The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A Case Study

Author: Catrin Przyrowski
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT,

The introduction of the GDPR, an updated data protection regulation for member countries of the EU, calls for changes in the management of private health information of healthcare providers. Due to the novelty of the GDPR, its effects have not been researched yet. A case study has been conducted at three different Dutch and German healthcare providers in order to analyse and compare the different effects the GDPR has on differently specialised and sized healthcare organisations. Under consideration of the Privacy Calculus, the functions of Information Systems, and other legal texts, the impacts of the GDPR have been analysed with regards to data management, disclosing behaviour, and healthcare quality. This study shows that healthcare organisations need to invest a lot of time and money in adapting their processes in compliance with the new law. However, the disclosing behaviour of patients does not seem to change. Healthcare quality suffers under the new law since data flow and communication between healthcare specialists are limited to a great extent. By applying these findings to a different knowledge domain, this study shows that also insurance companies are confronted with great restructurings and limitations in terms of targeted marketing and the profiling of prospective clients.

Graduation Committee members:
Dr. Fons Wijnhoven
Dr. Raymond Loohuis

Keywords

Privacy Calculus, Information Systems, GDPR, Data Protection, Healthcare Organisations, European Union

11th IBA Bachelor Thesis Conference, July 10th, 2018, Enschede, The Netherlands.

1. INTRODUCTION

Health institutions invest on average 6% of their budget in security while firms in the financial sector invest double the amount. Simultaneously, costs of data breaches are with an average of $380 per stolen record higher than in any other sector (Symantec, 2018a). Electronic health information is a rich target for cybercriminals. With the number of information systems healthcare institutions, such as hospitals, have in place, electronic health information about patients is being collected stored and shared on a massive scale. Privacy concerns may result in patients distrusting healthcare providers which could prevent them from seeking medical help in the worst case (Mackenzie, Mantay, McDonnell, Wei, & MacDonald, 2011). These data have been protected by the European Directive from 1995 until now. Within the last 20 years, technologies made a plunge forward and, with the world's digitisation, more and more cyber-attacks, data breaches, and mistrusting customers or in this case patients appeared (Finn & McMillan, 2016; Ponemon Institute, 2016). On the 25th of May 2018, the General Data Protection Regulation (GDPR) will be enforced EU-wide to replace the Data Protection Directive from 1995 (European Parliament, 1995). The GDPR is supposed to strengthen privacy rights, both on- and offline, to support individuals in controlling and managing their personal data, and to boost Europe's digital economy (Tikkinen-Piri, Rohunen, & Markkula, 2018). The new regulation was approved on the 14th of April 2016 by the EU Parliament to align regulations with the technical advances of the digital age. Organisations were given two years to adapt their systems and strategies to the new regulation. By ensuring more control by the data subject, the GDPR is going to limit existing practices health organisations use to offer adequate quality in their healthcare. To name a few examples, the GDPR limits the amount of data to be stored to a minimum and to only relevant data, gives the data subject the right to request portability or erasure of personal health records, and instructs data collecting firms to keep privacy and data protection in mind in every step along the processing of personal data (Tikkinen-Piri et al., 2018).

Due to the novelty of this regulation, there has not been much research on its consequences and effects. The GDPR will heavily influence the way data management has been done until now, however, the effects on the medical sector specifically have not really been taken into account. In order to gain insights into these influences, research will be done in the medical field by conducting a case study at three healthcare institutions in Germany and the Netherlands. The ultimate goal is to create an overview of the effects of the GDPR on data management to help other organisations, not only in the health sector but also in other sectors, with complying to the new EU regulation. The research question is formulated as follows:

What does the introduction of the GDPR mean for the management of patients' private data at healthcare institutions?

The case study will be performed at three different healthcare providers, differing in specialisation and size. Research thus has been conducted at ZiekenhuisGroep Twente (ZGT) in Hengelo, the Netherlands, IrisZorg Verslavingsbehandeling in Beekbergen, the Netherlands, and Clinic Geutingshof in Rhede, Germany.

In the Netherlands, there is an additional law defining the privacy rights of patients specifically enforced for the medical field: the "Wet op de geneeskundige behandelovereenkomst" (WGBO), or the "Medical Treatment Agreement Act". This regulation defines the patient's rights and duties before, during and after a treatment has been established between them and the healthcare provider (Lankhorst, Dahm, & Nederlands Koninkrijk, 2013). Following the regulation, the healthcare provider must only inform the patient him- or herself about the patient's condition as long as the provider does not need to be replaced or other experts need to be included in the treatment. Thus, a doctor is free to consult an expert on a different discipline without having to ask for the explicit consent of the patient.

The initial research is done in the medical field. However, it is crucial to have a look at other sectors and on their implications with the new European data protection regulation. Do the influences of the GDPR have similar effects on the data management of e.g. insurance companies? Are these effects less important or more severe? The WGBO will not be relevant to these fields of investigation.

2. THEORY

2.1 Data Management

2.1.1 Private Health Information

Personal Health Information (PHI) is defined as any personal data that is related to the physical or mental health of an individual (European Society, 2017). These include information about an individual's health status, provision of health care, or payment of health care. Such information is very sensitive and valuable - not only to the owner. Hoffman and Podgurski summarised multiple purposes for collecting PHI. Following the researches, PHI is being used for diverse purposes, including targeted marketing by insurers or drug companies, recruiting suitable candidates in the business world, and even attracting the best students to educational institutions (Hoffman & Podgurski, 2007).

2.1.2 Electronic Health Record Systems

Information systems (IS) play an important role in today's health sector. They collect, store, process and communicate patients' PHI in an efficient way (Fichman, Kohli, & Krishnan, 2011; Samy, Ahmad, & Ismail, 2009). If improperly applied, however, these systems can evoke the opposite: data leaks, individuals that do not trust healthcare providers with their health anymore (Mackenzie et al., 2011), or even such failures that lead to the death of a patient (Fichman et al., 2011).

Agarwal et al. found that Health Information Technologies (HIT) create a ground for new possibilities of care. Especially when it comes to long-term and preventive care, HIT integrate specialists from different backgrounds which can lead to higher productivity. Moreover, quality is being increased because of lower mortality rates, improved patient safety or higher vaccination rates. The use of such systems also comes with lower costs and higher revenues resulting from technical advances and digitisation (Agarwal, Gao, DesRoches, & Jha, 2010). Finchman et al. were led to similar findings in their research: Electronic Health Record Systems (EHRs) come with the benefits of reduced administrative costs, fewer medical errors, and the anonymity of the patients' personal data. Patient data are being transferred from one department to another within hospitals, or to external practitioners. Routinizing data collection procedures can minimise risk and facilitate the handling of life-death decisions. Entzeridou et al. surveyed a sample of individuals and physicians and came to the conclusion that EHRs improve healthcare quality through easier access to data, the continuity of the healthcare record, easier communication between specialists, and the availability of data for research purposes. Around 90% of the public believes that physicians should have full access to EHRs, and nurses, pharmacists, or other healthcare professional should have partial access. The trust in policymakers and pharmaceutical companies does not seem to be high, on the other hand, following the opinions of 60% of the public (Entzeridou, Markopoulou, & Mollaki, 2018). Mackenzie et al. focused on the nature of such failures and found the human error to be the most likely data breach. Resulting from this, the researchers formulated methods to prevent such breaches. Besides monitoring solutions, a code of conduct, strict personnel measures, and place procedures should be enforced to keep data leaks to a minimum (Mackenzie et al., 2011).

