain information about a person's racial origin, religious beliefs, political opinion, as well as health and medical information of a person (GDPR, 2021; Wong, 2007). If the sensitive data falls into the wrong hands, it can have a negative impact on both patients and healthcare organizations (Offner et al, 2020). Data that is leaked can be offensive towards the person it concerns, if information such as social security numbers or political thoughts is distributed. According to Ohm (2015), if sensitive data is leaked about a person, it can cause significant harm or damage in different ways and is also considered a threat against personal privacy.

An example of how unprotected sensitive data can be harmful can be demonstrated using the case where the data about a girl's pregnancy got leaked to baby care organizations (Abouelmehdi, Beni-Hessane and Khalouf, 2018). The girl unexpectedly received baby care advertisements to her home, without her parents' awareness of the pregnancy, until the advertisement arrived in their mailbox. In this case sensitive data about a person got leaked and used without her approval, which ultimately put her in a harmful situation (Abouelmehdi, Beni-Hessane and Khalouf, 2018). While this example demonstrated harm towards an individual, similar scenarios are also likely to take place against organizations (Offner et al, 2020). Intruders that leak data can, for instance, damage a healthcare organization's reputation, sell personal medical records online, or attack a healthcare organization with a financial target (Tao et al, 2019; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016; Offner et al, 2020). In that manner, sensitive information needs to be secured to not be at any risk of causing any harm to the person that the information belongs to, nor the healthcare organizations (Wong, 2007; Offner et al, 2020).

2.1.1 Data and Cloud Computing

Data can be managed and stored in different ways, where one solution is the use of cloud computing services (Vurukonda & Rao, 2016). Cloud computing is a digital tool that delivers various services over the Internet and can be used for many different purposes. The cloud can be accessed from almost any device and location and is frequently applied for data storage (Vurukonda & Rao, 2016). There are both benefits and risks of negative outcomes with applying this type of service. One of the benefits is that the data that is stored over the Internet and can thus be easily accessed by the users, which means that it is available whenever there is a need for it (Vurukonda & Rao, 2016). While accessibility is considered a benefit, it can also be an issue, since it can cause security issues in case of an attack generated by hackers (Hassan et al, 2019). To prevent data from being at risk of attacks or similar violations, both encryptions and firewalls can be used in combination with the cloud computing service (Vurukonda & Rao, 2016). Another risk with an application of cloud computing is that the providers of the cloud service, in general, have complete control over it, which means that they can carry out tasks that could ultimately interfere with the data (Vurukonda & Rao, 2016).

Despite some concerns, cloud computing is frequently applied in processes within healthcare organizations as it can generate cost effective benefits and provide a wide accessibility (Calabrese & Cannataro, 2015). Even though it is mainly connected to data storage, cloud computing can be applied to accomplish even greater tasks, including data analytics purposes within healthcare organizations (Dang et al, 2019). As an example of how a cloud computing service can be used within healthcare organizations is the actions of managing and analyzing big data (Dang et al, 2019). The cloud service could, for instance, be used to collect patient data from patient's respirators and then be analyzed within the cloud, to provide various results that could ultimately assist organizations in further research (Hassan et al. 2019).

2.2 Data Leakage

As a result of information technology (IT) developing and creating opportunities for organizations, it has become easier to manage and store data using various technologies (Soomro, Shah & Ahmed, 2016; Abouelmehdi et al, 2017). However, this development has also increased the distribution of security risks, where data leakage has become a critical issue when organizations no longer have the ability to protect their data (Stewart & Jürjens, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). Data leakage occurs when undesired information is disclosed, and can, in general, be the action of an intruder or inattentive employee (Shabtai, Elovici & Rokach, 2012; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016; Manmadhan & Achuthan, 2014).

The definition of data leakage is the "accidental or unintentional distribution of private or sensitive data to an unauthorized entity" (Shabtai, Elovici & Rokach, 2012). Data leakage is the result of transmitted data between different parties, without any tools for regulating or monitoring to whom or where it is transferred (Shabtai, Elovici & Rokach, 2012). As a consequence, the data might be shared to parties, such as stakeholders and individuals outside of an organization, which consequently endangers the data for exposure to unauthorized receivers (Shabtai, Elovici & Rokach, 2012; Abouelmehdi et al, 2017).

2.2.1 The risks and consequences of data leakage

To avoid undesired exposures of data, organizations generally protect them using various developed security measures, policies, and protection technologies (Alneyadi, Sithirasenan & Muthukkumarasamy, 2016; Soomro, Shah & Ahmed, 2016; Smys, Senjyu & Lafata, 2019; Abouelmehdi et al, 2017). For instance, it is common to apply technical security measures, such as firewalls, virtual private networks (VPNs) and intrusion detection systems for preventing intrusions (Alneyadi, Sithirasenan & Muthukkumarasamy, 2016; Soomro, Shah & Ahmed, 2016). Data can also be protected using technologies that include authentications, data encryption, data masking, and access control (Smys, Senjyu & Lafata, 2019; Abouelmehdi et al, 2017). Depending on the organization, the tools can vary based on what kind of data that is concerned, but also which type of organization it is, which means that there are a great number of methods and means for organizations to implement (Warkentin & Orgeron, 2020).

In many cases, organizations have, however, experienced their data protection measures failing to protect the data from intrusions occurring (Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). As a consequence, organizations are at risk of reluctantly having their data stolen and leaked (Tao et al, 2019; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). The consequences of organizations data getting compromised or breached is usually targeted by a financial benefit, and can be an act of blackmail, false information, fraud, and even property theft (Tao et al, 2019).

By considering the risks of data leakage there is a need for security measures to be incorporated into organizations in order to avoid breaches (Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). However, data leakage is not always the result of a third party attempting to access data without consent or authorisation, rather it can be a consequence of shared data between two approved parties (Shabtai, Elovici & Rokach, 2012; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). For instance, sensitive data can get exploited from internal parties sharing data containing business plans, financial reports, and agendas (Shabtai, Elovici & Rokach, 2012).

As previously established, data leakages are not always caused by intruders, rather it can be the consequence of an oblivious employee (Wall & Palvia, 2021). If an employee acts in a negligent way, dismiss security policies and rules, or disregard organizational values and beliefs, they can be considered a source causing vulnerabilities and breaches (Wall & Palvia, 2021). Human factors play a significant part in terms of adopting to security practises (Werlinger, Hawkey & Beznosov, 2009). It is important for employees to get an understanding of security risks, preferably united with the organization, in order to prevent them from taking place (Werlinger, Hawkey & Beznosov, 2009; Wall & Palvia, 2021; Soomro, Shah & Ahmed, 2016).

If employees portray themselves as contradictory, it can be a danger for organizations (Werlinger, Hawkey & Beznosov 2009; Wall & Palvia, 2021; Soomro, Shah & Ahmed, 2016). For instance, if employees are less compliant towards security policies, defiance towards authorities, and act in a contrary manner to traditional structures in society, they are more likely to violate the policies (Wall & Palvia, 2021). The security can be endangered if the employees have distinctive and divided attitudes, values, and beliefs in contrast to the rest of the organization (Wall & Palvia, 2021).

The consequences of data getting leaked to an unauthorized recipient can lead to reputational damage, a declining trust from customers and financial losses (van der Kleij, Wijn & Hof, 2020; Tao et al, 2019). An organization's credibility can also be compromised, including future projects, trade secrets and customer profiles (Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). With the exposure of data, competing organizations will also be able to consume these organization secrets and use them to their advantage (Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). Additionally, data leakage can also result in legal consequences and disturbance towards their customers (Tao et al, 2019; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016).

2.2.2 Data leakage in healthcare organizations

The exposure of data is particularly critical within the healthcare environment (Abouelmehdi et al, 2017; Tao et al, 2019; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). Healthcare organizations generate large amounts of data, containing and providing insights to clinical and organizational processes, including the safety and quality of care, patient experience, and medical records of patient data (Abouelmehdi et al, 2017). By managing this personal information about their patients, countries have realized the importance of protecting these sensitive data, by developing policies and laws for data privacy (Abouelmehdi et al, 2017; Alneyadi, Sithirasenan & Muthukkumarasamy, 2016). As a result, the European Union applied, the already existing, Data Protection Directive for protecting people's rights and freedoms, including the right to privacy regarding the processing of personal data, which is also known as the General Data Protection Regulation (GDPR) (Abouelmehdi et al, 2017; GDPR, 2021).

Although, regulations have been enforced, it does not completely decline intruders from targeting healthcare organizations from carrying out data breaches and violations, rather they are still under pressure by managing this large amount of private and sensitive data (Abouelmehdi, Beni-Hessane & Khaloufi, 2018; McLeod & Dolezel, 2018; GDPR, 2021). Healthcare organizations are considered lucrative targets, in consideration of the data they manage, including credit card numbers, bank account information, social security numbers and passport information, which in turn can be used by intruders for identity theft and creating new credit cards (Poyraz et al, 2020). In addition to this, they are also considered a subject to danger, considering the lack of possibilities of storing and managing their data (Hussein, 2021; Soomro, Shah & Ahmed, 2016; Abouelmehdi et al, 2017).

Privacy within the healthcare sector is important, considering the exchange of information between parties containing patient records, information about providers and payers, etc., (Appari & Johnson, 2010; Poyraz et al, 2020). While the GDPR is enforced to secure the privacy of all EU citizens, data breaches are still remaining (Poyraz et al, 2020). In most cases currently, healthcare organizations apply cloud-based systems and solutions for managing their data, including the sharing and exchange of health records (Abu-Elezz et al, 2020). Many healthcare organizations lack the ability to choose between various solutions, which consequently results in cloud solutions being the only option for managing their data (Hussein, 2021; Soomro, Shah & Ahmed, 2016; Abouelmehdi et al, 2017). As a result, organizations are likely to be put in a vulnerable situation, where threats from the outside can occur (Hussein, 2021; Soomro, Shah & Ahmed, 2016). Additionally, since cloud solutions do not necessarily guarantee any security, their data is at even higher risk of getting exposed (Abu-Elezz et al, 2020).

In this manner, healthcare organizations require a safe way for managing their data (Appari & Johnson, 2010; Poyraz et al, 2020).

2.3 Data Security Management

It is crucial for organizations to apply a safety net to avoid data breaches, thefts, and frauds to ultimately protect their data (Soomro, Shah & Ahmed, 2016; Werlinger, Hawkey & Beznosov, 2009). There are different recommended methods that can be applied for managing data security. Werlinger, Hawkey and Beznosov (2009) proposed that organizations include human, organizational, and technological factors for enabling security practitioners to perform in a satisfactory way.

Security management is, in general, performed by IT professionals, such as system administrators, who work in a complex, constantly changing environment and manage real time issues (Werlinger, Hawkey & Beznosov, 2009). These security practitioners often work in a collaborative environment, which means that there is a need for communicating explanations and analyses, to e.g., stakeholders, that in many cases cause security vulnerabilities, due to the exchange of information (Werlinger, Hawkey & Beznosov, 2009). However, it is not solely the exchange of information to invested parties, rather security issues can also occur as a result of collaborating with auditors, external parties, other IT specialists, different departments, end-users, vendors etc., (Werlinger, Hawkey & Beznosov, 2009).

To avoid security related issues, Werlinger, Hawkey & Beznosov (2009) examined how various organizations work with protecting and managing their data. One presented solution was the utilization of communication channels that are excluded from the organization's security tools, and if applicable, an integration of different communication channels (Werlinger, Hawkey & Beznosov, 2009). Instead of continuously sending and receiving notifications and reports to communicate to various parties, different communication channels could minimize traffic. Another possible solution was to implement security domains for communication about security issues, where all included parties are protected by confidentiality (Werlinger, Hawkey & Beznosov, 2009).

A different approach was to develop modified accounts (Werlinger, Hawkey & Beznosov, 2009). By providing customizable accounts it will only allow users with access to collaborate, which could also decrease security risks (Werlinger, Hawkey & Beznosov, 2009). Another presented solution was to create a correlation between data and sources external to IT databases, to more easily determine where an incident occured and by who (Werlinger, Hawkey & Beznosov, 2009). Lastly, the authors proposed to notify for configuration changes, and to manage tacit knowledge, for improving the security tool, and more easily determine if something is feasible (Werlinger, Hawkey & Beznosov, 2009).

Similar to Werlinger, Hawkey and Beznosov (2009), Soomro, Shah and Ahmed (2016) proposed the integration of security policies for identifying critical assets. By implementing an information security governance programme and policies, that includes quality of executive management support, continuous analysis of activities and the ability to adapt to new challenges, an organization could more easily protect their data and avoid security issues (Soomro, Shah & Ahmed, 2016). The authors believed that organizations should include

technological and managerial activities for providing an effective security management system, rather than solely relying on technical factors (Soomro, Shah & Ahmed, 2016; van der Kleij, Wijn & Hof, 2020). Additionally, since security issues often occur as a result of communicated data getting transmitted, it is of great importance to make the employees aware of attacks and vulnerabilities (Soomro, Shah & Ahmed, 2016; Werlinger, Hawkey & Beznosov, 2009). In a similar manner, van der Kleij, Wijn & Hoft (2020) proposed that an application of awareness campaigns can be useful for increasing employee's knowledge on risks and security management.

By integrating security policies and creating an awareness among employees, the risk of data getting stolen, violated, or used in a malicious intent might not be as critical, in contrast to an organization without these resources (Soomro, Shah & Ahmed, 2016). An incorporation of policies that include monitoring, controlling, and diversion of employee behaviour, could possibly decrease the risk of a breach occurring. If organizations are able to assist in cases where an employee lacks awareness and compliance to security policies, including the person's attitude towards violating policies and ill motives, they are more likely to reduce the risk of a security issue commencing (Soomro, Shah & Ahmed, 2016).

In addition to policies, Shabtai, Elovici and Rokach (2012) argued that organizations can benefit from upholding a so-called CIA triad for protecting and securing data. This triad stands for confidentiality, integrity, and availability, which represents an assurance that data cannot be accessed without authorization, nor modified by unauthorized parties, as well as it ensures that a service is available to users at any given time (Shabtai, Elovici & Rokach, 2012). By protecting data from getting accessed and changed by unauthorized parties and ensuring that information is only accessible to authorized parties, information that is considered strategic, protected, sensitive or proprietary are possibly less likely to be exposed (Warkentin & Orgeron, 2020).

2.3.1 Security Policies

What has already been established and cannot be stressed further, is the risk of data leakage when digital tools and services are utilized, in particular concerning patient records (Martino & Ahuja, 2010). In order to work as cautiously as possible, the application of policies in such cases can facilitate and reduce the risk of data leakage (Martino & Ahuja, 2010). Martino & Ahuja (2010) presented a model (See Figure 2.3.1: Relationship between privacy policy & policy notice) of the relations that are connected to policies. The model demonstrates what previous research has stated, i.e., that data security and privacy policies have strong relationships for various purposes, and can, for example, be used to reduce risks and to identify critical situations (Soomro, Shah & Ahmed, 2016).

Policies are influenced by and created according to the general laws and regulations that exist (Martino & Ahuja, 2010). When the security policies are implemented in the concerned organization, their working methods as well as their current processes also get affected. The processes that take place within the organization and the various tasks that are performed within that process will be shaped according to the policies that exist in the concerned areas (Martino & Ahuja, 2010). Additionally, the model also presents that the end user must have a contract where policies should be included from the provider to confirm that the end user is actually aware of the policies existence. The security and privacy policies are not only

mandated by laws and connected to business practices, but it is also an important link and a port of a flow between all the entities (Martino & Ahuja, 2010).

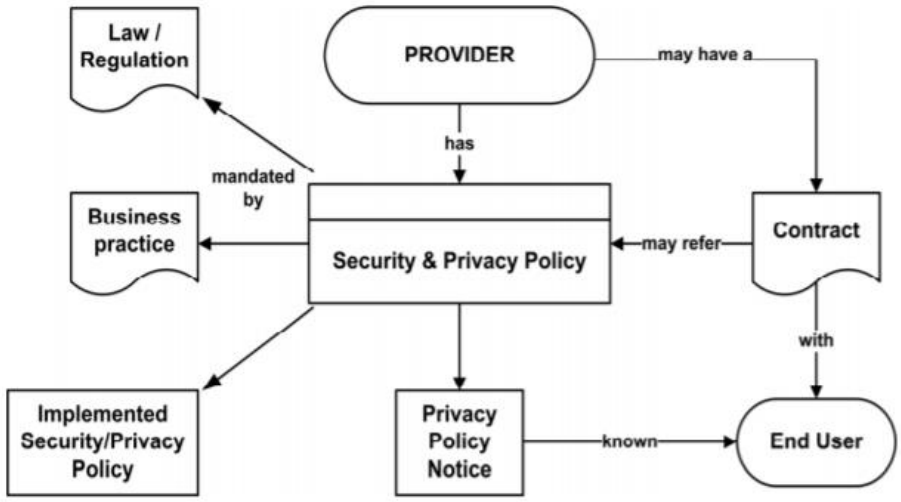

Figure 2.3.1: Relationship between privacy policy & policy notice (Martino & Ahuja, 2010)

2.3.2 The General Data Protection Regulation

Over the last couple of years, invasion of privacy has been a concern, with intruders attacking information systems to get access to data (Abouelmedhi et al, 2017). As a result, the European Union (EU) created and enforced the General Data Protection Regulation (GDPR) with the purpose of protecting personal data and preventing data from flowing freely, within Europe (GDPR, 2021). The General Data Protection Regulation is a European law which contains regulations for privacy and security. The law is practiced when data about any European citizen is stored, processed, analysed, or collected (GDPR, 2021). According to the GDPR (2021), data about any given person cannot be collected or stored until the person provides a consent to confirm that it is acceptable for the collector to use and store said data. Additionally, the data that is collected about a person should be gathered for a specific purpose, only be used for that specific person, and cannot be considered as completed before the purpose is presented and defined to that specific person (GDPR, 2021).

In addition to a confirmed consent from the person of interest, there are also special regulations for how the data should be stored and how it can and cannot be used (GDPR, 2021). For instance, the owner of the data that is being collected or used, always has the right to reclaim their approval of the processing of their data, according to Article 7 in the GDPR law (GDPR, 2021). This means that the collector must immediately delete the data in every given place where it is used and processed. If the collector of the data does not follow the law and corresponding rules, penalties are applied (GDPR, 2021).

Data protection laws are especially crucial for healthcare organizations, who maintain personal information, including financial, medical, and confidential data, that not any party

should be able to access or view (Abouelmedhi et al, 2017). With laws and regulations, like the GDPR, it becomes even more critical to confirm consent from patients, and preserving privacy in terms of collecting, sharing, and transferring data, both personal and sensitive (Larrucea et al, 2020). It is also important to account for all possible devices and systems that are connected and able to share data, like scanners, but also to whom the data is exchanged to (Larrucea et al, 2020).

