Authorization, privacy and informed consent – Who is allowed access to which medical information?

The development of an authorization model for the Datakluis application

A master thesis at Topicus

Edo Kant

29-06-2020

Abstract

The goal of this research project is to develop an authorization model for the Datakluis application, which is used in the sharing of medical information of patients from GPs to healthcare professionals. The purpose of the model is to help determine which medical information an outside party is authorized to access when this information is shared with them. Examples include when a patient is referred or a consultation is done concerning this patient. To do so, a literature review on access control, privacy and electronic health records in the systems of GPs have been done at first. An existing process at Topicus is analysed in which medical information of patients is shared with other parties for the care of several chronic diseases. Afterwards, interviews are done to gather the requirements for the authorization model. These are done with employees of Topicus and employees of healthcare groups who represent the healthcare professionals in question. Based on the literature review, an exploratory review of the GDPR law on privacy and an overview of the requirements from the two parties, an improved version of the existing process is made at first. Then, based on the improved process, a future-proof authorization model for the Datakluis is developed, upon which new process and actions for the sharing of medical information can be based. In this authorization model, the essential parts of information concerning authorization are described which should be stored when medical information is shared. The core steps in which this information is generated are described as well as the steps on how to retrieve this information.
This improved process and the authorization model have been developed successfully. Outcomes to the process include, among others, that the Role Based Access Control approach is a suitable access control approach for the model. A new step in which GPs can choose to omit or add medical information is added as well as new kinds of medical information which can be shared in this process. However, how to implement informed consent, in this case, has turned out to be a challenging subject, so more research on this is needed, in which the outcomes of this project can be taken into account.

Table of contents

1. Introduction

1.1 Preface

Patients value their legal right for privacy, as can be read in the publication by Meslin et al. [3].
If one would ask patients whether they would agree that all of their medical information could be shared to all kinds of parties for all intents and purposes, many would be inclined to say no. However, medical professionals need to have access to certain medical information of the patients in order to do their job and deliver care of a proper quality. Furthermore the systems and applications which manage this exchange of information need to have a manageable solution in order to facilitate all of this.

In this master thesis a case at Topicus will be researched. In the Datakluis application personal health information of patients is temporarily stored. Among other uses, this application is used in order to provide certain types of healthcare providers with personal health information about patients in the case of referrals and consultations. But which medical professionals should have access to which medical information of patients in which scenario? And how should an authorization model which would determine this work as multiple types of access control models exist? And what is a proper approach to take both privacy and informed consent into account? Finding a proper approach for authorization which takes into account the requirements from multiple parties as well as the legal requirements is a challenge.
In this project an authorization model is developed for the case at Topicus, after which the lessons and gathered knowledge may be added to the scientific literature on this subject.

1.2 Structure of the thesis

In order to develop a proper authorization model, multiple steps have to be undertaken. In order to explain the process of the project this thesis is structured in the following manner:

Further on in this introduction the wider context within which this project takes place will be elaborated upon. Afterwards the company within which this research project takes place, Topicus, will be introduced and the specific case in question will be explained. As a conclusion of the introduction the research questions and the added value of this project will be stated.

The research methodology is explained in chapter 2. The main phases of the research project in which the research questions will be answered are explained in detail.
In order to take literature on this subject into account a literature review has been done, which is described in chapter 3. This literature review has multiple functions: It serves as an exploratory research on the relevant subjects in order to gather more knowledge on the current state of the art of the researched subjects. It will also be used in order to provide insight in how the research subjects relate to each other, which will be summarized in a conceptual model. The conceptual model of requirements and other insights from literature are factors that are used in order to determine a proper research method and to construct an initial list of interview questions for the external parties. Furthermore the model in which the five aspects for an authorization process for EHR systems is designed based on the literature review.
In chapter 4 the current state of affairs at the case in question is explained. The approach of authorization in the process in which the PHI of patients is shared in the VIPlive application is explained.
In chapter 5 the results of the interviews will be elaborated upon, following the structure of the model concerning the aspects of an authorization process for EHR systems.
In chapter 6 the results of an exploratory analysis of the GDPR is explained.
In chapter 7 an improved version of the aforementioned process in which medical information is shared using VIPlive is developed. This will be done using the structure of the model of the aspects of an authorization process and based on the literature review and the results of the interviews. Based on this improved process a new authorization model is designed for the Datakluis.
In chapter 8 the conclusion for this research project will be given.
In chapter 9, the discussion, the limitations for this research project are described as well as recommendations for further research.

1.3 Context of the project

In order to provide care of a proper quality it is necessary for medical professionals to have access to certain medical information of the patients, as described by Caine and Tierney [5]. It is necessary for healthcare providers to have a health record in which the medical information can be stored.

However, there are many different kinds of healthcare professionals and many patients will be referred from their general practitioner to others for more specialized care. It is important in healthcare to have certain forms of cooperation between professionals of different medical specialisations, who have separate health records of their patients. Two examples of this kind of cooperation are to refer patients to other medical professionals or to ask for a medical consultation. There are other forms of cooperation which are left out of scope for this research project. These include a form of multidisciplinary care which is becoming more common in the Netherlands, in which a group of medical professionals share the responsibility of the care of a patient, as described in the Dutch law [21]. Another example is to have a multidisciplinary consultation on either a single patient or a group of patients, in this example medical information of the patients can be shared as well.
In the cases of a referral or a consultation it is necessary for the healthcare providers to either send the receiving party medical information or to give the other professional access to (part of) the health record concerning the patient. For healthcare professionals it is of vital importance to have access to the right medical information in order to provide care of a proper quality [5]. For example, if part of the relevant information in the health history of a patient isn't sent along in a referral, the receiving professional might miss vital details for his own treatment which can lead to mistakes, like the wrong diagnosis for example.

Within a chain of care, which is called 'ketenzorg' in Dutch, for example it is very important to transfer the right health information of patients to the other providers of care. A chain of care concerns the treatment of patients with a chronic illness, like diabetes or COPD, as can be read on the website www.regiozorgnu.nl. In a chain of care professionals from multiple medical disciplines are involved who will have to cooperate in a certain sense and have to take factors outside of their own practice into account. In order to improve the quality of life of these patients with chronic illnesses, this is very important. The main part of the treatment and control of this illness will take place at the general practitioner, but he or she will also refer patients to professionals of other medical disciplines. Medical consultations with other professionals will also have to take place. In both cases it is important that medical information about the patients is shared or that access is granted to (part of) the medical record.

But which healthcare provider should be able to access which PHI of patients in which scenario? Many find it a valuable principle that healthcare providers should only be able to access the medical information that they actually need to to do their job and provide care in a proper way. [3] Authorization for EHR systems, to determine which party is able to access which parts of the information, is the key to achieve this.

However, there are many kinds of EHRs and many methods on how to handle authorization. In the Netherlands an initiative was once started for a national system which was called 'Het landelijk EPD'. Although the name seems to suggest that it would be an EHR, it would not include a central database in which the information of patients would be stored. The medical information would still be stored in the local systems of healthcare providers. The idea was that by using the 'landelijk EPD' providers of healthcare could send a request for medical information of a patient, which would come from the systems of other healthcare providers.
However in 2011 the Dutch senate voted against the plans [23]. Part of the original plan, the LSP (the 'Landelijk Schakelpunt' in Dutch) was re-launched in 2012 with the help of Dutch health insurance companies and is in practice today.
It is quite different however when compared to the original plans [24]. The main differences of the current implementation of the LSP compared to the original plans of the 'landelijk EPD' are:

- Every patient has to give permission explicitly
- Providers of healthcare aren't obliged to participate
- The current system is implemented regionally, although the original plan was to implement a national system

As there currently is no national system there are many systems and applications in practice in the Netherlands. There are many different kinds of EHRs which are applied as well as many applications that are used for example to make consultations and referrals to other healthcare providers possible. However, as all of these systems and applications are quite different, they do not necessarily follow the same rules and practices or use the same frameworks. Many different methods and practices are used on the subject of sharing medical information between involved parties. There currently are many approaches and arrangements for access control in the context of the sharing PHI in place in the Netherlands.
One example is the case in question of this project.

1.4 Explanation of the case in question

Topicus is an IT company in the Netherlands, with over 1000 employees at the moment, as can be read on www.topicus.nl. It has 14 settlements in multiple cities like Deventer and is active in multiple sectors like finance, education and healthcare.
The VIPlive application of Topicus is connected to many practices of general practitioners in the

Netherlands, who are connected to other healthcare providers within a healthcare group (zorggroep in Dutch). The GPs can refer patients, that suffer from a chronic illness like COPD or diabetes for example, to other healthcare providers within the healthcare group using the VIPlive application. Consultations can also be performed using the VIPlive application.
Every quartile VIPlive receives medical information of patients from the information system of the general practitioner, the 'Huisarts Informatie Systeem' or HIS. This process is called an extraction. When a general practitioner performs a referral or a consultation to another healthcare provider within the healthcare group, like a medical specialist, he or she gives the other party access to part of the medical information.

These referrals and consultations take place within a healthcare group. A healthcare group is an organization in which multiple providers of healthcare are connected through the earlier mentioned chains of care. The goal of a healthcare group is to provide care for patients with chronic illnesses like diabetes, COPD, cardiovascular illnesses etc. Each healthcare group is responsible for delivering this care in a certain region of the Netherlands. A general practitioner within one of these healthcare groups can refer a patient with a chronic illness to other healthcare provider within the same healthcare groups.

Topicus has made separate agreements on the subject of authorization with each healthcare group that is connected to VIPlive. These agreements are based on role based access control models that take into account the disease of the patient and the profession of the receiving healthcare provider. For example: A healthcare group based in a certain city will have written in this agreement which medical information a podotherapist will be able to have access to when a patient with diabetes is referred to him or her from a GP. The access control agreements of every connected healthcare group on the relevant diseases are stored within the VIPlive application.

Due to the fact that VIPlive receives the medical information from the extractions only once per quartile the medical information that access is provided towards may be out of date at the time of a referral or consultation. This is why Topicus has started the development of a new system in cooperation with the suppliers of HIS systems. By using this system, medical information of the patients can be send from the HIS to VIPlive between the quarterly extractions. When a general practitioner opens the Topicus software from his or her HIS, a so-called 'professional summary' of the medical file of the patient will be sent towards VIPlive.
Therefore there are two kinds of medical information that originate from the HIS systems of the general practitioners: The data that Topicus has received due to the quarterly extractions and the professional summaries that can be send whenever a general practitioner opens his or her HIS. The general practitioner can choose whether to give access to data from the quarterly extractions or professional summaries in the case of referral or consultation.
A new system called the Datakluis is currently in development. The goal of this application in short is to temporarily store the two abovementioned kinds of information from patients, so that it can be shared with receiving healthcare professionals.
Furthermore It is important to note that when medical information is shared with another party, it is not simply sent like information added to an email. Instead, when other parties are authorized for medical information of a patient, they are allowed to gain access to that part of the information from the Datakluis. So when a GP for example makes a referral for a patient to a dietician, the GP authorizes the dietician to access certain parts of the medical information that is stored in the Datakluis. In order to make this possible certain information about an authorization should be stored in the Datakluis, so that it is clear which party is authorized to access which information.
Furthermore, when another party has received a referral for example and wants to access the

medical information, certain steps will have to be taken using the information concerning the authorization. These steps will check whether the dietician actually is authorized to view part of the medical information of that specific patient, and if so, which parts of it.

But which party should be able to have access to which data, considering both the professional summaries and the data from the extractions? Which data should the receiving healthcare provider be able to access when a patient is referred to him or her or when a GP requests a consultation? These questions can be answered by the use of an authorization model, which the Datakluis currently does not have yet. Therefore the final goal of this project is to develop a proper authorization model for this purpose.

In order to do so, the current process in which medical information is shared using the VIPlive application will be analysed. The requirements from Topicus and from the healthcare groups for such a model will be gathered and kept into account when developing such a model. As mentioned before, there are laws, rules and/or standards on the subjects of privacy, informed consent and access control/authorization which are relevant as well. Although not all of these can be researched within this project, an exploratory analysis of the GDPR (AVG in Dutch) will be done. An improved version of the process in which information is shared using the VIPlive application will be developed. And based on this process an authorization model for the Datakluis will be developed. In this model, it will be explained which information concerning authorization should be stored when a healthcare professional is authorized to access part of the medical information. Furthermore this model will describe the core steps which should be taken to generate this information as well as the core steps for receiving healthcare professionals to access the medical information. Future authorization processes, which potentially could use different applications than VIPlive, can be developed based on this new authorization model.
To summarize, an overview of the processes and the contribution of this project has been made in figure 1.

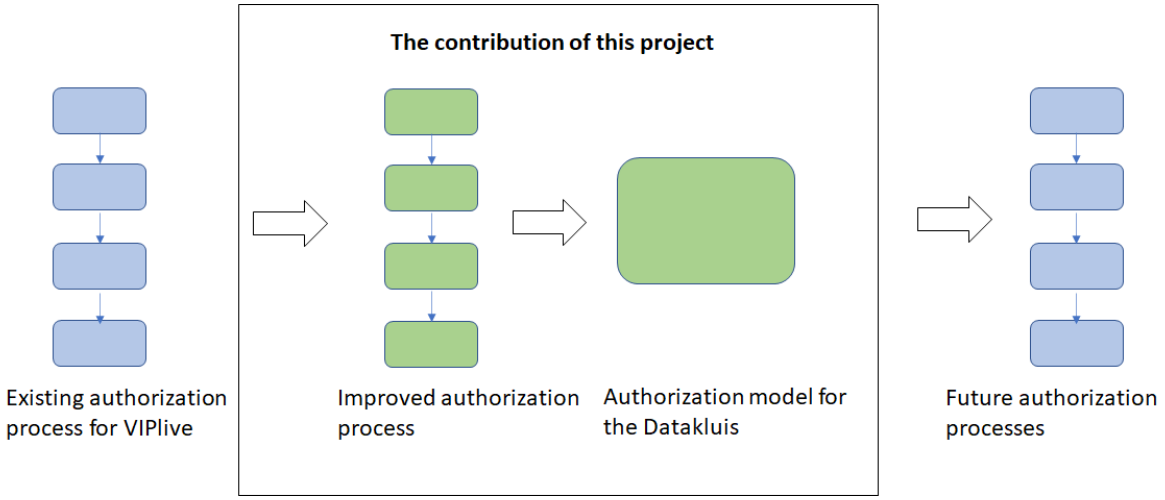


Figure 1. An overview of the contribution of this research project

1.5 Research questions

The main research question is:
What would be an appropriate authorization model for the Datakluis that determines which

healthcare providers are allowed to access to which medical information of patients in which case, taking into account the requirements of multiple stakeholders?

In order to answer the main research question, multiple sub questions have been stated:

1. Which methods and approaches for access control in the context of general practice EHRs, which take privacy and informed consent into account, are suggested in scientific literature?
2. What would be an appropriate authorization model for the case in question which determines which parties are allowed to access which medical information of patients?
    a. What approach for authorization is currently applied in the exchange of medical information between GPs and healthcare groups by the use of the VIPlive application at Topicus?
    b. What are the requirements from Topicus for this particular authorization model?
    c. What are the requirements from the healthcare groups for this particular authorization model?
    d. What should be the role of informed consent in the improved process and authorization model of the Datakluis?
    e. What would be an appropriate improved version of the authorization approach in the aforementioned process in which medical information is exchanged?

The added value of this research project will be:

- To gather the requirements from both a selection of healthcare groups and Topicus itself on an authorization model in this case
- To do a short exploratory analysis of the legal requirements of the GDPR for such an authorization model
- To develop an improved version of the authorization process for the sharing of medical information between the GPs and receiving parties with the use of VIPlive
- To construct an authorization model based on the gathered knowledge and requirements
- The insight and knowledge gathered during this project can provide an addition to the discussion and literature on how authorization in the sharing of medical information should be handled. Knowledge like how the requirements from different stakeholders can be kept into account as well as the legal requirements. Other parties in the Netherlands, or even outside of the Netherlands, could use these insights in their own process on developing or improving their approach on authorization to medical information.

2. Methodology

In order to provide an answer to the main research question as well as the sub-questions, a research methodology has been stated. This methodology has been developed based on exploratory research, document analysis, internal interviews at Topicus at the first part of the project as well as the results of the literature review of chapter 2.

Within this research, five main parts are recognized. Each will be explained in detail below.

1. The literature review
2. Preliminary research concerning the case in question
3. The gathering of requirements
4. An exploratory review of the GDPR

5. The development of the improved process and the authorization model

2.1 The literature review

The approach that was used for the literature review is based on the work of Wolfswinkel, Furtmueller and Wilderom [6]. They propose a five-stage grounded theory method to review the literature, which can be used iteratively. In the first stage of the method, 'define', the following steps have been made.

The primary fields of research have been chosen to be:

- Access control to electronic health records
- Electronic health records for general practice
- Informed consent for medical information

The secondary fields of research, researched for context purposes, have been chosen to be:

- Privacy in the context of electronic health records
- Electronic health records in general

This literature review has focused on the three primary fields of research. The highest priority was set on the combination of all three of the primary subjects. A lower priority was set on the combinations of two of the primary research subjects and subsequently a single primary research subject and the secondary fields of research.

The criteria for inclusion/exclusion into the literature research have been defined as follows:

- The paper has to discuss one or more of the main subjects in the literature research.
- The source of the paper has to be of a proper quality. Literature found in Scopus and Web of Science are considered to be of a proper source.
- Papers concerning modern technology should not be from an earlier year than 2010
    - An exception is made for the paper of Peleg, Beimel, Dori and Denekamp [15] from 2008. This is because the utility was considered to be high enough for this research and it properly describes a good example of a different method of access control than RBAC.
- Related subjects that are left out of scope for this research project include:
    - Pseudonymization of patient's identity
    - Encrypting the data of patients
    - Privacy-preserving data publishing
    - Authentication
    - Transmission protection during the transition of health care data between two parties
    - Protection of data in storage

The outlets and databases that have been chosen are Scopus and Web of Science. In order to find relevant literature, the main search terms that were applied are: Electronic health record, general practice, privacy, access control and informed consent.

The sample of paper has been refined in order to filter out the unusable articles and to keep a small sample of texts that are useful for this research. Many double results have been found and have been filtered out of the sample.
The inclusion and exclusion criteria have been applied while reading the title and abstract of the texts

and any texts that didn't fit the criteria were left out of the sample. The remaining articles were refined based on the reading of the full texts.
A significantly smaller sample was left after these steps were taken. Lastly, after all the search strings have been used, the forward and backward citations of the articles were checked in order to see if they contain other texts that are useful for this research. The same criteria of inclusion and exclusion were applied in this step of the process.

The final sample of texts has been thoroughly analysed. Useful findings and insights found in the texts have been highlighted, in this manner a large amount of excerpts have been gathered. Based on these excerpts, this literature review has been written.

In order to provide a clear picture of the context of the research, the subjects of Electronic Health Records and privacy will be elaborated upon first. Afterwards, the results of the literature review on the subjects of access control to electronic health records, electronic health records for general practice and informed consent for medical information will be presented.

Based on the literature review a conceptual authorization model for EHR systems has been developed, this is described at the end of the literature review chapter.

2.2 Preliminary research on the case in question

In this part of the project, the case in question at Topicus was analysed in order to gain a clear overview of the current situation. This was done through a process of document analysis, meetings with multiple employees at Topicus as well as attending a meeting in which the current process of sharing PHI was explained to general practitioners.
In this way information was gathered about the applications in question, the Datakluis and VIPlive as well as the current method of authorization to the PHI of patients. The processes in which the PHI of patients is currently exchanged, the referrals and consultations, have been analysed.

The results of this step are described in chapter 4, the current approach of authorization to PHI in VIPlive. The current approach of authorization in this process is also explained using the aspects of an authorization process model that is described earlier in the project.