2.2 GDPR

The GDPR implements common rules for data protection in all European member states, updates and defines several basic rights of data subjects regarding control of and access to their personal data, and consequently aims at improving the economic development of the member states (European Society, 2017). The GDPR introduces new regulations on key concepts such as data portability, transparency, rectification and erasure, and the clarity of the use of personal data. Tikkinen-Piri et al. researched the GDPR's key implications for data-collecting organisations, so that those could prepare for the requirements and avoid sanctions. The researchers highlighted twelve main implications data-collecting firms will be confronted with: '*general provisions* (including anonymization, encryption, and pseudonymisation, the data minimisation principle, the right of withdrawal)', '*transparency*', '*information of and access to personal data*', '*rectification and erasure* (i.e. the right to be forgotten, the right to erasure, data portability)', '*the right to object and automated individual decision-making*', '*general obligations*', '*security of personal data*', '*data protection impact assessment*', '*data protection officer (DPO)'*, '*codes of conduct and rectification*', '*transfer of personal data to third countries or international organisations*', and '*remedies, liability and penalties*' (Tikkinen-Piri et al., 2018). The Society of Radiology contributed to this list with their main principles the GDPR brings along: '*Portability of Data*', '*Personal Data Breach*', '*Anonymisation*', '*Encryption*', '*Pseudonymisation*', and the '*Clarification of the data use'* (European Society, 2017).

The key principles relevant for this research are as follows:

Consent: Consent must be freely given. It should be specific, informed and unambiguous, and the data subject's consent should be a clear affirmative action.

Data Minimization: Organizations are not allowed to store data that is irrelevant to their service. Data processors and controllers are thus supposed to only use the minimum amount of data required for the functionality of their service. Data should also be kept for 'the shortest time possible', although this definition varies per situation.

Breach Notification: Data controllers must notify the supervisory authorities within 72 hours of being aware of a breach that the data breach has occurred.

Right to Access: Clients have the right to request a copy of their processed personal data and data controllers are required to provide this.

Right to Erasure: Clients have the right to request organizations to delete all their personal data. They also gain the right to request the organization to inform all other organizations that received this personal data from the original organisation of the deletion.

Right to Data Portability: If it is technically feasible, data subjects have the right to request the transfer of data from one data controller to another. The data controller is not allowed to hinder and must transfer this in a structured and machine-readable format.

Right to rectification: Data owners have the right to rectify wrong information and can have incomplete data completed.

These principles have been selected as they appear to have the biggest effect on the handling of data management and the functioning of the information systems at the researched healthcare institutions.

2.3 Privacy Calculus

Fichman et al. state that the transfer of PHI comes with a certain risk - a risk of misuse, breach, or loss. Patients are aware of this risk and might be accordingly hesitant when it comes to disclosing private information. Zhang et al. found that privacy concerns are negatively related to the intention to disclose information (Zhang et al., 2018). How individuals make privacy-related decisions can be best explained by the privacy calculus theory. The privacy calculus is a trade-off between perceived risks and perceived benefits (Knijnenburg et al., 2017; Rumbold & Pierscionek, 2017). This theory is regarded as the basis of all decision-making in terms of privacy issues. However, in the health sector, making decisions about PHI might not be as simple as it seems. Whether disclosing PHI or not often depends on the severity of the disease, the trust put in the respective healthcare provider or the individual's attitude. Knowing of cases of data breaches or misuse of patient data does not improve the patients' trust in EHRs and leads to higher hesitance and uncertainty on whether to disclose private information or not (Rahim, Ismail, & Samy, 2013). Less need for data transfer logically leads to a lower risk of data leaks and data misuse (Fichman et al., 2011). The effects the GDPR has on healthcare information systems can be measured by applying the privacy calculus theory on both, individuals and systems. Thus, the privacy calculus also represents a trade-off between the risks information systems take to function properly and provide service quality versus the benefits of their functioning. These both factors influence the healthcare quality that can be provided. On the same side, the disclosing behaviour plays a crucial role in this context, as it forms the basis for the functioning of the IS. Without any PHI, e.g. EHRs would not function or even exist. Without disclosing PHI, patients do not have the chance of a proper treatment according to their diseases.

The GDPR is about to limit a number of systems when it comes to e.g. data portability and storage. It is then the goal to look for alternative ways to not negatively affect the functioning of these systems and their provision of quality for the healthcare provider and its patients. Furthermore, patients should be encouraged to keep disclosing PHI for the sake of their health.

2.4 Practical Implications

The Netherlands relies on a general health and data protection law composed out of multiple directives. "The Medical Treatment Contracts Act [Wet geneeskundige behandelingsovereenkomst]" (WGBO) and the "Personal Data Protection Act [Wet bescherming persoonsgegevens]" (WBP) can be regarded as the dominant laws regulating data collection, processing, and sharing. In 2013, the "Proposal on Patient's Rights with regard to electronic data processing [Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens]" (Proposal Patient's Rights) has been introduced to give data subjects more rights when data is requested and exchanged electronically (European Commission, 2014). Following the

WGBO, Dutch healthcare providers are required to keep medical records for 15 years after their creation or longer if necessary for the treatment. The patient's consent is not required for this. Specific legal obligations, in terms of data destruction at the end of the archiving period, do not exist. Copies of the medical record are being provided to the data subject, and third parties, only after consent has been given. If the disclosure is necessary for further treatment, the patient's consent is not required prior to providing the data to third parties directly involved in the treatment (Lankhorst et al., 2013). The WBP contributes to the expiring European Directive 95/46/EC. It limits the processing of health data and requires healthcare providers to implement appropriate technical and organisational measures to protect and secure all patient data against any form of unlawful processing. The WBP points out that private patient data must only be collected and processed in an adequate, relevant and non-excessive manner. Thus, only the data necessary may be collected, stored, and exchanged. Explicit consent for such data collection and processing, however, is not required (European Commission, 2014). Lastly, the European Commission mentions the Proposal Patient's Rights which introduces the healthcare provider's obligation to only disclose patient details after asking for his or her explicit consent, the information disclosure of the patient's right in terms of data exchange, the patient's access to personal health data, and more. In agreement with the proposal, healthcare providers, who have access to a patient's medical records, only have permission to access these data as long as it is necessary for the treatment fulfilment. Healthcare providers may be held liable for professional errors. Errors of the EHR or connected to its use do not fall into this category and it is not specified who to hold liable for.