2.4 Healthcare & Security Management

All information systems that are used within healthcare organizations need to follow standards and laws to maintain a level of security for the data and information available within the systems (Gomes & Lapao, 2008). Even if the data itself is not stored within the specific system, the system still carries a security risk as the data can be accessed via the system. It is thus important that the management, and possibly a CIO, of a healthcare organization ensure that the system matches the organization and that everyone within the organization is in an agreement and aware of the standards that apply (Gomes & Lapao, 2008). ISO 27002 is an example of a guideline that organizations can adhere to as a directory for creating their own security standard (Gomes & Lapao, 2008). There is also another version of ISO, called ISO 27001, which provides similar directories and information for organizations, as well as it is a standard that is certifiable, to get influenced by (Gomes & Lapao, 2008).

To provide a high level of protection, one proposed solution is that the systems used within an organization should apply access authorization (Tipton & Krause, 2006). The authors explained that not all employees should have the same access to everything, rather the access should be based on what data or information the employee needs to complete their tasks (Tipton & Krause, 2006). The type of access each employee has should also be documented so that it is possible to control what data that has been exchanged between the employees. The documentation is also helpful to use when employees are relocated in an organization or have to access other hardware components and track their activities (Tipton & Krause, 2006).

According to St-Hilaire (2020), data can require different needs of protection and therefore be divided into different categories and classifications depending on the demand of security. By considering that patient records are one of the most confidential types of data, it is important that it is heavily protected (Yeng, Yang & Snekkenes, 2019). Within healthcare organizations, it is common to apply a great number of different information systems to maintain this data, that are generally connected to other systems and tools (Yeng, Yang & Snekkenes, 2019). While the various systems may be applied for different purposes and are expected to protect the data, there is still a risk of privacy and security threats, if these are not employed appropriately (Dupont, Santos & Constante, 2020). An incorrect action could have a negative impact on the communication within an organization, but also result in data leakage (Dupont, Santos & Constante, 2020).

2.5 Data Security Conclusion

Table 2.5: Theoretical literature conclusion

Topic	Literature	Conclusions
Data Leakage	Stewart & Jürjens (2017); Alneyadi, Sithirasenan & Muthukkumarasamy (2016); Shabtai, Elovici & Rokach (2012); Manmadhan & Achuthan (2014); van der Kleij, Wijn & Hof (2020); Tao et al (2019). Abouelmehdi et al (2017); Tao et al (2019); Alneyadi, Sithirasenan & Muthukkumarasamy (2016): Abouelmehdi, Beni-Hessane & Khaloufi (2018).	The action of undesired information getting disclosed, unintentionally and intentionally, by an employee or intruder, can result in consequences like financial and reputational damage, a declining trust and compromised credibility. Data leakage is especially critical in healthcare organizations, who manage large amounts of sensitive and private data.
Data Security Management	Werlinger, Hawkey & Beznosov (2009); van der Kleij, Wijn & Hof (2020); Soomro, Shah and Ahmed (2016) Werlinger, Hawkey & Beznosov (2009); van der Kleij, Wijn & Hof (2020); Soomro, Shah and Ahmed (2016). Shabtai, Elovici and Rokach (2012); Warkentin & Orgeron (2020). Martino & Ahuja (2010); Soomro, Shah & Ahmed (2016); GDPR (2021); Abouelmedhi et al (2017); Larrucea et al (2020).	To protect the data from getting exposed, via e.g., the action of data leakage, there are some proposed methods: The combination of human, organizational, and technological factors, to not solely rely on technical solutions. The CIA triad which represents confidentiality, integrity, and availability. Security policies which are influenced by laws and regulations and applied to enforce rules and monitor employee behaviour. The GDPR is an influential law that is practiced when data about any European citizen is stored, processed, analysed, or collected. Data protection laws are especially important for healthcare organizations who maintain personal information.
Healthcare & Security Management	Gomes & Lapao (2008); Tipton & Krause (2006); St-Hilaire (2020); Yeng, Yang & Snekkenes (2019); Dupont, Santos & Constante (2020).	The access to various systems can carry out security risks and must therefore be controlled. This can be done by applying standards, including different versions of ISO.

3 Research Methodology

3.1 Research Philosophy

The aim of this study was to get a profound overview of how healthcare organizations structure their risk and security management in relation to data leakage. In order to do so, this study applied interviews as a means for understanding how healthcare organizations structure their risk and security management, in particular to avoid data leakage, but also what policies and routines that are enforced for controlling how their data is accessed and shared. The main topics of this study was thus Data security Management, Policy, Data leakage and Authorization. We found Patton's (2015) research philosophy called interpretivism suitable to follow for our study. This philosophy aims to make sense of people's experiences, i.e., to give meaning to an experience (Patton, 2015), which in our case was situated on healthcare organizations employees that are in control, preferable from the management, or employees that are responsible for applying the policies and routines. By interviewing employees and allowing them to share their experiences in relation to data security, managerial activities, and policies, we were provided with useful data that ultimately answered our research question.

The interpretivism philosophy generally holds a question of "how" to discover more easily what has happened in the past and to encourage people to describe and interpret their experiences (Patton, 2015). Seeing that our study intended to examine how healthcare organizations structure their data security management in relation to the risk of data leakage, it thus embodies a research question of a "how" rather than a "what" question, and therefore fulfils and complies with the interpretivism research philosophy. Additionally, in terms of collecting data for this study, we trusted that an interpretivism approach that encourages interviewing techniques, among others, will create room for the interviewee to express their descriptions, and thus be suitable for this study (Walsham, 2006; Patton, 2015). This philosophy was also appropriate in terms of acting as a guide to design, collect, and analyse data, seeing that our study was qualitative and thus required the action of collecting and analysing data.

There can, however, be some pitfalls with this research philosophy that should be accounted for to avoid any possible issues. For instance, it can be difficult to interpret what the truth is, if people have different interpretations of the same question or context (Patton, 2015). However, since the research concentrated on Swedish healthcare organizations, we trusted that there will be similarities between the organization's answers, since organizations must follow and act in accordance with the same laws and regulations, such as the GDPR for example. Though, by targeting healthcare organizations located in different regions, we anticipated the answers to vary to some extent. However, since we were interested in getting an overall view of how Swedish healthcare organizations work with managing their data in a proper and safe manner, we were interested in different viewpoints and frame of references, which the interpretivism philosophy supports. Additionally, according to Goldkuhl (2012), the interpretivism philosophy is one of the most appropriate paradigms to apply for qualitative research within the IS field, which means that despite certain issues, it is most likely successful to adopt.

3.2 Research Approach

This study applied a qualitative research approach to examine how healthcare organizations structure their risk and security management in relation to data leakage issues. A qualitative research approach was practiced, as our study aimed to explore a research question that was characterised by an exploratory and descriptive nature, as well as it was a topic that was yet to be discovered (Moen & Middleton, 2015; Patton, 2015). We chose this approach considering its nature of examining what people do, know, think, and feel through various techniques, including interviews (Patton, 2015). Seeing that we were interested in the practice and management of policies and security measures, the qualitative research approach would provide a deeper understanding of an employee's point of view, attitude, and allow them to explain scenarios and information in depth.

To answer our research question following a qualitative research approach, we applied interviews as the method for conducting the research. By conducting interviews for generating data, it will allow the participant to explain their experience from their point of view, in a more detailed way (Bryman, 2018). This type of qualitative research method is likely to result in further discussions of our research question, which is useful for confirming information but also to come to nuanced conclusions in relation to descriptions and analyses (Moen & Middleton, 2015). We chose interviews as a means to allow the interviewee to express their experiences in a more detailed way, which declines any room for speculations, but also creates a more open environment that can encourage questions and thought paths.

Seeing that our study did not concentrate nor rely on numeric data, but rather focus on interviews and empirical data, a qualitative research approach was considered the most suitable (Bhattacherjee, 2012). Additionally, while a quantitative research approach could provide more precision, it would, however, not be appropriate considering our research question and aim (Bhattacherjee, 2012).

3.3 Data Collection

As earlier established, we chose to apply a qualitative research method for our study, applying interviews as a method for collecting data. Patton (2015) clarifies different forms of interviews such as informal conversational interviews and standardized open-ended interviews as well as the utilization of an interview guide. The application of an interview guide can generate a possibility to collect detailed data about specifically chosen topics which for this study would be suitable to reach a valid depth of research (Patton, 2015).

An interview guide contains a list of either different topics or questions that are planned to be covered in the interview. To choose relevant and suitable topics for our interview guide, we defined the main topics from our collected literature, which will be further explained in the subchapter 3.3.2 Interview Guide. The use of an interview guide provides the interviewer and interviewee the option to create a more open conversation but still remain within the topic. One of the strengths with the application of an interview guide is, according to Patton (2015), that the data collection can become systematic while still remaining situational to the specific interview. For this purpose, we shaped different questions for our topics in a way which creates a more open conversation, while sustaining in the range of topics concerning our study.

For the interview guide, we began with background questions. These questions were providing us the opportunity to get a fuller understanding of the interviewee's relation to the data security management within the organization, as well as it allowed the interviewee to determine the level of depth in their expression of the answers on her or his terms. For the following questions we applied open-ended questions to discuss the present and past, as well as we were able to use key questions. The open-ended questions provided the interviewee the possibility to give a response about their experiences and knowledge, but also uncover questions and answers that may appear instinctively (Patton, 2015). The key questions were also asked to collect our required data in relation to the collected literature.

According to Patton (2015), an interview guide can result in absent topics or questions as a result of its semi-structured form. Because of the possibility to situational adjust the interview, it may reduce some of the comparability of the total collected data. To avoid and prevent these weaknesses from occurring, we made sure to be fully prepared to give concrete examples as guidance in case of absent answers, but also avoid presenting questions that may not be possible to answer. However, this weakness may not have a big impact on our research due to the fact that our purpose is not to compare every answer in our collected data, rather put it together to get an overview of how Swedish healthcare organizations develop their data security management.

When conducting the interviews, we asked for consent from each interviewee to record the interview to be able to analyse the collected data using transcriptions. After we had received the interviewees consent, we recorded the interview from personal devices, including phones and computers. This provides us the possibility to inspect and review each interview in detail, even multiple times if needed, since the data was stored on our own devices.

3.3.1 Informant Selection

In order to collect the right data for our thesis, we chose to target and interview healthcare organizations located in five different regions in Sweden. Since the purpose of our study was to examine how healthcare organizations structure their data security management in relation to the risk of data leakage, the specific employees that we wanted to interview needed to require the right type of knowledge and skills to match our aim. In order for the answers from the interviewee to be as valuable and rewarding as possible, we chose to interview the healthcare organization's employees who are in direct contact with or currently working with data security management and the activities and routines that are performed. During this step, we excluded individuals who might not possess adequate or valuable knowledge or experience.

To get a more general view of data security management, we decided to reach out to employees located in different regions of the country. This resolution was determined in order to deliver a more accurate and fairer overview of how Swedish healthcare organizations practice their management and protection of data, rather than targeting one specific location. The employees were contacted via email, where the aim of this study was presented to, including information regarding confidentiality and consent (See 3.5 Ethical considerations), estimated time of the interview and over which interview tool the interview would take place.

Table 3.3.1: Informant overview

Interviewee	Title	Region	Interview time	Interview tool
Respondent 1	Director of IT	Uppsala	35 minutes	Video meeting
Respondent 2	Information security coordinator	Stockholm	27 minutes	Video meeting
Respondent 3	Medical secretary	Halland	27 minutes	Video meeting
Respondent 4	Administrative manager	Kalmar	39 minutes	Phone call
Respondent 5	Director of IT	Stockholm	30 minutes	Video meeting
Respondent 6	Head of department / Operations manager	Kronoberg	21 minutes	Video meeting

3.3.2 Interview Guide

The interview guide was designed and structured to begin with introductory questions, regarding their background, in order to gather more in-depth data on the interviewee's general role in his or her workplace. By commencing the interview with introductory background questions, we created a non-threatening environment to make sure that the respondent felt comfortable (Bhattacherjee, 2012). Following the introductory questions, we structured the interview guide with our key questions that are connected to our aim and literature review. Since our study is formed with a interpretivism philosophy we formed our key questions to be able to give us answers that made it easy for us to discover how the employees had interpreted their experiences. The key questions were created in a way that they would be able to provide an answer that could be connected and discussed to our different main- and subtopics. According to Bryman and Bell (2011), it is of greater importance that the questions are not asked in a leading way, rather that the questions are shaped in such a way that the interviewee can have space and time to really describe and develop their answers but also to initiate other thought paths. Our key questions and topics are therefore not created in a leading way, rather for a path where we ensure that the interviewee has all the possibilities to provide detailed answers.

To make sure that we were able to structure an interview guide that contained the appropriate and relevant information, including the possibility and likelihood of receiving valuable and useful answers based on our determined questions, we made sure to keep a simple language, without any complicated terms to facilitate the interview. We avoided using ambiguous questions to avoid any confusion, dismissed any biased and overly general questions, as well as we

tried to keep questions simple without too many details. We also made sure that the respondents would be able to answer each question. In those cases where we expected either a yes or no answer, we included sub questions to receive as much information as possible. Before, during and after the interview we assured the respondent about the confidentiality of their responses, including the receiving of a PDF containing a transcript of the interview.

Table 3.3.2: Interview Guide

Topic	Question
Introduction	● Could you give a brief description of the organization that you are working at? ● What is your role at your organization? ● What does your role include - what type of tasks/responsibilities?
Data security management	● How does your organization manage your data/information? ● In what way would you say that your data is protected? ● What type of solutions do you apply for protecting your data? ● Is there any particular data that needs a greater protection or special policy/tool? (E.g., patient record?) ● Are there possibilities for some employees to work from home? ○ If yes, what tools or policies does the employee have to use or follow? ○ If not, is this because of a policy/data security management purpose or is it because all employees' tasks need to be done at work?
Policies	● Are there any specific policies for a security purpose? ● Are there specific policies to follow if working from home? ● Are there any specific tasks that an employee is not

	available to do from home because of data security policies? ● In what format are the policies created in? ● Do you update your policies? ● Have you experienced any failure from a security policy?
Data leakage	● Have all employees the same access to all of the data or information? ● Has your organization experienced any attempts or breaches/violations towards your data? ○ If yes, in what way was the approach formed to work against the violations? ○ If no, how would your organization act? ● Are there any special routines for when data is suspected to be leaked?

3.4 Data Analysis Methods

Qualitative analysis focuses on transforming data into findings, which is a way of making sense of the data that is gathered (Patton, 2015). At this stage, it is important to identify patterns and construct a framework for identifying what the data means, but also examine if the data is relevant (Patton, 2015). During the qualitative data analysis, it can also be of great importance to understand if the data is valuable, reliable, and valid in order to determine if the data should be revealed (Patton, 2015). When it comes to analysing the data, it can also be essential to be reflective and reflexive, i.e., to question the data, observe the processes and analyse the findings (Patton, 2015).

We found Patton's (2015) identified suggestions above to be useful in order to ensure that the data is useful for this study. In addition to this, Patton (2015) argues that it is important to firstly describe the research, or collected data, before making any interpretations. In consideration of this, we decided to collect all data after concluding each interview, to ensure that every valuable information was available. During this step, we made sure that we did not filter out any data that may be considered undesired for later use, to avoid making any predetermined conclusions and speculations, but also to get a bigger picture and draw connections between the respective collected data more easily. Following this step, we determined whether

the data was valuable for later use, by comparing each interview to the others. During this step, we dismissed any irrelevant information and observed if there were any recurring themes or topics, in consideration of possible patterns. We also observed if there were any, so-called rich descriptions, i.e., valuable data (Patton, 2015), to help provide detailed and concrete descriptions, as they can be helpful for making sense of and give meaning to an individual's experience.

Following each concluded interview, we transcribed all collected material and organized and reported it in a proper and readable manner (See 3.4.1 Transcribing). To work in the most efficient way, each transcript was completed directly after the interview ended, to provide an accurate translation of the interviewee's answers. Seeing that we are two authors, we were able to divide the transcriptions, but also assist each other in terms of examining each other's transcripts, to ensure that it was done in a correct manner or if something was missing. This also entailed effective processes, where various parts could be divided, constantly progressing, and advancing the movement of the analysis. Instead of both authors concentrating on the same part, we were able to cover multiple areas simultaneously. While we were able to deal with large amounts of data rapidly, there were occasions where we held different opinions. For example, when coding our transcripts, we did not always agree on what code should be referred to which answer. The outcome of this was that we were forced to analyse the data even further. This further analysis and questioning of chosen codes would maybe not have happened if there were only one author for example. Additionally, we were able to discuss and question credibility, reliability, and the value, from two different perspectives, leaving no room for speculation or uncertainties.

By acting in accordance with the qualitative analysis, we were able to get a more concrete and clear understanding of the interviewee's experience and their point of view, with detailed and comprehensive data from interviews, which consequently ensures some sense that the data was credible, of high quality, accurate, consistent, fit to our research, and provided the answers we were looking for.

3.4.1 Transcribing

After each interview was completed, they were transcribed. Since we decided to apply interviews as the qualitative method for collecting data, transcribing is the process of translating spoken meanings into written language (Bhattacherjee, 2012). According to Oates (2006), transcription is a good tool for preparing the analysis of the collected data. The transcripts were useful in terms of how to structure the data and then to be able to categorize it to present it as an empirical result. For all of our interviews, the interviewees allowed us to record the session. During the interviews, some notes were taken, however, we mainly relied on phones and recording tools on a videoconference technology, on our personal computers, for encompassing the information received from each interviewee. According to Bhattacherjee (2012), note taking can be a useful means for composing comments, observations, or responses.

Before, during and after each interview, we ensured the interviewee that she/he and her/his organization would remain anonymous, and that they would receive a PDF of the transcript containing the interview, to allow the interviewee to accept, remove, or make any changes to the transcript. All related information from each interview was analysed, translated, and reported in a proper and ethical way, i.e., by excluding any sensitive, confidential, or private

data about the interviewee and the organization (Bhattacherjee, 2012). We ensured that an interview guide was completed, the right interviewees were present, recordings were made with consent, and that the questions were defined in a correct manner, before conducting the interview, in accordance with Bhattacherjee (2012) suggestions.

3.4.2 Code

In order to be able to find the important key answers more easily from the interviews in the transcripts, coding was applied. The structure of the coding was to connect answers from the interviews with a code, which was created with a specific letter, or combination of letters, to represent a specific topic. The codes were created from the main topics of our interview guide, which is originally created from our review of previous literature. The codes are based on the topics: Data Security Management, Policy and Data leakage.

The code "OE" was created to characterize answers from an interviewee containing information about organizational training and their general daily activities, which we connected to the main topic Data Security Management. Other codes within the same main topic were "S" and "T", to illustrate and cover answers concerning information about systems and tools that were used within the healthcare organization for managing their data and keeping it safe. While these codes were created based on previous literature, other codes were created from the interviews conducted in this study. For instance, after the interviews were carried out and inspected, we noticed recurring answers, which included a specific card to enter systems and access data, from every interviewee. Thus, we decided to connect that data within the transcriptions and created the code "C" for that specific tool. Another example is the code "SAS", which we created to highlight answers concerning information about healthcare and data security combined, mainly concentrating on if specially applied security was applied and how it was used within the healthcare organization.