2.3 The gathering of requirements

This phase is focused on gathering the requirements from several relevant stakeholders for the new authorization model. In order to gain a better insight in the relevant subjects, parties, requirements and how these relate to each other, a conceptual model has been made. Resulting from this conceptual model, a specific list of subjects has been made on which more information can be gathered in this phase, including the requirements from multiple specific parties.
Taking the priorities of Topicus in mind, several types of stakeholders have been chosen from who the requirements for this model will have to be gathered. Firstly a preliminary document analysis will be done. Afterwards interviews with multiple parties will be held.
Once this step is completed the gathered requirements can be used for the development of the improved process and the authorization model.

The conceptual model

Based on the literature review and the preliminary research a conceptual model has been designed. This model consists of the subjects and variables on which more information can be gathered in order to construct a proper authorization model.

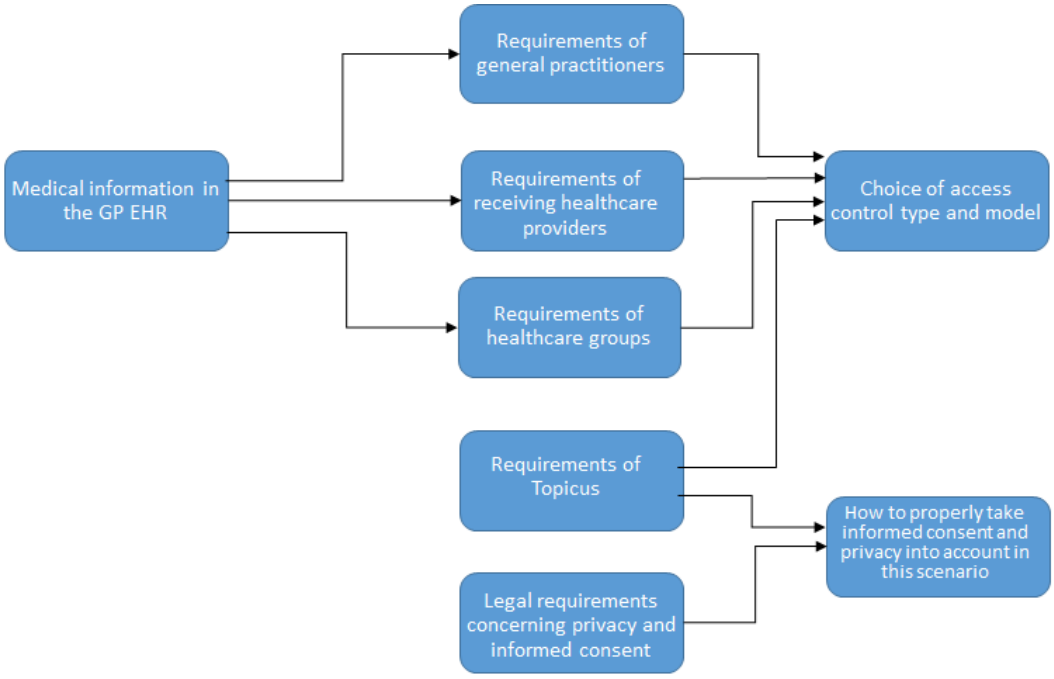


Figure 2: the conceptual model

The types of medical information that are concerned in this research come from the EHRs of the general practitioners. Resulting from the available data are the requirements of the GPs, the receiving healthcare providers and the healthcare groups. These are requirements on which type of access control model should be applied (like RBAC for example) and on which medical information should be accessible to which party in which scenario. Based on these requirements, and on the requirements of Topicus on this matter, the type of access control model shall be chosen and an overview shall be made on which party should be able to access which medical information. The chosen method on how to take privacy and informed consent into account shall be based on the requirements of Topicus in this matter and on the legal requirements concerning privacy and informed consent.

Therefore, in this research project more information could be gathered on the following subjects:

- The types of medical information in the EHRs of the GPs
- The requirements of the GPs
- The requirements of the receiving healthcare providers
- The requirements of the healthcare groups
- The requirements of Topicus
- The legal requirements concerning privacy and informed consent

In consultation with Topicus a choice has been made on which of these subjects this research will be focused.
The requirements of three different healthcare groups will be gathered. The choice has been made to investigate multiple healthcare groups instead of investing a single group more thoroughly, as the

authorization models of the groups can be quite different. Therefore a quite skewed result might turn out of this research if only one of them is researched as it is likely that other groups handle the authorization matter quite differently. Although Topicus has agreements with more groups than three, the choice for three groups is based on time constraints. However, as will be shown in the document analysis below, these three healthcare groups have quite different authorization models and are therefore likely to have different points of view on this subject.

The choice has been made not to interview the GPs or the receiving healthcare providers. There are multiple reasons for this: The healthcare group are representatives of their healthcare group, they are in touch with the GPs and receiving healthcare providers within their respective groups. The healthcare groups have made the agreements with them concerning which party would receive which PHI in which situation. Therefore, the representatives of the healthcare groups will have a clear overview on the needs and requirements of the healthcare providers within their group. Furthermore it would have been very difficult to arrange an interview with GPs. Although the opinions of the healthcare providers and GPs is very relevant and it would have made a valuable addition to this research, it has been deemed out of scope for this project.
The requirements of Topicus will be gathered through an interview and a group meeting with employees of Topicus who are knowledgeable on the subjects of this research.

The types of medical information in the EHR's is researched through document analysis concerning the current systems that are in place for this case as well as meetings with employees of Topicus. The result is explained in chapter 4, in which the current situation of the case in question is explained. An exploratory review of the GDPR, is done in chapter 6.

Document analysis

Firstly a document analysis will be done. At this moment, an authorization process which uses a RBAC access control type is already used by Topicus with multiple implementations for each healthcare group. This authorization method is applied in the following manner; When a general practitioner wants to refer a patient to another healthcare provider within the healthcare group, this process and its specific implementation determines which of the providers to whom a patient is referred are allowed access to which PHI. This is also based on the specific chronic illness of the patient. These implementations have been made by Topicus in agreement with the healthcare groups. Therefore these implementations are seen as an indication of the requirements of the corresponding healthcare groups on which party should be able to access which PHI.

These implementations are analysed in order to gain more knowledge on the current approach of Topicus and on the similarities and differences between the models of the healthcare groups. This knowledge will be used in order to prepare for the interviews with the healtchare groups. Furthermore this analysis is used in order to determine how different the implementations of each healthcare group are when compared to each other. If they are similar it might be worthwhile to consider making a single nationwide implementation of the authorization model.

Interviews

In order to gather the requirements from Tropicus as well as from representatives of three healthcare groups, interviews and a group meeting were held. The respective lists of interview questions can be found in the appendices.

For Topicus one group meeting was organized as well as an interview with two employees. The attendees of the meeting were employees knowledgeable on the subjects of this project. During this meeting the same questions were asked as during the interview. The main differences between the two were the number of attendees and that there was more discussion during the meeting as there were more attendees from multiple different teams.

Three different healthcare groups will be taken into account for this research, each belonging to a different region of the Netherlands. One representative of each group will be interviewed separately.

Describing the results

In order to give a proper overview of the results of the interviews with the healthcare groups and the employees of Topicus, the structure of the aforementioned model concerning the aspects of an authorization process will be used. The chapter in which these results will be described will have 5 parts, corresponding to the five parts of the model.

2.4 Exploratory analysis of the GDPR

In order to answer the research questions relating to privacy and the GDPR, an exploratory analysis of the GDPR will be done.
It is important to note that this will not be an overly thorough investigation into the GDPR. This part of the research is meant to provide a basic understanding of the relevant parts of the GDPR for this subject, after which further examination will be left for further research outside of this project.

2.5 The development of the improved process and the authorization model

At first, an improved version of the process will be described. This improved process will be described based on the literature review, the gathered requirements and the exploratory review of the GDPR. A diagram of the improved process will be given to give a clear overview. Afterwards the details of the improved process will be given, using the structure of the conceptual model. In each of the five parts of the conceptual model, the specific choices that have been made for the improved process are described.
Finally, the authorization model will be developed based on the improved process. The information concerning authorization which should be stored when medical information is shared will be described. The core steps which are required to generate this information will be explained. Afterwards the core steps are described which should be done when a receiving party wants to access the medical information.

3. Theory – a literature review

This part elaborates on the primary subjects of the literature review: Access control to electronic health records, electronic health records for general practice and informed consent for medical information. The primary focus was to find articles that contained a combination of all three of the primary subjects. A lower priority was set on the combinations of two of the primary research subjects and subsequently a single primary research subject. 20 of the gathered papers have been used for this literature review.
Resulting from the gathered knowledge of this literature review, an initial list of interview questions

was developed. This list will be elaborated upon during the research project and will be used in order to answer research question number 2. Furthermore the conceptual model that is described in chapter 3, which was used in order to determine a proper methodology for this research, is based on this literature review.
Finally, based on the literature review and on preliminary research on the case in question, the conceptual authorization model for EHR systems is developed. In this model the aspects of an authorization model that are taken into account for this project are described.

3.1 Electronic Health Records

As cited from Mamlin and Tierney [7] "EHR systems are longitudinal electronic records of patient health information." There are many EHR systems in existence and there is a large difference between EHRs. Hospitals tend to use EHRs from a limited number of large vendors, while outpatient practices commonly use EHRs from a large number of smaller sized vendors. There are large difference within these systems, for example in their approach for both storing the information and the method of presenting it.

Instead of the Electronic Health Records (EHR's) of today, people in healthcare used to work with paper health records. In a hospital for example there used to be a single paper record concerning a single patient which contained medical information from multiple medical disciplines.
When decisions were made concerning the treatment or diagnosis for example, people would look through the paper record. Of course they could look into just a part of the medical information that was in there, but all other confidential information was in the paper record as well. This can, understandably, lead to concerns about the privacy of health records.

But when paper health records are compared to the EHRs of today, which method is more suitable to protect the privacy of patients? After all, the paper file can be stored safely so that only those who are involved with the care of the patient can have access to it. Furthemore a paper file cannot be hacked, like an electronic one.
However, there were also disadvantages to the paper file concerning privacy. There are known cases in which the medical information of celebreties was leaked, even though they were stored in paper files. In practice it occurred that the files, who were filled with confidential information like their psychological state for example, were just lying on a desk, open to be read by multiple people, as can be read in the 'Argumentenwijzer EPD' [22]. Another important issue was that healthcare providers who had access to the paper file could see everything that was in there, including information that was not necessary for their own practice.

An advantage of an EHR, presuming the systems and applications work properly, is the wide range of possibilities to authorize who is able to access which parts of the medical record in which situation, as can be read in the publication of Fernández-Alemán et al. [2]. Many modern EHR systems make it possible to easily consult a colleague for advice about a patient and to send, or give access to, the medical information. This medical information is instantly accessible, which is an advantage when compared to the paper files. Another advantage is the possibility to give specific parties access to specific parts of the file, so that only the selected parties can see them. When presumed that the systems work as they should, only those who are authorized to be able to see the information, have access. Using these systems, when a patient is referred to a provider of healthcare, or a provider is consulted about a patient, the provider would only be able to access the information to which he or she is authorized.
However, there are difficult aspects of EHRs as well. There are concerns about the privacy of the

medical information as well as concerns about the security of the systems. People are concerned for the possibility that other parties, like criminals for example, are able to take advantage of the medical information of patients [2].

What should we think nowadays of paper health records? Despite the fact that EHRs have many advantages compared to them, it was useful that all of the medical information about a patient was stored in a single file. You could be certain that all relevant information was in there. However, this functionality could also be offered through EHR systems. And besides, is it useful for a physiotherapist for example to be able to access the psychological information of their patients?

Although EHR systems are very common these days since health professionals are moving away from the paper-based predecessors, a majority of healthcare professionals are frustrated or unsatisfied with EHRs. [7] According to Mamlin et al. EHR systems currently have not fulfilled the expectations in the improved quality, safety, efficiency or outcomes of care as predicted by early research. The amount of required documentation has become more and more, while its focus is increasingly concerned with administrative and medicolegal needs and less concerned with direct patient care. Of course the EHRs systems provide benefits compared to the paper records [2]. But, in order to successfully provide the full benefits of modern EHR technology, certain requirements have to be attained. These include among others: Completeness and protection of data, security, incident response, resilience to failure, legal issues, high availability, security and a consistency of security policies.

Within an EHR information about a patient is stored [1]. This includes, but is not necessarily limited to, patient-centric info, which contains information like the name and ID number, and healthcare centric information, also called Personal Health Information (PHI). Out of all types of personal information that can be stored, health information is regarded by many to be among the most confidential. [2].
The personal health information that is stored is often of a very personal nature and may include data of a habitual nature (like the diet of a patient or other factors concerning his lifestyle) besides physiological data [1]. As information about a patient may be stored over a large period of time, an electronic health record may contain an enormous amount of private information about this person. Furthermore the PHI often has to be shared with other parties like other health care professionals in the case of a referral or a consultation for example. The mismanagement, or lacking protection, of this data could hurt the privacy of the patients involved, as it could end up in the wrong hands. Besides that, it may very well be possible to access the PHI of a patient from multiple sites as the patient is currently visiting, or has visited, multiple health professionals and organizations [2]. This has consequences for the risk of the PHI to be accessed by unauthorized parties. If a hacker for example has managed to access one of these systems, the patient's data may be exposed.

Cyberattacks on e-Healthcare enterprises, which can severely compromise the privacy of the patients, are a significant problem [1]. In recent years there have been numerous reports of thefts or accidental loss of clinical data [2]. PHI is very valuable for criminals and is often protected by lacking security. Of all cyber-attacks on e-Health enterprises, identity theft accounts for 46%. Cyber criminals can earn a lot of money with these practices; Healthcare data and medical records are currently sold on the black market for an average of 40-50 USD for a record, which is even more than credit card numbers. Malin et al [7] write that between 2009 and 2015 over 1100 breaches of medical information have exposed the data of more than 120 milion users.
Even though there are a lot of efforts to improve security, these problems have caused many

patients to have a limited amount of trust that e-Healthcare systems can adequately protect their privacy [1].

There are multiple protocols for preserving the privacy of the patients in an e-Healthcare environment, these include [1]:

- Pseudonymization of patient's identity
- Encrypting the data of patients
- The creation of private and public clouds in order to handle sensitive and sanitized data
- Privacy-preserving data publishing
- Privacy-centered access control systems
- Authentication
- Transmission protection during the transition of health care data between two parties
- Protection of data in storage

It should be noted that none of these methods alone is enough to ensure the privacy of patients, a combination of methods is preferred. In order for a modern E-healthcare system to ensure patient privacy it needs both access control, a security system for the stored data and an anonymization mechanism, especially when health data is shared to other parties. For example: Access control determines who can access the PHI and who cannot but in the case of a cybercriminal succeeding in a privilege escalation, in which the access control system has failed, an anonymization technique can provide anonymity of the patients.
As mentioned in the inclusion and exclusion criteria, this literature review is aimed at access control, but these other privacy protecting methods like anonymization are left out of the scope.
The subject of health information exchange, in this case the exchange of information in the case of a referral or a consultation, will be researched during the research project itself and is left out of scope for this literature review.

In order to ensure that the privacy of the patients in EHR is protected, a distinction has to be made between those who are authorized to have access the records and those who are not [1]. And furthermore, who has access to which part of the records. For example, a distinction can be made between those who can see the patient-centric info, which contains information like the name and ID number, and those who can see the PHI.
However, it should also be taken into account that the right PHI should be available to the health care professionals so that the process of care is not hindered by inaccessible data. [2] The subject of access control is elaborated upon in the corresponding part of this literature research.

A possible way of gaining the trust of the patients is to give them control over who can see, edit and share their health records and who cannot. In fact, in healthcare it is a widely applied approach to enable the patient to control the disclosure of the content of his or her EHR. [4]. The subject of informed consent and the control of patients over the disclosure of their data is elaborated upon in the corresponding part of the research.

3.2 Privacy

Privacy is a dynamic and context-dependent concept which is understood in different ways in different societies and countries [4]. In the information sector, as well as e-Health, privacy should cover not only person-to-computer communication, but also computer-to-computer and organization-to-organization communication [8]. Privacy can be defined as an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data [1].

Privacy is seen as an important factor in healthcare. It is known for example, that some people will not seek medical help at all if they think that patient privacy is insufficient, or they might not tell important medical information [5].

There are multiple definitions of privacy and there is no globally accepted privacy model that is used in IT. Some privacy models that are often used include Altman's privacy model [8], the communication privacy management theory as described by Petronio [9] and Westin's privacy theory [10].
According to Altman's model, privacy is a process of interpersonal boundary control and concerns the selective control of access, both to the self and to a group.
The communication privacy management theory describes the privacy boundaries of a person as well. It describes how these boundaries (which information a person wants to share and which information a person wants to keep for themselves) are managed by a person for different communication partners like other people.
According to Vimarlund [4] Regulatory privacy models are often used in healthcare, which means that the rules concerning privacy are based on laws that are nationally/internationally accepted.

Although privacy in the context of health information privacy is related with confidentiality and security, it is important to make a clear distinction between them.

Confidentiality can be definied as "the obligations of those who receive information to respect the privacy interests of those to whom the data relate." [1] Another definition refers to it as "the process that ensures that information is accessible only to those authorized to have access to it." [2] In the research by Vimarlund [4] it is described as: "Confidentiality is about identifiable personal information (PII). It is an agreement about how the data will be managed and how it is access controlled by the data controller or processor. Confidentiality means that the entity processing PII has the responsibility to protect data against misuse and unauthorized use."

Security however, as described by Sahi et al. [1] "refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure''. The fundamental goals of security, as listed in Fernández-Alemán et al [2], are "confidentiality, integrity and availability". IT security is also described as: "Information security means protecting both information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Its elements are accountability, availability, confidentiality, and integrity (often nonrepudiation is also added)."[4]

Many of the security concerns in electronic health records are indirectly related to the privacy of the patients [1]. True privacy cannot be attained when subjects like access control, authentication, accountability and non-repudiation are not adequately handled. Privacy, and the feared lack of it, is one of the most considerable obstacles in gaining the trust of the patients in e-Healthcare solutions like EHRs.

The privacy level in e-health information system is dependent on multiple factors, as listed by Ruotsalainen [4]: "Legislation and norms, market features, the nature of information and its sensitivity, characteristics of information user, activities expected, the level of trust of the service provider, technical architecture of service provider's ITC system and expected benefits of the user".

The legislation in many countries demands that the privacy of patients in healthcare is adequately handled [1]. In the USA for example, HIPAA is in place. In Europe the General Data Protection Regulation (GDPR), which is called 'Algemene verordening gegevensbescherming in Dutch, is in place since 25 May 2018. It is a single law concerning privacy that applies to all members of the European

Union, and so also the Netherlands. In the Netherlands it has replaced the existing law that protected the personal data of its citizens, called the 'Wet bescherming persoonsgegevens'. It establishes rules on how personal data should be processed. In the research by Sousa et al. [11] a list is made of requirements for hospital information systems, which will be taken into account in this research for its applicability on the specific case that is researched.
The implications of legislation on the particular case of this research, including subjects like access control, privacy and informed consent, will be looked into during this research project.

A possible way in which the interests of patients concerning privacy, as well as multiple well accepted ethical principles, might be applied in practice is to give them granular control of their medical data, as it allows them to decide who has access to their personal information and who has not. [3]

This thesis will provide an answer by developping an authorization model for a specific case in which the aforementioned factores are taken into account.

3.3 Access control

The purpose of an access control policy is to define who has access to certain information and who doesn't, and to define who can use it to what extent [1]. Although access control alone is not enough to ensure privacy of an EHR, it is seen to be one of the essential elements to do so. Especially when used in combination with data anonymization.

