General Data Protection Regulation and its effects on healthcare in the Netherlands and Germany

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

ABSTRACT

On the 27th of April in 2016, the European Parliament adopted the General Data Protective Regulation to replace the directive on data regulation that was established in 1995. The General Data Protective Regulation got enforced after the 25th of May in 2018, meaning that organisations from this date on must be compliant with the new regulations. The regulation empowers people to be the owners of their personal data. This empowerment has consequences for organisations, who have to make sure that informed consent is retrieved when they start the processing of the data of their customers or patients. The purpose of this thesis is to evaluate whether healthcare institutions are affected by the consequences of GDPR on this industry and to assess whether the quality of care is distressed by these new privacy-security measures. Following the research at healthcare institutions up by surveys, research is done to evaluate whether disclosing behaviour of patients might change and whether this could have influences on these healthcare institutions. The results show that healthcare institutions so far have not suffered significantly from the adoption of GDPR, but that work has been more inconvenient and inefficient. Disclosing behaviour is currently not affected, but the surveys show that as privacy-awareness increases; disclosing behaviour might also be impacted; which could potentially lead to consequences for the quality offered in the healthcare sector in the future.

Graduation Committee members:

Dr. Fons Wijnhoven
Dr. Raymond Loohuis

Keywords

Privacy, GDPR, Disclosing behaviour, Health Sector, European Union, Information Systems, Perceived Risk, Trust.

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

1. INTRODUCTION

On the 14th of April of 2016, the EU Parliament approved of the General Data Protection Regulation, or "GDPR", which replaced the Data Protection Directive which was installed in 1995 to ensure the protection and processing of personal data inside of countries within the European Union. This replacement was done to make sure that regulations are appropriate in the current digital age. The GDPR comes into effect on the 25th of May, 2018; with organisations that do not comply to these laws possibly facing heavy fines of up to 20 million euros or 4% of global turnover ("General Data Protection Regulation," 2016).

There are several fundamental concepts to GDPR, although the central aspect to be considered is that clients and patients (individuals) become secure in their status as owners of their personal data. Data controllers and processors are obligated to emphasise security, accountability and transparency and at the same time enforce and institutionalise individual Europeans' rights to data privacy. (O'Connor, Rowan, Lynch, & Heavin, 2017)

This is established by the following rights and regulations ("General Data Protection Regulation," 2016):

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

Data Minimization: Data should not be stored by the organisation if it is irrelevant to the organisation's service. Processors and controllers of data are limited to using the minimum amount of data required for their service. Furthermore, data can only be kept for the shortest amount of time possible; although the definition of this varies per situation.

Breach Notification: Data controllers have up to 72 hours to notify supervisory authorities after becoming aware that a data breach has occurred.

Right to Access: Data subjects have a right to request a copy of their processed data and controllers are required to provide this upon said request.

Right to Erasure: Data subjects have the right to request organisations to erase all their data. This was already the case under the Data Protection Directive, but now they gain the right to request the organisation to inform this to all other third parties that have this information from the original organisation.

Right to Data Portability: Data subjects have the right to have their data transferred from one data controller to another upon request if this is technically feasible. The data controller must comply and transfer this in a structured, machine-readable format.

Right to Rectification: Data owners gain the right to have incomplete data completed and to rectify incorrect information in their files.

Privacy by Design: In every step of the way, actions of organisations regarding the processing of data must have privacy and data protection in mind.

To gain clarity over the influences of GDPR, research will be done in the medical field in the form of a case study at various healthcare institutions in combination with surveys to assess disclosing behaviour of patients.

The end goal is to determine whether the introduction of the GDPR will have an influence on the quality of healthcare and therefore the research question is formulated as follows:

"How does the disclosing behaviour of patients affect the quality of care that healthcare institutions can offer?"

The first part of the case study will be performed at ZiekenhuisGroep Twente (ZGT) in Hengelo, the Netherlands. ZGT consists of two hospitals in the eastern parts of the Netherlands and also has five different outpatient clinics in the same region. Other than caretaking and curing of patients, the group also has research facilities. Future research could also be strongly affected by the upcoming GDPR change, especially the "Data Minimization" concept of it. The second part of the case study is conducted at a Rehabilitation Clinic in Beekbergen (the Netherlands) called IrisZorg. IrisZorg has multiple offices and clinics spread out over the Netherlands. They are primarily concerned with the treatment of people that are suffering from addiction to drugs, alcohol or gambling. Lastly, the case study is concluded at a general practitioner's clinic in Rhede, Germany; which is concerned with the treating of widespread, minor diseases.

Important to note is that in the Netherlands there is an additional law surrounding the privacy of patients specifically constructed for the medical field: "Wet op de geneeskundige behandelovereenkomst" (WGBO), or the "Medical Treatment Agreement Act." This law is established in Boek 7, Afdeling 5 of the 'Burgerlijk Wetboek'**.** This regulation regards the rights and duties of a client when a treatment agreement is established between them and the caregiver. A key aspect of this law concerning GDPR is that the caregiver is not allowed to inform about the patient's condition to anyone but the patient itself. The exception being people directly involved with the treatment of said patient or in case the caregiver needs to be replaced (Artikel 457: 1-2 BW). This means that a doctor is free to ask consultancy of a physiotherapist without explicitly having to ask the consent of the patient in question.

2. THEORETICAL FRAMEWORK

2.1 Privacy Calculus

Core in the theoretical framework is the concept of 'Privacy Calculus'. This concept proposes that the disclosure of private information by an individual is based on examining the risks and benefits (i.e. trade-offs) of 'user-tailored privacy' (Knijnenburg et al., 2017). It is thus the comparison made by users between perceived risks and assumed benefits (Mary J Culnan & Armstrong, 1999). The customer or patient's willingness to disclose information is therefore dependent on the fact if perceived risks are less considerable than the expected benefits that result from this disclosure. (M.J. Culnan & Bies, 2003)

Knijnenburg et al. argue that attitudes and behaviours of users are also a sum of the lack of awareness surrounding privacy issues (Knijnenburg et al., 2017). Understanding what causes patients to disclose private information or causes them to wilfully not disclose it, is vital also in the medical sector. A patient arriving at a hospital with a life-threatening disease will supposedly be less careful with sharing their private information as all they care about is getting cured, whereas a patient with minor trouble might be more hesitant in sharing their private information. The life-threatened patient will most definitely feel that the benefits far outweigh the risks of disclosing information. In the original Privacy Calculus model, the factors 'perceived risk' and 'expected benefits' are independent of each other and individuals are ought to weigh these individually in order to make privacy-decisions (Dinev & Hart, 2006). However,

research found evidence that these factors are interdependent, 'implying individuals to use perceptions of benefits as a cue for risk valuation'. (Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Organisations ought to have a significant degree of value to their service to counteract the risk that comes with sharing private information with the organisation (Awad & Krishnan, 2006).

Furthermore, when looking at the transfer of information between health providers, perceived value thriving over perceived risk only becomes relevant when an organisation also takes into account policies to reduce risk and help with the construction of a cost-benefit analysis. When a patient has privacy concerns, they may not identify benefits of exchange of health information and can therefore opt not to provide consent (Esmaeilzadeh, 2018). It is suggested to provide information and education about having health information exchange services, to convince patients to show their positive intentions and thus provide consent (Esmaeilzadeh, 2018). Education to medical staff about privacy legislation is also vital since preventing is almost always better than solving after the fact (saving frustration and costs) (Mills, Yao, & Chan, 2003).

Various factors have been found in literature to influence privacy concerns in Electronic Health Records, Rahim et al. (2013) established nine of them through literature review: Trust, demographic info, information dissemination, computer literacy, sensitive data, consent, the potential of privacy breach, legal & policy, and training. All of these were found to be significant in influencing privacy concerns in Electronic Health Records (Rahim, Ismail, & Samy, 2013). These insights are possibly relevant in determining what data individuals will share and to whom. An individual is likelier to share data with a person they trust, and physicians or healthcare professionals are people that are generally high on the level of trust that people have. Consumers in countries that experience a low degree of trust such as Italy are likelier to avoid uncertainties than countries that experience a high degree of trust (Hann, Hui, Lee, & Png, 2007). On the other hand, familiarity and risk were found to have a more substantial influence on willingness to transact in e-commerce than trust did (Van Slyke, Shim, Johnson, & Jiang, 2006). This degree of trust could come into play when comparing a healthcare institution with a commercial business as consumers' may react differently to privacy concerns and threats dependent on different sectors (i.e. through risk beliefs and trust) (Malhotra, Kim, & Agarwal, 2004). Similarly, sensitive but relatively harmless data, such as a patient having a sexually transmitted disease, might result in increased carefulness in sharing this data due to embarrassment. People would become too worried about having interpersonal relationships affected when news could come out (Mills et al., 2003).