Germany relies on the "Federal Data Protection Act [Bundesdatenschutzgesetz]" (BDSG) when it comes to governing the handling of private data in electronic systems. The act first came into effect in 1978 and has been updated regularly since, with its latest amendment having become effective on the 25th of May 2018, conjoined with the GDPR. The BDSG acts jointly with the Data Protection Acts of each federal state and applies to the collecting, processing, and use of personal data (BDSG, 2018). The first principles are as follows:

Prohibition with reservation of permission: The collection, processing, and use of personal data are prohibited unless explicit consent has been given by the law or the person concerned.

The principle of immediacy: The personal data has to be collected directly from the person concerned.

The principle of data avoidance and data economy: Data should not be personally identifiable which can be achieved by the use of data anonymization or pseudo-anonymization.

The principle of transparency: If personal data is collected, the responsible party is obliged to inform the data subject of its identity and the purposes of collection, processing, and use.

The principle of earmarking: If data is permitted to be collected for a particular purpose, use of the data is restricted to this purpose.

Comparing the Dutch with the German laws shows that the Dutch laws are more differing from the GDPR than the German laws are. Thus, GDPR does not seem to be much of a change to German organisations since they always had to be compliant to a strict privacy law. This has also to do with the German history; the right of privacy is defined by the German Constitution and organisations always had to be very aware of and compliant with it.

3. METHODOLOGY

The focus of this research lies on the implications of the new General Data Protection Regulation (GDPR) on the data management of different healthcare providers. The research is of qualitative nature and was executed through the form of a case study. Besides the aim of gaining more insights into the effects the GDPR has on the healthcare sector in the Netherlands and Germany, the study identifies additional aspects relative to 'Quality of care'. Concerning the case study, the choice was made to conduct a multiple case embedded design so that some sublevels within each organisation could be analysed to receive data on the research objectives. Due to the novelty of the GDPR, the multiple case design has been chosen as it allows to compare different organisations and their adaptation to and thoughts about the new law (Gustafsson, 2017). Interviews were the primary source of evidence for this case study. The interviews have been held with a CIO at ZGT, a psychologist and head of social workers at IrisZorg, and the head of doctor's assistants at Clinic Geutingshof. Prior to these interviews, informed consent of the interviewees was asked to protect the participants' privacy and confidentiality. The interview questions were created by a joint effort between different authors and can be found in the Appendix. The interview questions were the same for all interviewees. The interviews took place on-site at ZGT in Hengelo, at IrisZorg in Beekbergen and at Clinic Geutingshof in Rhede and were communicated in English, Dutch, and German, respectively. The method of conducting interviews appeared to be the most suitable method for this qualitative research because of several reasons. First, doing research on legal texts and information systems calls for expertise and knowledge in those domains. By consulting experts at the three healthcare organisations we were assured of both. Second, it was expected to retrieve as much information as possible for analysing and answering the research question in the end. Third, interviews provide detailed information on the facts and limit the influence on interviewees by others. Face-to-face interviews come with the advantage of having the opportunity of analysing not only what is said, but also facial expressions and the body language of the interviewee. This minimises misunderstandings. Furthermore, interviews allow for more in-depth data collection and a comprehensive understanding of the facts. If responses are not clear enough, it is possible to probe for further explanations and clarification. Lastly, by researching the challenges the healthcare organisations are being confronted with by the introduction of the GDPR, this research method also offers the possibility of providing a problem-solving approach by highlighting possible inconsistencies with the regulation. Bias may have occurred due to e.g. language barriers or response bias (Yin, 2009). Credibility concerns internal validity and ensures that the study measures what it was intended to measure. In order to ensure credibility, an early familiarity was developed with the cultures of participating organisations. This was achieved by preliminary visits and conversations with contact persons at each organisation. All participants were aware of their right to withdraw from the case study. By this, we were more assured of truthful answers. Transferability, i.e. external validity, "is concerned with the extent to which the findings of one study can be applied to other situations" (Shenton, 2004). We were assured of that by conducting research at both Dutch and German healthcare providers, differing in size (large versus small) and specialisations (addictions versus general practitioners versus specialists). Furthermore, the differences in our interviewees developed diverse answers from different angles. Dependability, or reliability, is concerned with getting to the same research results if the same research, with the same participants and methods, was repeated. Ensuring reliability in qualitative studies is problematic, however, we tried to do so by clarifying the importance of the research to our participants and thus aiming at high trustworthiness (Golafshani, 2003). It may be the case that the same study would lead to different results if conducted later in time, owing to the possible familiarisation with the GDPR and more time available for interviews. This, however, was not in our control.

3.1 Data collection

For the case study interviews have been conducted in English, German, and Dutch since the organisations are located in Germany and the Netherlands and not every participant was fluent in English. To ensure validity, the interview questions were translated from English to German and Dutch. After the first contact with the participants was made, they all received an introduction to the topic and the interview questions, to familiarise with the research, via email. The interviews were constructed together with a fellow bachelor thesis circle member and conducted on-site by this fellow circle member and me. Each participant was asked independently to analyse the GDPR's effects on their job and the quality of healthcare by contrasting the organisation's privacy regulations before and after the introduction of the GDPR. After asking for the participant's consent, the interviews were recorded out of validity purposes. All interviews were conducted in June 2018. The interviews took 45 minutes on average.

4. RESULTS

4.1 Company Description

4.1.1 ZGT

ZiekenhuisGroep Twente (ZGT) employs more than 3,200 people on a full-time basis and another 4,000 people who do not work full-time. The hospital group treats around 860,000 patients on a yearly basis. Patients are being treated both in the hospital as well as outside. ZGT's network reaches from focus clinics like the ones in Hengelo and Almelo to collaborations with the University of Twente and general practitioners. The hospitals in Hengelo and Almelo have around 720 Information Systems in place. These IS sometimes overlap from discipline to discipline, e.g. surgery, urology, or oncology. Our interviewee, Ivo van der Kleijn, is the Chief Information Officer of the clinics. He is responsible for all data that are collected and stored. He oversees and manages the data, and is the contact person for any data related issue.

4.1.2 IrisZorg

IrisZorg is a Dutch organisation that has specialised in supporting individuals with struggles in their lives. The healthcare organisation is located in the Western part of the Netherlands with its centres in Apeldoorn, Beekbergen, and Nijmegen. The facility, we conducted our research at, employs around 90 people and is specialised on people suffering from homelessness, unemployment and gambling, drug or alcohol addictions. At IrisZorg Begeleiding Thuis Beekbergen patients are being admitted as in- and out-patients. The facility has 114 beds for in-patients. IrisZorg Beekbergen works in collaboration with a number of external organisations in the municipality of Apeldoorn, e.g. the police and childcare institutions. Our interviewees were Suzan van de Hel, who works as the head of social workers, and Ranjita Steinman, a treating psychologist. Suzan van de Hel’s duties cover the coaching of social workers, registering, planning and creation of care plans for patients. Ranjita Steinman is the first contact person for new patients. She creates treatment plans, overviews the actual treatments, and executes administrative work.