The codes "DP" and "L" represent the development of policies and law connections, which were both connected to the main topic Policies. These were created to identify answers about policies, with emphasis on how the healthcare organization acts in relation to updates of their policies and on what grounds their foundations are established in relation to laws and regulations. The codes "A" and "R" were created to demonstrate authorization and access, and routines in relation to data leakage, and were both connected to the main topic Data Leakage. These codes identified answers that provided information about how the healthcare organization acts in case of a situation of data leakage, and their views of authorization and access to data.

Table 3.4.2: Code overview

Code	Topic	Main Topic
OE	Organizational training and work procedures	Data security management
S	Systems	Data security management

T	Tools	Data security management
C	Tools - Card	Data security management
SAS	Specially applied security	Data security management
DP	Development of Policies	Policy
L	Law connection	Policy
A	Authorization and access	Data leakage
R	Leakage routines	Data leakage

In the transcripts, coding was also applied to clarify which person said which presented sentence. These were the following codes:

Table 3.4.3: Abbreviation overview

Abbreviation	Name
AJA	Author Amanda Javidi Agheli
JB	Author Josefin Boström
R1	Interviewee 1
R2	Interviewee 2
R3	Interviewee 3
R4	Interviewee 4
R5	Interviewee 5
R6	Interviewee 6

3.5 Ethical Considerations

When collecting data, interviewers are required to take ethical principles into account (Patton, 2015). Two important concerns are informed consent and confidentiality. According to Patton (2015), interviewers have an obligation to inform the interviewee about the purpose of the research and in which way the data will be used. This information should be presented in the beginning of the interview, be clearly delivered, and not presented as a long speech (Patton, 2015). For this study, we chose to inform the interviewee about our research purpose before the interview, via an email which included a description of who we were, the aim of our study and a short description of why we reached out to them.

In relation to conducting research, Bryman (2018) defines four principles of ethical considerations to recognize. These principles deal with information about participation, consent, the requirement of use of the collected data and confidentiality (Bryman, 2018). For our research we took all the principles into consideration when we conducted the interviews to ensure that it did not violate any ethical considerations.

Participation and consent are significant in terms of allowing the interviewee to be able to have the full control over the participation and possibility to give consent before the interview commences (Bryman, 2018). The interviewee should be aware that the participation is fully voluntary and that she/he has the possibility to be anonymous (Bryman, 2018). In this study, we required a consent from each interviewee, before and at the beginning of the interview, to receive an assurance and confirmation of participation and documentation, to ultimately complete the qualitative research method. We also informed the interviewee that they had the power to retire from the interview.

Before the interviews were carried out, our aim was to audio-record the interviews. For this reason, we required a confirmed consent and permission from the interviewees before the interview and documentation began. According to Patton (2015), it is important for the interviewers to present the purpose of the research and in what context the collected data will be used to the interviewee. Consequently, we made sure that the purpose of the research, including the interview and the use of collected data, was clearly described, and demonstrated via email, as this was our tool of communication with each interviewee.

To ensure confidentiality, we assured the interviewees that the data we would collect from them would be used for academic purposes (Bhattacherjee, 2012). Consequently, we explained that any personal or sensitive data would be disregarded, as well as we excluded any data that could be harmful towards the interviewee or their organization and concentrated on the data that was relevant for this study. As a result, the transcripts do not include the interviewees name nor the name of the organization. We also informed the interviewees that we would send a PDF of the transcript to allow them to confirm, alter or reject any responses if it was of significance.

To minimize the risk of the collected data getting distributed to unauthorized parties, the decision of recording, documenting, and storing the interviews on our personal devices, including phones and computers, was decided. We chose this to ensure that the collected data would be stored where no unauthorized person could get access, for instance by excluding the option of storing the data on the cloud. This meant that no other parties would be the owners of the data aside from us, and ultimately provide a sense of security.

3.6 Scientific Quality

Quality is linked to what people value and what different experiences mean to people, which can involve personal and cultural perspectives, but also concerns practicing certain standards (Patton, 2015). From a research perspective, one can expect a certain quality assurance, i.e., a promise that the collection of data and evaluation procedures is carried out based on "standards of excellence" (Patton, 2015). In other words, there should be an appropriateness, adequacy, and effectiveness considered in regard to the research, to create a sense of assurance that the provided data is useful and trustworthy (Patton, 2015).

To provide a sense of quality, we decided to target interviewees that would be able to answer any questions related to risk and security management in relation to data leakage issues. This step included filtering out some employee roles that would not be able to deliver any valuable or relevant answers. We wanted to target and select employees with a sense of competency and experience to deliver acceptable results, preferably a manager or employee with direct contact to organizational activities and knowledge about the management of data, to ensure that we would get high-quality data from a credible source. We decided to reach out to potential interviewees from different regions to get a broader overview, rather than targeting one specific area. After each concluded interview, all data was carefully analysed, and compared with previous research and evidence, to get an understanding if there were any connections and patterns, different views, to question the level of authenticity, consistency, and accuracy, but also to make sense of the collected data.

To ensure that the quality of our study is based on good standards, it is also important to be critical towards the findings and thesis, and that the data has been thoughtfully analysed (Patton, 2015). In consideration of this, we evaluated and examined the collected data, to make sure that it was credible, accurate and consistent throughout the study. After carefully observing the data, we also questioned the results, in order to provide and be able to create an assurance that the study is of good quality, including a clear purpose, compatible questions and hypothesis, appropriate applied methods, and consistent findings. We did not want to deliver any inaccurate or misleading information, which we avoided by being sceptical and researching any possible concerns.

To improve accuracy and credibility, we also informed and allowed our interviewees to confirm that our responses collected from the interviews were accurate, to not present incorrect information in this study. During the interviews, we also had the same approach, where we confirmed, summarized, and questioned some answers to make sure that we fully understood them, to avoid any wrongful interpretations. During the interviews, we were also interested in discovering negative instances or cases, i.e., answers that contain information of a deviant case which differs from prior hypothesis (Allen, 2017), to strengthen the quality of our study.

Throughout the study, we made sure that all materials were well-analysed, credible, accurate and consistent, to ensure that our work was carried out according to standards to ultimately present trustworthy data.

4 Empirical Results

In this chapter, the results of the conducted interviews will be presented and continuously structured in the different main topics. The following topics are Data leakage, Data Security Management and Policies. The six respondents will be referred to as their abbreviation, which is presented in 3.4.2 Code.

4.1 Data Leakage

4.1.1 Leakage threats and guidelines

Seeing that the research question of this study concentrated on data leakage, we were interested in discovering possible attempts and experiences of data breaches. Both respondent R2 and R5 described that they had experienced attempts of phishing. Respondent R2 explained that healthcare organizations, in general, are now more exposed to threats that can lead to data leakage during the current pandemic. Respondent R5 said that most of the attempts they have experienced as a threat of data leakage are in the form of phishing. The threats emerged from Russia, Asia and a small part from South America. Respondent R2 also described that the data that predators are targeting is often contact details and logins, to ultimately sell on the black market. Respondent R2 further stated that they generally target healthcare organizations via email and encourage the receiver to click on the link attached to the email.

Respondents R1 and R4 did not mention any special situations that have arisen regarding data leakage but were able to describe general risks. Respondent R1 explained that even if security measures are implemented, there is still a risk of employees acting in an inappropriate or irresponsible way towards the organization, since all data is accessible in the computers that can be used from a remote location, like home. However, in other cases, it can be the result of other parties putting the data in a vulnerable position. Respondent R4 mentioned risks that make data more easily accessible to predators, without the responsibility relying on the healthcare organization or an employee. A particular example included the action of receiving faxes where the data had not been encrypted, while respondent R4 explained that their organization, as well as other healthcare organizations, are clearly directed to use encrypted faxes. Similar concerns were illustrated by respondents R1 and R2, who discussed the problems and risks regarding the use of email, in particular the concern of not exposing details and attaching the patients complete social security number and name.

In view of data leakage, it was also of interest to understand possible actions healthcare organizations take, both to prevent but also to work against potential and occurring attacks. All respondents explained that if a suspicious case of data leakage occurs or that all security policies have not been followed completely, there are guidelines for how the organization should handle the situation. Respondent R3 described that if a suspicious case of data leakage were to take place, the manager is informed with guidelines and that the threatened parts of the systems are shut down immediately. Additionally, most employees receive directions that are transmitted higher up in the hierarchy from e.g., the IT section. Respondent R6 explained that

they heavily rely on their security department to control and provide instructions in case of a violation.

All respondents described that the first step to take in case of suspected data leakage is to report it. Respondent R4 stated that ever since the GDPR was introduced, the guidelines for such situations have been tightened. Both respondent R5 and R2 explained that the reporting is done to the Swedish Authority for Privacy Protection. Respondent R5 further explained that the affected patients and staff will be informed. In such situations, an assessment is also made of where the deviation has occurred, whether it is a care deviation, sustainability deviation, safety deviation or information flow. The deviation is then managed in the most appropriate way for the purpose of improvement. Respondent R1 described that the most urgent element within the process that they apply in a suspected data leakage situation is to track where the leak has occurred. Depending on what kind of data that is suspected to be leaked, the actions can also vary. If the data applies to patients, the region where the healthcare organization is located is informed, and if the data concerns employees, the employees are informed.

4.1.2 Specific Access

In relation to data leakage, this study was curious to learn if employees required specific access or if similar situations were to take place that would limit the accessibility to data. Both respondents R1 and R3 described that the actual data storage is not located at their place of work, rather it is maintained at their respective region. As a result, respondent R1 explained that they do not have to monitor that the storage of data acts in accordance with the GDPR, however, they do recognize and ensure that the regulation is applied correctly in terms of the accessibility of data. All respondents described that they use different tools to access the required data, as well as the level of accessibility can vary. According to respondents R2, R4, R5 and R6, the level of determined access and to what extent that you will be able to use and view various data will differ according to your role, including your tasks at work. In contrast, respondents R1 and R3 described that as long as the employee has access to a system everything is accessible, with the exception of information that is regulated by laws and special circumstances.

Respondent R5 described in further detail that the amount of data and the type of data you as an employee have access to depends on your role and what tasks you or your team have at the time. In a similar manner, respondents R2 and R4 described that the doctors can have access to more additional journal systems, including additional data, than e.g., an assistant nurse. Additionally, all respondents described that wherever they carry out their work, they need an identification card that is distinguished within healthcare organizations. This identification card, also known as a sith card, in combination with a card reader, is a necessity for logging in to and accessing all the systems which contain the data you require for various tasks.

To summarize this subchapter in the matter of data leakage, it was demonstrated that all respondents were well aware of data leakage threats and had incorporated guidelines of how they should act in case of a suspected data leakage situation. Even though these guidelines existed in all six cases, they were not identical, while some had similar reasoning. In terms of access there were some opposing approaches. Most of the respondents explained that their access to data was limited to what was required for their tasks, while other employees had access to all of the organization's data, which was contingent on their role.

4.2 Data Security Management

4.2.1 Education and Security

By reason of understanding the management of data, this study was interested in acquiring knowledge concerning which ways the data is protected, concentrating on organizational factors. Respondent R3 described that data about patients who are non-public for security purposes, is managed in a safe way, in a similar manner to all other data but with a bit more attention. Respondent R2 described that data such as medical records and patient data is considered to require the highest level of confidentiality, as it is considered sensitive data and often the most vulnerable in relation to data leakage. The systems that manage this type of data generally include extra policies to put emphasis on how to work with these systems to avoid any harm, by e.g., excluding employees from working at any location or issuing sensitive information via any printer.

Respondent R4 described that employees from their organizations are encouraged to withhold certain data when communicating with employees and patients, to protect any sensitive data. While this is clear for the employees, it is not always obvious for the patients. In those cases where patients contact them concerning their appointments, bookings, etc., via email, the employees try to refer to their digital services and portals, who are generally available via e.g., 1177, to avoid any sensitive data from exposure. This is proposed by the organization as a result of avoiding any data to be e.g., printed over email for security purposes. In a similar manner, respondents R3 and R6 also described that they do not prefer to use email in this way, i.e., to avoid forwarding patient details over email. In contrast, respondent R5 stated that all of their data is treated in the same manner. The respondent exemplified this by using patients with protected identity and explained that they are treated in the same manner as any other patient, despite e.g., code names, and that employees follow the same care throughout the processes to provide the same standards of protection.

To be aware of which actions that are regulated to follow, all of the respondents described that they apply internal training for security purposes. Respondents R1 and R2 explained that they include daily education, such as meetings and general communication at the office, within the organisations to sustain an appropriate behaviour of data management and protection. Respondent R1 further described that their organization provides a physical manual and uses their intranet to ensure that all employees understand how to act and behave in relation to the management of data. Respondent R2 also explained that they have an information campaign for the employees to draw attention to risks, such as phishing, which was proven to have a great effect.

Respondents R3, R4 and R5 described their education as development of knowledge in different laws and regulations. Respondent R3 explained that new employees are always introduced to and expected to complete an installation containing patient security. In a similar manner, respondent R5 described that they apply education in information security, data protection ordinance and patient data act, which covers the laws and regulations that are applied to the management of data and how the employees should act in relation to the data. Respondent R4 also explained that the new employees are expected to take a course about the GDPR to ultimately complete a one-hour long test and reach a certain number of points to pass. If the test is unsuccessful, the employee needs to retake the test until it is approved.

4.2.2 The use of systems and tools

In relation to the security and management of data, this study was interested to observe what types of solutions the organizations apply, including systems and tools, for protecting the data. To communicate in a safe way internally, respondent R1 explained that they use chat systems and Microsoft Teams within the municipality's servers. Respondent R5 also described that they use systems in a secure way for preserving data security. For instance, the respondent explained that they do not consolidate their data with others, which in turn leads to a smaller domain that becomes more secure. In terms of utilizing systems and tools from a remote location, all respondents explained that it is possible to work from home and still access all the data that is needed. Respondents R1, R2, R3, R6 described that when work is done from home, the healthcare organization's computers must be used, which means that it is not possible to work via any computer. Respondent R2 explained in further detail that their tasks are not able to be performed on personal computers or equipment as a result of the lack of awareness and knowledge in relation to what virus programs or software that are preinstalled, which consequently creates an impression of insecurity. Respondent R2 also stated that the employees who work from home must connect via an encrypted funnel to access any data. Respondent R4, on the other hand, described that it is possible to work on any computer as long as they use a remote login and an identification card that is used within their healthcare organization.

For accessing the data, all respondents explained that they require identification cards, also referred to as siths cards. Respondents R1 and R3 explained that these identification cards are used together with a card reader in connection with logging in to and entering the systems used in their work. Respondents R1 and R3 explained that these identification cards are used together with a card reader in connection with logging in to and entering the systems used in their work. Respondent R5 explained that these cards have been a requirement according to law regulations, since 2008. In addition to the identification card, R5 further described that the systems that they use within the organization are classifying its information to see what security level that is needed to apply, as well as they encrypt all information and use both external and internal firewalls. In a similar manner, R1 further described that when working within their organization, the login with card readers and passwords does not take place just once to access the systems used, rather there are three different security layers in order to get connected to the system. These steps include the employee entering a pin code to unlock the computer, a password for accessing the system, and then another password for accessing patient files. Then, as soon as an employee removes their card from the card reader, all systems lock and shut down automatically.

In terms of working from a remote location, like home, respondents R2, R5 and R6 explained that they need to ensure that no one other than themselves can hear phone- and video calls nor access data on their computers, by locating themselves in a secluded area. Respondent R3 explained that working from home is possible as long as employees use their identification card to access the systems, but also stressed that they must act in a careful way so that no one other than themselves can access or view the data. Respondent R6 emphasized the importance of always closing down and locking the computer, to ensure that no unauthorized parties can browse through the data, if the employee were to relocate. Respondent R1 mentioned that when they are working from home, they need to connect to a VPN to access data and also speculated that more strict regulations and laws may be applied in the future regarding

working from a remote location, which might change the ways that they apply and proceed according to.

To summarize this subchapter in the matter of data security management, it was demonstrated that all of the respondents applied some form of training to educate their employees on how to act. In some cases, it was influenced by information about security, while others explained that they expect their employees to pass an examination, as a means of educating the employees about their actions toward the management and protection of data. In terms of working from home, all respondents had security guidelines implemented, to protect the data, as the data is at higher risk of getting exposed from a remote location. Similar to the application of education, each organization had tools that slightly differed from each other.

4.3 Policies

4.3.1 Fundamental principles of policies

In regard to the management and security of data, this study was curious to determine whether policies had an impact on employee's behaviour and attitude. All respondents applied policies, rules, and regulations for instructing how, what, and what not to do, in terms of managing data and behaviour, that are valid for both employees and management. While the rest of the respondents mentioned specific foundations and details about their policies, respondent R4 explained that they mainly rely on a secrecy contract, as an assurance that employees will act in a proper and appropriate manner, in terms of security and the management of data. Respondent R1 referred to their policies as instructions of how actions are meant to be carried out, while respondent R2 associated their policies as rules for managing high levels of sensitive data, in terms of providing confidentiality, availability and accuracy, but also which rules individuals, or employees in this case, are meant to apply. In similarity to respondent R2, respondent R3 expressed their policies to be considered as guidelines for maintaining data in a safe manner, with respect to risks and access. Respondent R5 described that their organization concentrates on three areas in terms of instructing employees how to manage their data. The three areas were security in relation to accuracy and availability of the information, information security related to access, and cyber security associated with protection from risks from the outside world. Respondent R6 described their policies to be based on patient security laws, the GDPR and regulations from the National Board of Health and Welfare's, which was also the guidelines for how they manage their data.

All respondents clarified that their policies were based on and influenced by laws and regulations, where the GDPR played an important role, especially in terms of security and privacy. Respondents R1 and R2 explained that the regulation is constantly changing and developing, which means that it is important to be up to date and adapt to the changes at the same time. Every respondent mentioned that their policies are updated and revised in accordance with the laws, despite different time schedules, with respect to the development of information systems and corresponding security related questions and issues. Respondent R6 described that they have employees hired for a special responsibility to ensure that every process is performed according to the GDPR. ISO standards were also commonly applied in relation to policies. Respondents R2 and R3 mentioned that their policies were based on ISO standards, whereas

respondent R1 explained that they were in the process of certifying their organization with ISO 700/701. However, laws are not the sole factor for all organizations, rather some responses were connected to other determining influences. For instance, in contrast to the other respondents, respondent R2 explained that they also ground their policies on the recommendations from the Swedish Civil Contingencies Agency (MSB), as well as they account for political regulations and observe how other municipalities manage their policies. In a similar manner, respondent R5 also mentioned that their organization supports their policies based on a mix of old personal data legislation intuition.

In regard to the accessibility and accommodation of the policies in relation to the employees, the responses varied to some extent. Respondent R1 described that their organization was currently carrying out a four-year-old plan, which included continuous reinforcement. Additionally, the respondent explained that they are constantly reminding their employees of instructions, placing the policies on their intranet, have monthly meetings, readable manuals, both physical and digital, video recordings, and even the possibility to ask questions during office hours. In similarity to respondent R1, respondents R3 and R5 have also placed their policies on an intranet, for easy accessibility and availability. Respondents R2 and R4 mentioned that their policies are available on digital assets, such as computers, but did not go into further details. Respondent R6 did also place their policies accessible on their intranet, as well as they provided an physical emergency folder, in case of a situation where there is a current power failure and an employee needs to access the policies. The policies printed in the emergency folder were updated in correspondence with the updates made on the intranet.