There are multiple methods of access control that are used in EHRs. Among those are user-based access control, context based access control and role-based access control [12]. In user-based access systems there is a direct relation between persons and privileges, in such a system an individual doctor can have his own specific privileges for example. In context based systems access is granted based on the person, the context of the action and the action itself. Role-based access control, also known as RBAC, allows multiple roles to be defined, specific permissions and restrictions are tied to the role which cause a user of an application to only access the PHI that his or her role allows. Fernández-Alemán et al. [2] found in their literature review of 2013 that the preferred model appeared to be Role-Based Access Control (RBAC) as 27 out of the 35 articles that used access control models applied it. Although it is possible that RBAC was more prevalent in 2013 that it is today, it is an indication that it at least used to be frequently used model. When compared to systems in which the permission levels of each individual have to be managed, the use of roles that are related to job-titles within an organization makes the administration of access control easier [12]. This system also prevents the possibility that individual permissions are handed out which would allow malicious or accidental access to healthcare data. Other features that are found within proper RBAC systems are the least privilege principle, separation of duty and data abstraction.
The least privilege principle means that users should only receive the set of privileges they actually need to do their job, not more. Separation of duty entails that multiple roles are necessary in order to complete a task (a control measure to prevent fraud). Data abstraction means that abstract permissions are given for the actions of users, like the submitting of new data, instead of permissions like 'read' or 'write'.
According to Fernández-Alemán et al. [2], RBAC is considered to be a suitable method for systems in health care. The flexibility of RBAC is seen as an advantage. The access rights of many users can be updated just by changing a single role.

In the article of Helms and Williams [12] a list has been composed of evaluation criteria for RBAC implementations, gathered from multiple sources like the NIST RBAC standard and the HIPAA security rule. This list is intended to evaluate the state of practice in role-based access control and

includes examples of how to apply the criteria. These criteria include, among others: The presence of emergency access procedures, user role revocation without having to delete the user, role hierarchies and the lack of a super user.

However, the RBAC approach has received criticism for being inflexible. Also, scalability issues may happen as the number of roles and policies tend to increase as the amount of users and resources becomes larger. [1]. Also, the traditional model of RBAC does not allow the patient to have input [13].
According to Fernández-Alemán et al [2] a disadvantage of RBAC is the way it handles unplanned circumstances, like doctors asking a colleague for a second opinion for example, which can be difficult if the colleague lacks the right role. Often there are exception mechanisms, however, these open a window for security threats in which these are abused.

There exist multiple alternative approaches to access control that can be found in literature. Attribute based access control is a method in which policies are used that combine different kinds of attributes (depending on the specific system) to determine whether access is permitted or denied. For example, Seol, Kim, Lee, Seo and Baik [14] propose an attribute based access control model (ABAC) that, when compared to RBAC schemes, is said to provide more fine-grained and flexible access control. Another advantage of ABAC is that providers outside of the originating source, like a physician that is consulted, can be assigned to roles as well on which his level of access to the data is based [13]. A limitation of the model is that the patient does not have control over the level of access of each role that is defined within the ABAC system.

RBAC does not take the context or circumstances into account in which a user tries to get to the medical information, an alternative that does is called situation based access control, also called SitBAC [15]. In this model situations are defined in which access to data is either denied or permitted. This is based on a situation schema, a pattern of many interrelated concepts like the patient, the requestor of the data, the access task and the response. A situation is validated and is handled according to the situation schema, which can be adapted as the organization changes its policies.

3.4 Informed consent

Van der Linden, Kalra, Hasman and Talmon [16] describe two approaches for informed consent: Explicit and implicit consent. In explicit consent, a.k.a. opt-in consent, access is forbidden unless the patient grants it. In implicit consent, also known as opt-out, the patient is assumed to consent unless he or she indicates otherwise.

A trend can be recognized in both case law as well as bioethics scholarship that patients are given more information and more control over health decision making [3]. Over the past three decades there have been developments that supported informed choice and patient empowerment, which supported the argument that patients should have more autonomy in decisions concerning medical treatment. Today, a widely used approach in healthcare is for the patient to be able to disclose the content of his or her EHR [4].

However there exist many questions and concerns about informed consent and the control that patients can have on the disclosure of their data. Since the use of Electronic Health Records has become normal, these questions and their practical consequences have become more complicated. Modern technology allows a gigantic amount of health data to be stored and accessed by more people than before the rise of EHRs.

If you would ask a patient for consent to disclose all their health data for all potential uses and recipients, many would be inclined to say no. Patients may like to disclose only the medical information to a physician that is actually needed for the treatment in question [3]. A lot of patients may like to keep the information that they are using psychiatric medicines private from another medical professional they are visiting for example.
In fact, most patients in healthcare want to have control over to whom they want to disclose their data as well as control on how this information is exchanged to other parties [13]. It is also known that patients who have concerns about the security and privacy of EHR systems tend to disclose less information to the care providers [5]. In a study performed in 2014, 13% of patients have said that they didn't disclose full information to health care providers because of security concerns [13].

In a study by Caine and Hanania [17] it has been shown in research that none of the questioned patients would want to share their data with all potential recipients. The specific preferences regarding the sharing of data were different for each patient, but one of the outcomes from the research was that patients preferred to have granular privacy control over which data should be shared with whom.

However, in literature, both risks and benefits are recognized in giving patients more granular control of their PHI. For example, enabling patients to give permissions to individual users may provide problems in terms of scalability[12]. As healthcare organizations may contain a large number of employees it may soon be difficult to manage all the permissions for every one of them. The fact that users within an organization may come and go increases this problem. It is important to provide an access control system in which this is taken into account in a scalable manner.

Another risk is the possibility of clinical harm to the patients. As health care providers may miss access levels to certain medical information, there is a risk of missed opportunities in providing care that is needed for the patient [5] as well as the risk for care delays [13]. Lacking crucial information during medical decision making may cause errors in judgement, which can have consequences for both the patient involved and the health care provider if he or she is responsible.
In the context of primary care; As providers of primary care coordinate the care of a whole person, and coordinate their care across multiple specialties within medicine, having access to the necessary medical information is important indeed.
A different argument brought forward is that having access to too much data may have a downside for health care providers, namely that they don't have the time to process all the data that they have access to [5]. Many clinicians even try to lessen the amount of data that they have to process before an encounter with a patient.

It should also be kept in mind that the method of requesting the consent of patients may have influence on the decision whether they actually give it. The structuring of the questions for example alone can influence their decision [13].

Meslin et al. [3] have produced a number of Points to Consider for system designers that can be used by system designers to help in decisions around the matter of informed consent and granular control for patients. It is intended both to guide the decision making process but also to identify important issues in this matter. During the research at Topicus, the relevance of each of the points to consider' for this specific project will be looked into.

As cited from Meslin et al. [3], the points to consider are as follows:

1. How will the system make transparent the uses and flows of clinical information so that patients can make informed choices about disclosing/restricting their information?

This point encompasses at least three interconnected issues: How will patients be told about the flows, uses, and users of their health information? How will patients learn what information is contained in their EHR so they can appreciate what they are granting access to – a prerequisite for individual choices to be meaningful? How will patients be assisted in understanding the meaning of the medical information in their EHR (e.g.,terminology used in pathology, laboratory, and radiological tests/reports)? The three options, as stated in this study, are:

- Provide no education regarding what information exists in the EHR or the flow and uses of information besides the required, and fairly general, Notice of Privacy Practices. Patients will utilize whatever additional understanding they happen to have, including any misunderstanding, in exercising granular control.
- Provide educational materials for patients to review before exercising granular control. These materials can be more or less specific or customizable to the literacy and interests of different patients.
- Give all patients access to a trained educator or practitioner who can brief or tutor them on the EHR.

2. How will the system structure the array of choices patients can specify for disclosure and non-disclosure of their clinical information?
3. How will technologically and/or medically unsophisticated patients, or those with other challenges, exercise their choices for granular control of their information?
    - Provide an electronic input option for choices to be recorded by the patient (and/or his representative) only, and be available in a variety of languages (at least English and Spanish)
    - Devise a two-step process for input, giving patients a paper form containing the choices available, which is then taken by a medical staff member to be recorded in the electronic system
    - Provide other means for patients to learn about their options and indicate their preferences, for instance through discussion with a medical staff member (e.g., for those who have difficulty reading, or are sight-challenged) who would then record the patient's choices and preferences
4. How will the system inform providers of a patient's preferences for data access/restrictions? Three options may be considered:
    - When a physician views the patient's EHR, the system will specify which information exists and is accessible, and which information exists but is being restricted due to the patient's prior preferences and privacy settings.
    - When a physician views the patient's EHR, the system will only display the information that is allowed by the privacy settings, without disclosing the existence of other information that is subject to access restrictions.
    - When a physician views the patient's EHR, a broad statement that information has been restricted would be provided without specifying which types of information are not accessible.
5. Under what circumstances/conditions will the system allow health care providers to access patient data in ways that may over-ride stated preferences for granular control?
6. How will patients be told about mandatory reporting requirements (e.g., public health, gunshots, abuse, disease registries, etc.) and their impact on granular control? Three options are given:

- Do not explicitly inform patients regarding legally man-dated reporting requirements (i.e., that irrespective of her desire to restrict disclosure, some circumstances mandate disclosures).
- Provide a general explanation that there may be legal reasons why some personal health information must be disclosed, but do not detail those reasons. This could include, for example, putting posters in patient intake areas in clinics, physicians' offices, hospitals, outpatient facilities, etc., or very general statements in Notices of Privacy Practices given to patients.
- Inform patients more specifically what sort of situations would require disclosure of personal health information to public health authorities and/or law enforcement(e.g., STIs, communicable diseases, epidemic and/or pandemic outbreaks, abuse, gunshots, suspected bioterrorism), and what sort of information would be disclosed(e.g., name, address, diagnosis, etc.).

3.5 Application of informed consent in access control

How can the consent or the control of patients be taken into account in an access control model? Bhuyan, Bailey-DeLeeuw, Wyant and Chang [13] claim that flexibility and input from the patient are vital parts of an access control model. According to them such a model needs to be able to adapt as patient preferences may change as well as roles and circumstances.
Patient-centric access control, in which patients have control over who can have which access level to their PHI is advised by Sahi et al. [1]. Not only to meet privacy requirements but also to gain the trust of the patients. They also mention that it is important to consider that a single policy for access control is not enough to ensure the privacy for an e-Health enterprise, they propose the use of two or more access control policies. This approach, called hybrid access control, is seen by them as the best way to form a controlled and secure access policy.
Among their advice are the following features for the development of a hybrid access control scheme:

- The use of roles as in a RBAC scheme for the 'upper levels', certain roles will be defined and granted certain access rights. While identity/attribute based access control is also used in certain situations
- They advise to use graduated privacy levels for PHI, a compartmentalized approach. In this approach the lower levels only allow access to certain relevant data (like patient prescription requirements for example). Other healthcare professionals will have other levels of access which will allow them to access the data they need, like information about the medical condition, treatment and diagnosis in the case of a physician
- To use patient profiles that contain PHI in multiple categories as well as a list of people who are allowed complete access to all PHI
- A profile for doctors which contains a similar list, but in their case it contains the patients to whose PHI they have full access
- They advise to implement a mechanism in which patients can change their aforementioned profile, in order to update the list of people who are allowed access to their PHI or to change the privacy levels in their PHI

However, the consent of patients on which party can access which data might be quite challenging to take into account in practice. In a study performed by Leventhal, Cummins, Schwartz, Martin and Tierney [18] a system was developed in which the preferences of patients on two matters was taken into account: Which parties could view their EHR and which party could view which data within it. To

provide granular control to the patients proved to be complicated, a process in which expertise was necessary on multiple subjects like bioethics, informatics and programming. Multiple hard decisions had to be made on subjects like determining the level of data granularity and the balancing of the needs of clinician's to provide care of a proper quality with the rights of the patients.

But if patients would be offered the possibility of granular control, would they really use it? The answer to that question has a large influence on the consequences in practice on which party has access to which data when granular control by patients would be implemented. A research that studied patients that controlled who could access their personal information was done by Schwartz, Caine, Alpert, Meslin, Carroll and Tierney [19]. In this study, patients were given control on which parties within a primary care clinic (doctors, nurses etc.) could access their personal information in the EHR, in order to investigate their preferences on this matter. 43% of the researched patients chose to limit the access to some parts of the information in their EHR's to at least some of the health providers. 4.8% even gone so far to decide that all providers were inhibited from accessing all the information in their EHR's. 57.1% of patients decided not to limit the access to the information to their EHR's for all of the researched providers. Their results suggested that a large part of the patients believed that the health care providers can be trusted to handle the access to the information in their EHR's responsibly. Although a significant group of patients seems to think otherwise.
Another relevant conclusion from their study is that a large part of the patients, almost half of them, thought that the relationship that a patient has with their health care provider might be influenced by their decision whether or not to give them access to certain information. This may have been one of the reasons why patients choose to not restrict the access of providers to their information.

But what is the opinion of primary healthcare providers on the control of patients on who as access to their EHR's? In a study by Tierney, Alpert, Byrket, Caine, Leventhal, Meslin and Schwartz [20] the patients were able to decide which party received or did not receive access to either all data or only highly sensitive data. Although a large part of the researched health care providers claimed to be comfortable with the fact that patients had control on which party could access which part of their information, a significant part was not. Some of the researched providers thought that the limited access to the information may result in a lower ability to provide care of a proper quality. Another result of the study was that some providers believed that it could affect the relationship between the provider and the patient in a negative way. It appears from this study that there is a need for a balance between the requirements of healthcare providers and the requirements of the patients on the issue of which party should have access to which information.

One of the goals of the research project will be to investigate which approach for access control and informed consent is suitable for the case in question. Based on the knowledge gained in this literature review a conceptual model has been made as well as a list of interview questions with this goal in mind.

3.6 The five aspects of an authorization process for EHR systems

In designing an authorization process, there are multiple aspects that can be kept into account. For this specific project the focus will be laid upon several relevant subjects, while other subjects are deemed as out of scope for this project.
The subjects are chosen based on the knowledge gained in the literature review. The needs and priorities of Topicus for this particular project are kept into account in the choice of these aspects.

Using the lessons from literature a model for these different aspects in the context of authorization processes for EHR systems has been made for this project. It can be seen as a method of describing such a process, in which each of the five different parts can be 'filled in' differently for a process. Each part of the model will be explained further on in this chapter.
Aspects like security, pseudonymizations of patients identity, transmission protection etc. are out of scope for this project and so are excluded from this model.

This model will be applied in the following way:
In the next chapter the current authorization approach for the aforementioned process will be elaborated upon. This process will be filled into the five aspects model. This is done so that at the end of the chapter a clear overview of each relevant part of the current authorization model has been given.
In chapter 7 an improved version of the process will be designed based on the five aspects model. In order to do so, the current approach for authorization in the aforementioned process, the literature review as well as the interviews and meetings will be kept into account in order to design a proper new approach.

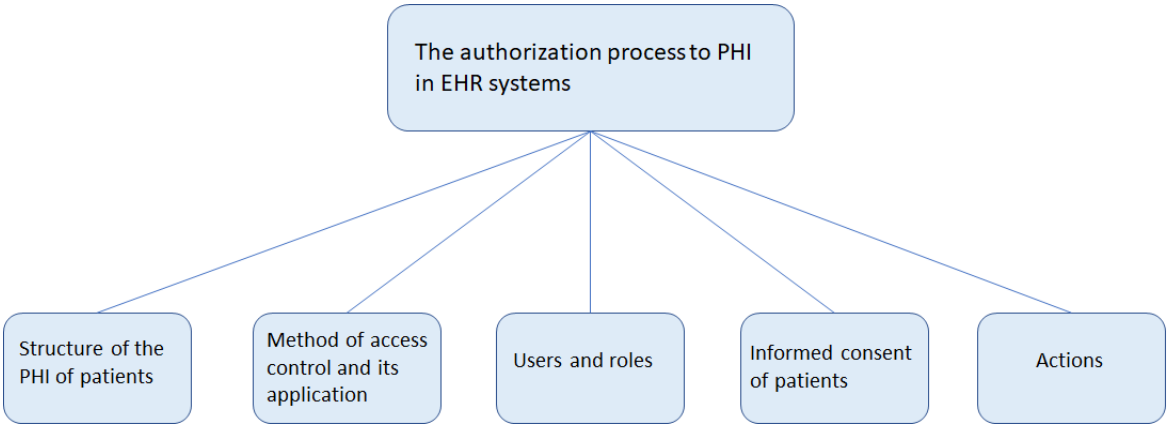


Figure 3: The aspects of an authorization process for EHR systems

Structure of the PHI of patients

The first part of the model is about the data of the patients that is stored into the system. Many kinds of EHR's are applied in practice and there are big differences in the kinds of information that are stored about the patients.
What is important in particular for this project is in which way it is structured in the context of authorization. Are there certain categories of patient information to which access can be granted as a whole? In which parts is the health information of patients structured in the system?

Method of access control and its application

Multiple methods of access control have been mentioned in the literature review, like role-based access control and attribute-based access control. This part model is about which of these methods, or which combinations of methods, is applied. The factors that play a role in the decision which person is granted access to which data (like role of the receiving party, chain of care, informed consent of patients etc) are described. The manner in which these factors are applied in this system is described as well.

Users and roles

This part concerns which kinds of users can interact with the system. Which users can be granted (or excluded from) access to the PHI of patients? Which users can grant access to the PHI to others? Are users tied to roles to gain access to the PHI?

Informed consent of patients

This part concerns in which way the process keeps the informed consent of patients into account. Is it a matter of explicit or implicit consent? How much control do patients have on which information is sent to healthcare professionals? How fine-grained is the control of patients in this matter? The method in which patients can give their consent is described as well in this part of the model.

Actions

Multiple kinds of actions can be performed in EHR systems in which the PHI of patients is involved. Referrals and consultations, in which PHI of patients has to be transferred to other healthcare professionals, are examples of this.
In authorization processes it is possible that the amount of PHI of patients that can be accessed is dependent on the action that is applied. Therefore, in this part of the model, a list of different actions that can be applied is filled in. Including a description if the amount of access is dependent on the action and if so, in which way.

4. The current approach of authorization to PHI of patients in VIPlive

As mentioned in the introduction, Topicus has made agreements on the subject of authorization with each healthcare group that is connected to VIPlive. These agreements concern the implementations of the RBAC access control process to determine which receiving party can or cannot see specific PHI of patients. In this chapter an explanation of the authorization approach for this process is given. In the next section the current authorization approach is described using the aforementioned model of the five aspects of an authorization process. Finally an analysis of the implementations of the authorization process by three healthcare groups is given.

4.1 An explanation of the authorization approach

There are two kinds of data in the Datakluis that can be shared as explained in the introduction: The PHI that originates from the extractions and the PHI that originates from the professional summaries. Depending on which data on the specific patient is more recent, that data will be shared to the receiving healthcare professional.

There are four main cases in which personal health information of patients is shared to other healthcare professionals using the systems of Topicus;

- Referrals, ‘verwijzing’ in Dutch
- Consultations, ‘consultatie’ in Dutch
- Further referrals, ‘doorverwijzing’ in Dutch
- Further consultations, ‘doorconsultatie’ in Dutch

As a lot of terms currently used by Topicus are in Dutch, translations to English have been made for this project. A list of all of these translations can be found in Appendix B.