4.1.3 Clinic Geutingshof

The Clinic Geutingshof is a fusion of four general practitioners, specialised in sports medicine, palliative care, internal medicine, and psychotherapy. It is located in Rhede, Germany, and has a headcount of around 14 employees. The clinic is treating approximately 18.000 patients on a yearly basis. Our interviewee, Heike Hovestädt, works as the head of doctor’s assistants. She is mainly concerned with administrative tasks, but also mentors and advises new doctor’s assistants and overlooks the treatments in the clinic. The clinic does not engage in medical research.

4.2 Presentation of Interview Findings

4.2.1 ZGT

4.2.1.1 Effects on Data Management

Since the announcement of the new data protection regulation in 2016, ZGT adapted its processes and information systems in accordance with the new principles. IS did not need many adjustments as they were already compliant with the WBP on which the GDPR is based. At the ZGT, there are 723 information systems in place. Data are not being transferred through these systems, as all PHI is kept in the EHR. Other IS are e.g. Word, Excel, and PowerPoint. Generally, each department is responsible for their data management, but there are distinct limitations in place to control and protect the data. First, patient records can only be inspected by the medical department the patient registered with. If other departments need these data for medical purposes related to the patient’s treatment, the data needs to be requested. Every time such data has been requested electronically, these requests are being recorded to monitor the data flow. If the system detects strange data transfers between departments, these transfers are being stopped automatically. Furthermore, ZGT engages in a “Zero-Trust-Network”. Only trusted computers are allowed in the secured network. In case misuse has been observed, this behaviour is being followed by sanctions. Sanctions can either be a note in the employee’s form (yellow card) or dismissal (red card), depending on the severity of misdoing. Checks take place regularly to ensure the safety of PHI. Small data leaks happen on a daily basis, especially when it comes to sending letters; with an average of 1,000 letters that are being sent from the hospital to patients every day, some letters happen to appear in the wrong envelopes. Data leaks like this have to be reported to the CIO, AP, and patients. These leaks are usually minor, as the letters only cover e.g. appointment reminders: “If it’s a leak at all, it’s a small one” (I. van der Kleijn, personal communication, 2018). At the moment, the monetary, as well as human resources necessary to detect and minimise data breaches, are sufficient. However, an Information Security Director will be appointed to support the DPO in security and policy matters. ZGT collects all kinds of PHI, which stay in the EHR for at least 15 years - this is stated in the WBP. PHI about genetic diseases needs to be kept up to 100 years after the patient's death for research purposes. The hospital's research has not been much affected by the GDPR as privacy approved medical research procedures had been in place for around five years now Research data is either being anonymised or pseudonymised; ZGT will soon hire a Data Scientist to ensure making the right decisions for their research projects. All data are encrypted. PHI is only collected after the explicit consent was given by the respective patient. If consent is not given, the medical staff treats the patient as good as possible, however, data cannot be shared with other hospitals or general practitioners, which limits the quality of care. Sometimes, patients are not in the state of giving consent for their treatments, e.g. elderly people. In such cases, ZGT uses the "breaking-the-glass-principle". Around 4-5% of all treatments start with this principle. Then, an alarm in the goes off to notify the CIO of it.

4.2.1.2 Effects on Organisation

The greatest challenge, the organisation was facing, concerned the financing of the restructurings. A Data Protection Officer and two privacy managers have been appointed. Additionally, awareness about the new regulation needed to be increased among the board of directors, and (information security and privacy) policies and processes needed to be adapted. In order to inform the hospitals' patients of the changes in data protection, new leaflets and banners have been designed, printed and distributed. Also, the web presence was updated to make it more transparent and easier to follow. Data protection experts, as well as insurance companies from the outside, conducted several audits; these, in any case, are conducted every year to ensure that e.g. authorisation matrixes are kept up-to-date. These preparations led to a high investment in terms of money and time. Approximately 30,000€ and 60,000€ in 2016 and 2017, respectively, were spent on the adaptation to comply to the GDPR, whereat most of these investments were due to the newly employed DPO. Board members and staff at ZGT received awareness training and a presentation about the changes the GDPR brings along, but end users, e.g. secretaries, have a scheduled training with an e-learning course coming up in the summer months. Doctors and medical staff received individual training, by explaining the changes and the expectations of them in face-to-face meetings. All employees, upon entering the healthcare facility, receive training about privacy matters.

4.2.1.3 Effects on Quality of Healthcare

Patients seem to become more privacy aware, however, our interviewee does not think that this is necessarily connected to the GDPR. Often, ZGT's doctors have conversations about privacy issues with their patients. But following our interviewee: "A better-informed patient is beneficial, as we can treat them better” (I. van der Kleijn, personal communication, 2018). Some patients have made use of their “Right to Access” of their personal data files, which faces the DPO with much additional work in putting together an overview of all data that is being stored about that specific patient. Patients making us of their “Right to Data Portability” have the data being transferred in a PDF format to the respective healthcare provider. The GDPR’s effects on health care generally are regarded as problematic. Specialists, especially external ones, cannot see laboratory results anymore but the ones they requested themselves. Limiting the data flow results in treatment delays, which are sometimes matters of life and death. A year ago, an infant died at the hospital because of test results the hospital did not have to its hand on time. Many healthcare providers from ZGT's network and the CIO of ZGT itself believe that the GDPR exaggerates in terms of privacy. Smaller organisations cannot deal with the regulations and fence off everything, e.g. the exchange of laboratory data. ZGT feels well prepared, but still needs time to adapt to the changes. "From the user point of view, it is just something that limits your job. [...] There are always trade-offs. If you want true privacy, we cannot take care of you” (I. van der Kleijn, personal communication, 2018).

4.2.2 IrisZorg

4.2.2.1 Effects on Data Management

In the healthcare sector, data leaks are always a big problem, due to the sensitivity and value of said data. Especially for IrisZorg, patients have to place their trust in the organisation and data leaks would create an irrecoverable breach of trust. Patients who lost their trust in their practitioner will most likely move to a different healthcare provider. The organisation itself does encrypt PHI in emails or phone calls; patient numbers are being used for in- and outside communications, however, in replies to these emails, actual patient names do appear. These are strictly speaking data leaks that happen on a day-to-day basis. The municipality of Apeldoorn makes use of the programme “CryptShare” to encrypt PHI in emails. However, even this does not prevent everyone from spilling a patient’s name via email. When communicating with the municipality, IrisZorg has to hope for Apeldoorn having the patient number in their systems so that the communication flow is easier and the least amount of time is wasted for clarifying which patient is being talked about. The clinic is making use of the EHR “User” and Excel to manage PHI, while communication amongst staff is being done via email, phone, or face-to-face. The EHR is lacking some instalments, such as pop-ups if a patient’s form of consent is missing. Moreover, there are many issues in terms of “who can see what”; some social workers spend day and night with their patients on a voluntary basis and still do not have access to their files. They cannot read or report on their patients' progress in the EHR while they are the ones who work mostly on the patients' treatments. The GDPR emphasized the importance of paying heed to whether consent was retrieved and of clarifying the purpose of what the clinic's patients are really giving consent to. Although, some processes go slower, such as the communication between different healthcare providers, the GDPR ensures that PHI is protected accordingly to their high value, as they are "the most privacy-sensitive information for an individual" (S. van de Hel, personal communication, 2018). IrisZorg's employees sign non-disclosure agreements and Codes of Conduct upon entering the job. The e-learning course is expected to be done by each staff member so that the employees' awareness of privacy issues is being raised. One of our interviewees had not completed the course until the day of our interview, which took place after their deadline. If data leaks happen, these have to be reported. A special control and monitoring of staff members in connection with privacy matters are not installed.