4.3.2 Policy awareness

To ensure that the policies are applied accurately, almost all respondents explained that they enforce education and training, for both management and employees. As all organizations manage and deal with large amounts of data, the respondents apply education as a form of informing general information about the management of data, information security and various risks. Respondents R1, R2 and R5 explained that they educate both employees and managers so that all parties are informed about how to proceed and protect the data in an appropriate manner. While respondent R3 argued that a great deal of data security is considered to be "common sense", they still educate their employees in patient security. Respondent R6 did not describe any specific details about their policy awareness within the organization but stated that they are heavily influenced by the GDPR. Respondent R4 described that they enforce a mandatory course in the GDPR and a test that must be completed before practicing, which consists of a general understanding of the basic information related to managing data. In addition to basic education, respondent R5 also mentioned that they apply training in the Patient Data Act and Healthcare legislation, considering that they are responsible for a great amount of data which must be managed in a correct manner. Additionally, respondent R2 explained that they have invested in information campaigns and education for enlightening their employees about risks and to encourage them to act in a sceptical manner towards emails containing links and to not to disclose any information, to prevent e.g., data breaches.

4.3.3 Policies when working from home

As a result of the pandemic spreading, it has led to employees working from home, rather than visiting the office, in order to minimize the spread of the virus. In consideration of this, we were interested in discovering if the respondents employ any specific policies designed to apply when they are working from a remote location. Respondents R1, R2, R3 and R6 explained that there are some specific and clear guidelines to follow for working from home. All four respondents mentioned that every employee has to keep the data safe from unauthorized parties viewing or accessing the data, including family members and neighbours. Respondent R1 mentioned that actions are especially influenced by the GDPR when you are working from home, in particular with respect to access, in consideration of possible risks that must be accounted for. Respondent R2 explained that they enforce special policies for employees working from home, such as regulations for IT, telephone policies, and the management of data with respect to privacy in terms of unauthorized people observing or glancing at the data without the employee's knowledge or awareness. While there were some instructions to apply, according to respondent R5, it was made clear that the same policies that are carried out at work are possible to attain from home, according to respondents R4 and R5.

Moreover, respondent R4 explained that most tasks are able to be performed from home, without any inconvenience. However, the employees need to proceed in a cautious and accurate manner, according to laws and regulations, as they might risk losing their license if they are not fulfilled. Respondent R6 also explained that when you are working from a remote location, physical meetings are not available, but if a meeting is required, it can be done digitally. When a digital meeting is conducted, the employee needs to receive consent and approval from a patient to have a digital meeting, since it is not performed from the office. According to respondent R6 these digital meetings are especially encouraged during the current situation.

4.3.4 Possible concerns

While policies are intended to encourage a sense of comfort, that employees act in accordance with stated rules and regulations and that data is kept confidential, the interviews presented contrary results, to some extent. For instance, in terms of complying with the GDPR, respondent R1 explained that employees can find it difficult to understand what the regulation entails, in consideration of its constant changes. Additionally, the respondent also described that while there have not been any unsuccessful or unsuitable applied policies, the respondent experienced slow levels of adaptation, in terms of the extent of sensitive information that could be exchanged, e.g., full names and social security numbers. In a similar manner, respondent R2 mentioned the importance of a clear statement regarding which information that is presented, from a confidential perspective. The respondent exemplified concerns regarding visible information of tablets, televisions, and public places that the everyday person passes by.

To avoid that any possible issues would occur, respondents R2 and R5 had a respective deviation system implemented. Respondent R2 explained that the system exists for learning if something has failed to succeed or does not add up and can be applied for evaluating and discovering if something works against the policies. Respondent R5 described the function of the system to discover if something is not in line with the rules or routines, equivalent to respondent R2. The system can report deviations to the management who ultimately decide the most

appropriate solution, in terms of the level of damage it can cause. Respondent R6 also described that policies of how to work within the organization does not always match the organization that they communicate or collaborate with. For instance, they sometimes receive emails containing complete social security numbers on patients from both other organizations and private external parties, which is not allowed within the respondents' organization, as well as other healthcare organizations. Respondent R4 explained that they had also experienced similar situations and shared interchangeable thoughts regarding the incorrect exchange of data.

To summarize the subchapter about the application of policies, all respondents had incorporated policies to support the management and protection of data. While the policies differed, to some extent, the foundation of each organization's policies were all influenced by the same regulations and laws, including the GDPR. The policies were demonstrated to control and monitor the employee's behaviour toward the management of data and became even more crucial to apply if work was conducted from a remote location.

In summary of the empirical results, including all subchapters, the responses from the interviews demonstrated that healthcare organizations recognize and have incorporated solutions in case of a suspected data leakage situation. The major factors that were demonstrated to protect data and minimize any chances of violations taking place were influenced by the level of accessibility, education, and policies. By limiting the accessibility of data to a lower number of employees, the risk of exposing data to unauthorized parties could possibly minimize or decline. An encouragement and integration of education and training can create an awareness among employees on how to act and manage data if risks and guidelines are highlighted. Additionally, an incorporation of policies, both from a remote and local office, could possibly minimize the risk of endangering the data, if employees are aware of what and what not to do in terms of protecting and managing the data in relation to laws and regulations.

5 Discussion

In this chapter the collected empirical data will be discussed in relation to the presented theoretical data about data security.

5.1 Data Leakage

5.1.1 Data leakage in relation to the GDPR

In similarity with previous research and literature, it was explained by the majority of the respondents that healthcare organizations are very likely to be exposed by threats that eventually lead to data leakage. While only a small number of respondents had experienced a situation where data could be at risk, all respondents were well aware of potential risks, and had implemented security measures to cope with any related security issue concerning their data. To manage data in an appropriate manner, in particular to avoid data leakage, it became clear that laws and regulations have a strong impact. All respondents were in agreement that the GDPR is an urgently important factor, in terms of acting in accordance with how to manage data in a proper way, but also for guidelines regarding reporting issues, including actions towards data leakage. The interviews portrayed that the GDPR plays a crucial role for healthcare organizations, mainly in relation to the storage of data, that the access of a certain data takes place in a correct manner, and how their work is carried out, in consideration of laws and circumstances.

The importance of the GDPR became apparent in relation to healthcare organizations abilities of protecting data from unauthorized sources to some extent. Some of the respondents acknowledged the important role the regulation plays and demonstrated this by applying education and training for ensuring and maintaining an appropriate and correct approach towards data protection. The answers from the respondents included the application of GDPR courses, video recordings as a guidance, introductory information to newly hired employees, rules, and education as instructions for what to do and not, and even appoint GDPR personnel for guaranteeing that actions take place in a correct manner according to the regulation. This confirms Abouelmedhi et al (2017) and Larrucea et al (2020) understanding of the regulation, including the importance of data protection laws for preserving privacy, such as sensitive data like patient records, that they both emphasize.

While the value of acting correspondingly to the regulations statements and to treat data in a correct manner was stressed by previously mentioned researchers, it was interesting to discover that it can be difficult for employees to act consequently, with the regulations constantly changing and the development of information systems. It became clear that at least two respondents had experienced their employees having conflicts with understanding the basis of the regulation and correspondingly dismissing their statements. For instance, respondent R1 explained that some employees had acted in a careless manner towards the regulation, as a result of its continuous development and improvements regarding its principles. During one of the six interviews it also became apparent that the GDPR may also be taken for granted. This was particularly apparent with respondent R3, referring to the GDPR as common sense and

not expressing further value to it. In consideration of the pessimistic view employees have had towards the GDPR, it could possibly be treated as risky in relation to the protection and management of data, considering that employees may be aware of its existence and consider it as an average influence, but not provide the attention it might need to avoid any mistakes in an exchange of information. Additionally, by not acknowledging the regulation could also result in legal consequences if an action is not performed in a correct manner.

Even though neither respondent have had any negative experiences with how well rules and regulations are applied, with the exception of poor control of employee's knowledge and attention to the regulation in some cases, previous research and literature argue that it could cause security vulnerabilities if the GDPR is not followed or applied in a correct manner (Werlinger, Hawkey & Beznosov, 2009; GDPR, 2021). By taking this into account, employees could put their organization in a vulnerable position, cause harm towards the management of data, and even risk legal actions.

5.1.2 Data breaches

Previous literature, in particular Offner et al (2020) and Abouelmedhi et al (2017), state that sensitive data, including patient records and information about healthcare organizations, that contain personal information, is likely to become targets for breaches. In accordance with said authors, the interviews all confirm that attacks and violations indeed take place and is a current concern. For this reason, the respondents argued that these types of risks must be accounted for in terms of how the data is managed. According to the respondents who had experience with attempted data breaches and actual breaches, they stated that they were mainly targeted by the action of phishing, where intruders try to access details including contact information, log ins, personal data, social security numbers, etc. For managing data in an accurate manner, Werlinger, Hawkey & Beznosov (2009), Soomro, Shah and Ahmed (2016), van der Kleij, Wijn and Hof (2020) all stress the importance of including the human factor and organizational activities for avoiding the exploitation of data to unauthorized parties. The authors propose the creation of awareness among employees and that they should be accounted for as possible sources of exchanging information in an incorrect manner.

The authors statements were also validated by the respondents. The majority of respondents believed that organizational activities like education, continuous information and a sceptical attitude towards emails and similar tactics could be an appropriate approach to avoid breaches and attempts. For those who had not experienced any breaches, still confirmed the importance of incorporating security measures for maintaining safe management of data, to avoid any exposure or leakage. To prepare for a possible attack, it was explained that all respondents had procedures, including reporting of an incident and informing the people involved, applying automatic shutdowns in their systems, and following strict rules and instructions, among others. Some organizations even had the ability to receive guidelines from support teams and departments.

5.2 Data Security Management

5.2.1 Education and Security

According to Werlinger, Hawkey and Beznosov (2009) and Soomro, Shah and Ahmed (2016), any kind of security measure is a necessity for organizations to manage and protect their data from any unauthorized parties trying to access it. In order to sustain a high level of protection, Werlinger, Hawkey and Beznosov (2009) expressed the advantage of incorporating a combination of human, organizational, and technological factors, rather than solely relying on technical solutions for protecting an organization's data. In a similar manner, Soomro, Shah and Ahmed (2016) and van der Kleij, Wijn & Hof (2020) stated the effectiveness of including managerial activities, including the creation of awareness towards risks and attacks, to protect the data. In a complementary manner, Alneyadi, Sithirasenan & Muthukkumarasamy (2016) stated that many organizations have experienced failure with technical solutions not performing as it is determined to be, consequently putting the data in a defenceless situation.

Considering that most of the respondents expressed that patient records are not intended to be viewed or accessed by the public or an unauthorized party, there is a high demand from healthcare organizations to keep this data safe and managed properly. For this reason, the respondents were able to confirm the authors statements by explaining that they include, and part take in education, both at work and from a remote location like home, to not risk positioning the data in a vulnerable situation. This could e.g., be avoided by not working on public transportation or opening the computer in front of family or neighbours. While most of the respondents were able to express their confidence in technical solutions, including firewalls, specific systems, servers and connections, the importance of organizational activities, inclusive of security policies and rules, became even more apparent. The respondents explained that not any possible task was able to be performed, either as a result of limited access, the role of the employee or the type of task it was, which is enforced by policies and rules. All of the respondents expressed how crucial it is for them to make sure that the data is protected, e.g., by ensuring that no unauthorized party is granted access to their data, as well as there are no indications made over mail or other platforms as to whom the data is associated with.

In relation to the protection and management of data, previous research, in particular Abouelmedhi et al (2017) and Larrucea et al (2020), stated how valuable laws and regulations are, including the GDPR. This was also confirmed by the respondents who explained that most of their activities and tasks are heavily reliant on regulations and laws. It was expressed that it is of utmost importance for employees working within the healthcare sector to understand how to manage personal and sensitive data in an appropriate and correct manner. In consideration of the personal and private data they manage, laws like the GDPR are greatly important to acknowledge, as they influence the privacy and protection of personal information, including how it is stored and used for various purposes.

5.2.2 Specific Access

According to Shabtai, Elovici and Rokach (2012), it is possible for organizations to advance their securing and protection of data by acting in accordance with the CIA triad. This triad emphasizes the importance of confidentiality, integrity, and availability, where it adheres to

an assurance that data cannot be accessed without authorization. Additionally, as stated by Tipton and Krause (2006), the level of authorized access can vary, as they stress the fact that not all employees should have the same access to everything, rather the access should be based on the required data for a specific task, which should also be able to be monitored. Furthermore, St-Hilarie (2020), also expressed that data needs various means for protection to enhance the level of security and is especially valuable for sensitive and confidential data like patient data (Yeng, Yang & Snekkenes, 2019). Smys, Senjyu and Lafata (2019) and Abouelmehdi et al (2017) also stated that data can be protected using technologies that include authentications and access control. This became apparent from the respondents' answers as well, who explained that they apply multiple means for protecting the data, including preserving confidentiality, integrity, and availability, with a certain focus on access and authorization.

For accessing the data, all respondents stated that they use personal cards, also referred to as a sith card by most of the respondents, with a corresponding card reader. Respondent R1 explained that the sith card usually encompasses three codes that must be correctly composed for logging in and accessing the data. This was applied by all employees as a safety measure to ensure that only authorized parties would be able to access systems, records, and journals. These two devices were also described as a necessity for accessing patient data and journals when the employee works from home. In regard to accessibility, respondent R2 explained in further detail that their organization also authority-controls all data, to make sure that the party truly has the right to access the data. Depending on which role an employee has, it can also determine whether it has a right to access data or not, but also which types of actions that can be made. For instance, an assistant nurse might have limited access to only viewing the data in a specific journal, while a doctor can make changes or observe data that might be disclosed in the same journal. So, there might be various types of access, depending on the employment. Additionally, in another case, respondent R6 explained that they have a logging system that saves every action, which means that they can go back in time to discover who did what. To discover any deviations or unusual activities, respondents R2, R4, R5 and R6 all explained that they have implemented a deviation system for picking up any abnormal actions. By doing so, they are able to quickly find out if something is not acting in accordance with their rules and regulations and apply suitable actions.

5.2.3 Security measures when working from home

Alneyadi, Sithirasenan & Muthukkumarasamy (2016) expressed that there is a need for incorporating security measures to avoid any data breaches or even data leakage. In a similar manner, Soomro, Shah and Ahmed (2016), Smys, Senjyu and Lafata (2019), and Abouelmehdi et al (2017) stated that security measures and protection technologies are valuable to include in order to avoid risks of data getting stolen and leaked. This was also presented by the respondents who described that they must use computers provided from their organization or region, as a precautionary measure, as a consequence of unknown preinstalled virus programs and other software on external devices. The majority of the respondents referred to the computers, sith cards and card readers as means for managing their data in a safe environment with a high level of security. In all cases, no personal equipment or computers were allowed to be used when work is conducted from home. Respondent R2 explained in further details that they need to access an encrypted funnel to connect to their data, and that some data is in particular not easily accessible, from a safety perspective. In a similar manner, respondent R5

mentioned that they must enter external and internal firewalls before accessing the data, as a security measure.

5.3 Policies

5.3.1 Policy awareness and education

According to Soomro, Shah and Ahmed (2016) and Martin and Ahuja (2010), the use of security policies can be useful to apply for discovering possible security risks but also provide an effective security management if employees are informed of possible risks. This was confirmed by all the respondents, who described that they apply policies within their organizations for ensuring that all employees receive thorough education in accordance with their respective laws and policies. For example, respondent R1 explained that they constantly remind their employees during office hours of how to proceed with certain processes and what not to do. This is determined to ensure that all employees are actually aware of the risks that exist if the policies are not followed. By applying these measures, Werlinger, Hawkey & Beznosov (2009) believed that an organization can achieve effective data security management, which was also validated by the respondents. For example, respondent R2 explained that they use campaigns to make sure that their employees are aware about specific security risks and threats, such as phishing.

In order to keep their employees aware of the rules and guidelines that apply, in addition to reminding them, all respondents maintained their policies available for everyone to read at all times. The majority of respondents explained that their policies are available on each organization's internal intranet. In addition to this, respondent R6 also described that they kept policies available in a so-called emergency folder, in case of a temporary power outage affecting the availability of the digital formats. This can be discussed to be an effective arrangement from a security perspective as it can be clever to have policies available in any given situation. Moreover, Soomro, Shah and Ahmed (2016) mentioned that attitudes towards policies can have an impact on how individuals appear in relation to policies. Considering that at least one organization supplies their policies accessible both digitally and physically, this can be an example of an attitude that encourages the importance of policies, and that it can be beneficial to have them accessible in any given situation.

According to Martino and Ahuja (2010), it is important that stakeholders are aware of the existence of policies, as demonstrated by all respondents explaining that their employees are. However, Martino and Ahuja (2010) further explained that policies can have an impact on how an organization and their organizational activities take shape. This indicates that policies that exist within organizations will affect how well employees are able to perform their tasks, which ultimately becomes an important factor to be aware of. The main focus and foundation of the respondents' policies are a bit different in comparison to each other. For example, according to respondent R4, their organization applies policies influenced by laws by providing a secrecy contract. Respondent R6, on the other hand, explained that their policies are also relying on laws and regulations to structure their processes, however they are more concretely defined. In contrast to respondent R6 and R4, the other respondents explained that their policies act as guidelines of how to manage and keep their data safe. It could thus be discussed

that although the respondents' policies are structured and originated based on different perspectives, they all create a policy awareness among their employees, which ultimately corresponds with Martino and Ahuja (2010) who defined the awareness as an important aspect. This means that an awareness can vary and be developed from different viewpoints, including conducting courses for educational purposes or by ensuring that policies are linked to a secrecy agreement.

In terms of education and instructions towards the management of data, the respondents highlighted laws and regulations as a great determinator. More specifically, respondents R1, R2 and R5 described that they focus on educating their employees on all areas concerning the laws and guidelines, to make sure they know how to manage and protect the data that is used in their work. This allows organizations to ensure that their processes and activities are shaped by policies, which is another important factor to recognize, according to Martino and Ahuja (2010). In a similar manner, respondent R4 explained that they apply a mandatory course with respect to the GDPR for their new employees to ensure that a general understanding of the law is implied, to act as a base for their data management. This also corresponds with what Martino and Ahuja (2010) stated, i.e., that policies of security and privacy are mandated by different laws and regulations. In contrast to the other respondents, respondent R4 explained that they concentrate on a secrecy contract, rather than relying on separate policies and contracts. This is a contradiction to what Martino and Ahujas (2010) theory acknowledged, in which it was explained that a contract should refer to policies of security and privacy. There is a noticeable difference in the attitude towards policies from respondent R4 in comparison to the other respondents. Respondent R4 seems to not distribute as much attention to policies as the other respondents. However, by taking Martino and Ahujas (2010) theoretical perspective into account, the key outcomes in terms of an application of contracts or application of policies does not seem to differ, given that they both can be viewed as different forms of guidelines that would still include the same key elements.