Research done on applying the Privacy Calculus theory on Electronic Health Records in Greece resulted in both the professionals (physicians) as well as public individuals agreeing that the benefits of using Electronic Health Records outweigh the possible risks that come with it. (Entzeridou, Markopoulou, & Mollaki, 2018). Nonetheless, both groups are in agreement that these systems can have a significant impact on privacy issues so sufficient guarantees regarding privacy and security are needed to ensure that as few data leaks as possible happen (Entzeridou et al., 2018).

Recent studies have explored the possibility of combining the Privacy Calculus theory with the theory of Risk Calculus: Dual Calculus. This theory assumes that both of these theories are interrelated and influence a patient's disclosing behaviour (Zhang et al., 2018). Zhang et al. (2018) developed the following model, combining the two and researched what factors influence each other through an empirical study (see Figure 1).

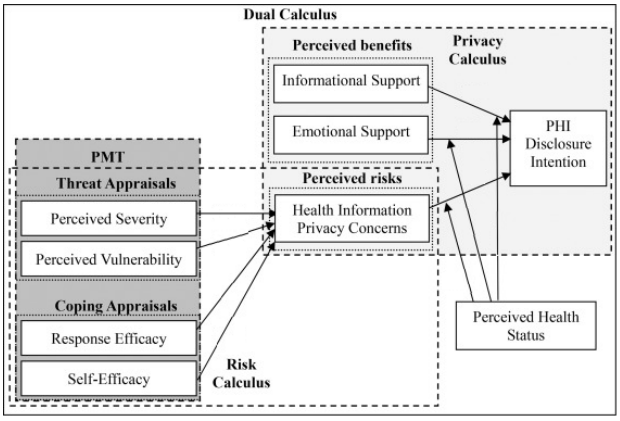

Figure 1. The Dual Calculus model (Zhang et al. 2018)

The study found that patients perceived two further benefits from disclosing privacy, namely informational support as well as emotional support. Other than the Risk Calculus influencing the Privacy Calculus, another factor that was tested was that of the perceived health status of the patient. The perceived health status had a moderating effect on 'privacy concerns' and therefore enhanced the negative effect of privacy concerns on disclosing intention. The same occurs when looking at its effect on informational support: a negative moderation. People with better-perceived health conditions thus experience less positivity from disclosing private information. On the other hand, the moderation-relationship between perceived health status and emotional support was found to be insignificant; which underlines that emotional support is both important for people with a lower perceived health status as well as those with higher perceived health status. (Zhang et al., 2018).

2.2 Incentives

(Monetary) incentives have a positive influence on individuals' disclosure of private information. When an incentives unlocks a particular advantage, decisions on the extent of disclosing will change. (Gómez-Barroso, Feijóo, & Martínez-Martínez, 2018). The results of these performed studies are not exclusively focused on the health sector but are discussed in general. Disclosing information often comes with benefits for the customer/patient; creating a personally modified and attractive product or service.

Research was also performed by Hann et al. in 2007 on how to overcome privacy concerns by looking at the Expectancy Theory of Motivation. This theory states that an individuals' Motivational Score consists of three aspects: Expectancy (the probability weight of having effort transformed into performance), Instrumentality (the likelihood that performance will lead to a certain outcome or outcomes) and Valence (the assigned value of the outcome). (Hann et al., 2007). Their results found that financial rewards or incentives and an increase in convenience were significantly increasing the 'valence'. Convenience was altered for instance by lowering frictional costs and by offering personalisation. It was not only found to increase valence, but also mitigated privacy concerns in individuals. Furthermore, their results found that the customer values having Privacy Protection Policies available and therefore they advise to state these policies more prominently. (Hann et al., 2007).

Factors that contribute to disclosing behaviours are also found to be emotional (affect-based) as well as fairness-based (cognition-based, i.e. perceived relevance of information and awareness of the privacy statement). Psychological factors such as fear and joy have an initial effect which starts already based on aspects such

as website impressions. This effect lasts for the entire process, and when the information exchange occurs, the fairness-based factors also come into play to adjust privacy risk belief and privacy protection belief. (Li, Sarathy, & Xu, 2011). This theory could identify incentives to convince patients to share their private information by first setting them up in an appropriate emotional state, for instance by having a joyful website design.

2.3 Practical implications

Tikkinen-Piri et al. constructed a table with twelve practical implications following GDPR and added recommendations for organisations in order to follow up with the requirements for implementation. (Tikkinen-Piri, Rohunen, & Markkula, 2018). These implications are as follows: 'Specifying data needs and usage', 'Considering conditions for data processing in international context', 'Building privacy through data protection by design and default', 'Demonstrating compliance with GDPR requirements', 'Developing processes to deal with data breaches', 'Reckoning with sanctions for non-compliance', 'Designating a DPO', 'Providing information to data subjects', 'Obtaining consent on personal data usage', 'Ensuring individuals' right *to be forgotten*', 'Ensuring individuals' right to data portability', and 'Maintaining documentation'. These implications and requirements are tested during the interviews in the Case Study to assessed whether the health institutions are ready for GDPR and if the information systems are properly prepared for relevant aspects such as the 'right to be forgotten' and the 'right to data portability' (Tikkinen-Piri et al., 2018).

The Society of Radiology investigated what the introduction of the GDPR would mean for them. They state that the access to databases such as the Electronic Patient Records are currently maintained and controlled by local rules such as the administration of hospitals or other healthcare institutions. However, they are fearful that they might lose access to medical data and medical radiology images from the past under GDPR; which might harm their job as they will be less enabled in their task to do diagnostics or perform research. ("The new EU General Data Protection Regulation: what the radiologist should know," 2017). However, with patient records possibly coming in useful in the future; they do not see the reason to erase medical data in a routinely matter unless the patient exercises their *right to be forgotten*. The GDPR is not completely clear about how long data should be kept (Data is to be held for the shortest amount possible, but this varies from situation to situation). Furthermore, various data protection methods can be used such as anonymisation, pseudonymisation or encryption. Encryption safeguards messages through encoding to ensure that only authorised people can read them. Anonymisation refers to the process of completely erasing identifiable information when it is not necessary, whereas pseudonymisation replaces this identifiable information with artificial identifiers. The idea of this is to perform research anonymously, but if this research delivers results that could be significant to the individual; it would be possible to trace back who it belongs to eventually. GDPR possibly negatively affects the field of medical research in this regard, since demands for anonymisation could be higher than their current standards. Medical Research where Pseudonymisation is currently sufficient or even beneficiary could, after the introduction of GDPR, require to comply with either true consent or anonymisation. (Rumbold & Pierscionek, 2017). True anonymisation might have adverse effects on future research in the case of new insights that could cure a life-threatening disease, making it impossible to trace back the data to the person it belongs to – potentially putting that person's life in jeopardy.

Another aspect to take into consideration is that of 'Informed consent'. O'Connor et al. (2017) describe it as specifying the rules of disclosure, making sure that the client or patient has adequate comprehension of what is done with the information and the obtainment of signatures. (O'Connor et al., 2017) O'Connor et al. further concludes that users have a strong desire not just to be customers, but to be made a partner in the process. This shows relevance to the surveys, when a preference is indicated for informed or explicit consent (i.e. through sliders). Users expressed an evident desire to gain more control over their Personal Health Information over privacy and security levels, and a comparison was drawn with those system settings available on Facebook. (O'Connor et al., 2017)

Organisations run the risk of backlash when consumers, users or patients feel that their information is misused. (Awad & Krishnan, 2006). With the introduction of GDPR, the possibility of doing so should be limited and the hefty fines should discourage companies from doing such things.

2.4 Hypotheses

The following hypotheses can be constructed based on the theoretical framework.

H1: Patients suffering from a severe disease are likelier to disclose their personal data compared to patients that have a minor disease.

H2: Patients that suffered from a severe disease are likelier to disclose their personal data for future research than people that suffered from a minor disease

H3: Monetary incentives and discounts on healthcare insurance will significantly increase the number of people willing to disclose their data for future research.

H4: The perceived risk of disclosing personal data will decrease following GDPR laws

H5: The amount of time spent on administrative tasks will increase significantly following the introduction of GDPR.

H6: The quality of care that healthcare institutions can provide will decrease following the introduction of GDPR.