4.2.2.2 Effects on Organisation

The rehabilitation clinic in Beekbergen has already been very concerned with privacy matters before the announcement of the GDPR in 2016. However, the new data regulation made the staff at the clinic become more aware of what privacy really means and what kinds of data are being shared. In January 2018, a Data Protection Officer has been appointed to run an audit at the clinic. For most employees, this appointment of a DPO was the first sign of the new law which has not been much of a deal before. An e-learning course had to be completed before 1st June 2018 by all staff members. This course was explicitly for Mental Health Care organisations and covered topics such as “privacy regulations on the work floor”, “privacy between colleagues”, “phishing”, or one’s own privacy; it was not related to the GDPR explicitly. A day before the introduction of the GDPR, on the 24th of May 2018, the municipality of Apeldoorn invited all healthcare institutions of the municipality for an informational event about the GDPR and how it works electronically. Adapting to the GDPR is regarded to be easier for larger organisations due to the resources available to appoint external DPOs and carry out audits. But the head of social workers at IrisZorg still expresses her mixed feelings about their own preparation for the GDPR as follows:” I think we are still going to run into a lot of practical problems, especially when we have to share data internally as well as to external sources. Ideally, you’d have a system that assists in being clean, right now we are reliant on the thoughtfulness of us employees" (S. van de Hel, personal communication, 2018).

4.2.2.3 Effects on Quality of Healthcare

The individual disclosing behaviour of patients does not seem to be affected by the GDPR, rather by patients individually. There is a case at the clinic where a patient is under treatment in another clinic as well. He does not want all practitioners to be involved in his treatment and communicating about him as a patient. Thus, this limits the treatment immensely since explicit consent needs to be given to every practitioner individually which slows down and hampers the treatment process. At the same time, such processes are being handled more attentively and thoroughly as more time is spent on optimising the patients' treatment and the cooperation between different practitioners. Patients who refuse to disclose their private data will not be treated by the organisation as mutual trust is of high importance in this healthcare domain. Requests for deleting patient records happen very rarely. If a patient requested for his records to be deleted, but relapsed after some time, the job performance of psychologists would not be very affected. The previous records have been deleted but it does not matter as it is always the current disease that is being treated. Whether the GDPR is believed to raise the quality of care or not is a question that employees at the clinic are not sure about. On the one hand, some think that the new law makes the processes more bureaucratic and leads to inefficiency which is on equal terms as lower quality; on the other hand, some are convinced that stricter rules and more attention lead to higher-quality care. The disclosing behaviour, however, stays a crucial factor in connection to the quality of care as best care can only be provided when the patient is willing and cooperative.

4.2.3 Clinic Geutingshof

4.2.3.1 Effects on Data Management

Patient data, i.e. everything that is relevant to the patients' treatments, is stored in an EHR but also in paper records which the doctors use for every appointment with a patient. These paper records used to be placed in the hallway in front of the doctors' surgery rooms, however, now this will not be possible anymore. The paper records will be given to each doctor individually ahead of the appointments. Old patient records, that were not relevant anymore had to be deleted, which took up the most time, following our interviewee. The EHR did not need any adjustments to the new standards; the communication methods however did. Communication is mainly done via email or phone calls. Instead of using full patient names, as it has always been done, the employees will now use patients' initials and patient numbers. Data leaks have never happened and employees are not really being monitored. If a wrong behaviour catches someone's eye, they will talk about it and remind and help each other. Besides that, everyone knows how to act when it comes to privacy issues, as each employee has signed the Code of Conduct upon employment. In order to get access to patient data, employees have to log in to the computer and the EHR.

4.2.3.2 Effects on Organisation

The preparations for the new law started three months ago, by appointing a data protection officer who conducted an audit at the clinic. Data privacy had always been of high importance before, so the new regulation was no big deal for the team, who received advanced training hours and informational texts about the GDPR.

4.2.3.3 Effects on Quality of Healthcare

The patients' reactions towards the new law were mainly curiosity. Some patients asked about the changes and what it would mean for them but did not refuse to sign the updated consent forms given to them. In our interviewee's eyes, they do not care about privacy matters as long as no data leak happens, and their diseases or discomforts are being treated. Concerning benefits, the GDPR brings along she said the following: "Everyone is being more careful and more attentive now. That's positive. At the same time, it's a bit annoying because we always need to double check whether we can exchange data with the hospital or not. It's time-consuming" (H. Hovestädt, personal communication, 2018). All in all, our interviewee feels optimistic about the clinic's compliance with the GDPR: "It needs time to adapt to the new processes. We have been working in a specific way for over ten years, and this cannot be changed within a day now. [...] I do not think that we have to worry. We are very concerned with privacy" (H. Hovestädt, personal communication, 2018).

5. DISCUSSION AND CONCLUSION

5.1 Information Systems and Data Management

Following Fichman et al. and Agarwal et al., EHRs are supposed to facilitate data flow between different healthcare institutions and integrate specialists from different backgrounds and organisations. Due to the GDPR now, patients have to give full consent to each specialist involved in the treatment. If a single doctor is denied the access to PHI, the whole care chain is affected. The data flow is being hindered by the new regulation, and healthcare organisations react differently. Smaller organisations are scared of failure to comply, so they "fence off" their outgoing data flows and e.g. stop the exchange of laboratory data with other healthcare providers. The quality that such facilities can offer is thus affected immensely. The worst example was given by ZGT, where an infant died by cause of laboratory results that could not have been provided. Therefore, it is getting back to the consequences of improperly applied EHRs, which Fichman et al. mentioned, which can lead to death. However, it is not basically that EHRs are being improperly applied, it is rather that EHRs do not work perfectly together with the GDPR right now. The request for getting a GDPR-conform system to share PHI, internally and externally, has been expressed. Such a system would e.g. automatically file requests for patient files or laboratory results, and handle the bureaucratic paperwork at the same time.

Data, at all facilities we conducted our research at, is being encrypted when being shared with other professionals. While Clinic Geutingshof and IrisZorg stick to a minimum by only using initials and patient numbers, ZGT engages in anonymisation and pseudonymisation to protect PHI. Furthermore, the IS to share data are protected by firewalls and individual login accounts at all three facilities. But still, some data leaks do happen from time to time. How are data leaks being defined? What actually is a data leak? For some of our respondents, this question was not easy to answer. Looking at the open-door policy IrisZorg was engaging in, this would have been multiple data leaks in the last years, accordingly to the regulations the GDPR notes. However, no file has ever been lost or looked at by people who were not authorised to do so. Nothing had ever happened and no file was accessed by unauthorised individuals. So, how to measure a data leak? Does it already start with open office doors, that, however, lead to no data leaking the organisation? Generally, all data leaks that happened at our case institutions, happened because of human errors. This proves Mackenzie et al.'s findings on the human error being the most likely data breach. These leaks are trying to be kept to a minimum by codes of conduct, and staff training. Monitoring only takes place at ZGT.