An overview of the kinds of data and the different actions has been made in figure 3, afterwards the different actions will be explained:

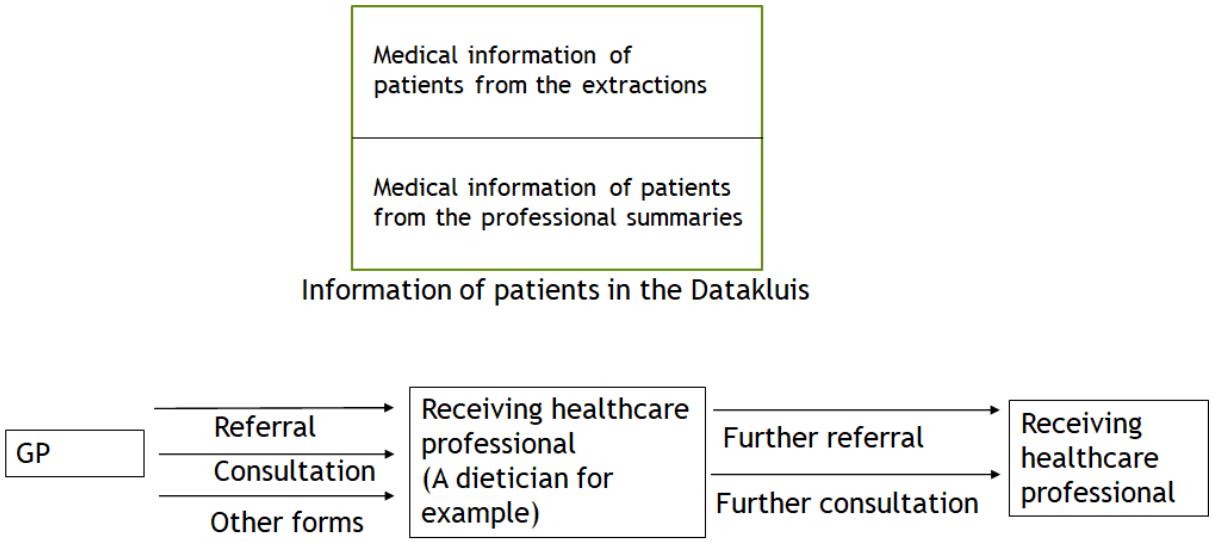


Figure 4; an overview of the medical information and actions to share it

In the case of a referral, a GP will refer the patient to another healthcare professional within the healthcare group, like a dietician for example. Afterwards the patient can get treated by the dietician.
During a consultation, the GP asks another healthcare professional within the healthcare group for advice concerning a specific patient. Information about the patient and his or her medical information is shared with the receiving professional so that he or she can give a medical judgement on the case in question. When a consultation is done, most often the request for a consultation is seen first by an assistant or secretaries of the receiving medical organization. Then, the assistant or secretary assign it to the medical professional who can handle the consultation.
It can occur that when a patient is referred to another professional, like a podotherapist for example, the professional will refer the patient again to second healthcare professional, like a pedicurist. This will be called a further referral in this research.
A comparable action can be performed for consultations, which is called a further consultation.
When a GP performs a consultation, the receiving healthcare professional has the possibility to call in the help of another healthcare professional to give a judgement on the case in question.
There are other forms, but these are seen as out of context for this research.

All of these actions are performed through the VIPlive application that is made by Topicus. The PHI that will be shared to the receiving professional is determined automatically within the VIPlive application based on the agreements that have been made within the healthcare organization.

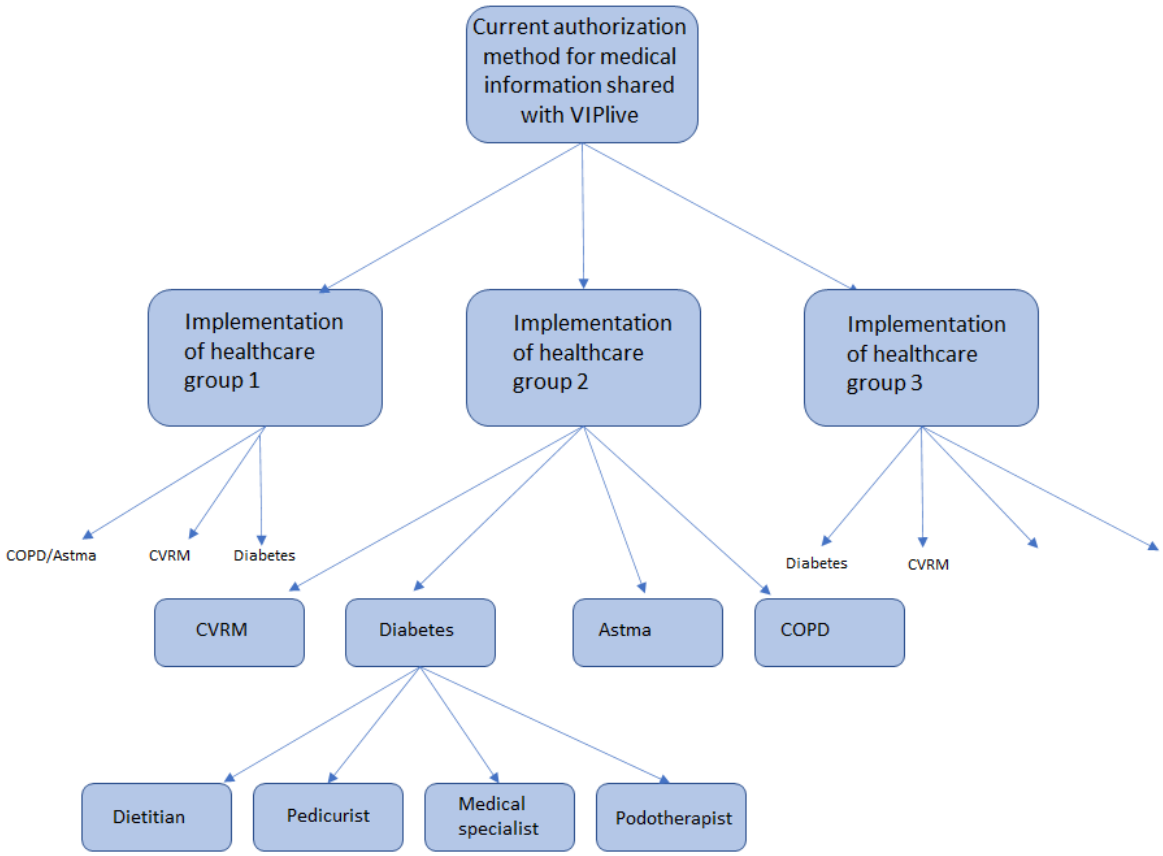


Figure 5; a schematic overview of the authorization method for medical information shared with VIPlive and the structure of the healthcare groups and chains of care

As can be seen in figure 4, every healthcare group has its own implementations of the same authorization method. Within each healthcare group general practitioners can refer their patients to multiple kinds of healthcare providers connected in multiple chains of care, like the chains of care for COPD and diabetes.

The healthcare groups can determine for each role of healthcare provider within each connected chain of care which medical information they will receive. This is structured in a table called the 'set of medical information' which is pictured in figure 5.

Medication	Yes/no
Additional medication	Yes/no
Measured values	Yes/no
Episodes	Yes/no
Non-relevant episodes	Yes/no
Measured values	
When 'measured values' is checked as 'yes', a list of the selected measured values that will be sent is listed below	

Table 1; the set of medical information of patients which can be filled in by the healthcare groups

This table is filled in for each role of healthcare provider for every chain of care in which they operate. If 'medication' is check as yes, the receiver will have access to the medication that is relevant for the disease for which the patient is referred. 'Additional medication' concerns other kinds of medication, like Viagra for example, which is used by the patient but is not relevant for the reason of referral.
When 'medication' is switched off, no medication will be sent at all. When it is switched on, only the medication that is seen as relevant will be sent. Which medication is considered to be relevant and which ones aren't is determined automatically based on the code of the specific medication and the healthcare chain of the patient. For example; for a patient that is referred within the healthcare chain of diabetes, only diabetes-related medication will be sent. If 'other medication' is switched on as well, all of the medication will be sent.
An episode is a health problem, like medical conditions and diseases for example. Within the system of the general practitioner, the GP can select which episodes have 'attentie', which ones are the most important. This is translated as priority in this project. If 'episodes' is switched on, only those which have priority will be sent, but there is no further distinction within it. So if someone is referred for diabetes within that healthcare chain but the patient also has mental problems which are 'flagged' with priority, those will be sent along as well although they can be unrelated to the problem for which the patient is referred. If 'non-relevant episodes' is switched on, the episodes which aren't flagged with priority will be shared as well.
If 'measured values' is checked as yes, a list is composed below of all values that will be sent to the healthcare provider, like weight and blood pressure for example. As an example with fictive data for a fictive city, in figure 6 the set is filled in for a non-specified role within the diabetes chain of care.

Medication	Yes
Additional medication	No
Measured values	Yes
Episodes	Yes
Non-relevant episodes	No
Measured values:	
Blood pressure	
Weight	

Table 2; a fictive example of a filled-in set of medical information

This type of authorization can be seen as a collection of implementations of a Role Based Access Control model. As the role of the receiving party (medical specialist, podotherapist, etc) within a certain chain of care determines who receives which medical information of patients.

Topicus uses a single approach for implicit informed consent of patients, this is not different for each healthcare group. When a GP wants to refer a patient or wants to consult another healthcare provider, he or she asks the patient for consent. The patient can then decide whether he or she gives permission to share the whole set of medical information as determined in the system described earlier. If the patient does not give consent, none of the information in the standard set is shared to the other healthcare provider.
However, when the data in the standard set would be shared in the VIPlive application, there is also an option to provide extra information in an open text field, which can be filled in by the GP. Additionally as an attachment ('bijlage' in Dutch) extra documents can be added to be shared with the receiving healthcare professional as well. Using these two methods, the resulting set of data that

will be shared can be customized if the patient does not want to share certain data in the standard set.

Furthermore it is important to note that there is a difference between the actions in the level in which information is shared. In the case of a (further) referral the information is shared on an organization-level. In the case of a (further) consultation the information is shared on an individual level. When a healthcare professional within the organization is assigned by the assistants/secretaries to handle the consultation, the information will be shared with this professional.

Lastly, a feature which is not included in the standard sets at the moment but is discussed during the interviews, are the journal lines ('journaalregels' in Dutch). When a patient has visited the GP, the GP can enter a journal line. A journal line includes different parts:

- Subjective: what does the patient say about the medical issue, what does he/she think is wrong.
- Objective: what the GP him or herself has archived about the current situation.
- The GP can link the journal line to an episode of the patient. It is also possible to link the journal line to the medical condition of the healthcare chain within which he/she is treated, like diabetes for example.
- The further procedure.

4.2 Describing the current approach using the aspects of an authorization process model

Based on the description of the current approach as stated above, the model will be used to give an overview of the current authorization approach on this subject.

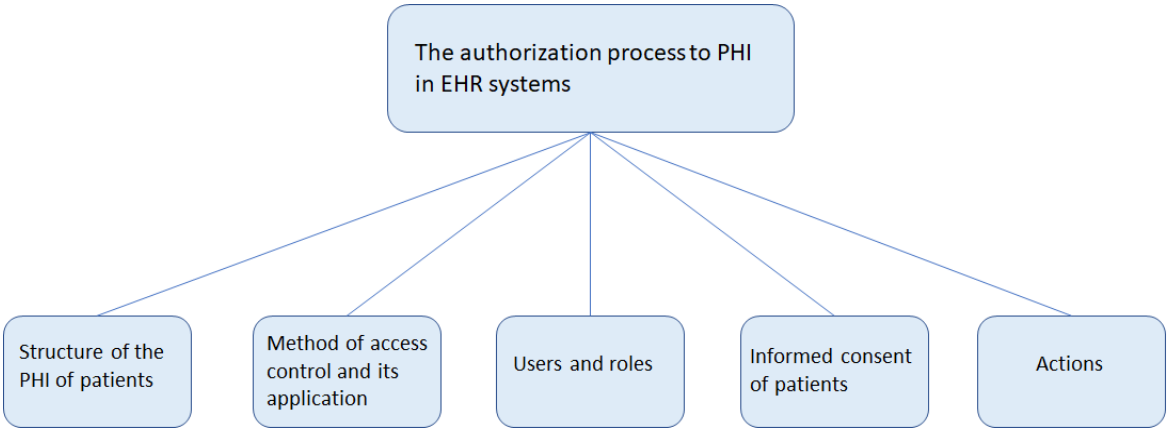


Figure 6; the five aspects of an authorization process

Structure of the PHI of patients	The 'set of medical information of patients', containing the following categories: medication, additional medication, measured values, episodes, non-relevant episodes and measured values
Method of access control and its application	Based on the 'set of medical information of patients', each healthcare group has different implementations of an RBAC model, based on the role of the receiver and the chain of care
Users and roles	A list of roles is defined based on the types of receiving healthcare professionals. Three types of roles can grant access to the PHI: General practitioners, (POH's) and receiving healthcare professionals that are able to refer to other professionals
Informed consent of patients	Implicit informed consent of patients
Actions	The actions that can be performed are: - Referral - Further referral - Consultation - Further consultation - Transfer of who is the main practitioner - Other

Table 3; using the five aspects model to describe the current authorization process to PHI in the VIPlive application

4.3 An analysis of the implementations of the authorization method

As mentioned before, each healthcare group has its own implementation of the authorization method, which consists of the filled in sets of medical information for each role of healthcare providers for each of the chains of care in which they operate. For this research project the implementations of three healthcare groups are analysed. This is done in order to gain more knowledge on the similarities and differences between the implementations of the healthcare groups.
This knowledge can be used in two ways. Firstly it is important to find out how large the differences in the implementations of the healthcare groups are. If the healthcare groups have implemented the model in practically the same way, wouldn't it be easier to use a single implementation of the authorization model for all healthcare groups? How much value would it add for each healthcare group to have a choice in their implementation if the result is practically the same?
Furthermore it is useful to have an overview on which parts the implementations of the healthcare groups are different and in which areas they are similar. This knowledge will be used in order to prepare for the interviews with the healthcare groups.

The implementations have been compared in the following way. For each of the researched roles of healthcare providers, a separate comparison table has been made. Within the table, comparisons are made between how the three healthcare groups have filled in the set of medical information for that role for each chain of care. An example of this with fictive information is given in figure 8.

Medical specialist								
		COPD						
Healthcare group 1			Healthcare group 2			Healthcare group 3		
	Medication	y		Medication	y		Medication	y
	Additional medication	n		Additional medication	y		Additional medication	n
	Measured values	y		Measured values	y		Measured values	y
	Episodes	y		Episodes	y		Episodes	y
	Non-relevant episodes	n		Non-relevant episodes	n		Non-relevant episodes	n
	Measured values			**Measured values**			**Measured values**	
	Weight			Weight				
	Length			Length				
	Smoking habit						Smoking habit	

Figure 7; a fictive example of the comparison tables used to analyse the implementations of the healthcare groups

If there was a difference in how the healthcare groups have filled in a category or measured value of the set of medical information for a healthcare provider within a certain chain of care, that part would be marked yellow. For example; In the fictive table in figure 8, which concerns the role of medical specialists, the implementations for the chains of care for COPD and diabetes are compared. As one of the healthcare groups has chosen to fill in 'yes' for 'additional medication' within the COPD chain of care, while the others have filled in 'no', that category has been marked yellow.
Using this method, an overview has been made of the differences between the implementations of the healthcare groups. The complete comparison tables can be found in appendix C. An analysis has been made below for each role of healthcare provider describing whether the implementations are comparable and what the most prominent differences are.

Podotherapist

The only chain of care in which podotherapists are involved is the chain of care for diabetes.

The implementations of the three healthcare groups for podotherapists were identical with only one exception: In healthcare group 1 the medication is sent along while in the other healthcare groups it is not.

Medical specialists

Medical specialists are involved in every chain of care that is included in this research (COPD, cardiovascular illnesses, diabetes and asthma).

The implementations of the healthcare groups for the role of medical specialists contained a large number of differences.
The most surprising result was that one of the healthcare groups has chosen to fill in 'no' for every category in each table, for every chain of care. In comparison, the other healthcare groups chose to fill in 'yes' for many categories, allowing the medical specialists to view many kinds of health information of the patients. In addition, long lists of measured values were listed. However, there are also many differences between the implementations of healthcare group 1 and 3. For example; In the chain of care for asthma, healthcare group 1 has chosen not to send any health information of patients to medical specialists, while healthcare group 2 has filled in 'yes' at every category and has filled in a list of measured values.

A large factor that can contribute in the large differences between the implementations is the variety of professions that fall under the role of medical specialist. There is for example a large difference between a cardiologist and a lung specialist and as such they may require different medical information of patients that are referred to them.
It is planned to split up the role of medical specialist in this system into multiple new roles. New implementations of the set of medical information will have to be made by the healthcare groups for these new roles.

Dietitians

Dietitians are involved in every chain of care that is included in this research (COPD, cardiovascular illneses, diabetes and asthma).

There are many differences in the implementations for the role of dietitians.
There is a large amount of disagreement between the healthcare groups differ on whether to send medication and/or additional medication to dietitians. Healthcare group 1 has filled 'yes' for both categories in every chain of care, while healthcare group 3 filled in 'no' for those categories in every chain of care. Healthcare group 2 also used the same approach for every chain of care but they filled in 'yes' for medication but 'no' for additional medication.
The healthcare groups do seem to agree on not to send them the episodes and the non-relevant episodes of the patients in every chain of care.

In the list of measured values that are filled in it is remarkable that the lists of healthcare groups 1 and 3 are very similar as they have filled in a large number of values that are missing in the list of healthcare group 2. However, healthcare group 2 has filled in multiple values in its list that aren't filled in in the lists of healthcare groups 1 and 3.

Pedicurists

The only chain of care in which pedicurists are involved is the chain of care for diabetes.

The implementations of healthcare groups 2 and 3 were identical. The only differences are that the healthcare group 1 also sends medication to pedicurists and sends multiple (meetwaarden) that aren't send by the other healthcare groups.

Conclusion of the analysis of the implementations

The implementations of the healthcare groups for the role of podotherapists were very similar, as well as the implementations of healthcare groups 2 and 3 for the role of pedicurists. However, besides this, the implementations of the healthcare groups differed greatly. The amount of differences was deemed too high for a single implementation for all healthcare groups to be realistic for this project. As the opinions on which role should receive which medical information are so different, it would be very hard to make agreements on this. Furthermore the healthcare groups themselves have mentioned that they value their freedom on implementing their own choices on which role can view which medical information.

Therefore the choice has been made not to build a single implementation meant for all healthcare groups in this project. Instead, the focus on this research will be to improve the working of the authorization method itself instead of the implementation. When this authorization process has been approved and implemented, each healthcare group will have the freedom to make their own choices on which party will receive which medical information in which situation.

5. Results of the interviews and the expert session

In this section the results of the group meeting and interviews will be discussed, following the format of the aspects of an authorization process that was described earlier. For each of the five parts of the model a separate paragraph is dedicated to discuss the results for that specific subject.
At the start of each paragraph, describing the corresponding part of the model, a table has been made containing an overview of the results of that part. The questions and main subjects within that part of that model are numbered. For each session it is noted in the table how the interviewees thought about the subject, which is done in the following way:

- A = Agreement
- A! = Strong agreement
- A* = Conditional agreement; for example when an interviewee agrees with the statement as long as certain conditions or other factors are held into account
- N = The interviewee was not sure whether to agree on the subject or was neutral
- D = Disagreement
- D! = Strong disagreement
- (Discussion) = During the group session and the interview with two employees of Topicus it happened that a subject was thoroughly discussed but at the end the participants didn't agree with each other. In those cases (discussion) is noted in the table

Within the table the subjects and questions that were present in all of the sessions are placed in the upper part of the table. Subjects that came up in several but not all sessions on the initiative of the interviewee are placed on the lower part of the tables below a blank row. For quick reference, the interviews and group meetings are referred to as numbered sessions when describing the outcomes.