3. METHODOLOGY

3.1 Research Design

This research was designed to be both quantitively as well as qualitatively. The quantitative part of the study is concerned with the consent and the conundrum of the privacy calculus theory and is concerned with the perspective of the consumer (patient) and is performed by the use of a survey. Questions are mainly asked about a person's disclosing behaviour and how this is affected by the changes due to GDPR. The quantitative part of the study was executed through the form of a case study in order to delve deeper into the perspectives of healthcare organisations. From this point of view, the influences of GDPR on the offered quality of care can be estimated. Specifically looking at the importance of informed consent following these regulations, the quantitative and the qualitative parts can be combined to draw conclusions about the influence of GDPR on disclosing behaviour and whether that causes the quality of care to be affected.

For the survey, the data subject is confronted with two hypothetical cases. In one case, the data subject assumes the role of a patient suffering from a minor disease (broken arm); whereas in the second the patient suffers from a severe disease (symptoms of cancer). This is done to assess whether people will share more data in the case of a life-threatening disease, or if the patient is equally cautious in such a situation. The constructed variable is "willingness to disclose" and looks at the amount of data a person is willing to share. It is measured in four different levels, starting

with a patient's decision not to disclose data at all and ranging to full disclosure of personal data. These levels show an ordinal scale and imitate a slider effect; giving the patient multiple options for medical data sharing.

The survey starts with fundamental questions to determine demographic factors such as age and nationality. Then it moves on to measure the baseline of perceived risk; inquiring about how much they trust organisations with their personal data, and how much they trust medical institutions, how important privacy is to them personally, and additional questions about how much they would currently disclose. This baseline can be helpful in determining the differences in answers between various people.

The participants are then confronted with the minor and severe diseases mentioned earlier. In either situation, the level of disclosure is measured by asking how much data they disclose. Then, the subject is given some information about the introduction of GDPR, suggesting that privacy and security are protected more under this law. The same questions are asked to see whether this changes perceptions regarding data sharing. Similarly, the opt-out options (Right to be Forgotten) are explained to assess the influence of this aspect of GDPR and see if people will disclose more information, since they can decide to remove their data at any time.

Additionally, the survey moves onto "Quality of care". The data subject is confronted by the hospital saying that they cannot provide the desired quality of care unless more data is disclosed.

Concluding, the survey ends with the aspect "Future Research", indirectly linking to the quality of care and improvement in this regard. The data subject is asked whether their data can be used for longitudinal research and under which conditions (no disclosure, anonymisation, pseudonymisation, encryption, full disclosure) (Rumbold & Pierscionek, 2017). And then additional questions are asked to see if people would allow their data to be shared when certain incentives are promised (e.g. monetary or discounts on health insurance).

For the complete list of Survey Questions, see Appendix A**.**

The case study, while primarily concerned with 'Quality of care', also assesses additional aspects of the effects of the introduction of the General Data Protection Regulation on healthcare organisations in the Netherlands and Germany. It investigated whether employees received training to deal with privacy issues, if employees spend more time on administrative tasks, and whether their daily jobs have changed following these regulations.

The choice was made to go for a multiple-case embedded design (Yin, 2014). Meaning that multiple sublevels within several organisations will be analysed to reveal the consequences of GDPR on the healthcare institutions as a whole. This choice was made due to the revelatory nature of GDPR and its novelty (Yin, 2014). The case study was performed at several organisations, namely: a hospital and a drug rehabilitation clinic in the Netherlands as well as a general practitioner's clinic in Germany. At the hospital, the Chief Information Officer was interviewed to determine the influences of GDPR on a broad level of the organisation. At the drug rehabilitation clinic, the treating staff are inquired about the effects of GDPR on their jobs. At the general practitioner's clinic, the head of the doctor's assistants is interviewed due to her expertise in administration. As for protection of the involved participants, informed consent was asked and their privacy and confidentiality is respected so that they do not end up in undesirable positions (Yin, 2014).

Interviews were the primary source of evidence from the case study. Interviews naturally have strengths and weaknesses. Bias may occur due to, e.g. reflexivity or response bias (Yin, 2014).

The case study at each organisation starts with some inquiries about basic information about the hospital and the interviewee in question, moving on to the subject "Adapting to GDPR". Here, insights are gained on what the interviewee and the organisation had to do to make sure that they are compliant with GDPR. Questions regarding received training or if staff had to attend an informational event were asked to determine whether employees are adequately trained for GDPR. Consequently, questions are asked about these individual jobs and how GDPR has affected them in this regard and if these privacy regulations enhance or limit their capability to execute their jobs.

The interview proceeds with "Quality of Care", trying to assess whether the GDPR has a direct influence on the quality of care that both the healthcare institution as an entity, as the person individually can offer. Important to know is whether there have already been cases about patients refusing to give consent and what the consequence of this was for them as treating staff.

The case study then moves on to the relationship between the various information systems within the healthcare institution and the security measures taken.

Concluding, the case study ends with questions about offered incentives for the disclosure of data and whether (future) medical research is influenced by GDPR.

For the complete list of Case Study Questions, see Appendix B.

3.2 Data Collection

The interviews were conducted locally at the hospital in Hengelo and Almelo, the Drug Rehabilitation Clinic in Beekbergen and the general practitioner's practice in Rhede, Germany. Before the scheduling of the interviews, the interviews and their protocols were constructed together with fellow bachelor thesis circle members. All interviewees were all asked independently to question how GDPR affected their jobs and to assess whether they found a difference in the quality of care they could provide when comparing the healthcare institution's privacy regulations before and after the introduction of GDPR.

The survey was created through Google Forms and was handed out in English to friends and peers, since respondents could be living in Germany as well as the Netherlands. The survey was sent through e-mail, WhatsApp or similar communication methods with a Google Forms link to peers, friends and family.

To measure reliably, a minimum threshold of 100 respondents was established. With the three people involved in the bachelor circle, this was established as an accomplishable task and 125 people filled out the survey. (Cooper & Schindler, 2014)**.**

3.3 Measurement of Concepts

The case study is primarily concerned with the perspective of the healthcare institutions and its staff. It is engaged with how the introduction of GDPR has influenced the hospital itself, but also the job performance of healthcare staff such as doctors, psychologists and nurses. Most importantly, it looks at the extent of the influence of a patient's disclosure behaviour on the quality of care for staff as well as for the hospital as a whole.

The survey was constructed to see how patients share their data and how perceptions change with the introduction of GDPR. It determines what factors are important for people when it comes to disclosing their data to a hospital.

The combination of the case study with the survey identifies whether the introduction of GDPR changes the way that patients look at their personal information and if this has an influence on the quality of care that they receive from the hospital. It can help in to assess whether incentives are needed to get patients to share more of their data.

3.4 Control variables

Control variables are established to make sure that the relationship between dependent and independent variables are clarified and not influenced or moderated by these control variables. Control variables are unchanged throughout the experiment and are there to prevent wrong conclusions from being drawn from the relative relationship between other variables.

The established control variables are as follows: Age, gender, and the country they live in at this time of completing the survey.

Another control variable was established in the baseline measures and was constructed in the form of: "Do you trust hospitals over commercial firms" to assess whether people understand the questions correctly, this could be done by comparing the results of this question with the difference between "Do you trust companies with your data" and "Hospitals are a trustworthy institution".

3.5 Data Sample

The largest proportion of respondents were between the age of 18-24 with 59% of respondents falling in this category. The second largest group was 25-34 with 24% of respondents (age <18: 1,6%, ages 35-44: 3,2%, ages 45-45; 5,6%; ages 55-64; 6,4%)

56,8% of the respondents were male, and 43,2% were female. From the respondents, 49.6% reside in the Netherlands, and 44.8% reside in Germany. The rest of the respondents come from the United Kingdom, Switzerland, Hungary, Belgium, Scotland, Australia and the United States respectively. While some of these countries are not directly affected by GDPR regulations, the disclosing behaviour can still be used for research as explanations about GDPR and opting-out are given before each question.