Generally, no IS at the researched institutions had to be highly restructured. The systems were complying to laws respective to the countries. However, other adaptations, e.g. external audits, appointing privacy managers and DPOs, and assessments by insurance companies led to high investments. Our contact persons did not see the absolute relevance of these investments, as security has always been of highest importance and no severe incidents had occurred. Besides being more consuming monetary wise, the GDPR is also more time-consuming. More consent forms call for more administrative work, as well as audits and patient requests (e.g. data portability or deletion of records). Whether this all leads to a higher efficiency is doubted by some interviewees.

5.2 Privacy Calculus

5.2.1 Influences on the Organisation

For all of the interviewed healthcare organisations, the safety of PHI is and has always been of high importance. Explicit consent is always asked for before PHI are being collected and treatments start. However, in some cases, patients are not able to give their consent, e.g. elderly people in severe health statuses. Sometimes children forget about applying for guardianship for their parents and are not in the position to give consent to disclose their parents' data in case of emergencies. In such situations, healthcare providers have to make a trade-off and “break the glass”. Breaking-the-glass refers to a person, or organisation, gaining access to e.g. PHI, although this person has no access privileges. From a legal perspective, this behaviour is wrong. From a medical, and ethical perspective, the duty of healthcare providers is to take care of the people's health, no matter what. ZGT argues that they "rather explain why data has been transferred without consent, than explaining why someone had died" (I. van der Kleijn, personal communication, 2018). Principles and regulations on "Breaking-the-glass" activities are needed and wanted by healthcare organisations. IS should be adapted to such principles so that the paperwork afterwards can be facilitated.

Generally, healthcare institutions always decide upon the best interests of the patients. Patients who do not want to disclose PHI have to accept that they cannot be treated by the specialists. Disclosing PHI is a profound origin of quality of care. The more is disclosed, the more a healthcare provider knows about this patient, which will result in the best treatment possible.

5.2.2 Influences on Patients

The influences GDPR has on patients and their disclosing behaviour does not appear to have changed that much. Patients entering a healthcare organisation usually come with a medical issue they want to be solved. Most of them do not give too many thoughts about what consent they are giving away to whom as long as they will get the treatment to be healthy again. Thus, signing consent forms is in their eyes in most cases just a bureaucratic measure. Often, patients do not even fully read what they are signing. Blind trust is given to the healthcare providers; if this trust was destroyed, the patient would move on to a different provider. However, this is not as easy in the rehabilitation sector as it is with e.g. hospitals or general practitioners. Patients in rehabilitation clinics are much more cautious and often ashamed of their circumstances. Thus, especially for rehabilitation clinics, like IrisZorg, building up trust and creating a familiar atmosphere is inevitable. Open-door policies have been the standard to build up this trusting atmosphere, however, under the GDPR, this behaviour can now be seen as data leaks and is to be disestablished. What effects would this then have on the treatment of e.g. drug or alcohol addicts? These patients could feel excluded and left alone, which could endanger the treatment process. A study conducted by Schneeberger et al. found that open wards in psychiatric treatment facilities have a positive effect on the aggression behaviour of patients (Schneeberger et al., 2017). This could be the same case for addicts or generally the patients at IrisZorg. Moving from closed-doors to open-doors will result in differences in the way patient treatments are being carried out.

5.3 Comparison of the Organisations

The healthcare facilities, research has been conducted at, differ in specialisation and size. Thus, each facility handled the introduction of the GDPR differently. The results of the comparison have been summarised in Table 1.

Table 1: Theoretical comparison of organisations

Theoretical comparison of organisations						
Organisations	**Start of preparations**	**Influence of GDPR on quality of care**	**Changes in disclosing behaviour** (Knijnenburg et al., 2017; Rumbold & Pierscionek, 2017)	**Appointment of DPO** (Tikkinen-Piri et al. 2018)	**Penalties of privacy breaches** (Tikkinen-Piri et al., 2018)	**Influences on Information Systems** (Fichman et al, 2011; Samy et al., 2009; Entzeridou et al., 2018)
ZGT	Early 2016, when GDPR was announced	Large negative influence, i.e. in collaboration with external organisations.	Patient talked with doctors and CIO. Some patient denied giving consent.	Appointed	Yellow and red card system.	Minor changes in the IS. Systems were already compliant.
IrisZorg	Spring 2018	Small, negative influence. Time-consuming and annoying.	Nothing changed.	Appointed	Not aware.	Nothing notable, already very privacy-sensitive before GDPR.
Clinic Geutingshof	April 2018	No significant change.	Patients asked questions, nothing changed.	Appointed	Not aware.	No changes in the IS.

While at ZGT preparations started right after the announcement in 2016, IrisZorg and Clinic Geutingshof did not start preparing for a couple of months before the law came into effect. Since ZGT is the biggest facility of all three (based on global headcount and the average number of patients treated every year), it also had more resources for restructurings than the other two facilities did. More money was available as well as human resources for consulting and supporting purposes. The interviewees also think that adapting to the new regulation is generally easier for larger organisations than it is for smaller ones, due to the resources and possibilities available. This approach could also be noticed during the interviews: many questions could not be answered by our interviewees at IrisZorg and Clinic Geutingshof. Striking was, however, that both IrisZorg and ZGT did not pay urgent attention to educate the end users in the organisations (i.e. administrative personnel, secretaries…) on the changes the GDPR brings along. At IrisZorg, e-learning courses were supposed to be completed by June 1st, 2018, however, were not by some employees. At ZGT, e-learning courses will not be broadcast until the late summer months of 2018, when the GDPR has been in effect for more than three months. All three healthcare facilities regard the new law as time-consuming and inefficient. Time is precious in the health sector; spending more of it on administrative tasks than on the patients' well-being can result in a powerful decrease in the quality of care. All interviewees did not notice a big difference in the patients' attitude towards disclosing PHI. While at Clinic Geutingshof patients asked some questions out of curiosity, ZGT had three patients asking for a copy or transfer of their data. But generally, patients do not seem to be more hesitant in disclosing their PHI now. All organisations need time to adjust to the changes and to adapt their long-established procedures to the GDPR. All healthcare organisations appointed a Data Protection Officer to conduct audits and change according to the new law. Privacy breaches (or data leaks) are only being sanctioned at ZGT, which is assumed to depend on the size of the hospital group. At smaller facilities, employees know each other and keep an eye on their colleagues' behaviour. At hospitals like ZGT, you need official measures and strict procedures to ensure smooth workflows and that data privacy is being maintained. All three organisations did not need to adapt their Information Systems to a great extent sine they complied to the national laws before, which are quite similar to the GDPR.