Another concern of interest that could be discussed as an effective way of combining the mandatory laws, such as the GDPR and policies, is that they have been proven in this case to cover the same purposes, by analysing how the respondents' attitudes are towards policies. The GDPR is a mandatory law within the European Union (EU) that contains regulations of how the data should be managed, and is argued to be important to healthcare organizations, according to Abouelmedhi et al, (2017), considering the need for patient consent and protection of confidential data. In addition to the regulation, respondents R2 and R3 also mentioned that their policies were influenced by ISO standards, which could be discussed to create an even more complete policy content in relation to Martino and Ahujas (2010) theory, which stated that policies should be mandated and connected to both laws and business practices.

While the awareness of policies is highly crucial for employees to follow, it is also essential for collaborating parties to support and recognize these as well. According to Martino and Ahuja (2020), who established the importance of stakeholders' awareness towards the policies that are applied, it can also be considered crucial that collaborating organizations and other external parties are attentive and recognize the healthcare organizations policies. If they are not acknowledged, there are risks of miscommunications and exposure of data that could ultimately affect an organization in a negative way. This was demonstrated in two cases, where respondents R4 and R6 had experienced dismissive and ignorant actions toward their policies, in particular concerning their approach towards encryption of data via email and fax, which was neglected by collaborating and external parties. These two examples emphasized the

value of collaborating parties' attentiveness, which may affect the likelihood of the exposure of data.

5.3.2 Policies and working from home

Since it is important for healthcare organizations to follow standards within their processes according to Abouelmedhi et al (2017), the individual employee also needs to adapt to these standards even if the work is carried out from a remote location like home. All of the respondents explained that it is possible to work from home, and that it has become more accepted, as a result of the current situation in the world. While the rest of the respondents explained that there are specially developed policies to apply when work is conducted from a remote location, respondents R4 and R6 clarified that all of their tasks are available to be performed from home. The statements made by the majority of the respondents corresponded with Martino and Ahujo (2010), who stated that it is common that policies can change, considering that they are so well integrated in and connected with the practice of organizations. Moreover, respondents R4 and R6, on the other hand, did not incorporate any changes, despite the change of location, which can be considered dubious, considering that Larrucea et al (2020) argued that it is important for organizations to have clear guidelines of how to act and manage data using various devices.

The change in location of the workplace also affected the employees' tasks negatively to some extent, and even interrupted them from performing some assignments. For instance, respondent R6 explained that when they are working from home, no physical appointments are allowed. Additionally, to carry out a digital meeting instead required an additional approval from the patient, to make sure that they were aware of how their data will be collected and managed, considering the change in appointment. This can be discussed to be an act that is in line with the GDPR where it becomes even more critical to confirm consent (GDPR, 2021). These acts can also be considered important to continue to develop since the form of business practices might develop or change when work is conducted from home, and as Martino and Ahuja (2010) described, i.e., that business practices are influenced by policies and regulations.

To summarize the discussion, it becomes clear that laws, in particular the GDPR, is an important regulation that has a great impact on healthcare organizations data security management. The importance of the regulation was demonstrated in relation to data breaches towards healthcare organizations, as a crucial factor for facilitating organizations' abilities to protect their data from unauthorized parties accessing and leaking data. It was also apparent that it is an essential determinant of managing data in an appropriate manner, considering the advantages of connecting human, organizational, and technological solutions, rather than solely relying on technical solutions. The regulation was also illustrated as important in relation to policies, which are highly influenced by laws and regulations. While the GDPR was considered a great authority, this chapter also highlighted the significance of limiting the access of data based on the role of the employee and its corresponding task. The value of said execution could possibly prevent unauthorized parties from accessing information that may be considered sensitive and ultimately minimize the risk of data leakage, but also prevent employees from making errors. Additionally, the implementation of policies was also established as critical in relation to managing and protecting the data, in particular to monitor the actions made by their employees. By including policies, healthcare organizations are able to educate them

about the appropriate methods of managing data, as well as it provides opportunities for creating an awareness of risks and corresponding guidelines. While this study concentrated on organizational activities, technical security measures were also presented as dependable, in spite of potential risks of failing to protect the data.

This chapter also emphasized that while technical solutions have been treated as the focal point in previous research, this study illustrated the importance of incorporating organizational activities, including security policies, laws and regulations, and elements from the CIA triad and ISO standards. Since the risk of data leakage is equally great to be caused by an employee, it becomes crucial to educate employees, rather than mainly having confidence in technology. Even though some respondents expressed concerns about the GDPR and issues in relation to policies, their contribution and advancement directed toward healthcare organizations data security management is vital for protecting data against any possible attacks.

6 Conclusion

The aim of this study was to achieve an overview of how Swedish healthcare organizations structure their data security management in relation to the risk of data leakage. To achieve this, the following research question was generated: “How do healthcare organizations structure their data security management in relation to data leakage?”. The research question was examined by conducting six interviews as a qualitative research method for discovering how they manage and protect their data, while incorporating routines formed to decline the risk of data leakage. Additionally, the study was also able to reach an overview of the most important organizational factors that healthcare organizations apply to manage and protect their data. This study answered the research question where healthcare organizations do structure their data security management with education and knowledge about data leakage as well as development and usage of policies.

This study also led to the findings that Swedish healthcare organizations account for and emphasizes that there are various risks and threats that can result in data leakage, and thus structure their data security management in relation to these risks accordingly. Even though the attitudes and definitions of policies may differ among the organizations and employees, the basis of each structure is relatively similar. All organizations included and highlighted that they also structure their security management with distribution of access to data and the awareness of laws, policies, and risks to educate the employees on how to behave and manage the data that is required in their daily activities. According to the respondents, the level of access and which role the employee has is one way of observing what data is viewed and limiting the access to various data, to avoid any unauthorized parties from entering systems and journals, but also on which device the data is available. The ability to encourage employees to care for laws, policies and risks by applying education is another important factor that can influence how well the data is protected and managed, to ultimately avoid any risks of incorrect exchanges of data. The GDPR was in particular valuable for healthcare organizations to adapt to and act in accordance with, considering its continuous development and improvements, but also for strengthening the protection of personal data.

In this study, the importance of applying organizational activities to prevent any mistakes from taking place in relation to the management of data was also discovered. The respondents stated the value of incorporating organizational activities for determining the most appropriate methods of action to avoid activities that could be considered harmful to an individual or organization. While a confidence in technical solutions were clarified, they may not be as easily controlled or attain a favourable and consistent outcome. By taking this to account, it may be of even greater significance that organizations can rely on their employees, in case of a failure in a technical solution. For this reason, the combination of human, organizational, and technological solutions may be more efficient and beneficial for healthcare organizations, rather than solely relying on technical solutions for managing and protecting their data.

6.1 Limitations and future research

This study was limited to Swedish healthcare organizations to achieve an equitable overview where all the selected healthcare organizations follow the same main laws, which means that the conclusions were drawn from Swedish organizations only. For future research it could be of interest to examine how healthcare organizations in other countries structure their data security management in relation to data leakage, to get a more global perspective. To achieve an even greater overview and additional data, this study could have targeted a higher number of respondents.

As we are moving towards a more digital workplace, it could mean that healthcare organizations must account for other concerns, excluding our findings. For future research it could be of interest to examine further details on how healthcare organizations act when the work is conducted from home since it is becoming more common nowadays.

While a high level of collected data from the interviews corresponded with previous research and literature, a further investigation within laws and regulations could possibly contribute to rules and governance being accurately applied by employees, and not dismissed in certain circumstances, which may ultimately have a beneficial impact on the management and protection of data.

Appendix 1 – Interview 1

Person		#
AJA	Hello! Thank you for participating in this interview for our thesis. Let me introduce myself, Amanda, and my thesis partner Josefin.	
JB	Hello!	
R1	Hello!	
AJA	Could you give a brief description of the organization you are working at, your role and the responsibilities your role include?	
R1	I have a background as an engineer, have been working with IT for 26 years, and will soon get a degree in Datavetenskap from Uppsala University. This organization is called .... We are a organization that owns three different health centres, and also owns a organization that provides houses, which we foster kids that have drug issues or were mishandled, and stuff like that. So, basically we are, you could say that we are a healthcare organization. My responsibilities, I am the IT boss of the main organization, which is the umbrella for the sister companies, or daughter companies, and I am the one in charge of writing the policies for all that is related to IT. All the procedures, all the restrictions, and right now I am the one in training to be the data security officer in the organization.	
AJA	Since you are the one responsible for policies, how does your organisation manage your data and information? Like the patient records or other data?	
R1	It's a bit complicated, because you guys need to remember that, or you girls need to remember that, we are working in the healthcare sector. So that means that we have to work with the database of the people in the whole country. But at the same time, we work directly to the database that is located inside the region that you work in. Like, we are in Uppsala right now, so we work with region Uppsala. So they have the data in their servers/service and we access the data. We don't manage the data in that sense, we just create that data. We access the data that they have and we modify it, basically patient records and so like that. We don't have to worry about how we store it, we don't have to worry about any GDPR regulations. What we do need to worry about is how, what our doctors and nurses do with the data when they access it. So we have created policies that control how doctors and nurses use the data, where they can send the data and how they can send the data. Because we have.. Only accessing the data is no problem, and doctors and nurses use it to record things in your medical record. But the problem is what happens when someone wants to or needs a remiss? Or someone needs to send or move doctors or such like that. So there's policies that we have to ensure that	S, T, L

	they do not send patient information to do mail, by example. Or they use a chat system. Also we have made policies for them not to attach, in the same mail, the name of the person and personal number by example. Also we made policies so they understand that they cannot put the whole name of anyone in the mail, so they can put their full name and the initial of the last name, or they can put the initial of the first name and the last name. Even though in Sweden, you can find information about anyone, because it is open to the public. You can find how much they earn, where they live, their phone number and what not. We still have to be careful to not link any of the information to make it easier if someone manages to access it, it doesn't, it is not easy for them to link it to the person, to any person in this case. We do not have inside services for this information, because it is a no-no, so all the information that we use and handle patient wise, is directly handled in the service of region Uppsala.	
AJA	Okay, so the chat system that you were talking about. Is that also within that?	
R1	Yes, there are two. We use Teams and we also use a chat system that is also in the servers/service of Uppsala. So they have to handle the information themselves. But of course, they also have rulings. So we have to apply by their rulings. So I have to, I meet with them often, to discuss their policies, and then I have to instruct the people here of what not to do in their systems also. Because we are not liable for what happens if they get a breach in, but we are liable if we cause the breaching.	S, T, DP
AJA	So do you have any, or do you use any not education, but how do you inform the..	
R1	How do I enforce the policies is what you are trying to ask?	DP
AJA	Yes.	
R1	How do I police that people are doing what they are supposed to be doing? And how do I teach them? You can quote me on this, everybody is a child, and all in organisations that work with data security is a child. And they do not understand why you are saying no to them. They get annoyed with it. So, what we have been doing for the last four years is to, its been a plan of reinforcing little by little, reminding them every week a little about everything. We post it on the intranet, we meet, all the companies by themselves meet every month for two hour discussion on how things are going, and we make a point to take and list ten-fifteen minutes to remind people what they are not supposed to do and what they are supposed to do. We have, evidential, manuals, written down what you can, what you cannot do, and of course they come to my office a lot of times to ask questions. We have drilled that if you don't know, don't do it, just ask me. It is much better.	DP

AJA	Have you experienced some issues before when there was a risk that some data would have been leaked? If not, if this question is not available to be answered, how would the organisation act, in hence with the policies?	
R1	I can answer that question that we have never had a leak. Thank god. But if there was a leak, we have procedures. What I can tell you is that, first of all we will find out how it happened. That's the first thing that we try to do. How it happened and what leaked out. Once we determine that, we inform the people that are involved. And then we have to, depending on the data, there are two rows. One - we inform the region Uppsala, if there is information that concerns patients. If it is not information that concerns the patients, let's say information about people that work here. Then we inform them and then we have to try to mitigate the spread. It depends on the information though. There are tons of cases. Like a hundred or something things that could happen. The other thing is that if, depending on the confidentiality of information, we have to inform the government. There is an institution, I don't remember the name, is something very long with information. You can't hide it, by law you can't hide the breach. You have to report it. But you do have seven days to try to fix it. To mitigate it basically.	R
AJA	So, are there possibilities for employees to work from home? Maybe it's different depending on what role you have in the organization.	
R1	Yes, there is a possibility. There is a system that allows, that uses citrix software, which is very famous for new VPN accessibility. In a normal computer, I think you can access the system of region Uppsala, to check patient information and work. Not everyone is allowed to, but that's more of a policy of the bosses that say that you should work here instead of home. We do have some doctors that work from home. We have a digital platform, like Doktor.se and such. We have an app that people can have a videoconference and you can see the patient and what not. And some of those doctors can work remotely, because they use a platform that is secured. But we try not to let people work from home. Also, you need to remember that they handle data from their houses, it is also a human resources thing. They don't want people to work from home. They should be resting at home. There is balance between how much you should let them work. And now with the pandemic, it has changed a lot. Half of my floor is empty most of the days because of the pandemic. And the world is gonna change. Because people are gonna realize that you are not gonna need to take a plane anymore, if you can do this. That will imply in the end that you will get more regulations, sooner or later there are gonna be more regulations, specifically here in Europe. The GDPR is probably gonna add more regulations, add videoconferencing and such.	S, T, A, L

AJA	Are there any specific tasks that an employee is not allowed to do from home? Even if it is allowed to work from home, maybe there are still some specific tasks?	
R1	Let me think. No, when it's patient related, they have access to the whole system. And there is a videoconference system directly integrated to region Uppsala, so you can even see patients like that. There are no restrictions really, as long as they are following, and are connected properly to the VPN and such, they can probably work from home.	A, S
AJA	Are there any specific policies that the employees need to follow when they work from home or are they the same as from working at the office?	
R1	Half and half I would say. They still have to follow the same professionalism. Even if you are looking at the patient through a camera, you still have to do the same thing as possible, you are looking in front of you. But no, they have to be way more careful in the computers that they use for this. So, we have the policy that we provide the computers that they are gonna use. If they are gonna work from home, to see patients, we provide the computers. Because, in that way we can ensure that the computers are safe.	DP
JB	And speaking of safety, could you see any risks with working from home or using an app or platform for videoconferences?	
R1	Yeah, this is what keeps me awake at night. Because, people are very careless with what they do with information. People still don't care about GDPR, and imagine someone that has access to all the patients information that they want and they do something stupid with that computer. Then of course, since I can't be 24/7 on what they are doing, there can be a big leak through that. So, yes, it is very stressful to let them work from home.	L, R
AJA	Okay, so they can't use any computers at all?	
R1	No, so we provide. And in Uppsala also, they provide certain... We provide certain computers that they can use, and we can also rent computers from Uppsala that have extra security. Also, to be able to connect to the system you need one of these (presents a card on Teams video). So, if you don't have any of these, you can't connect. So there is an extra layer of security, and then it has a two step authentication, and then it has a password. So it is secure, that not anyone can connect. We try to contain it as much as possible.	T, S, A, C
AJA	So that was a card that you were showing.	
R1	Yes.	
AJA	And what do you do with the card?	

R1	It is called a siths kort, and it has a certificate in it that is issued by region Uppsala, in this case. So, it has a microchip on it and you need a card reader for it. So, this card has two codes, one that allows you to get in to the system, and one that allows you to sign in the patients records. So, because when the doctors write it down, it might be that you leave your computer open with the things there, if you are on call/a colleague you cannot sign the journal by example. So that means that the information is not real to sign. It is the first line of defence of the system. Without it you cannot go anywhere. Once you pass the first stage, selecting the certificate and the password, the pincode sorry, then you can put your username and password, to allow you to get in. And after that, when you open the main system, it will ask you again for the password. So there are three different layers of it. The moment you remove the card from the card reader, it locks the system off.	S, T, A, C
AJA	So, the policies, are they updated or read through, every once a month or year? Do the policies change? Maybe now with the pandemic? Have the policies changed?	
R1	Yes, they have changed a little bit of course. We update the policies, so I have contact with Uppsala, so when they change something, I change something. As soon as possible. When its our policy, they get revised every six months. Most of the policies dont change, because things don't change that much. But GDPR does change every year. So, we have to modify them. So every six months we revise. There is a, I am the head of the IT department, I have a, we have a lawyer, that sits with me, and we go through them. Then of course, it is the same with all the other departments. But basically, for IT, yes we have to. Most of them don't change, to be fair. But some of them. A little bit. It is not a full rewrite, we haven't had to do a full rewrite yet.	DP
AJA	So the lawyer helps with explaining the new changes in the laws so you don't need to sit down and search and read through?	
R1	Most of the time, the half part of this job is understanding the law (distent?), and the changes are very self explanatory, because there are just little changes here and there. The lawyers is most there to tell me if the changes that I am doing are legal or not, and explain that. I have an IT policy in the organization, which tells you how can you, what can you do with the computers, what can you do with the internet, if you are blogger by example, what can you blog about the organization or not. Normal basically, but before I do any changes with that I have to pass it through to the lawyer so he checks that I am not doing or putting something illegal in it. Something that violates their rights or even leading to problems with the facket basically.	L
AJA	Okay, so we don't have any more specific questions.	

JB	I just had a question that came to my mind. Have you ever applied any policies that you deemed as unsuccessful or were not suitable?	
R1	Yeah that's the million dollar question. No policies were unsuccessful, but the level of adaptation is very low. By example, it took me like two years to make people stop sending their full name of all their colleagues in the mails. It took, I don't know, a year to make people stop uploading things that they shouldn't do, to their intranet by example. I had to delete most of the things. I think that is not that they failed, but it's like it took a while to stick.	DP, R
AJA	Do you have any small tests that the employees need to pass for the policies?	
R1	Not a test as such. We are in the process of certifying the organization with ISO 700/701, something like that, which will require something along those lines. What we do have is a little manual that explains what you need to do and what you are not supposed to do. We are also in the process of recording videos for it. Because it seems that, we noticed that the attention cannot be, it is easier watching a video instead of reading. So we are trying to teach as a class now. We are trying to teach like we are in kindergarten. I thought we would be working better than expected. The problem that I had is that I was a little bit too technical, at the start, on the dos and don'ts. So we had to rewrite those things to make it more non-IT friendly. Because that's one of the problems with GDPR today, no one understands half of it. So we tried to make it really simple and directed to the point. And even that is still hard for people to grasps, some of the concepts.	OE, DP, L
AJA	So there is a big importance of the form of the policy? What language it is written in?	
R1	Correct.	
AJA	Maybe its easier for people to take in policies if they watch a video of it or sound recording? Maybe people are used to, when buying any product and you get a big paper of how you should use it and don't. And then everyone is just okay.	
R1	When I write a policy or a manual, by example, I have a person in the marketing department, which actually sits with me and helps me rewrite it in a way that anyone would understand. Because, the problem is that I can write simple things, but they still seem complicated somehow. So, she helps me write it for a five year old to understand it. Actually that has been good, it sounds strange but it works, it works very well. Trying to make it as simple as possible, and it's in Swedish anyway, it's not like we are writing it in English, but still it sounds complicated. So she helps dum down things to an easy level that is easy to understand.	DP

AJA	If an employee would start at the organization, and only speaks English. I don't know if that is possible?	
R1	No it's not possible. I speak Swedish and understand Swedish. But to have this conversation we are having right now, it's too complicated for the level of Swedish that I need. And I have to think about it. English is a stupid language anyway. Anyone can speak it. And no, you can't only speak English here. It is not possible, especially because the work here is to see patients, so you need to speak Swedish.	OE
AJA	That is understandable. I was thinking if the policies then would be translated to English?	
R1	We have both. Because when we did the policies, I suggested we get English in case we would get audited, by a organization that is not Swedish. Or, you also need to think about that we see a lot of patients that are foreigners and international. So, they don't speak Swedish. And when they want to, by example get a request to, they wonder data, we might have some data that we can give them to answer them so they can read our policies and so on. It has to be in English also.	DP
AJA	So you have made the policies readable for everyone?	
R1	Basically. Swedish and English. Here in Sweden it's like 72% of the population that speaks English, so it's very rare that we have cases of Spanish people that dont speak English, but we always have someone that can. But yeah it's very rare that, English and Swedish is just good enough.	OE
AJA	Okay, so I think we got a lot of data from this interview.	
JB	Yeah, and good answers.	
R1	Thank you.	
AJA	We would like to thank you very much for participating, and it actually taught us to really understand. We will email you a PDF with our transcription, so that you have access to our interview.	
AJA&JB	Thank you so much! Goodbye!	
R1	Goodbye, have a nice day!	
AJA&JB	Thank you, you too!	