4. RESULTS

4.1 Case 1: IrisZorg

4.1.1 Introduction of the organisation and the interviewees

IrisZorg is a mental healthcare institution located in the Netherlands, spread out over 60 locations in the provinces of Gelderland, Flevoland and Overijssel. The organisation is mostly concerned with the treatment of people that suffer from addiction from drugs, alcohol or gambling. The organisation has various shelters and clinics where clients can stay for more extended periods of time, but also works with ambulatory care; where clients are served on an outpatient basis. Not exclusively busy with recovery, they are also concerned with the reintegration of clients through for instance day-to-day activities, schooling, or assisting in getting used to working again. ("over IrisZorg," 2018)

The interviewed people at IrisZorg were located at the establishment in Beekbergen, Gelderland. This location hosts 114 clients at maximum capacity and also features ambulatory care and daytime planning. One of the interviewees was the head of the social workers and also worked as a "healthcare broker", in which she is active in determining what type of care is most suitable to the client (i.e. hospitalization or ambulatory care) and takes care of healthcare logistics of the clinical patients. The other interviewee is a so-called "GZ-Psycholoog", a psychologist that graduated with a Master in Healthcare and is classified in the BIG-register in the Netherlands. She is the head-practitioner and is the end responsible for the treatment of a group of patients. She is concerned with constructing treatment plans for clients, and assures that every other psychologist/practitioner is doing their job correctly. She also has the first contact with incoming patients.

4.1.2 Influences of GDPR on the organisation

The healthcare broker is convinced that the introduction of GDPR is mostly a positive influence on the healthcare industry in general as well as the quality of care that IrisZorg can offer: "Being attentive of what we can and cannot share among each other internally or even externally is always a benefit. Yes, it might slow down some processes; but it is all in the benefit of the client – whom we work for."

Disadvantages are also mentioned extensively, such as added costs for the organisation; for instance, the appointment of a Data Protection Officer in January 2018 to ensure that the organisation is compliant with the GDPR when it is enforced and to supervise the situation after enforcement. An external audit was also conducted, though the details of this audit are unknown to both the healthcare broker and the psychologist.

Similarly, another investment that cost time and money was the requirement for every employee to do an e-learning course regarding privacy. Not only privacy between employee and patient, but also that on the work floor between employees and the employee in question. She adds that they were as a healthcare institution already very concerned with privacy, but that some minor stuff had to be changed; such as namedropping a clients' full name in an internal email. She added that the organisation as a whole has become a lot more aware of what data is shared.

Asked on what changed for her job specifically, she answered: *"we have to make sure that clients are attentive of what they sign, even when we need that signing for treatment. Clients have to give informed consent. It has become crucial to pay heed to whether consent was retrieved."*

The psychologist has a different opinion about the bureaucratic nature of the GDPR, saying that it is very inefficient to conform the law. Being aware that the law is necessary for the sake of the patients, she admits that work is done in a much less efficient manner and that everything takes a lot more time: "Small things have changed. It is incredibly inconvenient because we cannot say names anymore, either on the phone or in quick e-mails. We have to look up every client number manually, and it takes a lot of time that could be used better."

Regarding the quality of care, the psychologist had a final note to make: "It is important to be attentive, but I do not see how this law could improve the quality of care. That is two different things for me. People become almost scared of data protection topics and that is not what our work is about. We need our patients to trust us. This regulation has two sides."

4.1.3 Influences of GDPR on the patients

The healthcare broker stated that patients that arrive at IrisZorg are generally too naive when it comes to the sharing of their data. They are very willing to write their signature on every paper given to them, as long as they get the care they desperately need. She states: "*Signing the request forms is only bureaucratic, no patient cares for them anyway. Clients do not read what they are signing anyway, but I personally always warn clients that they actually have to read it beforehand; even when we explicitly need them to sign the consent forms in order to treat them."* She clarifies that this helps in the establishment of a relationship between her and the client and that it shows good faith or honesty. She has not gotten the impression so far that clients have become more aware of their private data due the introduction of GDPR, but that it might follow in the near future and encourages it, saying that it can only increase the quality of healthcare they can offer.

Recently the 'Right to Erasure' and the 'Right to Data Portability' came into play (Tikkinen-Piri et al., 2018), as a client requested his/her data to be transferred to another healthcare institution followed up by a request towards IrisZorg to destroy all of his/her data. The healthcare broker further adds that the 'Right to Erasure' can have negative influences on the quality of care: *"I remember a time where a client was unwilling to share what had happened at the previous institution he was admitted to. I had a bad feeling about the situation and could not fully trust this client. When this faith is missing, there cannot be a solid relationship between caregiver and client, and you can only tell the person that he or she cannot be treated here."* This is most relatable to the security of both personnel and the clients among each other. When there is a lack of trust, employees do not feel completely safe when dealing with the client, and that the client could not be trusted among other patients too.

Further described is a situation where a client was in treatment at two different organisations for different problems, however he/she was unwilling (due to his/her illness) to share their personal data between these firms. She admitted that it really slows down the process of the treatment at IrisZorg and that the patient could be helped in a much more efficient and faster way if the disclosing behaviour was not as problematic. In the client's case, consent had to be asked by every single treating practitioner individually.

Another case of a client not being able to give consent is when a client becomes psychotic (possibly due to relapsing in drugs) and is unable to give explicit consent. In that case, the GZ-Psychologist has to write down why they are still treating him; justifying that treatment is done without consent.

4.1.4 Influences of GDPR on the Information Systems

In terms of monitoring of how private information is being handled, nothing has changed. Employees are told to put notes away or destroy them. Colleagues notify each other of this on an informal basis. Information Systems have not faced any changes in general as far as both interviewees are aware.

Furthermore, the psychologist admits that the information systems are not fully waterproof (yet): "Our system is accessible for different people and jobs, and I heard that some people have access to files they should not have access to. No one makes use of this possibility. We are not interested in looking up records of patients we do not treat. Professionals do not do that." Further inquired about whether a situation like this occurred, she states that it had happened where a colleague had information about a client that should not have been possible.

4.2 Case 2: ZiekenhuisGroep Twente (ZGT)

4.2.1 Introduction of the organisation and the interviewees

ZiekenhuisGroep Twente is a healthcare institution with two hospitals located in the east of the Netherlands: Almelo and Hengelo. Other than treatment of various kinds of diseases, ZGT is also a research-hospital that is concerned with multiple disciplines such as the creation of new medication for heart diseases or the creation of new technologies to be able to diagnose difficult diseases more accurately and more rapidly.

ZGT also closely collaborates also has a so-called 'regional function', closely working with general practitioners in the area as well as nursing homes. ("over ZGT," 2018)

The interviewed person at ZGT is the current Chief Information Officer of ZGT and is located in Hengelo, Overijssel. As the CIO, he is the highest executive in the IT-department of the hospital and has a leading role when it comes to finding solutions in IT-based services, managing Information Systems within the hospital and managing its personnel.

4.2.2 Influences of GDPR on the organisation

Since the announcement of the new regulations in 2016, ZGT immediately started with preparations to be able to be compliant in 2018. This was done by the appointment of a Data Protection Officer, improving the Information Security System and updating the information security policy. In addition to these changes, several external audits were conducted and an additional two privacy managers were appointed. Furthermore, they had to change internal processes, privacy policies as well as information security policies, and awareness (especially in the board of directors).

Specifically talking about the performance of employees, the CIO mentions that doctors and nurses experience frustrations following GDPR. Medical staff is unable to see all the lab results from a specific patient anymore, since they are only allowed to see the results of tests they specifically asked for (retrieved consent for). Similarly, medical staff is estimated to spend thirty minutes per day extra on administrative tasks; leading to more annoyance. A training course regarding GDPR for all employees is scheduled for this summer, but there was already a presentation and an awareness training for all staff members and the board of directors.

Asked whether GDPR has affected the hospital, the CIO responds with a resounding: "Absolutely. I think we 'over shifted' in Privacy. We see a lot of caretaking companies that do not know how to take care of GDPR and fence off everything; that is not beneficial (e.g. the exchange of laboratory data). We need to find a good work-around, but that is going to take at least one year. This is one of the areas we are not fully compliant with GDPR yet. The external audit concluded that this was a case of "accepted non-compliance".

4.2.3 Influences of GDPR on the patients

While consent was already asked, the consent forms that are distributed to patients were updated to conform with GDPR and to make sure that patients are handing out informed consent; explicitly informing patients about what they comply with, which also increases the likelihood of cooperation (Esmaeilzadeh, 2018). The CIO follows this up, by saying that doctors and patients currently are more likely to have talks about "Who can see my data?" or "Who can see what you wrote down in this conversation?"; but doctors experience this as beneficial: "Yes, the doctor has conversations about this with patients. But it means a better-informed patient. A better-informed patient, means that you can treat them better."