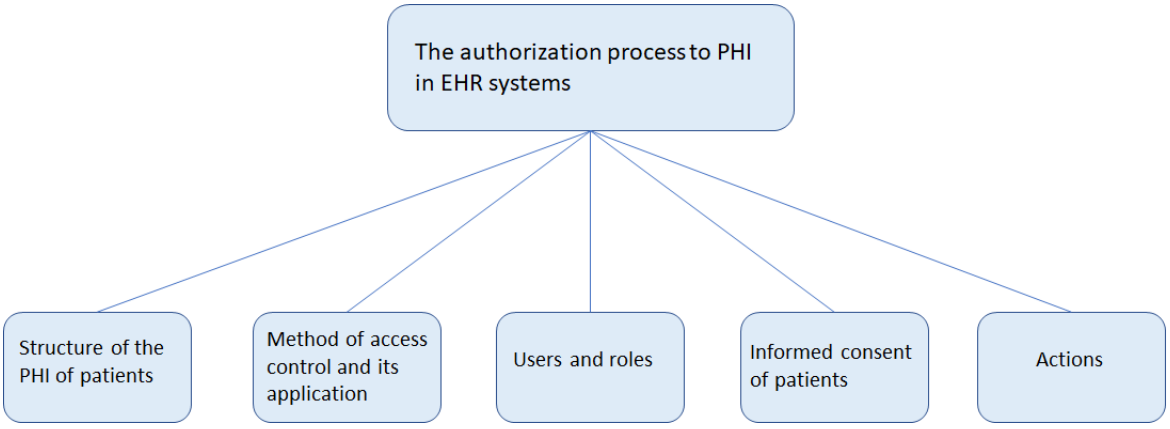


Figure 8: The five aspects of an authorization process

5.1 Structure of the PHI of patients

	Employees of Topicus		Healthcare groups		
	Session 1. Group meeting	Session 2. Interview with employees	Session 3. Healthcare group 1	Session 4. Healthcare group 2	Session 5. Healthcare group 3
5.1.1 More specificity within the episodes, medication and/or measured values	A*	A*	D	A*	N
5.1.2 Addition of journal lines	A*	A*	A*	A*	A*
5.1.3 Addition of health plan	A*	A*	D	A*	D
5.1.4 Addition of the results of measurements from home	A	A*	A*	A*	A
5.1.5 Addition of questionnaires	A*	A*	N	A*	N
5.1.6 Only the most important episodes are necessary			A	A	

Table 4: The results of the interviews on the structure of the PHI of patients

5.1.1 More specificity within the episodes, medication or measured values

A point that came up in multiple interviews was that there was a requirement to be more specific in which episodes and/or medication to give access to.

During session 1 it was noted that it would be better if there was more room for specificity within the episodes and medication. Although in the measured values it is possible to be very specific in which ones should be sent and which weren't, within the medication you either send everything, or only the ones that are automatically considered relevant, or nothing. When 'episodes' is switched on all the episodes which have priority are sent along while you may only want to send the episodes concerning diabetes, which is not possible at the moment.
The interviewees of session 2 also thought that there should be more specificity within the medication part. It would be ideal if only the medication that is related to a certain disease/illness can be included to share with other professionals. Currently the division which medication is considered to be relevant for which healthcare group is based on a rapport from Proigia. However it would be better if medical professionals, in consultation with the healthcare groups, would take a look at it and determine which medicine should be standardly sent in which case.
They did note that a problem with the medication category is that there are so many kinds of medication. The measured values is a relatively short list, which makes it easier to determine what should be sent in which case. But within medication there are many different kinds (for example, there are around 25 kinds and quantities of paracetamol), which can make it harder to decide what should be sent in which case.
In session 4 a need for more specificity was also given, for both the categories of episodes and medication. She thought that it would be better if each specific episode and kind of medication can be included or excluded from the standard set. However, if this is to be implemented, the GP should be able to make adjustments and additions to it during the referral itself.
The two other interviewees from healthcare groups thought differently however; one of them didn't have a preference on whether the set should be more specific except for the case of medical specialists, more information on that will be given in a later section of this chapter. The other

disagreed and thought that in the current system the set of medical information can be adjusted specifically enough.

A note on this that came up at both sessions with employees of Topicus is that more specificity and the ability to customize the set on a deeper level will primarily be relevant for referrals outside of the healthcare chains. Although it could also make a difference within the healthcare chains.

Furthermore it was discussed during session 1 whether the set of medical information should have different possible categories of information for different healthcare groups. It was decided that this is unnecessary; if a healthcare group does not want to make use of a certain category that is provided in the set they can simply switch them off.

5.1.2 Addition of journal lines

A point in which the opinions were quite different was the possible addition of journal lines. During two of the sessions it was mentioned that journal lines could be important to include when it concerns second-line care. One other interviewee said that the addition of journal lines would only be useful if the receiving professional has a clear picture of what kind of care the patient has recently received. During two sessions it was said that it would be ideal if this was a category that would not be standardly included in the set, but one which could be added if the GP finds the line useful in that specific case. In that case it would be good to check whether the journal line is linked to the episode for which the referral/consultation is done.
It is noted that if this would be implemented, a decision should be taken on how to do so. You could choose to only send the last journal line, but you could also choose to send the journal lines that concern the episode of the patient for which he/she is consulted or referred. During both sessions with employees of Topicus the remark was given that this would probably be primarily useful for referrals/consultations to second line health care.

5.1.3 Addition of health plan

The opinions differed on whether to include the health plan of the patient in the set. Two of the interviewees from healthcare groups where against this idea. One of them mentioned that in the current situation too much PHI is shared to healthcare professionals and that the addition of an healthcare plan would only worsen this.
The third interviewee from a healthcare group thought that this would be a valuable addition for both the elderly care as well as the chains of care. She did note however that if this would be implemented, it must be considered in which way. There are multiple different domains within a healthcare plan so it should be considered which party has access to which domain, a physiotherapist for example doesn't need access to the parts concerning mental health. One approach for this could be that for a certain healthcare provider and healthcare chain a selection of parts of the health plan is standardly included in the set, after which p arts can be included or excluded during the referral/consultation.
During session 1 it was said that the health plan could possibly be useful to send to medical specialists. But this was primarily considered to be useful for elderly care.
However it was said in session 2 that this probably isn't useful for professionals of the 2nd line. It was added that in the case of the health plan the ownership of the data should be kept in mind; there is a difference between medical information from the system of the GP (like measured values) and care related ('zorginhoudelijk' in Dutch) information like the health plan. In a legal aspect this should be looked at before the health plan can be added. Furthermore another difference is that in the case of measured values you would just send the data for the use of the receiver, but in the case of a health

plan it would be more like an invitation to cooperate together on the health plan.

5.1.4 Addition of measurements from home

During all sessions the interviewees agreed that measurements from home, which are called 'thuismetingen' in Dutch, would be a valuable addition. However, several requirements and conditions were stated on how this should be implemented.
One interviewee from the healthcare groups said that it is very important to keep in mind that there is a difference in the reliability of 'normal' lab values and measurements from home. Therefore it is important to make clear which values are measurements from home, for example by using a different colour or by putting a 'thuismeting' label next to it.
Another interviewee from the healthcare groups said it is important to keep in mind that the measurements from home should be executed properly. When these are done sloppy by the patient the resulting values can be inaccurate.
The interviewees from Topicus agreed as well that measurements from home can be a useful addition. It was noted however that this could provide a problem concerning ownership of the data, as this is information that belongs to the patient. So the legal implications and consequences of this should be looked into before this would be implemented. They thought it would be better if these measurements from home can be sent when this information has been added in the system of the GP. But not yet when this information is available for them in VIPlive but hasn't been added yet in their own system.

5.1.5 Addition of questionnaires

Another possible category that can be added are questionnaires that have been filled in by the patient. In both sessions with employees of Topicus it was mentioned that certain standardized and regular questionnaires within the mental healthcare can be shared so they don't have to be filled in again by the patient.
In the interviews with healthcare groups it turned out that the results of several questionnaires are already sent, these are included in the measured values (the results of the ACQ and CCQ in this example). One interviewee from healthcare groups said that if this would be added it is important to only send the conclusion of the questionnaire, not the entire list. She also added that this isn't a category to standardly include in a set for certain receivers, but would be something which can be added by the GP during a referral if he/she thinks it would be useful for that case.
During the sessions with employees from healthcare groups no questionnaires were brought up which aren't implemented yet but which would be useful to add.

5.1.6 Only the most important episodes are necessary

During two interviews the interviewees mentioned that too many episodes can be sent. At the moment a selection can be made whether to send episodes and/or other episodes, but these interviewees said that there was no need for the other episodes. In the cases of a consultation or a referral only the more important episodes are really relevant to send to the receiving healthcare professional. However, this category in the set can currently also be switched of for certain receivers.
Additionally one of the interviewees from the healthcare groups said that it would be better if only

the episodes which are still active would be sent along instead of all of them.

5.2 Method of access control and its application

	Employees of Topicus		Healthcare groups		
	Session 1. Group meeting	Session 2. Interview with employees	Session 3. Healthcare group 1	Session 4. Healthcare group 2	Session 5. Healthcare group 3
5.2.1 RBAC is a suitable approach for this case	A	A	A	A	A
5.2.2 Additions by the GP during referral/consultation	A	A	A	A	A
5.2.3 Omissions by the GP during referral/consultation	A	A	D	A	A
5.2.4 Influence of contents of health record	D	(discussion)	N	D	N
5.2.5 Nation-wide implementations	A*	A*	D!	D!	N
5.2.6 In the case of medical specialists the layer of chain of care is unnecessary in the model	A	A			
5.2.7. Sets of PHI based on the episodes instead of the healthcare chains	(discussion)	N			

Table 5: The results of the interviews on the method of access control and its application

5.2.1 RBAC is a suitable approach for this case

One point at which all interviewees agreed upon was that a role-based system, in which the information sent is partially dependant on the role of the receiver, was a proper approach for this case. When asked about the possible inflexibility of RBAC, as mentioned in the literature review, the interviewees from Topicus said that they didn't experience this in the current system.

5.2.2 Additions of the GP during referral/consultation

A point on which all parties agreed was that it would be a good addition if general practitioners would be able to make additions to the standard set of medical information during the referral or consultation. If the GP thinks a certain part of information is relevant which is not included in the standard set for that particular case, it can be added in this way.
One of the interviewees of the healthcare groups did mention that although it is fine if extra information is sent, it isn't necessary. Within the healthcare group the sets of information for each receiver have been made very carefully, they only ask for the medical information that they really need.

5.2.3 Omissions by the GP during referral/consultation

Another possible future implementation would be to make it possible for GPs to 'switch off' certain medical information which is included in the standard set during the referral or consultation. If the GP thinks some information, like a certain type of medication or one of the episodes or measured values, is unfit to send along it could be omitted in this way. In four of the five sessions the interviewees agreed that this should be implemented. One interviewee of a healthcare group was against this addition however, as she thought that all the information that is included in the sets is

necessary for the receiving healthcare professional to do their job. If certain information is lacking it is harder, if not impossible, to form a decent medical judgement on the situation of the patient.

5.2.4 Influence of contents of health record

A question that was asked during sessions was whether the contents of the health record of the patient in question should have influence on which medical information is sent. During the sessions it turned out that at the moment there isn't a clear need for this yet.
In session 1 it was said that if the GP is able to make adjustments during the referral/consultation, the GP can also make decisions on this matter based on the medical information of the patients. This would mean that this feature would already be implemented in that way. During two of the sessions the interviewees weren't sure whether this would be a suitable addition, but that it is possible that this would be a useful feature for the medical specialists. But as there isn't a clear picture on the requirements of the medical specialists, they weren't sure on that. The last interviewee of the healthcare groups didn't think that this addition would be useful.

5.2.5 Nation-wide implementations

During the group meeting it was mentioned that the current system has a high administrative burden. As every healthcare group has a collection of implementations for each healthcare chain, the current system results in a large amounts of sets which have to be taken into account. One possible solution in order to lighten this burden would be that instead of each healthcare group having its own collection of implementation, there would be one national collection of implementations.

In session 1 this administrative burden was clearly stated, the interviewees were in favour to work towards nation-wide implementations. However it was also said that this can get complicated as the regional implementations are also dependant on the agreements that are made between medical parties in the region. For example, a contract is made between the healthcare groups with podotherapists concerning which information will be sent towards the podotherapists. If those contacts state that certain medication is to be sent to the podotherapists, the systems of Topicus should be able to support this. Therefore, if nation-wide implementations are to be worked towards, this is an important factor to keep in mind.
In session 2 it was said that it would be nice if nation-wide implementations would be implemented, but it is hard to achieve agreement on this with all of the involved parties. It was also questioned whether it was feasible to make the same national approach for medical specialists as they could have very specific requirements for information.

However, all three of the interviewees of healthcare groups said that it was greatly appreciated that the healthcare groups can make their own implementations. Two of the three were strongly against a national collection of implementations. Multiple arguments have been brought forward for this: That the approaches and ideas on this subject vary for a large amount between the healthcare groups which causes different requirements on this subject for each group. That different agreements have already been made concerning healthcare programmes. That every healthcare groups has already made their own agreements with other parties like hospitals, insurance firms and 2nd line organizations. That healthcare in general can work in quite different ways for each region. Th One of them did question whether it was really necessary to have separate implementations for each healthcare group. The medical specialisations and professions that are concerned in this case exist in every region so a similar approach could be feasible.

5.2.6 In the case of medical specialists the layer of chain of care is unnecessary in the model

A point that was discussed during both sessions with employees of Topicus was that the layer of healthcare chain wouldn't be necessary in determining which information to send to medical specialists. In session 2 it was said that if you are referred to specific medical specialist like a cardiologist, you wouldn't want the medical information to be sent to him/her depend on the healthcare chain. Instead you would want to be able to adapt the information that is sent for each case, making use of the additions and omissions as described earlier.

5.2.7 Sets of PHI based on episodes instead of the healthcare chains

A suggestion that came up in session 1 was that if referrals would take place outside of the healthcare chains it would be possible to base the sets on the episode(s) of the patient. In this case, for each relevant episode certain information (like specific medication, measured values etc.) would be linked, based on which the set would be determined.
However, both within this session as in session 2 there were quite some doubts on this. It could become quite a high burden on maintenance if this would be implemented. It could also become a quite rigid system if the set is determined purely based on the episodes. Another suggestion was to discuss with the patient which episodes the patient wants to send, after which the medication and measured values that are linked to the 'approved' episodes are added as well.

5.3 Users and roles

	Employees of Topicus		Healthcare groups		
	Session 1. Group meeting	Session 2. Interview with employees	Session 3. Healthcare group 1	Session 4. Healthcare group 2	Session 5. Healthcare group 3
5.3.1 Is a different approach needed for the role of medical specialist?	A	A	A	N	A
5.3.2 Should the role of who makes the referral/consultation influence which information can be sent?	D	D	D	D	D
5.3.3 Addition of role for medical assistants		A	A*	N	

Table 6: The results of the interviews on the users and roles

When the interviewees were asked about their opinion on the roles that are currently used in the system and whether there should be additions or changes, the answers were quite similar. The role of medical specialist was the only role currently in the system for which there was a need for adjustment. In multiple sessions a need came up for a role for medical assistants. These roles will be elaborated upon later in this chapter. Furthermore there was no need for more or less specification of the current roles or further additions of roles.

5.3.1 Is a different approach needed for the role of medical specialist?

At the moment there is a single role that is used for every kind of medical specialist, however a widespread requirement of all interviewees was that a different approach is needed for this.

However, action is already undertaken as new roles that would replace the role of medical specialist are under development at Topicus.

It is important to note that the three interviewees of the healthcare groups said that they didn't have a clear picture yet of the needs and wants of all kinds of medical specialists concerning the information they need to receive. One of them also mentioned that she wasn't sure what the best approach for the medical specialists would be as there are so many specialisations. She said that if a separate role would be made for each specialisation, you would easily get about 25 new roles. Another interviewee mentioned that it would probably be the best approach if a separate role would be made for each kind of specialist. But within her healthcare group the requirements of the specialists on this matter still had to be collected.

It is worthwhile to note that these specialists may have very different information requirements than other healthcare providers; One of the healthcare groups has even made separate forms for the pneumonologists as the medical information they would like to receive could not be entered in the VIPlive application. In these forms specific kinds of information can be entered like whether the patient sometimes forgets to take his/her medication or if he/she has experienced side effects from the medication.

5.3.2 Should the role of who makes the referral/consultation influence which information can be sent?

The interviewees were unanimous on the matter that the role of the person who does the referral, like a GP or a practice nurse('praktijkondersteuner' in Dutch) should not influence which medical information is sent. It was noted however, that if a practice nurse does a referral is should really be done in consultation with the GP, which is an important requirement for the healthcare group.

5.3.3 Addition of role for medical assistants

During two of the three sessions it was mentioned that an added role for medical assistants, in which it would be defined which medical information they would be able to access, would be a valuable addition. In session 3 it was said that in such a role it would also be useful to define what an assistant can or cannot do, like that they cannot start a consultation for example.
However, in session 4 it was said that this would be hard to realize. It is difficult to determine which medical information an assistant or secretary should be able to see. For example; within a medical practice the choice which doctor is the most suitable to pick up a consultation can be based on the medical information of a patient. Based on the medical information it can also be determined whether the situation at hand is one of urgency or not. There can be differences between practices in how this process is implemented which can make it more difficult to determine which information they standardly should be able to access. Furthermore it would be impractical it for a referral of a patient two separate referrals (one for the assistant, one for sending the data to the receiving healthcare professional) would have to be sent.

5.4 Informed consent of patients

	Employees of Topicus		Healthcare groups		
	Session 1. Group meeting	Session 2. Interview with employees	Session 3. Healthcare group 1	Session 4. Healthcare group 2	Session 5. Healthcare group 3
5.4.1 Patients should have more control over which information is sent	A*	A*	D	A	D
5.4.2 The consent of patients should be centrally recorded	A	A		A!	A
5.4.3 Insight for the patient on which information is shared with whom	A*	A		A	

Table 7: The results of the interviews on informed consent of patients

5.4.1 Patients should have more control over which information is sent

One of the matters in which there was a high amount of difference in opinion was how much control the patients should have over which healthcare professional would receive which information.

- In both sessions at Topicus the interviewees mentioned that it is important to take into account in the development of systems that patients will probably get more influence on this process in the future. It was remarked that patients should be able to make adjustments afterwards on which matters/transactions of information they give their consent.
- It was noted that if this would be implemented, it is important that the medical information is categorized in a manner that is understandable for patients. Furthermore, patients should have an easy to select option to give consent for the sharing of the information that is relevant and important for his healthcare.
- One of the interviewees of the healthcare groups said that it would be better if the patient would be able to remove each type of medication, episode or measured value from the set of information that would be sent. This would be a form of granular control on which information is sent to the receiver.
- The two other interviewees of the healthcare groups however were against granular control of patients. According to one of them it is better to not send a consultation at all if the patient was against sending a part of medical information that is included in the set, as all of the information is needed to make a proper medical judgement.
  According to the other the patients cannot oversee which medical information is important to send, so they should have faith in the medical professionals in that they know what is best to send in their situation.
- During two of the sessions it was mentioned that it is very important that the information that is sent to the receiver is still useful for the receiver. If important information is left out because the patient doesn't give consent to it, the receiving professional may be limited in his/her ability to asses the medical situation of the patient.
  During the group meeting an idea was also brought up for a system that makes sure that the medical information that is sent, after possible omissions from the patient, is still relevant for the receiver.