5.4 Ambiguous Law Texts

Germany and the Netherlands do not only have to comply with the GDPR but also with country- and state-specific privacy regulations. These regulations sometimes contradict the GDPR, e.g. when it comes to data storage. Following the GDPR, organisations are obliged to delete personal data as soon as they are not needed anymore; thus, data is supposed to be stored for the shortest amount of time possible. The WGBO in the Netherlands, however, states that healthcare organisations are to keep PHI for a minimum of 15 years. If the data concerns genetic diseases, these data have to be stored for 100 years after the data subject's death. A similar case concerns the patient consent in the collection and sharing of PHI with third parties. Following the WGBO and WBP, explicit consent does not need to be given. The GDPR, on the other hand, dictates the opposite. In such cases, organisations have to work out which law stands above the other law in order to continue working lawfully. Another critical point in the law texts concerns data leaks and their definition. Are open office doors already data leaks or does data actually have to leak to count as a breach? The CIO from ZGT also did not regard sending appointment reminders to wrong patients as a data leak. So, where do data leaks need to be classified?

6. ADAPTATION TO OTHER KNOWLEDGE DOMAINS

What does the introduction of the GDPR mean for other sectors but the healthcare sector? This question will be answered by looking at insurance companies. Insurance companies collect and store great amounts of private data, including PHI. These data are needed for e.g. targeted marketing and profiling. One could actually say that insurance companies' most valuable asset is private customer data. The GDPR is limiting insurance companies' day-to-day businesses now by restricting the types of data that are stored, increasing the data subjects' power in controlling their own data, and threatening with high sanctions in case of failure to comply with the regulations. A survey conducted by KPMG in the UK shows that less than 50% of the insurance companies interviewed feel prepared for cyber-attacks, i.e. data leaks (KPMG, 2017). Insurance companies keep their clients' data for as long as possible in order to maximise the potential use of that data. Such use can be targeted marketing, client profiling, fraud detection or favourable client identification. Now that people can request their data to be deleted, insurance companies will need to provide clear reasons for why specific data is being kept. Thus, data for ancillary purposes, such as targeted marketing, is hard to keep but also to collect in the first place, since only data that is needed for insurance purposes is supposed to be collected and stored. Data that has been received by third parties need to be reviewed and amended to ensure that explicit consent by the data subject has been granted (DAC Beachcroft, 2018). The new regulation on data access will presumably lead to more data access request in the long run. These requests need to be handled which consumes time and money input. Resources like time and money are also being spent on staff training and system and control reviews, i.e. audits, to ensure the insurers' compliance with the regulation. Cybersecurity Ventures notices that the demand for cyber insurance options is rising (Mello, 2017) - not only with individuals. Insurance companies themselves are looking for ways to protect themselves against the increasing cybercrime to not having to pay the penalties outlaid by the European Union in case of actual data leaks (Symantec, 2018b). All in all, insurers have to invest just as many resources in complying with the GDPR as healthcare providers. Due to the sensitivity of private data, organisations from both sectors deal with on a day-to-day basis, the risks of unauthorised data accesses or negligence of employees, i.e. data leaks, are incredibly high. Thus, measures have to be taken to ensure the security of such data. Measures like additional privacy managers, audits, or insurances against cybercrime, are expensive and call for more human resources, however, they are inevitable. The insurers' biggest difficulty will be to become more transparent and show which data is being used for what purposes. Profiling and targeted marketing make up a great deal of the insurers' day-to-day business, however, the GDPR places limitations on both in order to only use data that are needed for the insurance purpose. Screening for and attracting new clients might hence become much more difficult. INCE & Co. (2018) created a fact sheet for insurance companies on how to prepare for the GDPR. This sheet summarises the actions to take very well and presents a good help for organisations in this sector.

7. RESEARCH LIMITATIONS AND FUTURE RESEARCH

Owing to the small sample size, it is hard to generalize the findings of this study. The research is based on three different healthcare organisations that allowed for one to three interviews at each facility. If the number of interviewed people had been higher and more diverse in terms of function and expertise, the findings could have been different. We would have liked to conduct an interview with a DPO, however, because of the bad timing, no DPO of the case study participants could schedule a meeting with us. Furthermore, due to the diverse professions of our interviewees, some interview questions could not have been answered. Conducting the interviews at both German and Dutch facilities allowed for a nice comparison between the countries, however, organisations in other countries might have even other opinions on the topic which were not included in this study. Considering the research method, language barriers might have led to misunderstandings or interviewees not being able to express what they really wanted to express. Although, this was tried to be kept to a minimum by conducting the interviews in English, German, and Dutch. Besides, interviewees might not have clarified specific topics to non-professionals like us, as they took the understanding or arguments for granted and did not realize the importance of mentioning them. Lastly, time was a big limitation as well. The total time available for this research summed up to ten weeks, however, due to the simultaneous introduction of the GDPR within this time period, it was difficult to get interview appointments at the three facilities. If the time had not been that short, it would have been possible to conduct more interviews at the facilities. To measure the effects of the GDPR on healthcare organisations, even more, qualitative research on the long-term effects of said law appears to be a good possibility. Our interviewees often mentioned that the effects are not too powerful at this point in time, but it would be interesting to investigate how that changes after two or five years under the new law. Looking at the future, the Netherlands are tightening their laws on data privacy to close any gaps that might still exist. A new law on the exchange of digital data will be released in 2020. The “Generieke Digitale Infrastructuur” will be an extension to the “Wet Digitale Overheid” and covers and updates the management of digital information in organisational IS. Data management and its associated security and safety are becoming more and more important with the upcoming digital innovations; laws need to be regularly updated. This has been happening in Germany on a regular basis for the last years, which led to the GDPR being not too much of a change for many organisations. Legal updates and adaptations create hence other grounds for future research.

8. ACKNOWLEDGMENTS

I would like to thank all people who supported me and cooperated working on this thesis. First, I would like to thank IrisZorg, Clinic Geutingshof, and ZGT and their representatives for collaborating and supporting us with such valuable information. My thanks also go to my fellow colleagues without whom this research would not have run so smoothly. Also, many thanks to our supervisor who has always been there for questions and advice. Lastly, I like to thank my family and friends for the never-ending support and belief in me throughout my studies.

9. REFERENCES

Agarwal, R., Gao, G. G., DesRoches, C., & Jha, A. K. (2010). The digital transformation of healthcare: Current status and the road ahead. *Information Systems Research*, *21*(4), 796–809. https://doi.org/10.1287/isre.1100.0327

BDSG. (2018). Bundesdatenschutzgesetz (BDSG), 1–38.

DAC Beachcroft. (2018). The European General Data Protection Regulation: A guide for the insurance industry.

Entzeridou, E., Markopoulou, E., & Mollaki, V. (2018). Public and physician’s expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. *International Journal of Medical Informatics*, *110*(June 2017), 98–107. https://doi.org/10.1016/j.ijmedinf.2017.12.004

European Commission. (2014). Overview of the national laws on electronic health records in the EU Member States - National Report for the Netherlands, (March), 40.