Appendix 2 – Interview 2

JB	Hi!	
R2	Hi!	
JB	Thank you so much for participating!	
R2	Of course.	
JB	I will start off the interview by informing you about us and our work. Me and Amanda are studying an international masters programme in Information System at Lund University and are currently writing our thesis. Our study aims to examine how healthcare organisations manage data in relation to data leakage, concentrating on policies and organisational solutions. You will, of course, be anonymous, so we will not disclose any information about you or your organisation. I also want to ask if it is okay to record the interview?	
R2	Yes, that is okay.	
JB	Perfect, thank you. So, as I previously said, we are studying an international programme, which means that we are writing our paper in English. So, I wanted to ask if you want to proceed with the interview in Swedish or English?	
R2	Swedish is better for me.	
JB	Okay! Let's get started in Swedish then.	
JB	Could you give a brief description of the organization that you are working at? What is your role at the organisation?	
R2	The organisation is a unique collaboration between municipality and county council in Sweden. It started out as a project 06'. What's unique about it is that we run both a municipal care of health and a county council owned, or regional owned, care in Norrtälje municipality.	
JB	Okay. What is your role? What are your tasks?	
R2	I have quite a few tasks, but I am the information security coordinator (informationssäkerhetssamordnare). So, I work with information security and systematic information security related work.	

JB	Okay, and how does your organisation manage data and information?	
R2	Well, we have many different types of information. It is not possible to say we do it like this, but we adapt according to the situation. We also follow rules and policies, since we manage high volumes of sensitive data. But we also have a need to inform and communicate to the public. So, we use a lot of open data, on websites, we have Facebook, we have Twitter, and other communication channels. It is the type of data that is important to us, and what the purpose is. So, we even store data in cloud solutions to provide more patient benefits. data. But we also have a need to inform and communicate to the public. So, we use a lot of open data, on websites, we have Facebook, we have Twitter, and other communication channels. It is the type of data that is important to us, and what the purpose is. So, we even store data in cloud solutions to provide more patient benefits.	DP, S, SAS
JB	Okay. Could you describe more in detail what types of policies you apply? Or rules?	
R2	Our policies are based on MSBs guidelines, to provide confidentiality, availability and accuracy. That is what we construct our management of information based on. So, it's the fundamental policy. Regulations are about how you as an individual can manage what applies to you, so it's clear. When we work, and for those who work from home (distans), we must consider overhearing privacy, privacy protection on computers to prevent anyone from observing, and how we work from home. These kinds of regulations are built to make it as simple as possible for the employees to proceed in a correct manner. In the office, these systematic concerns, where we place the printer, how our computers are placed, which information is available on tablets, and places where general patients and relatives can pass by. So, we are clear to preserve confidentiality, but sometimes we need to be very sharp with where the information is presented too. For instance, considering people's age, on the waitroom tv, and which information that is displayed there.	DP, S, T
JB	That sounds really exciting! Have you ever experienced any attempts or data breaches?	
R2	Yes, we do. What I can say is that healthcare organisations are very much exposed to that, to a higher degree now, in the middle of a pandemic. It is actually really tragic to think that the predators are focusing on disturbing/destroying healthcare organisations as they struggle with a pandemic. The most common attempts are phishing. It is also focused on mail, accessing contact details, logins. What we know is that it is sold on the black market afterwards. What is going on right now is ransomware, that says	R

	click on this link. Which often occurs on Microsoft OneDrive, where a ransomware is planted. We cannot close this link to OneDrive for Microsoft since we would need access. But that's how they work. We have had attacks and others. So yes, we have definitely been exposed to it.	
JB	And how have you worked against it or prevented it from occurring? How do you take actions?	
R2	In terms of phishing, it is mainly information campaigns and education for the employees. When I started working here, we did not really talk about this, however, we have made a big investment where we notice that we can make systematic differences, enlighten employees to be sceptical towards receiving mail, not to click on any links, not to disclose any information, in terms of (bank) account information and others. We have noticed that this has had a high effect, since we have experienced mass mailing, when hackers/predators have stumbled across another municipality's contact information and then mass mail it. We receive this really quickly, to the support, where we access and systematically delete and isolate these mails, quickly. To then enlighten the employees that something is going on, that degree of caution has become increasingly higher.	DP, OE
JB	Okay. Is there any particular data that requires a higher level of protection or special policy, that is extra exposed or sensitive?	
R2	We talk about journal data and patient data. These are the ones that we care most about, since it is extremely crucial to have access to, and extra sensitive to leakage, as everything is included in the journals, everything about the patents is described. We have the same concerns regarding healthcare systems (omsorgssystem), where all efforts, management, and treatment is recorded. So, these systems have extra policies supporting them. We make sure that employees are aware of secrecy management, like where to print, how to do it, that you cannot sit on a bus and work within these systems at all. In these regards, we have more rigorous policies, and also efforts with continuity plans. We have more continuity plans around these systems, like if the system would go down, rather than if our financial system went down, which would be less important.	SAS,A, S, DP, OE
JB	Okay. Are there any possibilities to work from home?	
R2	Yes, there is. We who work with administrative tasks are ordered to work from home as much as possible, during the pandemic, to minimize contagiousness. So, I have been working from home, almost one year now. We are allowed to work from the office, from time to time, but there it is also possible to do administrative tasks and video calls from home. But if we	T

	work from home, we have to sit in a separate room to have these calls, and make sure that the family does not overhear.	
JB	Are there any specific tools or policies that you have to follow when you work from home?	
R2	Yes, we have regulations for IT, telephone policies, and management with regard to privacy to observations (insight), and make sure that you don't place anything so people on the streets can view it, e.g., watch the neighbors journal and them walking by. There are policies and regulations for these situations to be followed.	T, DP, L
JB	Okay. Is it okay to use your own computer? Or is it provided by the organisation?	
R2	Personal computers and their own equipment is not allowed, because we do not know which precautionary measures and virus programs are installed. When you work from home, we also have a connection that must be accessed through an encrypted funnel for accessing data that is of sensitive nature. So, no, it is corporate computers that apply when you work from home.	S, A, T
JB	Okay, and does all employees have access to all data, or is some limited or requires a certain access or authorization?	
R2	No, we authority control all data. You are only allowed access to what you need for your work, just like the Data Protection Regulation (Dataskyddsförordningen) says. So, even if you have access to the journal system, an assistant nurse may only have a limited access, another nurse has another access, and a doctor has a third access, of the same patient in the same system. So it is authority controlled. A judgement is made if an employee needs access in the system. Networks are also limited.	A, L
JB	Okay. Are there any specific policies for the security that you apply?	
R2	Yes, above all, in regard to cloud storing, Data Protection Regulations, that it is within the EU, the Privacy Shield judgement, Seamus/Schrems 2. Because that is something that affects our management of information, since there is not any basis to keep data in the USA right now, as there is a judgement against it. So, that is a management that has an impact on us.	DP, L

JB	Okay. Are there any specific information or tasks that an employee working from home cannot do as a result of security policies or similar regulations?	
R2	Yes, there are parts of information that is not easily accessed, and some information that follows the Security Protection Regulation law (säkerhetsskyddslagen).	L
JB	Okay. What are your policies based on when created?	
R2	We mainly base them on laws, we also based them on political regulations, since we are politically controlled. So, there are officials in groups that check the information security policies and produce the foundation that the politicians decide around. But we base them on recommendations, what the evidence is, what is known to work, ISO standards, MSBs regulations, if we talk about information security. But also, how do other municipalities work with this, and the region, before we structure something that is going to work for us. When we then work with policies, we need to make them similar, because there are many policies that the organisation must follow, like the information security policy, environmental policy, and work environment policy. We make them equal/similar so they are gathered together and to avoid them from pulling into different directions. This is also made to make it easier for the managers to make the right actions, but also in a collaborative manner, where one analysis is made instead of four, as we obey so many policies. If everything is written in the same place it is more easily followed and completed. So that is how we work with the policy formats, and then we also try to make it according to organization standards, as they are written with a purpose that the organization and managers follow these. Since the policies are based on what's going on in the outside world, we need to transform them into organization format to ensure that they work together with us. By doing so, you might not complete 10 things, rather only 1 is necessary.	DP, L, OE
JB	Okay, and do you update your policies?	
R2	Yes. Some are set to be revised at least every other year, while some need revision each year, so it depends on how much is going on in each area. If you consider the working environment, it might not be much activity, since they are so well established. So these are reviewed every other year. Information security is a more shifting area, it is new, MSB comes with regulations, so there are parts that we review every year. If something has happened, if something needs to be renewed, needs to be more clear, to work better, or if something has not been presented clearly and the	DP

	employees are unaware if an action is not improper. These kinds of things are reviewed and clarified for next year.	
JB	Okay, so if employees find anything unclear, is that something you can test them on, or how do you know that the policies are being applied?	
R2	We have some education that they participate in. We communicate with them on a regular basis, in the office, have meetings, educate managers about these parts, and then we also have a deviation system to learn if something has not worked or does not add up. So, from that we can discover if something goes against our policies and to evaluate the policies.	OE, DP
JB	Okay. Have you experienced any failure in a security policy, or it not acting as expected?	
R2	It is difficult to make a security policy act according to how the legislation is built, considering the development of information systems. Having everything in the cloud for large scale operations is the biggest problem from my point of view. We are not a government, however, there is a legislation that says that you cannot do this, and then you have a digital progress pulling the other direction. So you might get stuck working with these kinds of questions, before we have any relief or if we can find a Swedish cloud.	L, DP
JB	Yes, that is interesting. And what do you think can be improved within data security and keeping data protected?	
R2	Some more standards. With this development going on now, it gets more difficult, in particular for smaller companies, to keep it safe if you do not follow a good standard. Or maybe a common classification model, with the security support that may be needed. A minimum standard could ease it also. It is common that individual competency is needed. But for a sole proprietorship within healthcare it can be seen as a jungle to know this and that, and unconsciously leak data, by communicating with patients over mail and displaying details, if you lack this competency. While others might be aware that information has been leaked, and must be reported to Datainspektionen. That kind of standard could probably be helpful.	SAS, R
JB	Absolutely, it sounds really important and interesting! That was actually all the questions we had prepared. So I want to thank you again for participating. As I said before, you and your organisation will remain anonymous, and we will send a PDF of our transcript for you to check that it looks okay.	

R2	Okay, thank you and good luck with your thesis. Bye!	
JB	Thank you, bye!	

Appendix 3 – Interview 3

JB	Hi, okay, so a short presentation of me and Amanda, we are studying the masters program of information systems at Lund University and we write our exam paper about data security management.	
AJA	Yes okey so could you give a brief description of your role at the organization that you work at and what tasks you have etc?	
R3	-Yes I work at a healthcare center organization in X as a medicine secretary. Here we all have the same responsibility. To meet with the patient and to write the documentation after the patient has had an appointment with the doctors. So we all have the same tasks to do within administration.	
AJA	Yes okey, and this is done digitally i guess?	
R3	Not all the time, sometimes we can't send everything digitally so then we use physical letters instead. Because it is not always that the journal systems are connected.	T
AJA	Okey.	
R3	But most of it is possible to do digitally.	
AJA	How does your organisation manage your data/information?	
R3	We do not save too much. Everything is sent for scanning if we do not already have the information on our computers. So we send the information to be scanned by putting it in a secrecy box and send it with internal mail. It then gets stored in an e-archive.	T, S
AJA	Okay, so that is to secure a certain level of security?	
R3	Yes, we do not want to send it with regular mail. Only when the mail is directly sent to the patient itself.	T
AJA	Yes okay, In what way would you say that your data is protected?	
R3	It is secured more centralized from the journalsystem	S
AJA	Yes I understand,but do you use any type of solutions or tools that is applied for protecting the data? For example do you write notes from a patient's appointment digitally?	
R3	No we can write notes on paper too, but we of course have secrecy on those papers. And we have a type of secrecy box in every room which we empty	T

	everyday and put in a real big secrecy box. So that there are never any loose papers with patient data.	
AJA	Have your organisation experienced any attempts or breaches/violations towards your data?	
R3	No not here, but in the region it might have happened.	
AJA	Okay, does your organization receive any notifications if there has been any attempts or data that has been put out to risk?	
R3	Yes our organization boss does, and in some cases, all our systems are shut down during the investigation to prevent any more data from being at risk. So then we can not have access to some parts. When they have located the risk and solved it, the systems are started again.	R
AJA	Yes I understand, are there any specific data that needs a bit more security than other data? Or is everything managed in the same way.	
R3	Data about persons with that is non public for security reasons, with no visible population registration address, is being handled in a more secure way, we can not write down full name or personal identification numbers so that it would be possible to track which person the data is about. But other than those cases, all data is being managed in the same secure way. Patient security is the most important in general.	SAS
AJA	Is it possible for you to work from home?	
R3	Yes it is, yes.	
AJA	Okay, do you use any specific tools when working from home?	
R3	Ah yes we have something that is called siths card. It is like an identification card. So you need that card to be able to log in.	T, C
AJA	Ah so do you have a card reader at home then?	
R3	Yes we have it on our keyboard or it's connected to our laptop.	T
AJA	Okay so you can't just log in to the system from any computer?	
R3	No, absolutely not. We need to have our special laptop from work. Where we have special softwares downloaded that requires that we log in with our siths cards.	T, C
AJA	Yes I understand, are there any specific work tasks that you can not do from home because of security?	
R3	No, not that I know of, maybe the doctors have some tasks but I don't know. But I think we can do most of the tasks from home as long as you have your card.	S

JB	Are there any data that you don't have access to from home?	
R3	Well as long as you have the software downloaded and your card, you will have access to all of the journal systems etc. If you don't have that software, you can still use your email.	A, C
AJA	Is that the same for every employee? Does all employees have the same access to the same data, or are there some data that only a specific type of employee has access to?	
R3	No, I think we all can access the same data.	
AJA	Do you have any specific policies for security?	
R3	Yes we have that clearly implemented and presented at our intranet from our Region, so that everyone can have access to it and read it. And if you work from home, there are clear guidelines for that too. For example that you should keep all data safe and not risk that anyone other than you or other employees can access or see the data when working from home. For example no family member should have the possibility to walk past your computer and read from it etc.	DP
AJA	No of course, are there policies specially created for work that is being made from home?	
R3	No, I think it is generally created, data security in general. And we also get educated in patient security, so for me this is common sense.	OE
AJA	Yes I understand, so maybe then there are some parts of the policies that are more important to be aware of and follow when working from home? Like the part that no family member should be able to access information by walking by.	DP
R3	Yes it is like that	
AJA	Yes, in what formats are the policies made?	
R3	They are written and uploaded with word documents on our intranet.	DP
AJA	Okay, are there also policies in physical paper form?	
R3	If you want to, you can print out the pdf but for me that is ISO educated, we rather not use papers since they update from time to time and we want to make sure that everyone has the absolute most recent version. And also, we all should know where we find these policies, everyone should know. And it shall be easily found.	DP
JB	But you talked a bit about ISO, but what are your policies based and grounded on? Is it based on for example GDPR or ISO etc.	

R3	ISO is something that I have with me from before but GDPR absolutely. So there we needed to change a lot and ensure that we do not use physical folders with patient records etc. And this with the scanning is also very good to keep it secure	L
JB	Yes you talked a bit about education also, how is that implemented?	
R3	That is being made when you are newly employed with an introduction and then you get updates all the time when changes are being made. As an employee you should be aware of new information on our intranet. And read there every day. We also have weekly news where we get updates from the region etc.	OE
AJA	Yes i see, have you ever felt like the available and active policies were not complete, or that it felt like something was missing?	
R3	There is always something that could be improved but I actually think that they are well written.	DP
AJA	Okay, do you ever have discussions or education about what the employees should do if there is a suspected data leakage?	
R3	No not really because we get our directions from higher up in hierarchy, from the IT section. We can not do much directly from the organization if the leakage is not coming directly from our physical workplace.	R
AJA	Okay so you wait for IT to give you guidance on how to act?	
R3	Yes exactly and hopefully they have been able to solve the issues before anything has happened.	
AJA	Yes I understand, but the secrecy boxes that you were talking about before, can anybody empty the boxes and put it in the main secrecy box, or is it a special employee that has that responsibility?	
R3	No we all try to help eachother out and empty them, but it is usually every employees own responsibility.	T
AJA	Is that something you write down somewhere? Like a documentation of when and who emptied the boxes.	
R3	No	T
AJA	Can every employee open and send the the documentations in the main secrecy box?	
R3	No I think it is SOS who's taking care of that, so it is really secure and not just anybody.	A
AJA	Okay so it is not just a random post organization?	