5.4.2 The consent of patients should be centrally recorded

In four of the five sessions it was mentioned that it should be recorded centrally for which parties and which medical information the patient gives consent.
One of them mentioned that it would be very useful if this is recorded in the app of VIPlive.
One of the interviewees from a healthcare group said that this centrally recorded consent of patients shouldn't only be for the sharing of information through the use of VIPlive, but for the sharing of patient information through other applications as well. A centrally recorded collection of cases on which the patient has given or hasn't given consent, which can be adjusted during the referral.
In the sessions with employees of Topicus it was brought up that there are already initiatives on this matter: OTV(from the government) and NUTS (from the company Nedap), projects to centrally record which information patients want to share with whom.

5.4.3 Insight for patient in which information is shared with whom

Another aspect that came up is that it is important to provide insight to patients into which of their health information is shared with which parties, this came up during three sessions.
During one session it was remarked however that if insight is given to patients on this matter, it should be in a format that is understandable and less abstract for them. It would be more useful if the shared information was categorized into different purposes or illnesses, in which diabetes-related information would be separated from others for example.

5.5 Actions

	Employees of Topicus		Healthcare groups		
	Session 1. Group meeting	Session 2. Interview with employees	Session 3. Healthcare group 1	Session 4. Healthcare group 2	Session 5. Healthcare group 3
5.5.1 The performed action should influence which medical information is sent	D	A	A*	A*	D
5.5.2. The case of a further referral should be handled differently	D	(discussion)			
5.5.3 The case of a further consultation should be handled differently	D	(discussion)			
5.5.4 How long should a referral stay active?	(discussion)	(discussion)			
Difference between referrals and consultation in to whom the information is sent					

Table 8: The results of the interviews on the actions

5.5.1 The performed action should influence which medical information is sent

Concerning the question whether the action that was performed should influence which information is sent, the opinions differed for a large amount. In two of the sessions it was said that there should be no difference between the performed actions on which information is shared. This is including the case of a referral/consultation towards a medical specialist.
During three other sessions however it was said that this should make a difference. Arguments that

have been brought forward for this include; That a consultation is quite different from a referral and so the information requirements between the two are probably quite different. That there are multiple kinds of referrals as there are multiple kinds of receivers (other professionals in the healthcare chain, second line healthcare, elderly care, etc.) which require different sets of information. Although it could be argued that this is more related to different roles than different actions.
During two of the sessions with healthcare groups it was said that currently there already is a difference between the different actions. This is due to the fact that the transfer of main caretakership is done using a different application, which involves a different set of information. If this could be done by VIPlive in the future, a different set for this action would be required as well, but the current situation was considered to be suitable for them.
One of those interviewees said that in this situation you would want to transfer all medical information in most cases, in which this action would be different from the other actions, although it should still also be dependent on the role of the receiver.

5.5.2 Case of a further referral

The case can occur that when a patient is referred to a podotherapist, the podotherapist later refers the patient further to a pedicure (a 'doorverwijzing' in Dutch). Then it isn't the GP who refers the patient but the podotherapist, while the information that is sent to the pedicurist comes from the system of the GP. The patient is asked for consent in this case, and the pedicurist receives a different set of information than the podotherapist.
The opinions differed on how this should be handled. During the group meeting the consensus was that the current approach is currently the only workable one; although it would be better if the GP could give consent in the meantime, that would mean that this will take extra time for the GP, so a workable solution should be found for this. During session 2 it was mentioned that the GP should give his/her consent in this case. The participants agreed that it would be most important that the patient has given consent.

5.5.3 Case of a further consultation

In the case of a further consultation ('doorconsultatie' in Dutch) a medical professional receives a consultation, after which he/she in turn consults another medical professional to look at it as well. The consultation is 'forwarded' in order to give a more proper judgement on the case at hand, however, the GP is often not aware that the consultation has been forwarded.
In session 1 the current approach was seen as the currently only workable method, as other approaches would hinder the proces.
In session 2 there was a difference in opinion on this matter; it was said that a notification should be sent to the GP in this case, but GPs should also be informed that these cases can happen, that they should keep in mind that consultations can be forwarded.
On the other hand it was said that the current situation is fine, but if a consultation is forwarded to a specialist in another hospital, it would be important to ask for permission.

5.5.4 How long should a referral stay active?

As long as a referral stays active, a receiving healthcare professional like a dietician has access to certain medical information about the patient which originates from the system of the GP. The information that the dietician has access to is also updated as long as the referral stays active.
When asked about how long a referral should stay active, the answers were quite different.

During session 2 there was a clear preference for giving a maximum duration of the referral. The opinions were different on how this maximum duration should be, one preferred a maximum of 1 year, the other preferred to let the maximum duration depend on the kind of receiving healthcare professional.
During session 1 no maximum duration of the referral was given. The preferred outcome was that the referral should stay active for as long as the receiving healthcare professional is treating the patient. Both the general practitioner as well as the receiving healthcare professional are able to close the referral. The referral is also closed when the patient moves to a different location or is removed from the healthcare chain. It is preferred that the patient will also be more involved in this process in the future, so that he/she is also able to close referrals to healthcare providers who aren't relevant anymore for his/her care process.

6. An exploratory review of the GDPR

In order to gather information on the legal requirements on informed consent for the improved process and the authorization model an exploratory review on the GDPR has been done. The GDPR is known as the 'AVG' or 'Algemene Verordening Gegevensbescherming' in Dutch. The purpose of this chapter is to gather basic information on the GDPR and on its rules and guidelines on informed consent when applied to the case in question. When clear legal requirements and/or guidelines for this case are found, these can be used in the development of the new authorization model. When rules and/or guidelines are found that might be relevant for this case but require further investigation, these are noted in section 9.2, for further research. As this is an exploratory review, a professional legal assessment is recommended in order to gain an conclusive overview of the legal requirements on informed consent for the improved authorization process and the new authorization model.

6.1 An introduction to the GDPR

The GDPR is a regulation in the law of the EU that concerns when and how companies in the EU are allowed or are not allowed to handle information of persons. Within the GDPR there is room for EU countries to give further specifications in the form of implementation laws. The Dutch implementation law for the GDPR, the 'uitvoeringswet algemene verordening gegevensbescherming', has been taken into account as well in this chapter.

The first thing to note is that the GDPR makes a clear difference between a controller of personal data and processors of personal data. The controller is the leading party in this exchange, the processor's role is to process the personal data commissioned by the controller. As seen from this viewpoint, Topicus is considered to be a processor, which gives Topicus different duties and factors to keep in mind when compared to a processor. Among others, important duties of a processor of personal data include:

- To document what your organization is doing with the personal data and why, who has access to them and where they are stored.
- Make sure that within your organization only the persons who actually need to have access to the data can access it.
- To delete personal data when it is not necessary anymore for the assignment that you have been given from the controller.

The GDPR gives multiple fair information principles and numerous rules on how the processing of personal information of individuals should be handled. For this research the focus will be on the rules on how informed consent of patients should be implemented in the improved authorization process and authorization model. An overview of the other rules and principles can be found in the 'Handleiding Algemene verordening gegevensbescherming' [26].

In order for an organization to be allowed to process personal data, at least one of the six legal basis's to do so should apply. One of these basis's is that the person involved has given consent that his/her data is processed.
However, information concerning the health of a person is one of the kinds of data that is included in a special category which is called 'sensitive personal data'. Other kinds of sensitive personal data include information about ethnic origin, sexual orientation and religious beliefs. As these kinds of data are considered to be more sensitive than other categories of data, it is forbidden for organizations to process sensitive personal data under the normal conditions.
Several exceptions for this are defined in the GDPR [26]. The processing of sensitive personal data is allowed when the requirements for one of these exceptions is met, as well as the requirements to handle non-sensitive personal data. One of these exceptions is when a patient has given 'explicit consent' for the processing of his/her data. Before consent can be seen as explicit, even stricter requirements will have to be taken into account compared to the requirements for consent for non-sensitive data.

Therefore multiple requirements will have to be met before informed consent of a patient can be used as a basis to process his/her medical data: the requirements that are stated for consent to process non-sensitive personal data, as well as the requirements for 'explicit consent'.

6.2 The requirements of the GDPR for informed consent in this case

For this case, the following conditions for consent for non-sensitive personal data are seen as particularly relevant:

- Freely given: The person has to have a realistic option to refuse to give consent, without having to face negative consequences when he/she does so.
- Specific and informed: Consent should be given for a specific processing and a specific purpose. If the information will be processed for multiple purposes, consent should be asked for every one of them. The person in question should be well informed on the purposes for which the data is processed. Other relevant information that is important for that person to be able to make a proper judgement must be given as well.
- Non-ambiguous: The consent will have to be non-ambiguous, there can be no doubt that the person has given consent. The opt-out approach of consent, as described in section 3.4, is not allowed as the giving of consent should be a separate, conscious action. The opt-in approach is allowed.

There is an additional requirement for when consent is given in a written declaration that is applicable for multiple affairs. In these cases a clear distinction will have to be made between the matters on which the patient has given consent and the other matters.

In order for the consent to count as the required 'explicit consent', there can be no doubt at all whether the patient has given consent on a specific matter [26]. The act in which explicit consent will be given has to be specifically aimed at the giving of consent, in which it must be very clear for which matters the patient will or will not give consent.

As translated from the GDPR itself [27]: The prohibition to process medical data is not applicable, when the person in question has given explicit consent for the processing of these specific personal data for one or more well-defined purposes.

Furthermore, when patients have given consent to process their personal data, they are allowed by the GDPR to revoke their consent later on. This has no influence on the processing of their data before they revoked their consent. But from that moment on the data for which they have revoked their consent cannot be processed anymore.

Based on the requirements as stated above, it seems likely that some form of granular control of patients will have to be implemented in the new authorization model. This will preferably be one in which specific entries of data can be omitted instead of entire categories of data. For example; that specific kinds of medication can be omitted to be shared, instead of the entire medication category.

To process medical information without one of the exceptions is prohibited; if the exception of explicit consent is used as a basis, only the medical information to which the person in question has given consent can be processed. For example; a patient in the case of the improved authorization process could give consent to share data about his/her episodes and the measured values, but no consent to the sharing of certain types of medication. It is important that the involved application allow this distinction to be entered.

There is a requirement that the patient has to have a realistic option to refuse to give consent, without having to face negative consequences when he/she does so. In a system which allows for granular control, in which specific kinds of data can be omitted to be shared, this requirement can be met. If only entire categories can be omitted, the entire medication category for example instead of specific kinds of medication, it is questionable whether this requirement is met. If the entire medication category is omitted this can be considered a negative consequence as the other pieces of information may include important parts for the receiving healthcare professional. This may have consequences for further treatment if the patient is referred, as the receiving professional lacks certain data and may have to test for this data.
Additionally, what if a patient wants to revoke their consent to the sharing of certain parts of their data after a referral? If the patient is able to revoke consent for specific entries of data the amount of data the receiving healthcare professional has lost access to can still be limited. If by doing so other kinds of medication to which the patient has given consent must be omitted as well as only entire categories can be omitted, it could prove to be much more problematic. Furthermore, if a consultation takes place but no data can be shared at all while the patient just wanted to omit one piece of data, the receiving professional cannot make a proper medical judgement.

Lastly the abovementioned requirement concerning a written declaration that is applicable for multiple affairs may be relevant here as well. It states that a clear distinction will have to be made between the matters on which the patient has given consent and the other matters. If this applies to the different kinds of medical information that can be shared, this certainly is an important part to keep in account when the implementation of informed consent is developed.

Another point to consider is that according to the GDPR the party that is responsible for processing the data must be able to prove that the patient has given consent. It is recommended to investigate this further and take the legal requirements on this matter into account during the development of the new approach.

It seems likely that according to the GDPR some form of granular approach for informed consent is needed for the improved authorization process and the new authorization model. However, to give a

definitive conclusion of the requirements of the GDPR, further research is needed. Furthermore there are other laws in the Netherlands besides the GDPR that are relevant on the subject of informed consent [25], like the 'wet op de beroepen in de individuele gezondheidszorg' and the 'wet op de geneeskundige behandelovereenkomst'. A professional legal assessment is recommended in order to be sure the legal requirements on this subject are met properly.

Furthermore, when the legal requirements on informed consent have been found, it should be properly investigated how the approach for informed consent should be implemented in practice. The requirements from both Topicus and stakeholders like the healthcare groups and patients should be kept into account when this new approach is designed. The results of the interviews of this project can provide useful information for this process, as an overview of the opinions of the interviewees on this subject has been made.
It is important to note that two of the three interviewed healthcare groups were not in favor of granular control of patients. During the development of the new approach for informed consent it is certainly important to take their concerns seriously. Besides the legal requirements, it is recommended to develop the new approach in consultation with other important stakeholders like the healthcare groups.

7. Designing a new authorization model for the Datakluis

In the development of the improved process and the new authorization model, three factors were originally planned to be taken into account: the results of the interviews, the literature review and the results of the exploratory review of the GDPR. The results of the literature review were applicable for several choices of the resulting model, like the choice for the access control method. The results of the review of the GDPR were planned to be used in the choices concerning informed consent. However, that chapter did not yield any results on how that subject should be handled. Therefore, the results of the interviews have been taken into account for all choices and the results of the literature review have been taken into account as well where they were applicable.

The model itself consists of three parts: Which information concerning authorization should be stored, the core steps on how the information concerning authorization is generated and the core steps on how to retrieve information as a receiver.

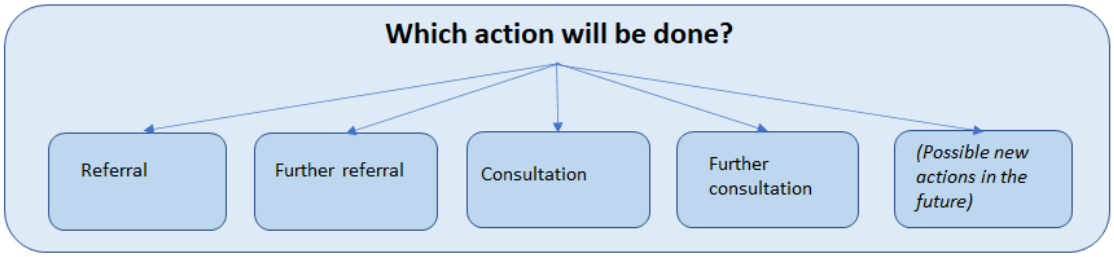
In 7.1 a short overview of the improved process will be given based on a diagram. The goal of this part is to give a clear picture of how the process works, without giving too many details or explaining how each choice was made.

In 7.2 the individual choices for the process and more specific details are explained, corresponding with the 5 aspects of an authorization process as described in earlier chapters and the subjects of discussion in the interviews.

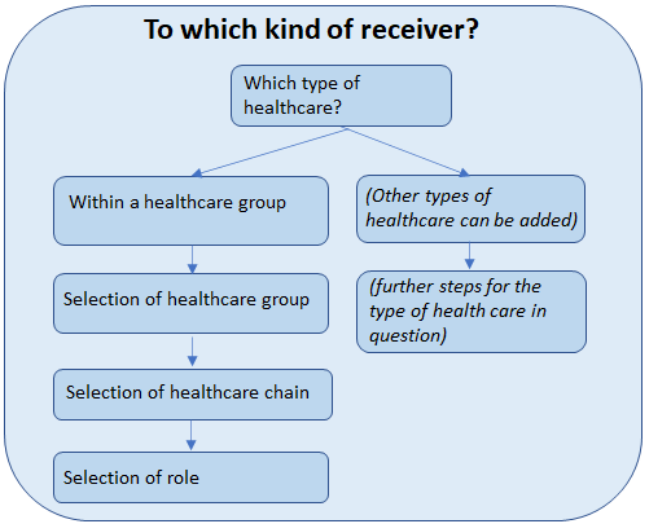
In 7.3 the authorization model itself is explained. The storage of the information concerning authorization is described. Afterwards the core steps in which this information is generated are described as well as the core steps to how a receiving party can gain access to the medical information.

7.1 An overview of the improved process

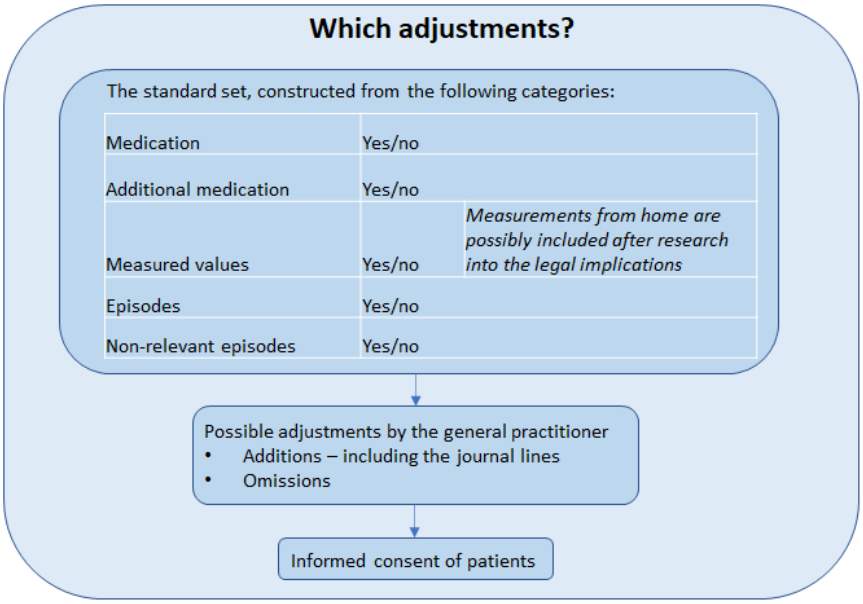
This diagram has been made to give a clear picture of the steps and choices that determine which medical information is sent to which receiver.



Based on the action, the level at which information is shared can be determined



Based on these steps, a standard set of medical information is chosen



Based on these choices, a final set of medical information is made

Figure 9; an overview of the improved process

In the first part of the process, the choice which of the four possible actions is made. As new actions can be added in the future, an extra space has been made in the diagram to show where they can be added. This choice does not influence the set of medical information. However there are differences between the actions concerning at which level the medical information will be shared with the receiving organization.

The next part of the process concerns to which kind of receiver the medical information of the patient is sent. This is relevant as which information is sent to which receiver is largely dependent on the kind and/or role of the receiver. This diagram was based on this research, which has focused on the exchange of medical information to healthcare groups. However, this model may also be used for other kinds of healthcare (like mental health care for example) in the future. This is why a choice between the types of healthcare has been added as well as a space where new types of healthcare and their further steps could be added. But this research was not focused on these other types of healthcare however, so whether this diagram in its current form is suitable for them should be researched beforehand. It is quite possible that the diagram will have to be adjusted if other types of healthcare would be added.
Within a type of healthcare in this diagram, like the receivers within a healthcare group, several choices can be made like which healthcare chain and role of the receiver. Based on the choices in this part in which the specific type of receiver is determined, a standard set of medical information is automatically determined, which corresponds to the type of receiver.
At the moment each healthcare group has their own collection of standard sets, the same is true in this improved process as there was a large difference of opinion in the interviews on that matter. In the case that there will be a national collection of standard sets in the future the step 'selection of healthcare group' can be omitted.

The next steps concern the set of medical information and which adjustments are made to it. The standard set contains multiple categories, which are switched on or off depending on the standard set. A notable change to the earlier model as applied by Topicus is that measurements from home could be added to the category of measured values. However, the legal implications concerning the ownership of this type of information should be looked into before it can be included in that category.
The GP is now able to make adjustments to this set, on the level of individual types of medication, episodes and measured values. Types of information that were present in the standard set can be omitted and other types of information that were not present in the standard set can be added if the GP wishes to do so. A point of note is that journal lines are a type of medical information which is never present in the standard set, but can be added to the set by the GP if he or she wishes to do so. More information on this can be found in part 7.2.
Afterwards the patient is asked by the GP whether he or she gives consent to send this set of medical information to the receiving healthcare professional. However, it is currently still an unanswered question what the best approach for informed consent is in this case. Until a new approach has been found in further research the current approach can be applied in this process. More information on this can be found in part 7.2.
After these steps have been made, a final set of medical information of the patient has been made.