European Parliament. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, (L281/31), 31–50. https://doi.org/ISSN 0378-6978

European Society. (2017). The new EU General Data Protection Regulation: what the radiologist should know. *Insights into Imaging*, *8*(3), 295–299. https://doi.org/10.1007/s13244-017-0552-7

Fichman, R. G., Kohli, R., & Krishnan, R. (2011). The role of information systems in healthcare: Current research and future trends. *Information Systems Research*, *22*(3), 419–428. https://doi.org/10.1287/isre.1110.0382

Finn, D., & McMillan, M. (2016). Addressing Healthcare Cybersecurity Strategically.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research, *8*(4), 597–606.

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. *Academy of Business, Engineering and Science Halmstad University, Sweden*, 15. Retrieved from http://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf

Hoffman, S., & Podgurski, A. (2007). In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information. *Boston College Law Review*, *48*(2). Retrieved from http://lawdigitalcommons.bc.edu/bclr/vol48/iss2/2

INCE & Co. (2018). Is the Insurance Industry prepared for GDPR?

Knijnenburg, B. P., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). Death To The Privacy Calculus? Retrieved from https://poseidon01.ssrn.com/delivery.php?ID=42100008912208507706909212109509603105700706804505802408902308612608302208608702801003306012200505200304911507402300708210408511200807807708508609302010806907410712400007805312107908412511912300500208911406506500

KPMG. (2017). Closing the Gap The changing threat, (July). Retrieved from https://home.kpmg.com/uk/en/home/insights/2017/08/the-growing-cyber-threat-for-insurers.html

Lankhorst, G. H., Dahm, P., & Nederlands Koninkrijk. (2013). Afdeling 5. De overeenkomst inzake geneeskundige behandeling. *Burgerlijk Wetboek Boek 7, Afdeling 5, 5*.

Mackenzie, I. S., Mantay, B. J., McDonnell, P. G., Wei, L., &

MacDonald, T. M. (2011). *Managing security and privacy concerns over data storage in healthcare research*. *Pharmacoepidemiology and drug safety* (Vol. 6). https://doi.org/10.1002/pds

Mello, J. P. J. (2017). *Cyber Insurance Report 2017*. Menlo Park, California. Retrieved from https://cybersecurityventures.com/cyberinsurance-report-2017/

Ponemon Institute. (2016). Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute*, (May), 1–52. Retrieved from https://www.ponemon.org/local/upload/file/Sixth Annual Patient Privacy %26 Data Security Report FINAL 6.pdf

Rahim, F. A., Ismail, Z., & Samy, G. N. (2013). Information privacy concerns in electronic healthcare records: A systematic literature review. *Research and Innovation in Information Systems (ICRIIS), 2013 International Conference On*, *2013*, 504–509.

Rumbold, J. M. M., & Pierscionek, B. (2017). The effect of the general data protection regulation on medical research. *Journal of Medical Internet Research*, *19*(2), 1–6. https://doi.org/10.2196/jmir.7108

Samy, G. N., Ahmad, R., & Ismail, Z. (2009). Threats to Health Information Security. *2009 Fifth International Conference on Information Assurance and Security*, 540–543. https://doi.org/10.1109/IAS.2009.312

Schneeberger, A. R., Kowalinski, E., Fröhlich, D., Schröder, K., von Felten, S., Zinkler, M., … Huber, C. G. (2017). Aggression and violence in psychiatric hospitals with and without open door policies: A 15-year naturalistic observational study. *Journal of Psychiatric Research*, *95*, 189–195. https://doi.org/10.1016/j.jpsychires.2017.08.017

Shenton, A. K. (2004). Strategies for Ensuring Trustworthiness in Qualitative Research Projects. *Education for Information*, *22*(2), 63–75. Retrieved from http://www.lhemoodle.ch/course/view.php?id=3229

Symantec. (2018a). Addressing Healthcare Cybersecurity Strategically.

Symantec. (2018b). ISTR Internet Security Threat Report, *23*. Retrieved from http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, *34*(1), 175–179. https://doi.org/10.1016/j.clsr.2017.05.015

Yin, R. K. (2009). *Case Study Research - Design and Methods*. *Applied social research methods series ;* (Vol. 5.). https://doi.org/10.1097/FCH.0b013e31822dda9e

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information and Management*, *55*(4), 482–493. https://doi.org/10.1016/j.im.2017.11.003

Quality of care:

10. APPENDIX

10.1 Appendix 1: Interview Questionnaire

General:

- Information about the hospital:
    - Size
    - Location (rural/urban)
    - Teaching status
    - Systems applied
    - Integration with physicians
    - Culture
    - IT history
- What is your organisation’s global headcount?
- How many patients do you have on average in a year?

Adapting to the GDPR:

- When did you start preparing for the GDPR?
- What challenges were you facing?
- What things did you have to change?
- Are there parts where you are still not 100% compliant with the rules?
- Roughly, how much did it cost you to change the organisation’s strategy to make it compliant with the GDPR?
- Was there an external consultant? Did he/she do an audit?

Training:

- Have you received any information from your superiors regarding the upcoming General Data Protection Regulation enforced from May 25th, 2018?
- Have you received any training on how to deal with privacy and security?
- Have you received any training on the changes that influence your job?
- How well prepared do you feel to deal with issues regarding the General Data Protection Regulation?

Job:

- How has the introduction of GDPR affected your job? Have you experienced changes to your job after the introduction of GDPR?
- Do you feel that the privacy regulations are limiting or enhancing the way you perform your job?
- Does GDPR affect your job performance?
- How much (extra) time are you spending on administrative tasks now? (e.g. retrieving informed consent)
- Do you experience benefits from the introduction of GDPR on your job?

- How do you feel that GDPR has a direct influence on the quality of healthcare that the hospital can offer?

- How do you feel about GDPR and its direct influences on your own job?
- How do you feel that GDPR has an indirect influence on the quality of healthcare that the hospital can offer?
- How do you feel about GDPR and its indirect influences on your job?
- To what extent do/did patients become more privacy aware?
- Do you have experience with clients being reserved about their private situations (e.g. refusing to give consent)?
- What effect does disclosing behaviour of a patient have on the quality of care?

Information Systems:

- To what extent have information systems been changed over the past two years to accommodate GDPR?
- What kind of patient data do you collect and store?
- What are the information systems these data are stored in?
- How do your Information systems collaborate?
- How are these data being transferred from one IS to another?
- Which department is most responsible for the collection, storing and sharing of patient data?

Data Security:

- What kind of policies and strategies do you have in place to secure patient data?
- How are employees handling data being educated and monitored?
- Would you say your organisation has sufficient resources to quickly detect unauthorised patient data access, loss or theft?
- Would you say your organization has personnel who have the technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data?
- Would you regard your organisation's security budget as sufficient?
- Do you think that healthcare organisations should be more attentive with data than organisations in other sectors? Why (not)?
- In your opinion, what harms do patients suffer if their data were lost or stolen?

Incentives:

- Do you currently offer incentives for people to share their information in order to give the best quality of care available? What kind of incentives?
- What type of incentives would or could you offer to gain informed consent?
- Do you think the GDPR evokes a change in the patients' disclosing behaviour?

Research:

- To what extent does GDPR influence medical research at your hospital?
- How can the hospital incentivize patients to give consent to share data for research purposes?