R3	No absolutely not, not even we here on the health care center have the password kode to the box so.	A
AJA	Okay, then it is well secured.	
R3	Yes, but I dont know if it is like this everywhere. When I worked at another healthcare center, things were different and we could access the key to the box.	
AJA	Ah okay, where in X did you work?	
R3	I did work at healthcare center X.	
AJA	Okay, interesting. So that was all the pre designed questions, is there something else that you noticed that we have missed out on?	
R3	No, but I think that all of our security is good and that we all have to take responsibility with our cards and laptops etc.	C
JB	Let's say for an example that you would lose your sith card, what would happen then?	
R3	Then you would need to call the support and make sure to deactivate your card directly. And the codes to cards etc it is not something that is accessible for others.	C, T
JB	What do you think could be done to improve the security?	
R3	I don't think that we can do anything more that what we already do here at organization, It is more of an IT thing to do.	
AJA	Would you think that it would be more secure to do everything digitally directly instead of using the boxes before scanning and put the data in a digital form?	
R3	You work in that way in X, but no. It can cause many issues, when new employees don't know how to do everything correctly something might be added to the wrong patient journal etc. This system is much more secure to do it centralized in the organization.	T
AJA	Okay, have you experienced that wrong things have been added to the wrong patients journal etc before?	
R3	Yes, absolutely, many times. By sloppy employees.	
AJA	Maybe there needed to be more education on how to correctly do that?	
R3	Yes but now, because we all got enough of education about that, but yes maybe they needed more education in patient security. Could be something. If you're an educated healthcare employee you have that from the beginning, but if you are a receptionist you get teached how to charge for appointments when	OE

	it really is much more than that. To take wrong price for an appointment is not the whole world but to add someones test result to the wrong patient is bad	
AJA	Yes especially in these covid-19 situation	
R3	Yes exactly	
AJA	Okay, so I think that we have gotten all the answers that we need, so thank you for all your time and your participation. We would like to send you the transcript if that is okay so that you can confirm that it is okay for us to use this.	
JB	Yes, thank you for you participation and good information	
R3	Yes that sound good, thank you	
AJA	Okay thank you, bye!	
R3	Yes thank you bye!	
JB	Bye!	

Appendix 4 – Interview 4

JB	Hi, I could start by introducing me and Amanda. We are both studying the master program in Informations system here at Lund University and are now writing our thesis about data security management. So we want to look at the more organizational parts rather than the completely technical, so policies etc. You will of course be anonymous and we will not use your name or anything. We will also send the transcript to you when it is done so you can confirm once more that it is okay for us to use that information.	
R4	Yes, that is perfect.	
AJA	Yes okey so could you give a brief description of your organization and your role at the organization and your task?	
R4	Yes, so I work at a healthcare center called X and we are connected to X. But we have primary health care agreements. So when it comes to information and data security we need to adapt both after X and the reigon. So for example all our computers and the technical solutions for that comes from X as firewalls etc.	L
AJA	Okey	
R4	So everyone here needs to complete a GDPR course when they start working here. And I am the Administrative manager. And GDPR came for some years ago, but we have let every new employee participate in an education course about GDPR that they have to pass. We also document who has passed the test so that we have control over that.	L, OE
AJA	Okey	
R4	And when GDPR came into force we needed to look over how we manage our patients. And we have 2 different contact contact options,one for 1177 and one for the email. So when patients use the email they email their full identification number which is not could because they are not allowed to do that. Then we have to answer them that they need to use 1177. And then we need to see how they respond since most of them are elderly people and do not have the same understanding of digital identification etc as younger people do. So sometimes they come in to the receptions or call instead. But otherwise we recommend them to use 1177.	T
AJA	Okay, so the GDPR course is something that you internally in the organisation is providing?	
R4	That is X who has implemented that as a mandatory part to complete when you are starting as an employee here and is connected to X.	OE

AJA	Okay. What different tools do you use to keep the data secure at your organization?	
R4	Yes that is a bit tricky, but we use a system called X which many regions are using. But we do not need to worry that much about that but if there are any papers that we need to save we save them securely or we put it in a secure box that the region is managing.	T
AJA	Okay	
AJA	Have you ever experienced any threats or data leakage? Where you had to follow specific instructions or guidelines etc.	
R4	Not really what I can think of right now	
AJA	I understand, let's say that it would occur a threat or issue, do you have a pre-structured plan or something of how your organizations should act and behave in that situation?	
R4	Yes we do have that, if that happens we need to report it to X and X directly. So when GDPR came into force we got more strict rules. There were laws before of course but GDPR made it more strict. So for me when I create an invoice I need to create it first to send it to the insurance organization etc and now I need to create a letter as a pdf file to add which patient it is connected to etc. So it were more secure for the patient but required more time.	R
AJA	Okay, but the plans or structure that you had to implement when there is a suspected data leakage for example, is something that the new employers get educated in?	
R4	Yes they do, it is actually my colleague who is managing that course and did it today. It is during an hour as a test, and the employer needs to retake the test until the employee passes the test	R, OE
AJA	Okay, If changes are made, would all the employers need to retake the test or? Or do they just get maybe a notification that new rules have been implemented.	
R4	I think that if there are many and big changes that have been made. Because we need to think that there are many employees at X and if all of them would need to retake the test that is during at least an hour it would be a very big expense, so we need to see what is necessary. But all needs to take part in all the basics. But for example when you are handling the checkout you need to retake a test for that every year, so it depends.	DP
AJA	Ah okay. Are there any specific data, or some data that need to be kept more secure than others?	
R4	Like it is encrypted?	

AJA	Yes like it is managed differently with more security, or is everything managed the same. Like booked appointments data, is that the same for documentation from an appointment.	
R4	Well I would say that it is all pretty much the same, it's the same for the system. But I can't recall that there should be any different	SAS
AJA	Okay, is it possible for you to work from home and complete tasks from home? are there any specific extra tools that you use for a security purpose in that case.	
R4	We get a remote login to our software that we use. Before you could just go through the program with a password, but now I need to have a card and a card reader and order a remote login	T, C
AJA	Ah okey, do all employees have access to all data?	
R4	From our system we can access different data, but I think that if you have access to the system then you have access to everything there. But I can not access exactly all the same data as doctors for example because they might need access to other journals and other records. So there is some differences	A, S
AJA	Okay so the access to the data can differ a bit depending on what role you have?	
R4	Yes and it is like we work with the system X and then you might have other systems that you connect to that system. The data is not implemented but can be accessed through the system that is connected.	S, A
AJA	Okay, are there some tasks that cannot be done from home because of security reasons?	
R4	I think that most of the tasks can be done from home.	
AJA	Okay so basically everything that you can do digitally, can be done from home as well?	DP
R4	Yes basically	
AJA	Okay, all the systems that you use, can you access them from any computer? Or do you need to use a specific laptop or computer?	
R4	No, I can access everything from my own computer	A
AJA	Okay so it is like as long as you have the card,	
R4	Yes I need to have the remote login and the card and card reader that we have got from the region. And also the sith card that I also use at work.	T, C
JB	Okay so you could use any computer that you like without any issues?	

R4	No, I work sometimes from my personal computer with the cards and everything, but yes sometimes I think that it does, as the firewall really holds this etc.	T, DP
AJA	Okay, do you have any specific policies of how to handle the data etc, for security of the data?	
R4	We do not have many physical papers, so everything is available and stored in the system. So all sensitive data is managed there, so any other data is not on paper. And we use id numbers for the tickets to be able to track backwards, and those we need to save for seven years.	DP, SAS
AJA	Ah okay	
R4	But we do not really have any other information about that there	
AJA	Okay but do you have any other guidelines for how you should behave or do your tasks? For example that you need to be sure that no one can see or access the data and information on your computer when you are working from home etc.	
R4	Well everyone needs to sign a secrecy contract	L
AJA	Ah okay so everything is written there of how you should handle the data and what to do and what not to do etc.	
R4	Yes	
AJA	Okay, so the “policies”, the format of them are digital, or are they directly found when you are a new employee?	
R4	Yes now it is changed so now you have to read it on the computer where you also sign the agreement	DP
AJA	Okay, but do these contract updates? For example if I were recruited 10 years ago, do I receive any notification of the updates.	
R4	I don't know if there have been any changes in the secrecy agreement but with GDPR many new things needed to be done, so at that point all the employees needed to do it. But I have not seen any updates on the secrecy agreement.	OE
AJA	Okay so instead of having written down policies you use mandatory courses and most are found also in the secrecy agreement of what to do and what not to do.	
R4	Yes	
AJA	Okay, have you ever felt like there have been some missing parts in your data security management or something like that?	

R4	From the secrecy perspective, healthcare uses encrypted fax boxes, so it is important for the receiver to have that as well, so we can decode it later etc. But I have experienced before that sometimes they have faxed non encrypted faxes without coding it, so sometimes the security does not work as it should and may not only depend on the organisation itself.	S, R
AJA	Okay, does that affect your work as well when you receive faxes like that?	
R4	Yes it does, because we need to do a deviation reporting regarding the failure.	
AJA	Okay who do you report that to?	
R4	We need to report it to the region and the other organizations that we are connected to. And after that they define the issue and analyze the risks etc.	R
JB	Okay you talked about the GDPR courses before, and that it sometimes causes some issues?	
R4	Maybe, but the ones we had now were not within our organization. So sometimes that does not really work in general.	R
AJA	Okay, data leakage, the issue itself, is that something that you include information about in the mandatory introductions or GDPR courses? And how you should behave.	
R4	The region is directing, but if the issue occurs at them, we can not do anything about it, but it affects us. But we are not allowed to even say hello to a patient that we see outside of the appointment because we can show that they even are patients at our organizations.	OE
AJA	Okay, Is there something that you feel like we have missed to ask about?	
R4	No I don't think so, but sometimes things can differ from healthcare center to healthcare center. But we need to check identification for every patient that comes here before we start the appointment, and it is a lot more to think about than before.	L, T
AJA	Okay	
JB	Yes I think that we got everything.	
R4	Yes, you could always email me if there is some more information that you want	
JB	Oh thank you, yes, we will also email you the transcripts from this intervju so that you can confirm it. Really thank you for you time, and hope you have a continued good week	
AJA	yes thank you very much for your time and participation	

R4	Your welcome, yes of course	
AJA	Thank you bye!	
JB	Bye!	
R4	Bye!	

Appendix 5 – Interview 5

Person		Code
JB	Hi, I could start by introducing me and Amanda. We are both studying the master program in Informations system here at Lund University and are now writing our thesis about data security management. So we want to look at the more organizational parts rather than the completely technical, so policies etc. You will of course be anonymous and we will not use your name or anything. We will also send the transcript to you when it is done so you can confirm once more that it is okay for us to use that information.	
R5	Yes that is okay.	
AJA	Okay, so could you give a short description of the organization that you work for? And what your role in the organization is and what your tasks are?	
R5	Yes, okay, I am the IT manager at X., Sweden's only large emergency hospital that is managed and run privately. One of the first hospitals to be incorporated under the auspices of the county council in the nineties and X took over or won the procurement and the hospital 99 and twenty hundred began to provide emergency care under private auspices. I am also a Data Protection Officer, partly because when you talk about privacy issues, you need a great deal of knowledge about how the organization works. And since I have worked at the hospital for so long overall and know the organization very well, it suits me well. In addition, my personality is regulated and I am well acquainted with the legislation that exists to conduct emergency care, not just the Data Protection Ordinance but health care legislation, data laws, economics, legislation and drug research and a few other things that are needed to be able to conduct.	
AJA	How does your organization handle data and information and so about patients?	
R5	We show them in the care flows where the exact amounts of information needed for why the patients are here, so they must arise as information for the patient to get the best quality you can get for the process that the patient is currently involved in and we store them in the care systems. applicable. It is partly the main journal system, so there can be more than one. These are the medical support systems that are required for the exact type of care that we provide, which of course are different and then we fix them in our system that is required here at the hospital.	S
AJA	Exactly, In what way would you say that the data is secured?	

R5	In terms of IT security, we have good protection. Our systems are designed according to very clear rules. We have very good physical protection and in addition we have chosen not to consolidate our data with others, which means that you are more protected if you have a domain that is much smaller. Which means that you are not as big a target, the type of cybersecurity that is starting to become quite common. We also have a couple of different storage systems, not just a system that keeps storage issues in order to reduce vulnerability.	T, S
AJA	Okay, what solutions or tools do you have to keep your data secure from an organizational standpoint?	
R5	So that all security is based on those who work with the systems have their own login to be who they are, to fill in their flex and when they come to work, they apply for vacation and check food lists, fill in APT minutes and so on. But when you are just administering systems, you have special tasks for them and it is also the case that it is done in very specific forms. So that there is an arrangement for staff who work with these technologies that are required to make the systems work at as real a level as at server, storage level, server and system level. Perhaps the most important issue for maintaining the accuracy of the information. It is that you have specified test routines and a careful process for what you are allowed to do with each system and that you connect the suppliers very closely to what you dare to do, because it creates corrupt information. Then we have external and internal firewalls. We encrypt information, so it is quite a common procedure to maintain high security.	T, S
AJA	Is there any special data that is handled in a slightly extra secure way?	
R5	All systems we have at the hospital start with a procedure of information classification and this information classification then says what level of security you end up at, how much of organization and handling we need for the system itself and for some systems it is quite low. If the food list becomes a bit corrupt and ends up going astray, it is not so heavenly dangerous and there is also other information that is not so heavenly important. These are schemes that do not require such a high level of security in the form of others taking part in it. This is precisely where the thing perhaps puts more order in that it must of course be safe. We need to know which are the correct version of routines that we work with. We work in 3 areas, it is security that is about the accuracy and availability of the information.	SAS, DP

	And then we work in the area of information security, i.e. the people who should have access to the right type of people who have the right access at the time and then we work with cyber Security, i.e. how to protect themselves from the risks of the outside world.	
AJA	Is it possible to work from home even if it is a certain specific data that requires a little higher security?	
R5	Yes, it is perfectly possible to work from home, of course. The most important information resources for any given occasion are those that arise in the mixture between the medical technology systems and the main medical record system. There are perhaps 15, 20 systems per patient and it is clear that that information is super important. But since both the information and the machines and systems are here and the weakest link here is the individual healthcare staff because the individual healthcare staff can influence the information contained in the systems that it is clean.	S, A
AJA	If people have a protected identity, is it handled differently then?	
R5	It is handled the same everywhere, you have a personal task where it is probably not possible to see who it is as an individual, but for healthcare it is the same identity, we do not care what it stands for task, only we know that it is the same whole the road. It doesn't really matter. I just need to know that it's the same all the way in that case. it's like any identifier, we healthcare and especially healthcare in X are extremely used to working with data where it is not clear who the person is. If you write from home, the information is encrypted on your way to the hospital.	SAS
AJA	When you work from home, do you then need something specific to log in to your systems, such as a card with a card reader?	
R5	all our staff always have a personal card. It is not possible to enter the care system otherwise. It is a legislation we have had since 2008. But of course always when you work at home, you should make sure that you do not invite the whole neighborhood or let the children play with the computers when you are logged in and so on. It is also used between servers as well. Yes, we send when you should have access to information via the national patient overview or when the Swedish Social Insurance Agency should have access to a medical certificate or something else. So it is used as a method for how we should check that the information is encrypted and protected.	T, S, C
AJA	And are there any specific policies that you follow when working from home?	

R5	Yes, we have policies and instructions for how to do when you are at home, but otherwise the same policy applies when you are at home or if you are here at work. Where you sit does not matter much We have an IT security policy. We have information security issues and policies, we have personal data policies and to them we have linked guidelines and then there are routines and instructions for how to behave.	DP,
AJA	What a good thing it is on your intranet so it becomes very clear. If they are updated or a new policy appears, do employees receive a notice then or is an email sent out that changes have been made?	
R5	It depends on what it is, if it affects the regular employee, the training is updated and you have to do your training again.	OE
AJA	Okay, so your goal or type is maybe undergraduate education when you start here?	
R5	You get training in information security, general information security and then you get training in the Data Protection Ordinance. You get training in the Patient Data Act and you get training in the Health Care legislation. The patient safety area overlooks quite a lot of information and is about how to deal with information. Otherwise there is a risk that you will lose your license. You must understand the laws and regulations that apply so that you do not risk stepping in the ditch. Among other things, we write what the duty of confidentiality entails and what part it has in health and medical care legislation.	OE, DP
JB	I do not know if we asked that question, but have you experienced any attempts or data breaches or the like?	
R5	Yes, we all have it and the most common ones come from Russia, a lot from Asia and a little from South America. Then it is mainly phishing that is most common.	R
JB	Do you have any special type of routines then for how things should happen?	
R5	Yes, but it is quite clearly regulated that if personal data has gone astray, then we report it to the privacy protection authority on their special form and then we inform the patients who have been involved and staff. That is, we have a system in care called deviation management, so everything that happens is not in line with the rules and routines we have. They have been reported as deviations and then we managers have to assess whether it is a care deviation or a sustainability deviation or safety deviation or information flow. And so we handle them like that and investigate them and deal with them in the way that we deem most appropriate. In other words. What's this big? Is there anything that needs to be improved	R, L

	or is there any damage that has occurred and how should we handle that damage in that case?	
AJA	Okay, do all new employees have access to the same data?	
R5	You don't really have that. It depends on why you are employed. So that depends on the role and mission and so you have access to the information you need.	A
AJA	So you do not have access to all data if you only have a role that will handle 10% of it, for example?	
R5	Yes, then when you provide care, you are one of the team, so depending on which assignment you can assign, you must have information so that you can perform the team's tasks. You have to deal with the information required for why you work here quite simply and of course there is a very big difference if you work as a HR or if you work as a nurse in a ward.	A
JB	Are your policies based on gdpr or something, for example?	
R5	Yes, but it is one of those where the one called data protection policy where it is understood is GDPR as well and a bit of a mix of the old personal data legislation intuition.	L
AJA	Okay, then we've got answers to all the questions we had planned to ask.	
R5	Oh perfect.	
AJA	Thank you very much for your time	
R5	Get in touch with me if you need additional information, so you do not have to keep on looking elsewhere.	
JB	Absolutely thank you very much. Have a nice day!	
AJA	Yes thank you very much. Bye!	
R5	Bye!	

Appendix 6 – Interview 6

Per-son		Code
JB	Hi and welcome! Thank you so much for participating!	
R6	Hi.	
JB	Before we start, I just want to ask if it is okay if I record the meeting?	
R6	Yes that is okay.	
JB	Okay, perfect, let us begin. I can start with introducing me and Amanda. We are two students at Lund University, studying a master's programme in Information Systems and are currently writing our thesis in Data Security Management in relation to Data Leakage, how healthcare centres manage their data, more specifically policies and organisational solutions rather than technical.	
R6	Okay.	
JB	So, that is a short introduction about us. Could you give a brief description of the organization that you are working at?	
R6	My name is … and I work as the head of the department / operations manager (verksamhetschef) at a healthcare centre in …. which is called …We have around 10 500 listed patients. We work with care choice assignments (vårdvalsuppdrag) that we receive from the region we belong to. So, even if we are a private health centre, we work in a similar manner to public healthcare centres with the same assignments (uppdrag) as them, in this region. We are a healthcare centre that works with traditional tasks, so there is nothing special that makes us stand out among other centres.	
JB	Okay, and what does your role include, what are your responsibilities?	
R6	I have the ultimate responsibility, for all staff, the financial parts, and the contact between management and employees located here. Since I do not have an educational background in healthcare, that you need to be in order to be the operations manager, I have a delegated responsibility as a medical	

	manager together with a doctor that I work closely with. Since we have a large number of employees here, I also have a person that is the head of the unit working closely with the people on the floor and a district nurse.	
JB	Okay, interesting! How does your organisation manage information/data?	
R6	We manage it according to the GDPR. We manage it locally, but also try to keep in on a central level, where the central level focuses on working its way out into the organisation. We also have specially appointed GDPR personnel with an overall responsibility concerning GDPR, which makes me confident that we manage GDPR in the proper way.	L,
JB	Okay. Are there any specific solutions that you apply for protecting the data, excluding the GDPR?	
R6	Firstly we have a record keeping system for all journals that security routines are composed around. Then, concerning the management of personal files and personal maps, we manage them by locking them, so that they are password protected. In terms of other concerns, most is located on a central level and forwarded to them, e.g employment concerns.	S, A
JB	Okay, is there any particular data that is in need of a greater protection or special policy/tool?	
R6	That would be all patient data, but also personal data concerning the employees of course. But mainly patient data.	T, S
JB	Yeah, of course. Are there possibilities for some employees to work from home?	
R6	Yes it is, especially now in covid-times, we had to make sure that it works to work from home. And working from home is highly connected to a great level of security. You need to have special log in possibilities, get access, so it is not possible to just place yourself in front of the computer. We also have siths cards, staff cards, so there is a bit of a procedure to access the computer and work from home.	OE, A, S, T, C
JB	Okay, and then you maybe provide computers to the employees?	
R6	Yes, absolutely, it must be the region's computer that the employees borrow, which are connected to a special computer ID and connected with the siths card. Then the employees can receive a security code sent to them via their phone or connect to a VPN connection.	OE, A
JB	Okay, then you also answered the following question. But are there any special policies to follow when you are working from home? Perhaps it is not possible to complete the exact activities that you were able to do at work from home?	