When it comes to emergencies, consent is not often possible to be retrieved directly from the patient. A situation from the past is described where a laboratory refused to give results from tests on a child with a fatal disease. The hospital was forced to re-do all these tests on the patient, but the results came back too late and the patient had died. In this case, now a "breaking-the-glass" principle is used: "We would rather explain why data has been transferred than have to explain a person's family on why that person has died." To assure that quality is maintained, he states: "We need to change on the long term. We need to get consent and make sure everybody understands how important it is to exchange your data in the healthcare chain. If you know how important it is, and still explicitly say no; you need to know that your life could be in danger. This is another reason why we have the "breaking-the-glass principle" (which is used in 4-5% of all patients being treated, mainly elderly people and people in life threatening conditions that are for instance unconscious). When people wilfully say no, he states that they do not offer incentives

to convince them to share data anyway: “We try to treat them as good as we can then, we do not have time for discussion.”

Following GDPR, there is already a change in privacy awareness being noticed. Replacing the DPO due to holidays, the CIO had already gotten two patients who requested access to their data. They wanted to know who has had access to their files. “We are thinking about asking a small fee for this service, as to make sure we do not all of a sudden get requests from all of our million patients.”

4.2.4 Influences of GDPR on the Information Systems

Making use of the “breaking-the-glass” principle to access data they should not have access to, is recorded in the system for future investigation; to make sure if the use was justified. Misuse of the ‘button’ is followed by sanctions. Internal audits, on old as well as live data, are regularly conducted to make sure that private data is not leaked. Old, irrelevant files are also removed every 15 years as obliged by law (100 years after a person’s death in the case of a genetic disease); records are thus usually only removed upon explicit request of the data owner.

In the information systems itself, very few changes were done as the regulation in this regard is very similar to the former law in the Netherlands: “Wet Bescherming Persoonsgegevens (WBP)”. Regarding security measures in place, the CIO mentions that they have a mechanism in place that tracks strange data transfer activities. “If we suddenly see a lot of data being transferred from segment 1 to segment 2, there is a red flag raised and it alerts people higher-up. This has not happened yet, but we tested it through simulations.”

4.3 Case 3: Group practice Geutingshof

4.3.1 Introduction of the organisation and the interviewees

Geutingshof is a clinic located in Rhede, in the province of North Rhine-Westphalia in Germany. It features four general practitioners that have a specialisation in sports medicine, psychotherapy, internal medicine or palliative care. Furthermore, it has ten doctor’s assistants and roughly 18.000 patients per year visit the clinic on average; most of them from Rhede. The clinic has a strong focus on the treatment of general, basic diseases.

The interviewee is the head of the doctor’s assistants and has several tasks within the clinic. She mainly does administrative work, but is also concerned with the overlooking of treatments and the advising, managing and monitoring of new doctor’s assistants.

4.3.2 Influences of GDPR on the organisation

The practice started preparing for GDPR in April 2018 and did so mainly by the appointment of an external Data Protection Officer and conducting an external audit. They said that not many aspects have changed in the organisation, since privacy awareness was always of high importance in the clinic. Minor changes occurred, such as not keeping the records of patients on side tables in front of another doctor’s office. The most time-consuming event so far has been the destroying of files and cases of patients that were not relevant anymore to the practice; administrative tasks cost a lot more time and are not as efficient anymore. Asked whether Geutingshof is fully compliant with GDPR as of now, they say: “We need time to adapt to the new processes. We have been working in a specific way for over ten years now and this cannot be changed within a day. Everyone is getting used to it, and we have to help each other out”. Additionally, training was given on how to deal with the new law and informational texts and brochures were handed out to the employees.

GDPR is experienced to enhance the quality of the service that the clinic can offer, but it also comes with disadvantages “Everyone is more careful and attentive now, which is positive. At the same time, it’s rather annoying because we always have to double check now whether we can exchange data with the hospital or other external practitioners. It is more time-consuming.”

There is no current active monitoring on how employees handle private data or on potential data leaks. They state that every employee knows what is expected of them and that they help remind each other to be attentive. Training is offered to every employee in advance and employees have to sign a code of conduct when they start a job, while computers and its software are only accessible with secured log-in data.

4.3.3 Influences of GDPR on the patients

Patients are well willing to give their consent. The interviewee adds that they have never run into the situation that a client has refused to give consent; all of them signed consent forms so far. These consent forms have been updated to comply with GDPR.

When the clinic asked patients to sign the new and improved consent forms, some of the patients had questions and wondered why it was necessary. The disclosing behaviour so far has not shown any changes, but their awareness of their private situation has improved. People come to the clinic to have their disease cured or treated, so they are not reluctant to give up their private data to get better.

4.3.4 Influences of GDPR on the Information Systems

The Information Systems have not changed at Geutingshof. The clinic works with one Electronic Patient Database and it did not need any further adjustments to comply with GDPR.

A change caused by the GDPR that has an impact on the way they communicate with external organisations is that e-mails cannot contain the names of patients anymore: “We used to use the patient’s full name, but we have to change this now due to the new regulation. We are aiming at only using Initials combined with patient-numbers. Adapting to these new measures will take time.”

4.4 Survey: Disclosing behaviour and the influences of GDPR

4.4.1 Established baseline

Measured on a Likert scale from 1-5, from 1 being “Strongly disagree” to 5 being “Strongly agree”, it is notable that people on average find that their Personal Data is important (mean of 4.11) and that their data is private (mean of 4.00).

Report

	Pers_Data_Imp	Pers_Data_Priv	Trust_Companies	Trust_Hospitals	Trust_Doctors	Value_Custom	Incentive_Sharing	Med_Hist_Research	Hosp_Over_Comp
Mean	4.11	4.00	2.75	3.58	3.97	3.92	2.64	3.43	4.02
N	125	125	125	125	125	125	125	125	125
Std. Deviation	.935	1.078	1.029	1.002	.975	1.060	1.073	1.234	.954

Figure 2. Means and descriptive statistics

Asked whether people trust companies with their data, compared to the question if they trust hospitals with their data; it can be concluded that people are generally more trustworthy of hospitals than of commercial firms. With a mean of 2.75 for trusting commercial firms, compared to a mean of 3.58 for trusting hospitals; a t-test with a 99% confidence interval concluded that the difference is significant (Two-tailed sigma of 0.000).

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	99% Confidence Interval of the Difference Lower	Upper			
Pair 1	Trust_Companies - Trust_Hospitals	-.824	1.093	.098	-1.080	-.568	-8.429	124	.000

Figure 3. T-Test trust companies & hospitals

This is confirmed by the control variable "Do you trust hospitals more with your personal data than commercial firms?" with 101 out of 125 respondents (80,8%) answering this question with "Agree" or "Strongly Agree". Important to note is that doctors are generally more trusted than hospitals (mean of 3.97) as an organisation. This is in line with past research done in the field. (Rahim et al., 2013)

Regarding future research, the mean is found to be 3.43; implying that there is not a substantial majority that wants their medical data to be used for future research purposes. Incentives are not generally found to be helpful in getting people to share more data (mean of 2.64).

4.4.2 Changes of disclosing behaviour following GDPR

Utilising a Paired Sample T-test, a clear distinction can be found between disclosure behaviour in the case of a light disease and in the case of severe disease. For each category, the two-tailed sigma gave a result of 0.000; meaning that there is a significant difference in disclosing behaviour between severe and light diseases (confidence interval of 99%).

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	99% Confidence Interval of the Difference Lower	Upper			
Pair 1	Basic_Light – Basic_Heavy	-.760	.712	.064	-.927	-.593	-11.940	124	.000
Pair 2	GDPR_Light – GDPR_Heavy	-.704	.696	.062	-.867	-.541	-11.311	124	.000
Pair 3	Opt_Light – Opt_Heavy	-.664	.761	.068	-.842	-.486	-9.750	124	.000
Pair 4	Quality_Light – Quality_Heavy	-.560	.689	.062	-.721	-.399	-9.092	124	.000

Figure 4. T-Test light-severe disease

Looking at the influences of GDPR security measures, the possibility of opting out (utilising the Right to Erasure), and the influence of Quality of Care show more effects on the disclosing behaviour of the data subjects by using a Paired Sample T-test.

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	99% Confidence Interval of the Difference Lower	Upper			
Pair 1	Basic_Light – GDPR_Light	-.072	.443	.040	-.176	.032	-1.816	124	.072
Pair 2	Basic_Heavy – GDPR_Heavy	-.016	.458	.041	-.123	.091	-.391	124	.697
Pair 3	Basic_Light – Opt_Light	-.232	.649	.058	-.384	-.080	-3.995	124	.000
Pair 4	Basic_Heavy – Opt_Heavy	-.136	.600	.054	-.276	.004	-2.533	124	.013
Pair 5	Basic_Light – Quality_Light	-.272	.734	.066	-.444	-.100	-4.145	124	.000
Pair 6	Basic_Heavy – Quality_Heavy	-.072	.709	.063	-.238	.094	-1.135	124	.258

Figure 5. T-Test between categories

The data user being told about the fact that organisations need to have their data security as a top priority to avoid hefty fines, did not influence the disclosing behaviour of data subjects significantly for either light (Two-tailed sigma of 0.072 with a Confidence Interval of 99%) or severe (Sigma of 0.697).