7.2 The improved process in detail

In this part of the chapter details are given concerning the choices made in the improved process, following the structure of the five aspects of an authorization process as described before.

7.2.1 Structure of the PHI

Concerning the specificity of the standard sets of medical information, there have been some changes compared to the current situation. Multiple recommendations for future research have been given as well.
Concerning medication this new process works in a quite similar way as the current approach; a certain set of medicines of the patient are automatically added to be sent to the receiving healthcare professional, which types of medication these are is dependent on the healthcare chain of the patient. The changes are as follows; The GP is now able to adjust the list of medications that is to be sent to the receiving healthcare professional by using the additions and omissions features, which are explained further ahead in this chapter. Another change is that, as advised in session 2, which types of medication are associated with which healthcare chain is redetermined by healthcare professionals of the healthcare groups, to make sure relevant lists are automatically generated to be sent.
The system of the episodes works in the same way as the current process as is explained in chapter 4, although the GP can also edit the list of episodes which are sent by using the additions and omissions feature.
By the use of the additions and omissions feature, more flexibility and more room for specificity has been added in the sets of medical information, as was desired in the interviews. By using these features, the final set of medical information which is sent can be completely customized by the GP.
In one of the interviews it has been said that it is desirable that the healthcare groups should be able to edit the standard sets on the level of individual types of medication and episodes, for every role and healthcare chain. The choice has been made to not implement this as the administrative burden for Topicus would grow by a large amount. Furthermore, the workload for the healthcare groups to make the standard sets would be far greater, as for every role in each healthcare chain a choice should be made for all kinds of episodes and medication. Lastly, only in three of the five sessions a requirement for more specificity was given, so to implement it in such a way seems excessive.

A possible downside of this process would be that the additions and omissions feature could increase the workload of GPs, as they possibly have to adjust the sets of a certain part of their patients. Therefore, multiple recommendations for further research in order to implement this model properly have been given:

- To research whether the workload of the GP would actually increase in a significant amount in this way.
- If so, whether it would be worthwhile to implement a feature, that would enable a GP to automatically add or remove episodes and/or medication that are linked to other common healthcare conditions. For example, so that the GP can choose to automatically remove the medications and/or episodes that are related to depression while doing a referral, instead of having to remove each individual one individually.
- Concerning episodes, it is advised to look into the current system of automatically adding all the episodes which have priority. Which is done despite the fact that some of those episodes may have nothing to do with the reason of the referral/consultation. This research project was too limited to determine whether a different approach for this subject would be more suitable.

- To redetermine which types of medication are ‘linked’ to each healthcare chain, which determines which types of medication of the patient are automatically added. This should be done by, or in cooperation with, healthcare professionals of the healthcare groups to ensure that relevant lists of medication are sent.

The measurements from home would be added to the same category as ‘measured values’ along with the regular measurements. However, this can only be implemented with the condition that it would be clear for the user that the specific value concerns a measurement from home. The choice to add it in the same category instead of a separate category has been made as a preference for this method was given in the interviews. Besides, adding a new category would increase the complexity of the set of medical information.
However, as mentioned before, the legal implications should be looked into before this feature can be added.

Journal lines have been added as an optional part that a GP can manually add to the set by using the additions feature, it will not be added to the standard sets. This has been done as a preference for this was given during the interviews. How exactly this feature should be implemented is added to the recommendations for future research as there are multiple options on how to do so.

The health plan has not been added to the set of medical information yet as there was a high difference of opinion on this subject. In two out of five sessions the interviewees were against the addition. If this feature would be added in the future there are also two matters which should investigated first:

- How the health plan should be added, as there are multiple different domains within such a plan and not every receiver would require all of them.
- The legal implications of adding the health plan.

The results of questionnaires are already included within the measured values category, which is seen as a fine approach. No new questionnaires are added.

Although it has been mentioned in two of the five sessions that the other episodes were most often unnecessary, no change has been made in the model on this matter. This is due to the option for healthcare groups to switch the category of other episodes off for a specific role within a healthcare chain, which would solve the issue.

7.2.2 Method of access control and its application

RBAC is kept as the basis for the new process. In the literature review RBAC is seen as an often-used and suitable access control method for similar systems, and in the interviews it was unanimously seen as a proper approach. A disadvantage of RBAC as written in the literature review, the possible inflexibility, was not experienced in this particular case.

Additions to the standard set by the GP during the referral/consultation have been added as all of the interviewees were unanimously positive on this subject. This can be done on the level of individual medications and/or episodes. As written in the literature review, the context of the situation can influence which information is desirable to share. By using additions, measured values and/or omissions to the standard set, the GP can take contextual factors into account when making the final set of medical information.

Omissions to the standard set by the GP during the referral/consultation have been added as in four out of five interview sessions were in favour for this feature. However, the aforementioned matter

that omitted information may make the decision for the receiving professional harder is advised to include in further research. Just like the additions, the omissions can be done on the level of individual medications, measured values and/or episodes.

One of the interview questions was whether the contents of the health record of a patient could automatically influence which medical information would be sent. For example, if a patient has a certain illness in his or her record, that the standard set that would be sent would automatically be adjusted. But as there wasn't a clear need for this, this feature is not added. As the features of additions and omissions have been added, the GP can make these changes during the referral/consultation if this is desired.

There was a high amount of disagreement on the subject of nation-wide implementations among the interviewees. Due to this disagreement, in this model the nation-wide implementations have not yet been added.
However, among the subjects that are advised for further research, this matter has a relatively very high priority due to the aforementioned high administrative burden for Topicus.

In two sessions the option was discussed whether to base the standard sets on episodes instead of the healthcare chain. However, this was not implemented as in both sessions there was quite some doubt and discussion on this subject. This subject has been added to the list of advices for further research.

7.2.3 Users and roles

Topicus is currently working towards the replacement of the 'medical specialist' role with new roles, as there are many kinds of medical specialists. The results of the interviews have also shown that there is a clear need for a new approach for the medical specialist. In the new authorization model the new roles for medical specialists would be implemented that Topicus would like to add in the future.
For further research it is advised to look into the requirements of the medical specialists concerning the information they will receive, as the interviewees from the healthcare groups did not have a clear picture on that subject.

Just like the current situation, the role of who makes the referral/consultation will not influence which information will be sent, as none of the interviewees gave a preference for this.

The role of the medical assistant has been added in this model. However, as said during the interviews, it should be looked into which medical information this role should be able to access.

7.2.4 Informed consent of patients

A separate step has been made in the diagram of the authorization model to indicate where in the process the informed consent of patients should be handled. However, this research project is seen as too limited and the results on this matter where seen as too divergent to make a final judgement. Not only was there a high amount of disagreement on this subject among the interviewees, both advantages and disadvantages for this matter were found in the literature review. Furthermore, the exploratory review of the GDPR did not result in an answer on this matter should be handled from a legal aspect. Furthermore, due to the limited scope of this project, multiple important groups have not been interviewed for their opinion, like the general practitioners, the receiving healthcare professionals and the patients.
Therefore, further research is certainly needed to make a final decision on this subject. The relevant

factors and opinions that are found during this project are recapped below. Until a new approach has been found in further research the current approach can be applied in this process; that during a referral for example the GP will ask the patient if he or she gives consent to share this information to the receiver. The patient can choose not to send any medical information, or all the information that is included in the resulting set.

From the literature review, it turned out it is a widely applied approach in healthcare to enable the patient to control the disclosure of the content of his or her EHR, a trend is seen that patients are given more control over health decision making. It also turned out in an earlier research that most of the researched patients want to have control over to whom they want to disclose their data [13]. According to the research of Caine and Hanania [17], the researched patients prefer to have granular privacy control over which data should be shared with whom. As aforementioned, in a study by Schwartz et al. [19] it turned out that a large part of the researched patients would actually use this feature as 43% of the researched patients chose to limit the access to some parts of the information in their EHR's to at least some of the health providers. 4.8% decided that all providers were inhibited from accessing all the information in their EHR's.
In the study by Tierney et al. [20] the researched health care providers had multiple different opinions of on this subject. Although a large part of these healthcare providers claimed to be comfortable with the fact that patients had control on which party could access which part of their information, a significant part was not. Some of the researched providers thought that the limited access to the information may result in a lower ability to provide care of a proper quality. Another result of the study was that some providers believed that it could affect the relationship between the provider and the patient in a negative way. It appears from this study that there is a need for a balance between the requirements of healthcare providers and the requirements of the patients on the issue of which party should have access to which information.
As health care providers may miss access levels to certain medical information, there is a risk of missed opportunities in providing care that is needed for the patient [5]. There is also a risk for care delays due to this granular control [13]. Lacking crucial information during medical decision making may cause errors in judgement, which can have consequences for both the patient involved and the health care provider if he or she is responsible.
Among the interviewees there was a large amount of disagreement as described in chapter 5, although the majority was in favour for more control for patients. Among other arguments, it was claimed that is was better not to send a consultation at all if the patient was against sending a part of medical information that is included in the set, as all of the information is needed to make a proper medical judgement. Furthermore it was said that if important information is left out because the patient doesn't give consent on it, the receiving professional may be limited in his/her ability to assess the medical situation of the patient.

It is advised to record the consent of patients centrally, as a clear preference for this has been given in the interviews. It is included in the section for further research to look into the method in which this would be implemented.

In three of the interview sessions the subject came up to give patients insight in which information is shared with whom. It is advised to implement this, although it should be looked into how this should be implemented.

7.2.5 Actions

It is decided that, for now, there should be no difference between the actions in which information is sent. During the interviews, most of those who agreed with the statement that there should be a difference, did so with the referral to medical specialists in mind. Outside of that specific case, which is deemed to be out of context for this model, it was mentioned in only one session that there should be a difference. If there is a need for differences between referrals and consultations, this could also be adjusted using the additions and omissions of the GP. Furthermore it should be kept in mind that if this would be implemented, it would mean that there would be even more standard sets, which would result in a higher administrative burden.

No change has been made on the approach for the further referral, as has been described in chapter 4. This is due to the high amount of disagreement on how the case of a further referral should be handled, combined with the preference to keep the current situation in one of the two sessions.
If there would be a way in which the GP can give consent without making this process sluggish, it would be advised to look into this in the future.

Concerning the further consultation it has been decided not to change the current approach, which is described in chapter 4. This was due to the high amount of disagreement on this subject and that the current situation was seen as relatively fine.
It is advised however to look into giving the GPs a notification when this situation occurs and to look further into whether the GPs would like to give permission if the consultation is forwarded to an expert in another hospital.

On the matter of how long a referral should stay active, no maximum length has been implemented for now as the opinions on this matter differed for a large amount.
For further research, it is advised to look into a possible maximum duration of a referral, as a clear preference for this was given in session 2. Furthermore it is advised to look into if and how patients could be more involved in this process. For example so that he/she is also able to close referrals to healthcare providers who aren't relevant anymore for his/her care process.

7.3 The storage of information concerning authorization and its retrieval

For Topicus it is important to know which elements should be stored concerning authorization when information of patients in the Datakluis is shared with other parties. This is relevant as the information of patients is not simply sent to other parties; when other parties are authorized for medical information of a patient, they are allowed to gain access to that part of the information from the Datakluis. So when a GP for example makes a referral for a patient to a dietician, the GP authorizes the dietician to access certain parts of the medical information. In order to do so, certain information concerning this authorization will have to be stored in the Datakluis. Furthermore, when the dietician has received this referral and wants to access the medical information, certain steps will have to be taken using the information concerning the authorization. These steps will check whether the dietician actually is authorized to view part of the medical information of that specific patient, and if so, which parts of it.

But which information concerning the authorization should be stored in the Datakluis? And what are the decisions and steps that should be made before this package of information can be made? And lastly, which steps and decisions should be made before a receiving party can access the medical information?
The improved process, as explained in 7.1 and 7.2, can be used as a basis to give an advice for this. However, care must be taken when doing so. The improved process in 7.1 and 7.2 was made based on the aforementioned cases and subjects that were researched in this project, which concern the

current sharing of information using the VIPlive application. However, it is quite possible that this process will be further altered in the future as new developments present themselves. Furthermore in the future the Datakluis could be used by many other applications, using other processes, other kinds of healthcare etc. Therefore, in order to determine which elements should be stored concerning authorization, it is important to look at the elements that are most likely to be essential for future processes. So that the decisions above can be made in a future-proof way and to prevent that they have to be adjusted for new processes or other developments.

7.3.1 What should be stored in the Datakluis on the subject of authorization?

Based on this research and the cases investigated within it, the following information elements are advised to store in the Datakluis application when information of patients is shared with others.

1. An identifier for the patient in question
2. Elements that concern the receiver(s) in question. These elements are added in order to properly determine which party and individual is authorized to access the information and to determine which of parts of it he/she can access.
   Identifiers will have to be stored for the organization of the receiver and for the type of healthcare in question (like chain of care, mental health care, regular healthcare etc.
   Secondly at least one 'group' of receivers is defined. Multiple groups of receivers can be added, in which each group is numbered.
   For example, if a patients data is shared in a referral, only group 1 will be filled. An example in which the feature of additional groups would be useful is a consultation, as the data shared in a consultation is accessed by the secretaries/assistants and the medical specialist. In this case the medical specialist could be placed in group 1 and the secretaries in group 2, group 2 would have other access rights to the resulting dataset than group 1 in this case. The purpose of these additional groups is that in this way, one action can be used to simultaneously share data with multiple groups who have different access rights to the data that will be sent.
   For each group a separate set of identifiers for multiple elements will be stored: The role of the receiver(s) and/or identifier(s) for the receiving person(s).
   A difference is that the additional groups, (group 2 and further) do not to be added while group 1 needs to be present and have at least one entry; in the action of a referral for example there is no need to use the second group, so no entries will have to be stored for that group.
   In the figure below the additional groups are pictured as group N.
   Elements like the healthcare group and healthcare chain are not added as those only apply to healthcare in healthcare groups, but these elements have to be usable for other types of healthcare as well.
3. The resulting dataset. This concerns the categories/pieces of healthcare information of the patient to which an authorized receiver can gain access. This can be different from the standard set which would normally be sent to a receiver of the role in question, as possible alterations of the set are taken into account. Examples of alterations are additions/omissions of the GP and changes due to informed consent. As the Datakluis can be used in other types of healthcare in the future, or using other kinds of medical information, the resulting dataset can look similar to those described in 7.1 but can also be totally different. This information element includes a collection of references to *a* resulting dataset, but does not define how

exactly such a dataset would look like. The resulting dataset will be stored as a collection of references to parts of the actual dataset of the patient in question.

4. An identifier for the action that is performed, like a referral for example, will be stored. An identifier of the level at which the information is shared with another organization, and thus how many/which persons within the organization can access it, is stored as well. Information can be shared to: a specific individual, to a group within an organization (like the secretaries of the medical specialists) or to an entire organization.
   In the current process for referrals etc. as described before, the level at which information is shared is dependent on the action. In this model the level is also advised to be determined by the choice of action. However, in the future it may be decided that the level of sharing may be determined by other factors. Therefore, in order to make future-proof decisions in which information to store, it is advised to store the level at which the information is shared as well as the action.
5. The last part consists of the overviews of which parts of the resulting dataset the two groups are allowed to access, the access rights.
   For each group a separate overview will be made, based on the rules and agreements that are active at the moment the action is performed. For example, if a consultation is done to a medical specialist, medical information is shared with two groups; the specialist and the secretaries. An overview will be made of which parts of the resulting dataset the specialist can access and a separate one for the parts the secretaries can access. These overviews are made based on the agreements at the moment the action is performed in order to prevent the access rights for this action from changing when the agreements are changed. So if the agreements are changed in the meantime, the access rights in the action are still based on the older agreements. The overviews consist of a collection of the parts of the resulting dataset to which the group in question has access.

To give a clear overview of the information concerning authorization that will have to be stored figure 11 has been made. This has been written in pseudo-code in order to give the employees of Topicus who will work on this in a later stage enough room to implement it as they think is suitable.

```
{
   patient: “patient identifier”
   organization: “organization identifier”
   healthcare type: “healthcare type identifier”
   receiving group 1: {
      role: “identifier for the role of the receiver(s)”
      and/or
      list: “collection of identifiers for the receiving persons”
   }
   receiving group 2: {
      role: “identifier for the role of the receiver(s)”
      and/or
      list: “collection of identifiers for the receiving persons”
   }
   resulting dataset: “collection of references to parts of the dataset of the patient”
   action: “action identifier”
   level in which data is shared: “level identifier”
   access rights group 1: “collection of parts of the resulting dataset”
   access rights group 2: “collection of parts of the resulting dataset”

}
```

Figure 10 an overview of the information concerning authorization in pseudo-code

For many of the elements the choice has been made to store an identifier. This is done in order to give each patient, organization etc. a unique way to identify them. If for example there would be two or more patients with the same name in the system, confusion concerning the identity of the patient in question can be prevented in this way.

The abovementioned identifiers should be known at least within the Datakluis and the applications that are/will be used to share and receive medical information from the Datakluis. However they should not be made public. The users, those who share medical information as well as the receivers, should be able to select the patients for example without risk of selecting a different patient with the same name. If the identifiers should be used directly in the user-interface of these applications or if the applications should determine the identifiers based on the input given by the user, is left for further research. Whenever a new patient/organization/etc. is entered into the system the unique identifier for it should be added as well so it can be used in the abovementioned way.

Furthermore there are two additional things to keep in mind: After data has been shared in a referral for example, a further step like a further referral or a further consultation can take place. Other actions in the future may also include such possibilities.
Another point of notice is the matter of the difference of access rights between the groups. Which factors should determine which group should be able to access which parts of the resulting dataset is currently still unclear. How to implement this in a proper way is a subject for further research.

In order to generate the necessary information concerning an authorization as described above, the core steps and decisions are defined as shown in diagram 7.