R6	What we mostly do from home are telephone operations, we have digital meetings without patients, or at least some of us are able to. Then if you have some documentation or journal related tasks to complete, it is also possible to do them from home. Even secretaries can complete tasks from home, for some hours. So, basically most of the activities are possible, however physical patient meetings are not able to be completed.	OE
JB	Okay. Are there any specific tasks that an employee is not available to do from home because of data security policies?	
R6	Yes, you cannot have a reception at home, no personal meetings. We can have digital meetings, as long as the patient is willing to do so, as it requires consent or approval to conduct such a meeting. We also encourage these kinds of meetings, considering the current conditions, so we have the patients wellness in mind, including the risk of spreading the virus.	DP
JB	Yes, of course. And how are your policies established?	
R6	They are based on patient security, the National Board of Health and Welfare's (Socialstyrelsen) routines and regulations.	DP
JB	And maybe the GDPR and other laws?	L
R6	Yes, absolutely, precisely.	
JB	Are the policies available in a paper format or digital for your employees to view and read?	DP
R6	They are available digitally, but we also have a so-called emergency folder in case of a power failure, and you need quick access to information. The policies are completely updated digitally. We do not update the physical folder daily, however, we try to update it as soon as possible.	DP
JB	Okay. Have you experienced any failure from a security policy?	
R6	Yes, that happens quite a lot. You are not supposed to exchange social security numbers over computers, and me and my staff never do that. However, it has occurred that we receive social security numbers sent over mail, both from private people but also other clinics. So, sometimes we need to remind others that it is not okay to send that via mail. If we need to exchange these types of information, we do it over our record keeping system that contains all journals and is available to everyone.	DP, R
JB	Okay. Have all employees the same access to all of the data or information? Or can it differ between employees?	
R6	No, it can differ between different employees. Some employees only have access to read. All my staff have the access to view the journal, however, not everyone has the same authority to make actions within the system. We also have a logging system that saves every action, regularly and	S, T, A

	irregularly, all the time over the year. This can be done with or without any suspicion, where a cluster sample is applied on all staff members at least once a year.	
JB	Okay, interesting. Are there any specific policies for a security purpose? Specific instructions?	
R6	There are regulations and routines to follow. We apply routines presented by the region, for one. For you to be able to access a patients' journal, you need to have a health related relation to that patient, it must be a special reason for you to access a journal. You cannot just view it because you felt like it in the moment. It must be some sort of health relation as a reason behind it.	DP, A
JB	Yeah, of course. We previously talked about working from home. Are there any special policies to follow when you are working from home? For instance, keeping data unavailable to family members and neighbors?	
R6	No, that is super strict. You have to place yourself in a secluded place that is considered safe and secure. And always close down or lock the computers once you leave it.	DP
JB	Yes, sounds reasonable. Have your organisation experienced any attempts or breaches/violations towards your data?	
R6	No, we have not. Our region has a pretty solid protection and shell, so it is not easy to invade our computers.	SAS
JB	Okay, and how do you work against the violations?	
R6	We have a security department within the region who is accessible if something would happen.	OE, R
JB	Okay, so they can provide instructions for how to act?	
R6	Yes, and then we must follow them accordingly. What can be done is to view it as a deviation or synergi matter, where you write down what has happened, while you also contact the head of security.	R
JB	Okay. What do you think can be improved within data security and keeping the data safe?	
R6	It would facilitate activities if all regions shared a joint computer system, but also deliver a feeling of stable care of data. I think that too many record keeping systems can be sensitive, and to create one for the entire country would be easier to keep track.	
JB	Yes, that sounds like an interesting idea. That was actually all our questions. Is there something you would like to add that could be interesting for us and our paper?	

R6	It would probably be to inform patients and people in societies to not send social security numbers or similar information via mails. Even today, with intruders trying to get older people to expose their digital bank id. So a continuous enlightenment of what to do and not, and also what authorities do and do not, to avoid intruders tricking them into doing stuff. More information and education to patients and individuals in the society.	
JB	Yes, that is really important. Okay, thank you again for participating. I will send you a PDF with our transcription so you can check if it is okay. Have a nice day, bye!	
R6	Bye!	

References

Abouelmehdi, K., Beni Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy, Journal of Big Data, vol. 5, no. 1, Available online: https://doi.org/10.1186/s40537-017-0110-7 [Accessed 4 December 2020]

Abouelmehdi, K., Beni-Hssanea, A., Khaloufi, H., & Saadib, M. (2017). Big data security and privacy in healthcare: A Review, Procedia Computer Science, vol. 113, pp. 73-80 Available online: https://doi.org/10.1016/j.procs.2017.08.292 [Accessed 1 March 2021]

Allen, M. (2017). The sage encyclopedia of communication research methods, SAGE Publications, vol. 4, Available online: https://dx.doi.org/10.4135/9781483381411.n373 [Accessed 3 April 2021]

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. Journal of Network and Computer Applications, vol. 62, pp. 137-152. Available online: https://doi.org/10.1016/j.jnca.2016.01.008 [Accessed 4 March 2021]

Appari, A., Johnson, E.M. (2010). Information security and privacy in healthcare: current state of research, International Journal of Internet and Enterprise Management, vol. 6, no. 4, pp. 279-314, Available online: https://dx.doi.org/10.1504/IJIEM.2010.035624 [Accessed 4 April 2021]

Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abs-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review, International Journal of Medical Informatics, vol 142, Available online: https://doi.org/10.1016/j.ijmedinf.2020.104246 [Accessed 3 April 2021]

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices, 2nd edn, [e-book] Global Text Project, Available online: http://scholarcommons.usf.edu/oa_textbooks/3 [Accessed 4 April 2021]

Bini, S. A., Schilling, P. L., Patel, S. P., Kalore, N. V., Ast, M. P., Maratt, J. D., Schuett, D. J., Lawrie, C. M., Chung, C. C., & Steele, G. D. (2020). Digital Orthopaedics: A Glimpse Into the Future in the Midst of a Pandemic. Journal of Arthroplasty, vol. 35, no. 7, pp. 68-73, Available online: https://doi.org/10.1016/j.arth.2020.04.048 [Accessed 12 March 2021]

Bryman, A. (2018). Samhällsvetenskapliga metoder. 3rd edn, Stockholm: Liber

Bryman, A., & Bell, E. (2011). Business Research Methods. 3rd edn, Oxford: Oxford University Press

Calabrese, B., & Cannataro, M. (2015). CLOUD COMPUTING IN HEALTHCARE AND BIOMEDICINE, Scalable Computing: Practice and Experience, vol 16, pp. 1-18, Available online: https://doi.org/10.12694/scpe.v16i1.1057 [Accessed 10 April 2021]

Chinnasamy P., Padmavathi S., Swathy R., & Rakesh S. (2021). Efficient Data Security Using Hybrid Cryptography on Cloud Computing, Inventive Communication and Computational Technologies, vol 145, pp. 537-547, Available online: https://doi.org/10.1007/978-981-15-7345-3_46 [Accessed 4 April 2021]

Chinnasamy, P., & Deepalakshmi, P. (2018). Design of Secure Storage for Health-care Cloud using Hybrid Cryptography, 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 1717-1720, Available online: https://doi.org/10.1109/ICICCT.2018.8473107 [Accessed 4 April 2021]

Dupont G., dos Santos D.R., Costante E., den Hartog J., Etalle S. (2020). A Matter of Life and Death: Analyzing the Security of Healthcare Networks, In Hölbl M., Rannenberg K., Welzer T. (eds) ICT Systems Security and Privacy Protection. SEC 2020. IFIP Advances in Information and Communication Technology, vol. 580, Available online: https://doi.org/10.1007/978-3-030-58201-2_24 [Accessed 4 April 2021]

Galetsia, P., Katsaliakia, K., & Kumarb, S. (2019). Values, challenges and future directions of big data analytics in healthcare: A systematic review, Social Science & Medicine, vol. 241, Available online: https://www.scienirect.com/science/article/pii/S0277953619305271 [Accessed 2 December 2020]

GDPR. (2021). General Data Protection Regulation (GDPR), Available online: https://gdpr.eu/tag/chapter-1/ [Accessed 2 April 2021]

Goldkuhl, G., 2012. Pragmatism vs interpretivism in qualitative information systems research. European journal of information systems, 21(2), pp.135-146. Available online: https://orsociety.tandfonline.com/doi/full/10.1057/ejis.2011.54#.X9MeHmhKg2w [Accessed 4 December 2020]

Gomes, R., & Lapao, L.V. (2008). The Adoption of IT Security Standards in a Healthcare Environment, Studies in Health Technology and Informatics, pp. 756-770, Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.490.3085&rep=rep1&type=pdf [Accessed 2 April 2021]

Hassan, M.K., El Desouky, A.I., Elghamrawy, S.M., & Sarhan, A.M. (2019). Big Data Challenges and Opportunities in Healthcare Informatics and Smart Hospitals, Security in Smart Cities: Models, Applications, and Challenges, pp. 3-26, Available online: https://link.springer.com/chapter/10.1007%2F978-3-030-01560-2_1 [Accessed 10 December 2020]

Hussein, A. (2021) Data Migration Need, Strategy, Challenges, Methodology, Categories, Risks, Uses with Cloud Computing, and Improvements in Its Using with Cloud Using Suggested Proposed Model (DMig 1). Journal of Information Security, vol. 12, pp. 79-103. Available online: https://doi.org/10.4236/jis.2021.121004 [Accessed 2 April 2021]

Islam, M.M., Razzaque, M.A., Hassan, M.M., Ismail W. N. & Song, B. (2017). Mobile Cloud-Based Big Healthcare Data Processing in Smart Cities, IEEE Access, vol. 5, pp. 11887-11899, Available online: https://ieeexplore.ieee.org/abstract/document/7933943 [Accessed 4 December 2020]

Kitchin, R. (2014). The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences, [e-book] London: SAGE Publications Ltd. Available at: http://www.doi.org/10.4135/9781473909472 [Accessed 4 December 2020]

Larrucea, X., Moffie, M., Asaf, S., & Santamaria, I. (2020). Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0, Computer Standards & Interfaces, vol. 69, Available online: https://www.sciencedirect.com/science/article/pii/S0920548919304544 [Accessed 2 April 2021]

Manmadhan N., Narayanan H., Poroor J., & Achuthan K. (2014) Design for Prevention of Intranet Information Leakage via Emails. In: Mauri J.L., Thampi S.M., Rawat D.B., & Jin D. (eds) Security in Computing and Communications. SSCC 2014. Communications in Computer and Information Science, vol. 467, Available online: https://doi.org/10.1007/978-3-662-44966-0_13 [Accessed 2 April 2021]

Martino L, Ahuja, S. (2010). Privacy policies of personal health records: an evaluation of their effectiveness in protecting patient information, Proceedings of the 1st ACM International Heath Informatics Symposium, pp. 191-200, Availlable online: https://dl.acm.org/doi/10.1145/1882992.1883020 [Accessed 10 April 2021]

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, vol. 108, pp. 57-68. Available online: https://www.sciencedirect.com/science/article/pii/S0167923618300368 [Accessed 12 March 2021]

Moen, K., & Middelthon, A.L. (2015). Qualitative Research Methods, in P. Laake, H.B. Benestad & B.R Olsen (eds), Research in Medical and Biological Sciences, Academic Press Available online: https://doi.org/10.1016/B978-0-12-799943-2.00010-0 [Accessed 13 March 2021]

Oates, B. K. (2006) Researching information systems and computing. London: SAGE

Offner, K.L., Sitnikova, E., Joiner, K., & McIntyre, C.R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intelligence and National Security, vol. 35 no.4, pp. 556-585. Available online: https://www.tandfonline.com/doi/pdf/10.1080/02684527.2020.1752459 [Accessed 15 April 2021]

Ohm, P. (2015). Sensitive Information, Southern California Law Review, vol. 88, no 5, pp. 1125-1196, Available online: https://heinonline-org.ludwig.lub.lu.se/HOL/Page?public=true&handle=hein.journals/scal88&div=39&start_page=1125&collection=usjournals&set_as_cursor=20&men_tab=srchresults [Accessed 15 April 2021]

Patton, M.Q. (2015). Qualitative Research & Evaluation Methods, 4th edn, Thousand Oaks: Sage Publications

Poyraz, O.I., Canan, M., McShane, M., Pinto, C. A., & Cotter, S. (2020). Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches, The Geneva Papers on Risk and Insurance - Issues and Practice, pp. 616-638 Available online: https://link.springer.com/content/pdf/10.1057/s41288-020-00185-4.pdf [Accessed 1 May 2021]

Shabtai, A., Elovici, Y., & Rokach, L. (2012). A survey of data leakage detection and prevention solutions. Springer Science & Business Media. Available online: https://link.springer.com/book/10.1007/978-1-4614-2053-8#reviews [Accessed 1 March 2021]

Shakil, K.A, Zareen, F.J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare in cloud, Journal of King Saud University - Computer and Information Sciences, vol 32, pp. 57-64, Available online: https://www.sciencedirect.com/science/article/pii/S1319157817301143 [Accessed 19 April 2021]

Sjödin, H., Johansson, A.F., Brännström, Å., Farooq, Z., Katre Kriit, H., Wilder-Smith, A., Åström, C., Thunberg, J., Söderquist, M., & Rocklöv, J. (2020). COVID-19 healthcare demand and mortality in Sweden in response to non-pharmaceutical mitigation and suppression scenarios, International Journal of Epidemiology, dyaa121, Available online: https://doi.org/10.1093/ije/dyaa121 [Accessed 4 December 2020]

Smys, S., Senjyu, T., & Lafata, P. (eds). (2019). International Conference on Computer Networks and Communication Technologies: ICCNCT 2018, Springer Nature. vol 18, Available online: https://link.springer.com/content/pdf/10.1007%2F978-981-10-8681-6.pdf [Accessed 1 March 2021]

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, vol. 36, no. 2, pp. 215-225. Available online: https://www.sciencedirect.com/science/article/pii/S0268401215001103 [Accessed 1 March 2021]

Stewart, H. & Jürjens, J. (2017). Information security management and the human aspect in organizations, Information and Computer Security, vol. 25, no. 5, pp. 494-534. https://doi.org/10.1108/ICS-07-2016-0054 [Accessed 12 March 2021]

St-Hilaire W.A. (2020). Digital Risk Governance Security Strategies for the Public and Private Sectors, Springer, Available online: https://link-springer-com.ludwig.lub.lu.se/book/10.1007%2F978-3-030-61386-0 [Accessed 1 March 2021]

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. Future Generation Computer Systems, vol. 98, pp. 660-671. Available online: https://doi.org/10.1016/j.future.2019.03.042 [Accessed 1 March 2021]

Tipton, H.F., & Krause, M. (2006). Information Security Management Handbook, [e-book], Boca Raton, FL: Taylor & Francis Group, Available at: Google Books: https://books.google.se/books?hl=sv&lr=&id=mBDNBQAAQBAJ&oi=fnd&pg=PP1&dq=healthcare+security+management&ots=6IUD8RJjPo&sig=iuJs1UWr1ITTOJKh6ZM2JHG3QrY&redir_esc=y#v=onepage&q=healthcare%20security%20management&f=false [Accessed 1 April 2021]

Van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations, Computers & Security, vol 97, Available online: https://doi.org/10.1016/j.cose.2020.101970 [Accessed 26 April 2021]

Van Velthoven, M.H., Cordon, C., & Challagalla,G. (2019). Digitization of healthcare organizations: The digital health landscape and information theory, International Journal of Medical Informatics, vol. 124, pp. 49-57, Available online: https://doi.org/10.1016/j.ijmedinf.2019.01.007 [Accessed 10 April 2021]

Vurukonda, N., & Rao, T. (2016). A Study on Data Storage Security Issues in Cloud Computing, Procedia Computer Science, vol 92, pp. 128-135, Available online: https://doi.org/10.1016/j.procs.2016.07.335 [Accessed 10 April 2021]

Wall, J. D., & Palvia, P. (2021). Understanding employees' information security identities: an interpretive narrative approach. Information Technology & People. Available online: https://doi.org/10.1108/ITP-04-2020-0197 [Accessed 26 April 2021]

Walsham, G., 2006. Doing interpretive research. European journal of information systems, vol. 15 no. 3, pp. 320-330. Available online: https://www.tandfonline.com/doi/pdf/10.1057/palgrave.ejis.3000589?casa_token=ZSFvI9Sil1MAAAAA:efKJ_gDwt30YqaZcxAuH9vvPxo9suM0PiahHwa490oOBLdX8CYU3neejXgSZ5ND1wOXBBijd5aUrw [Accessed 4 December 2020]

Warkentin, M., & Orgeron, C. (2020) Using the security triad to assess blockchain technology in public sector applications, International Journal of Information Management, vol. 52, Available online: https://doi.org/10.1016/j.ijinfomgt.2020.102090 [Accessed 10 April 2021]

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, vol. 17, pp. 4-19, Available online: https://doi.org/10.1108/09685220910944722 [Accessed 1 March 2021]

Wong, R. (2007). Data Protection Online: Alternative Approaches to Sensitive Data, Journal of International Commercial Law and Technology, vol. 2, no. 1, pp. 9-16, Available online: https://heinonline-org.ludwig.lub.lu.se/HOL/Page?public=true&handle=hein.journals/jcolate2&div=4&start_page=9&collection=journals&set_as_cursor=2&men_tab=srchresults [Accessed 10 April 2021]

Yeng, P., Yang, B., & Snekkenes, E. (2019). Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices, 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), pp. 397-404, Available online: https://doi.org/https://doi.org/10.1109/COMPSAC.2019.10239 [Accessed 10 April 2021]

Zhang, H., Li, J., Wen, B., Xun, Y., & Liu, J. (2018). Connecting Intelligent Things in Smart Hospitals Using NB-IoT, IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1550-1560, Available online: https://ieeexplore.ieee.org/doc [Accessed 10 April 2021]