The other influence of GDPR, namely the ability to Opt-Out (utilising the Right to Erasure) does have a positive effect in people's disclosing behaviour for light diseases (Sigma of 0.000), while for severe diseases this conclusion can barely not be drawn based on a 99% confidence interval: sigma of 0.013).

Learning that the hospital needs further access to the person's data, once again marks a significant change for light diseases (0.000); but disclosing behaviour for severe diseases does not change significantly (sigma of 0.258).

Important to note is that the reliability analysis between questions shows a high covariance, with a Cronbach's alpha of 0.896; meaning that the reliability of the questions asked is good (see Appendix C1).

4.4.3 Future research and incentives

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	99% Confidence Interval of the Difference Lower	Upper			
Pair 1	Fut_Research_Light – Fut_Research_Heavy	-.432	.945	.084	-.653	-.211	-5.112	124	.000
Pair 2	Monetary_Light – Monetary_Heavy	-.416	.952	.085	-.639	-.193	-4.886	124	.000
Pair 3	Discount_Light – Discount_Heavy	-.152	.708	.063	-.318	.014	-2.401	124	.018

Figure 6. T-test light-severe incentives

In terms of disparity between light and severe diseases, a significant difference is found within two of the three categories investigated. With a two-tailed sigma of 0.000 (99% confidence interval), people tend to disclose more of their personal information for future research in the case of a severe disease than in the case of a light disease. This is the case without monetary incentives, as well as when the hospital does provide a monetary incentive. When health insurance comes into play, there is no significant difference found between light and severe disease (sigma of 0.018, slightly above the alpha of 0.01 following the 99% confidence interval).

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	99% Confidence Interval of the Difference Lower	Upper			
Pair 1	Fut_Research_Light – Monetary_Light	-.008	.778	.070	-.190	.174	-.115	124	.909
Pair 2	Fut_Research_Heavy – Monetary_Heavy	.008	.746	.067	-.167	.183	.120	124	.905
Pair 3	Fut_Research_Light – Discount_Light	.408	1.165	.104	.135	.681	3.917	124	.000
Pair 4	Fut_Research_Heavy – Discount_Heavy	.688	1.214	.109	.404	.972	6.335	124	.000

Figure 7. T-test incentives

Assessing whether monetary incentives or discount on healthcare have a positive influence on disclosing behaviour, a paired t-test is conducted and results in the following: for neither the light or the severe disease does the disclosing behaviour of patients radically change (Sigma's of 0.909 and 0.905 respectively, see Appendix C2). When the health insurance comes into play, there is a significant difference found (Sigma's of 0.000); but it is a negative change. The mean decreases from 2.77 to 2.36 in the case of light disease, and the mean declines from 3.20 to 2.51 in the case of severe disease – showing that people want to disclose less when a third party (i.e. health insurance) is involved.

To ensure the reliability of the asked questions, the Cronbach's Alpha was tested and found to be 0.905; showing excellent reliability (see Appendix C3).

5. DISCUSSION

The research had the intention to gain insights on the preparation of various healthcare institutions for the General Data Protection Regulation, how a change in disclosing behaviour can affect the quality of care that healthcare institutions can offer, and how disclosing behaviour might change following the new regulations.

5.1 Hypotheses outcomes

5.1.1 Hypothesis 1

H1: Patients suffering from a severe disease are likelier to disclose their personal data compared to patients that have a minor disease.

Based on the Paired Sample T-test, it is confirmed that patients are likelier to share more of their data (or with more people) in the case of a more severe disease (cancer symptoms) than in the case of a lighter disease. While the disclosing behaviour increases in every scenario (Security improvement of GDPR, Opt-Out possibility in GDPR and the hospital asking to disclose more information since they need more information for further treatment), the difference between light and severe disease is

significant in every situation. This means that people will still be more reluctant to share data when it only concerns a minor disease, even when the quality of care is at stake or when there are assurances that security measures are met. Thus, we confirm *H1*.

Hypotheses 2-3

H2: Patients that suffered from a severe disease are likelier to disclose their personal data for future research than people that suffered from a minor disease

Comparing the difference in means, we see that people are likely to allow healthcare institutions to access their data for future research when they have suffered from a severe disease. Only 2 out of 125 respondents (1.6%) had the desire to have their data unavailable for future research in the case of their cancer being cured, while 9 respondents (7.2%) had that desire in the case of a broken arm.

Pseudonymisation was also a more popular alternative when the patient experienced cancer-symptoms, with 28% opting for this scenario compared to 16.8% in the case of a broken arm. This can be explained since cancer has a possibility of recurring in the future. (Ojha & Goel, 2017) With people potentially aware of this, they might be likelier to opt for this solution. Therefore, we confirm *H2*.

H3: Monetary incentives and discounts on healthcare insurance will significantly increase the number of people willing to disclose their data for future research.

In the case of monetary incentives, the difference in disclosing behaviour for future research is not significant for either light or severe disease. Monetary incentives are thus not proven to be more useful in getting people to disclose more information for future research.

In the case of discounts on health insurance, there is a significant difference in the case of both light and severe diseases. Delving into the data, the difference is a negative change rather than an increase in disclosing behaviour. Where only 2 out of 125 respondents did not want to share their personal data without incentives (in the case of cancer), 33 decided to opt-out of sharing data for future research when health insurance got involved. An explanation could be that people do not want their health insurance provider to know the details of their health situation, showing a lack of trust compared to what they were willing to disclose to healthcare institutions. This shows a disparity with the research done by Gómez-Barroso et al., that stated that monetary incentives would have a positive effect on disclosing behaviour (Gómez-Barroso et al., 2018). Based on this, we reject *H3*.

5.1.2 Hypothesis 4

H4: The perceived risk of disclosing personal data will decrease following GDPR laws

The perceived risk of disclosing personal data was only found to be decreasing (more people were willing to share more) in the case of light diseases. Finding out about the Opt-Out possibility of GDPR, where patients can choose to have the organisation remove all their data upon request, a significant change was found (Sigma of 0.000). Learning about the fact that security measures are a top-priority following GDPR did not have a significant difference between disclosing behaviour for either light diseases or severe diseases. The Opt-Out possibility was barely found to not be conclusive in a 99% confidence interval (alpha = 0.99) with a Sigma of 0.013. From these findings, it is clear that people value the possibility of having their data removed upon request. Hence, *H4* is partly confirmed: the opting-out part of the GDPR laws decreases perceived risk of disclosing data.

5.1.3 Hypotheses 5-6

H5: The amount of time spent on administrative tasks will increase significantly following the introduction of GDPR.

The practitioners all agreed on the fact that they currently have to spend more time on administrative tasks and how attentive they must be of the patient's privacy data. Quick communication with external practices (e.g. hospitals, municipalities) need more care and quick namedropping of patients is out of the question now. It requires more effort to look up a patients client number following an e-mail or phone call, rather than quickly discussing the patient by name. The CIO at ZGT estimated that thirty extra minutes per day were spent on administrative tasks. Thus, *H5* is confirmed.

H6: The quality of care that healthcare institutions can provide will decrease following the introduction of GDPR.

Based on the interviews with the treating practitioners, no direct relationship could be found between the quality of care and the introduction of the GDPR. However, following the confirmation of *H5*, it can be argued that the quality of care is indirectly influenced by the fact that more time has to be spent on administrative tasks by all people involved. With every practitioner stating that they have to get used to the new law and that it is so far inconvenient and time-consuming, the assumption can be made that the quality of care indirectly takes a minor hit in the short term. On the other hand, the same practitioners argue that the law has benefits as well; stating that being attentive of a patients' privacy is only beneficiary and can only be perceived as positive in the patients' mind.

The CIO at ZGT states that collaboration with other organisations has become more difficult and has a direct influence on the quality of care.

While none of the practices has had examples of patients refusing to disclose their personal data to the organisation itself, the survey showed that many people's perceptions are already changing and that this might change in the future. Asked what the influences of limited consent could be, the practices said that in some cases the organisation could not offer the service they are asked to do or that it severely limits how their job is done (e.g. when they have to consult external practitioners). Summing up all three interviews, *H6* can neither be confirmed nor rejected.

5.2 Conclusion

Clear from the results of the survey is that people that have suffered from a severe disease are less 'careful' with their information than people with a light disease; with monetary incentives not having a significant positive influence on the disclosing behaviour or a positive influence at all.

While a direct influence on the quality of care is not directly noticed by the practicing employees working in health care clinics following the introduction of GDPR, a change of disclosing behaviour is admitted to be a potential problem: the quality of the treatment could suffer due to time-consuming processes of having to fill out more consent forms per individual doctor. This change in disclosing behaviour is not yet apparent, but as the results of the survey show: people's disclosing behaviour might in fact change as they become more privacy-aware. Since the GDPR is enforced, people might become increasingly aware of becoming owners of their data and this could have direct influences on the quality of care that healthcare institutions can offer. However, the survey results show that the protection and opt-out possibilities that come with the new regulation have a positive influence on people's disclosing behaviour; people tend to share more when they know that GDPR enforces security measures and that they always have the possibility to have their data removed. The survey results show

that people value the possibility of customising their privacy settings (73.6% agreeing or strongly agreeing), like it is currently possible on social media such as Facebook or Twitter. Corresponding with research done by O'Connor et al., with people showing a strong desire to gain more personal control over their health information. (O'Connor et al., 2017)

As of now, most organisations are not convinced that GDPR has had a significant influence on their quality of care. The negative consequences are minor, but noteworthy: processes regarding administration are inefficient, time-consuming and lead to annoyance. The CIO at the hospital, on the contrary, believes that it absolutely had an influence on the quality of care; namely in collaboration with other organisations.

While organisations admit that they might not be fully compliant with GDPR, the recommendations by Tikkinen-Piri et al. in 2018 are followed up mostly by all the organisations where the research was conducted. A data protection officer was appointed, the 'right to data portability' is utilized, informed consent is asked prior to treatment and the 'right to erasure' is easily enforced upon request. The only recommendation that was unclear for any organisation but the hospital, was the 'Reckoning with sanctions for non-compliance'. In both the clinic and the general practitioner's office, it was not clear whether there were sanctions for improper use of personal data.

For a full comparison between organisations, see the table in Appendix D.

6. LIMITATIONS

Several limitations arose in our study when conducting research. First of all, our survey was distributed mostly among healthy people that did not actually suffered from the diseases we mentioned (broken arm or cancer-symptoms). While results in the real scenario should be similar, patients that speak in a hypothetical sense might still act differently compared to people that actually suffer from the disease when discussing disclosing behaviour. Another issue that came to light was that the survey was only available in English, even though the majority of respondents were either German or Dutch; and thus not all fluent in English. An issue of validity also comes into effect, as not all age-groups were represented equally; with peers mostly being between the age of 20 and 30.

Secondly, due to budget and time constraints, the research was 'region-locked'; meaning that research could only be conducted within the Netherlands and Germany. During the first interview with the CIO of ZGT, he mentioned that he expects Germany and the Netherlands to be relatively well prepared to the adoption of GDPR when comparing it to countries in the south of Europe such as Portugal, Spain or Greece. Results from this study are thus not translatable to the entirety of Europe, especially since disclosing behaviour in these countries might also be very different.

Thirdly and perhaps most importantly, the study suffered from a time constraint and was limited due to the timing of the research as well. The research was conducted in the middle of the enforcement of GDPR, and it was severely noticeable when trying to schedule interviews. Potential interviewees such as the Data Protection Officer, the head of nursing or physicians simply could not find time within our timeframe; even though many shared that they were willing to help. The Data Protection Officers specifically, said that they could not find the time due to the interviews falling in the same timeframe as the introduction of the GDPR. Not everything was as airtight as it should be and a lot of work still had to be done. Therefore, they were too busy to comply with our interviews.

A fourth limitation, connected to the third, is that interviewees were not of similar disciplines in each case study. Ideally, it would have been appropriate if the functions of the interviewees within each case study would be the same or at least similar. For instance, an interview with the Chief Information Officer of both IrisZorg and ZiekenhuisGroep Twente. Unfortunately, due to the time constraint of this bachelor thesis and the lack of time of various asked people; it was impossible to schedule an interview with similar jobs at the various organisations.

A fifth limitation arises in the survey. Due to technical problems related to Google Forms, the description that preluded a question was not clear enough; and people thought they had to answer the same question repeatedly which might have skewed the data.

The final limitation comes because the dust is not entirely settled on the GDPR. Due to its novelty, with GDPR only being enforced for a few weeks since the writing of this thesis; consequences and influences of the introduction of the law on the quality of healthcare might not be evident just yet. Since its recency, interviewees stated that they have not noticed that clients have become more privacy-aware so far; time will tell whether this awareness will come into play and to what extent this may affect the quality of care and future research in the medical field.

7. FUTURE RESEARCH

It is vital to expand further on the final limitation mentioned. The recency of the law has positive effects on the research, but perceptions about personal data and people's disclosing behaviour might change the more prolonged the law is in effect; people may become increasingly aware of the fact that they are the owners of their personal data and thus behaviours might change. Therefore, research in the future can be done with a similar scope to assess whether the law has its desired effect and to see if there is indeed a change in disclosing behaviour and what the effect of this is on the quality of healthcare to be provided.

This study was also limited to the healthcare sector. It would be rather interesting to find out if disclosing behaviour changes even more in other sectors such as marketing or the financial industry due to the introduction of GDPR. The quality of the services provided in these services could also take a strong hit when they are reliant on people disclosing their personal data.

8. ACKNOWLEDGEMENTS

Thank you to my supervisors dr. Wijnhoven and dr. Loohuis. A special thanks to dr. Wijnhoven for setting us up with background information and with interview possibilities in the medical field. Secondly, thank you to Sven Kruthoff and Catrin Przyrowski for the collaboration in the bachelor thesis circle. A special thank you goes to all the interviewees and to all the respondents who completed the survey.

9. REFERENCES

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13–28. https://doi.org/10.2307/25148715

Cooper, D. R., & Schindler, P. S. (2014). *Business Research Methods* (12th ed.). Boston: McGraw-Hill/Irwin.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Culnan, M. J., & Bies, J. R. (2003). Consumer privacy: Balancing economic and justice consid- erations. *Journal of Social Issues*, *59*(2), 323–342. https://doi.org/doi:10.1111/1540-4560.00067

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

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*, 98–107. https://doi.org/10.1016/J.IJMEDINF.2017.12.004

Esmaeilzadeh, P. (2018). Healthcare consumers' opt-in intentions to Health Information Exchanges (HIEs): An empirical study. *Computers in Human Behavior*, *84*, 114–129. https://doi.org/10.1016/J.CHB.2018.02.029

General Data Protection Regulation. (2016). Retrieved April 15, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

Gómez-Barroso, J.-L., Feijóo, C., & Martínez-Martínez, I. J. (2018). Privacy calculus: Factors that influence the perception of benefit. *El Profesional de La Información*, *27*(2), 341–348.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. L. (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems*, *24*(2), 13–42. https://doi.org/10.2753/MIS0742-1222240202

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). *Death to the Privacy Calculus? SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2923806

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434–445. https://doi.org/10.1016/J.DSS.2011.01.017

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Mills, S. K., Yao, R. S., & Chan, Y. E. (2003). Privacy in Canadian Health Networks: challenges and opportunities. *Leadership in Health Services*, *16*(1), 1–10. https://doi.org/10.1108/13660750310458399

O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science*, *113*, 653–658. https://doi.org/10.1016/J.PROCS.2017.08.329

Ojha, U., & Goel, S. (2017). A study on prediction of breast cancer recurrence using data mining techniques. In *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence* (pp. 527–530). https://doi.org/10.1109/CONFLUENCE.2017.7943207

over IrisZorg. (2018). Retrieved June 12, 2018, from https://www.iriszorg.nl/over-iriszorgover-de-organisatie/aanbod-iriszorg

over zgt. (2018). Retrieved June 14, 2018, from https://www.zgt.nl/over-zgt/

Rahim, F. A., Ismail, Z., & Samy, G. N. (2013). Information privacy concerns in electronic healthcare records: A systematic literature review. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 504–509). https://doi.org/10.1109/ICRIIS.2013.6716760

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), e47. https://doi.org/10.2196/jmir.7108

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

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/J.CLSR.2017.05.015

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444.

Yin, R. K. (2014). *Case Study Research Design and Methods* (5th ed.). Thousand Oaks, California: Sage Publications.

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 & Management*, *55*(4), 482–493. https://doi.org/10.1016/J.IM.2017.11.003

10. APPENDICES

10.1 Appendix A: Survey questions

Would you say that

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Your Personal Data is important					
Your Personal Data is private					
You trust companies with your data					
Hospitals are a trustworthy institution					
You trust doctors to not take advantage of your private information					
You value the possibility of customising your privacy settings (e.g. like you can on Facebook)					
Monetary incentives could persuade you to share more data?					
Your medical history can be used for research purposes?					
You trust hospitals more with your personal data than commercial firms?					

You are admitted into a hospital with a broken arm. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

You are admitted into a hospital with a yet unknown disease, showing cancer symptoms. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

Under the new EU legislature for the General Data Protection Regulation, hospitals are required to improve the security and the procedure design of internal data handling. Hospitals and organisations can face heavy fines of up to 20 million euros in case of infringement, so security is a top priority.

You are admitted into a hospital with a broken arm. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

You are admitted into a hospital with a yet unknown disease, showing cancer symptoms. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

Opt-Out
After giving the data to the hospital, you have the option to opt out. This means that at any time after the treatment you can choose to have your data erased from any database. Does this change the way you look at your personal data?

You are admitted into a hospital with a broken arm. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

You are admitted into a hospital with a yet unknown disease, showing cancer symptoms. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

Quality of healthcare
The hospital reports that they cannot guarantee appropriate quality of healthcare if they do not possess the necessary information from your medical history.

You are admitted into a hospital with a broken arm. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

You are admitted into a hospital with a yet unknown disease, showing cancer symptoms. What personal data are you disclosing to the physician?

- You do not disclose any data about you.
- You give the treating physician full access to your data
- You give the treating physician full access to your data and the right to share to other physicians
- You give the treating physician full access to your data and the right to share and store your data over an indefinite time period

Future Research
The hospital requests your personal data to be used for future longitudinal studies, inquiring whether they can make use of it over a long period of time.

In the recent past you were admitted into a hospital with a broken arm and it has healed. Can the hospital use the data for this treatment for future research?

- You do not give them the right to use your data in the future.
- You give them the right to use your data, under the condition that your data is anonymized (cannot be traced back to you)
- You give them the right to use your data, under the condition that your data is pseudonymized (can be traced back to you in the case of a breakthrough)
- You give them the right to use your data, under the condition that your data is encrypted (only authorised users can access your data)
- You give them full rights to use your data.

In the recent past, you have undergone treatment for cancer and you are cured. Can the hospital use the data for this treatment for future research?

- You do not give them the right to use your data in the future.
- You give them the right to use your data, under the condition that your data is anonymized (cannot be traced back to you)
- You give them the right to use your data, under the condition that your data is pseudonymized (can be traced back to you in the case of a breakthrough)
- You give them the right to use your data, under the condition that your data is encrypted (only authorised users can access your data)
- You give them full rights to use your data.

Future Research and incentives
The hospital requests your personal data to be used for future longitudinal studies, inquiring whether they can make use of it over a long period of time. They offer you a monetary compensation in exchange for your data, are you willing to do so?

In the recent past you were admitted into a hospital with a broken arm. Can the hospital use the data for this treatment for future research now that they offer money in exchange?

- You do not give them the right to use your data in the future.
- You give them the right to use your data, under the condition that your data is anonymized (cannot be traced back to you)
- You give them the right to use your data, under the condition that your data is pseudonymized (can be traced back to you in the case of a breakthrough)
- You give them the right to use your data, under the condition that your data is encrypted (only authorised users can access your data)
- You give them full rights to use your data.

In the recent past, you have undergone treatment for cancer. Can the hospital use the data for this treatment for future research now that they offer money in exchange?

- You do not give them the right to use your data in the future.
- You give them the right to use your data, under the condition that your data is anonymized (cannot be traced back to you)
- You give them the right to use your data, under the condition that your data is pseudonymized (can be traced back to you in the case of a breakthrough)
- You give them the right to use your data, under the condition that your data is encrypted (only authorised users can access your data)
- You give them full rights to use your data.

In the recent past you were admitted into a hospital with a broken arm. The hospital requests you to share your data with them and with your insurance company in exchange for discounts on your health insurance. Do you give consent?

- You do not give them the right to use your data in the future.
- You give them the right to use your data, under the condition that your data is anonymized (cannot be traced back to you)
- You give them the right to use your data, under the condition that your data is pseudonymized (can be traced back to you in the case of a breakthrough)
- You give them the right to use your data, under the condition that your data is encrypted (only authorised users can access your data)
- You give them full rights to use your data.

In the recent past, you have undergone treatment for cancer. The hospital requests you to share your data with them and with your insurance company in exchange for discounts on your health insurance. Do you give consent?

- You do not give them the right to use your data in the future.
- You give them the right to use your data, under the condition that your data is anonymized (cannot be traced back to you)
- You give them the right to use your data, under the condition that your data is pseudonymized (can be traced back to you in the case of a breakthrough)
- You give them the right to use your data, under the condition that your data is encrypted (only authorised users can access your data)
- You give them full rights to use your data.

10.2 Appendix B: Case Study Questions

The Healthcare institution in general:

- Information about hospital/rehabilitation clinic:
    - Ownership (non-profit, for-profit, federal)
    - Size
    - Location (rural/urban)
    - Teaching status
    - Systems applied
    - Integration with physicians
    - Culture
    - Leadership
    - IT history
    - Capability
- 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?

Quality of care:

- 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 organisation has personnel who have technical expertise to be able to identify and resolve data breaches involving the unauthorised 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 patient's disclosing behaviour?

Research:

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

10.3 Appendix C: SPSS Outputs

10.3.1 Appendix C1: Cronbach's Alpha for light and severe diseases, GDPR, opt-out, quality of care.

Reliability Statistics

Cronbach's Alpha	N of Items
.896	8

10.3.2 Appendix C2: Means t-test

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Fut_Research_Light	2.77	125	1.158	.104
	Fut_Research_Heavy	3.20	125	1.136	.102
Pair 2	Monetary_Light	2.78	125	1.211	.108
	Monetary_Heavy	3.19	125	1.169	.105
Pair 3	Discount_Light	2.36	125	1.253	.112
	Discount_Heavy	2.51	125	1.324	.118

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Fut_Research_Light & Fut_Research_Heavy	125	.661	.000
Pair 2	Monetary_Light & Monetary_Heavy	125	.680	.000
Pair 3	Discount_Light & Discount_Heavy	125	.851	.000

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	99% Confidence Interval of the Difference Lower	Upper			
Pair 1	Fut_Research_Light - Fut_Research_Heavy	-.432	.945	.084	-.653	-.211	-5.112	124	.000
Pair 2	Monetary_Light - Monetary_Heavy	-.416	.952	.085	-.639	-.193	-4.886	124	.000
Pair 3	Discount_Light - Discount_Heavy	-.152	.708	.063	-.318	.014	-2.401	124	.018

10.3.3 Appendix C3: Cronbach's Alpha for Future Research/Monetary Incentives

Reliability Statistics

Cronbach's Alpha	N of Items
.905	6

10.4 Appendix D: Table of comparisons between organisations

Theoretical comparison between organisations							
Organisation	**When preparations started**	**Influence of GDPR on Quality of Care**	**Changes in disclosing behaviour of patients** (Dinev & Hart, 2006; Esmaeilzadeh, 2018; Zhang et al., 2018)	**Appointment of Data Protection Officer** (Tikkinen-Piri, Rohunen, & Markkula, 2018)	**Penalties for privacy breaches** (Tikkinen-Piri et al., 2018)	**Incentives** (Gómez-Barroso, Feijóo, & Martínez-Martínez, 2018)	**Security measures to prevent dataleaks** (Entzeridou, Markopoulou, & Mollaki, 2018)
IrisZorg	Spring 2018	Small, negative influence. More time-consuming and annoyance.	Nothing new	Appointed	Not aware.	Not offered	Nothing notable, already very privacy secure prior to GDPR
ZiekenhuisGroep Twente	Early 2016, when GDPR was announced.	Large negative influence, namely in collaboration with external organisations.	Multiple talks with patients by the CIO, doctor also discussing privacy with the patient. Some people do not give consent anymore.	Appointed	Yellow (warning) and red card (dismissal) system.	"Do not have time to convince patients."	Minor changes in the Information Systems. "GDPR based on the former Dutch privacy law, so system was already up to date."
Geutingshof	April 2018	No significant change. It's positive that employees are more privacy aware, but it is very time-consuming administratively.	Patients asked questions, but nothing changed.	Appointed	Not aware.	Not offered.	No changes in the Information Systems.