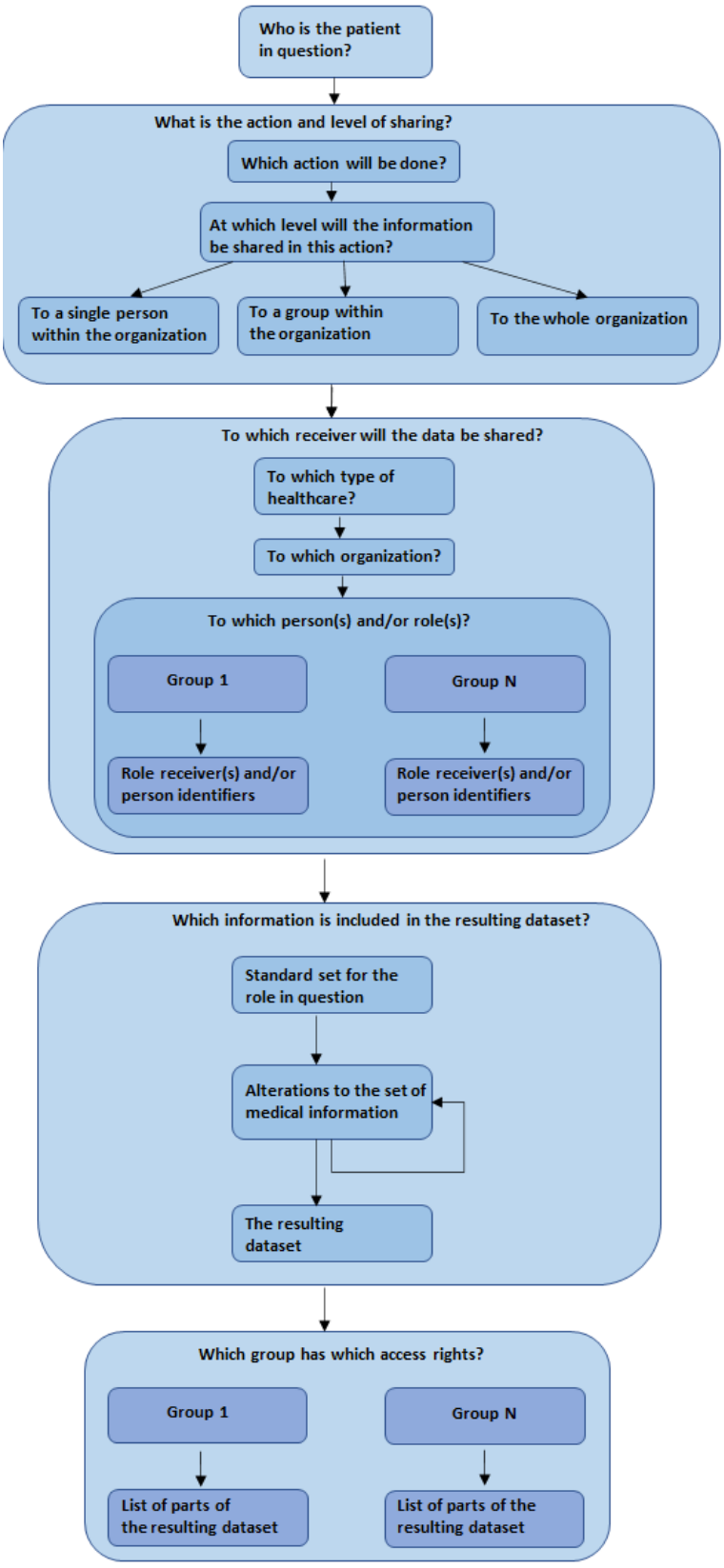


Figure 11; the core steps to generate the information concerning authorization

7.3.2 Which steps should be made when a receiver wants to access the information?

After a person or multiple persons within an organization have received a referral for example, they can attempt to access the resulting dataset of the patient. However, multiple steps have to be made before access can be granted.

Firstly it has be checked whether the organization in which this person works has actually received this. Therefore a step has to be implemented to make sure that an action has been made in which medical data of the patient in question has been shared with this organization as a receiver. If not, this person will not gain access.

However, medical information can be shared in different levels of an organization. So it has be checked if this action shared the medical information the whole organization, to just a group within the organization (and if this person is part of that group) or if this action specifically authorized this person. Based on these steps it is determined whether this person is authorized to access (part of) the medical information of the patient in question.

If an authorized person that works for the receiving organization wants to access the resulting dataset, how much of the data this person can access is dependent on his or her role. For example; If a consultation is meant for a medical specialist, the specialist can access the complete resulting dataset. An assistant/secretary would only gain partial access to the resulting dataset and can view the information for which his or her role is authorized. Therefore a check will be made which role this person has and whether he or she will gain partial or complete access to the resulting dataset.

An overview of these steps is made in diagram 8.

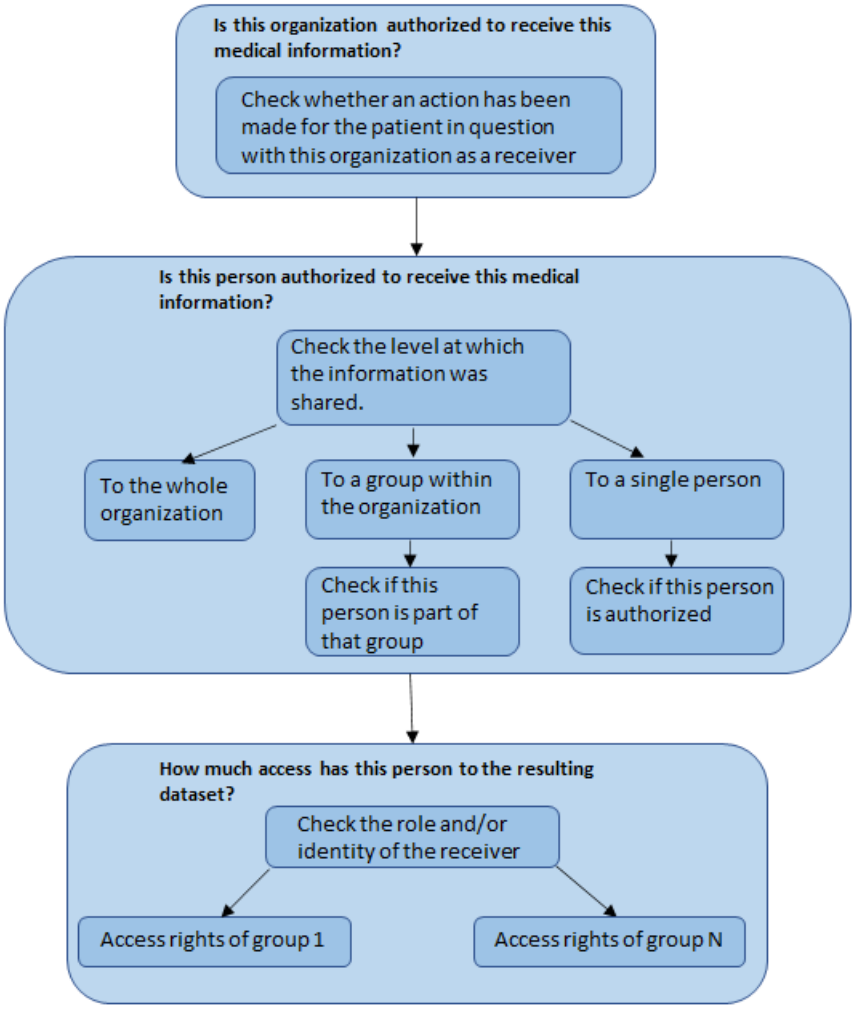


Figure 12; the core steps for when a receiver wants to access shared medical information

A final note on this matter is that there were actually two options in how the information concerning authorization and the core steps could have been developed. In the chosen option, a single resulting dataset is stored and two groups are defined, for both groups a set of access rights is stored. However in the alternative option two resulting datasets would be stored, one for each group. As each group has his own dataset, there would be no need to store the access rights for each group and to include the logic to check these access rights. However, to store two resulting datasets has its downsides as it takes more memory and identical information would be stored twice.
The question was whether situations in which the second group would be used, and thus a second resulting dataset would be stored, would occur often. In the current set of actions the consultations and further consultations already make use of the second group. Furthermore, new actions and processes which make use of the second group can be added in the future. Therefore in order to prevent the extra storage costs and data duplication of the second option, the first option was chosen, even though it contains more logic.

8. Conclusion

In the introduction multiple research questions were stated. In this conclusion these are stated again together with the answers to these questions.

Which methods and approaches for access control in the context of general practice EHRs, which take privacy and informed consent into account, are suggested in scientific literature?

In the literature review, many useful articles have been found in the aforementioned areas, of which 20 have been used. The paper of Sahi et al. [1] for example described a form of access control to medical information in which privacy and informed consent was taken into account.

However, the cases and scenario's which have been found in literature were quite different than the case in question for this project. The case in this project concerns many healthcare groups, in which each had their healthcare chains in which many healthcare organizations were connected. The cases which were found in literature concerned smaller cases which were difficult to compare with the case in question. Furthermore, many of the articles took the laws and rules of other countries, like the USA for example, into account which led to a quite different situation than the Netherlands. Additionally, finding suitable articles which included the element of EHRs for general practice, instead of EHRs in general, provided a challenge. To find articles about EHRs in general practice in which the other elements like access control or informed consent could be find as well was even more difficult.
Therefore, no article in scientific literature has been found in which approaches for access control in the specific context of general practice EHRS, which take privacy and informed consent in account.

Nevertheless the information gathered in the literature review was valuable for this project. For example multiple methods for access control have been found. Role Based Access Control (RBAC) turned out to be a method which is frequently used for EHRs [2]. In this method, access rights are assigned to the roles that users can have, instead of towards the user directly. Advantages to this method are found, like the relatively easy administration of access control rights and the ability to update the rights of many persons by updating the rights of a single role. In the current authorization approach to medical information of VIPlive, a variant of RBAC is in practice.

Based on the literature review, the model in which the five aspects of an authorization process can be described has been developed. The interview questions were largely based on lessons from literature, like the advantages and disadvantages of RBAC for example. And finally the insights from literature could be used in the development of the improved process and the authorization model itself.
Therefore, even though a direct answer to the research question has not been found, the literature review provided useful information on the subjects within the research question to this project nevertheless.

What approach for authorization is currently applied in the exchange of medical information between GPs and healthcare groups by the use of the VIPlive application at Topicus?

During the preliminary research the current aforementioned approach for authorization in the exchange of medical information has been analysed.
This approach is based on an Role Based Access Control model, in which the healthcare groups can make standard sets for each role within each of the healthcare chains. Therefore, the factors that determine which standard set of data will be shared to the receiving healthcare professionals are: the role of the receiving healthcare professional, the healthcare chain in question and the healthcare

group.
The format of the standard set, which can be filled in by the healthcare groups, is given below.

Medication	Yes/no
Additional medication	Yes/no
Measured values	Yes/no
Episodes	Yes/no
Non-relevant episodes	Yes/no
Measured values	
When 'measured values' is checked as 'yes', a list of the selected measured values that will be sent is listed below	

Table 9; the standard set

Episodes are health problems, like medical conditions and diseases for example. Measured values are measured data in the system of the GP, like blood pressure or length for example.
Each healthcare group therefore has a collection of filled in standard sets. For example, a healthcare group in a region would have a certain filled-in set for the healthcare chain of diabetes and the role of dietician.
An overview of this system is given in the figure below.

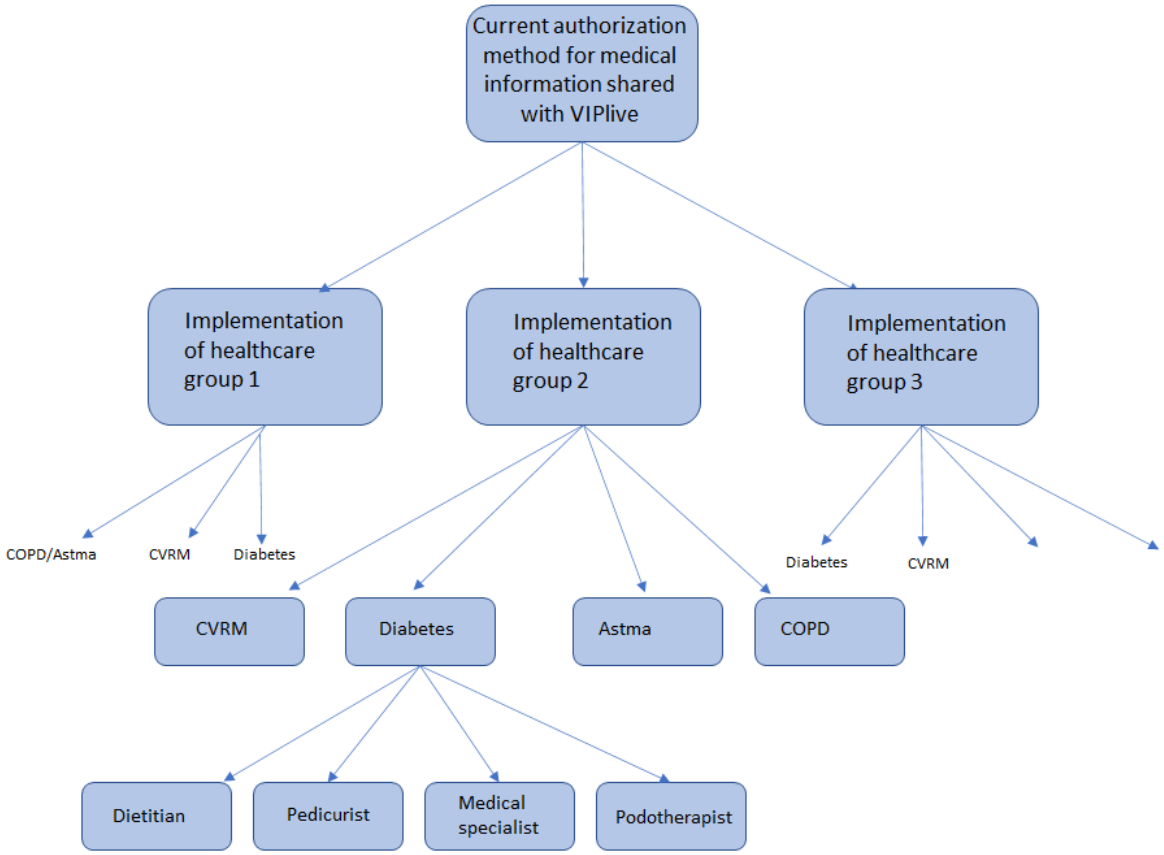


Figure 13: a schematic overview of the authorization method for medical information shared with VIPlive and the structure of the healthcare groups and chains of care

These factors above determine which standard set of data will be shared with a receiving healthcare professional. However when data is shared, during a referral for example, VIPlive also gives the GP

the option to fill in information in an open text field and to add additional documents as an 'attachment'. In this way extra information can be shared if the GP wishes to do so.

What are the requirements from Topicus for this particular authorization model?

The requirements of Topicus will be explained in five parts, the five aspects of an authorization process for personal health information of patients: Structure of the personal health information of patients, method of access control and its application, users and roles, informed consent and actions.

Structure of the personal health information of patients

- The interviewees were in favour of more specificity compared to current approach of standard sets; Within some categories of information you either send all data within that category (like medication or episodes) or none. They did add that this will primarily be relevant for referrals outside the healthcare chains. Furthermore it would be a good idea to redetermine which kinds of medicine should automatically be included to share with which healthcare professionals
- The interviewees were in favour to add journal lines. Although how this feature should be implemented needs further research.
- The opinions differed on the possible addition of the health plan. It was noted that it could be useful to share with medical specialists in the context of elderly care. However if the health would be added the ownership of this data should be kept in mind; the legal aspect should be investigated first.
- All interviewees of Topicus agreed that measurements from home would be a valuable addition. However the legal aspects concerning the ownership of this data should be investigated properly before this can be added.
- The interviewees of Topicus also agreed on the addition of questionnaires that are filled in by the patient. Certain standardized and regular questionnaires could be shared so they don't have to be filled in again by the patient.

Method of access control and its application

- The interviewees agreed that Role Based Access Control is a suitable access control method for this particular case. They were all in favour to add the additions and omissions features as well. Using these additions feature general practitioners can add certain data, like a specific kind of medication for example, to the set of data that will be shared with the receiving healthcare professional. With the omissions feature data that is included in the standard set to be shared can be omitted.
- The interviewees were not in favour to make the contents of a health record one of the factors which automatically determine which standard set of data would be shared. In session 2 there was a discussion about whether it could possibly be useful for medical specialists in the future.
- The interviewees were in favour of nation-wide implementations. In the current system each regional healthcare group has its own standard sets. But when nation-wide implementations would be implemented standard sets for healthcare chains and specific roles would be agreed upon on a national level.

Users and roles

- The interviewees of Topicus were quite content with the current set of users and roles. The role of medical specialist was the only role currently in the system for which there was a clear need for adjustment, but Topicus is already working on that subject.

- They were unanimous on that the role of who performs one of the actions, like a referral for example, should influence the standard set. Those who can make a referral in the current system are general practitioners and practice nurses (‘praktijkondersteuner’ in Dutch).
- It was also remarked that a separate role for medical assistants could be a valuable addition.

Informed consent of patients

- In both sessions at Topicus the interviewees mentioned that it is important to take into account in the development of systems that patients will probably get more influence on this process in the future. It was remarked that patients should have an easy option to give their consent for the sharing of their medical information that is important for his healthcare.
- The interviewees agreed that it should be centrally recorded for which parties and which medical information the patients give consent.
- Another aspect upon which they agreed was that it is important to provide insight to patients into which of their health information is shared with which parties. Provided that it would be in a format that is understandable for patients.

Actions

- There was a large difference of opinion on whether the action that is performed should be influence which medical information is shared. As an example; this would mean that when a referral is done a different set of data would be shared compared to when a consultation is done. While some interviewees thought it shouldn’t make a difference, others thought otherwise.
- Concerning the cases of the further referral and the further consultation there was also a significant amount of disagreement from the interviewees of Topicus. In these cases, healthcare providers to whom data has been shared by the GP, would share data of the patient to another receiving healthcare provider. However when such a case occurs the GP is often not aware that this happens. It was discussed whether the GP should be notified or should give consent before this can happen.
  A large number of the interviewees thought that for both cases no changes are necessary, as the current approach is the only workable one. Others thought that either the GP should be notified when this happens, or that the GP should give his or her consent for this.
- Considering the question how long a referral should stay active, there was a large amount of disagreement as well. While some had a preference for a maximum duration, others thought that it should stay active for as long as the receiving professional is treating the patient. They also preferred that the patient will be more involved in this process in the future.

What are the requirements from the healthcare groups for this particular authorization model?

The requirements of three healthcare groups will be explained in the same five parts as the requirements of Topicus: Structure of the personal health information of patients, method of access control and its application, users and roles, informed consent and actions.

Structure of the personal health information of patients

- Concerning the question whether there should be more specificity in which medical information is sent, only one of the three healthcare groups agreed. The others were quite content with the current approach on this matter.
- The healthcare groups were in favour for the addition of journal lines to the set. Although further research should be done on how this should be implemented.

- Concerning the addition of the health plan to the set there were two healthcare groups who disagreed. The one who was in favour did remark that when this would be added it should be researched how to do so, as a healthcare plan consists out of several parts. When the whole plan would be shared, multiple parts of the plan could be irrelevant to the receiver.
- The healthcare groups were unanimously in favour for the addition of measurements from home in the set. However the difference between the measured values and the measurements from home should be made clear.
- In the interviews with healthcare groups it turned out that the results of several questionnaires are already sent, these are included in the measured values. During the interviews with the healthcare groups no questionnaires were brought up which aren't implemented yet but which would be useful to add.

Method of access control and its application

- The interviewees unanimously agreed that Role Based Access Control is a proper approach for this case.
- The proposed feature of additions was welcomed by all as well.
- One of the healthcare groups disagreed with the possible addition of the omissions feature, although the other two agreed. Reasons for the disagreement include that data that is important for the receiving healthcare professional could be removed in this way. If important data is removed it becomes harder, if not impossible, to make a proper medical judgement.
- None of the interviewees were in favour of the contents of the healthcare records of the patient to automatically influence which standard set would be shared.

Users and roles

- All of the interviewees agreed that the approach for the medical specialists should change. However Topicus is already working on an improved approach.
- The interviewees unanimously thought that the role of who performs the actions (like a referral for example) should influence which standard set of data is shared.
- One of the healthcare groups thought that the addition of a separate role for healthcare assistants would be a good idea. However another healthcare group was neutral in this matter, as it was deemed hard to properly determine which data this role would be allowed to access. Furthermore it would be impractical if two separate referrals (one for the assistant, one for the receiving professional) would have to be sent.

Informed consent of patients

- Considering the question whether patients should get more control over which information is shared the opinions were heavily divided. Two of the healthcare groups disagreed, while the other thought that patients should get granular control. One of the arguments from those who disagreed was that the patients cannot oversee which medical information is important to send, so they should have faith in the medical professionals in that they know what is best to send in their situation. Furthermore if important information is left out because the patient doesn't give consent to it, the receiving professional may be limited in his/her ability to asses the medical situation of the patient.
- Two of the healthcare groups brought up the requirement that the consent of patients should be centrally recorded.
- One of the healthcare groups brought up the requirement that insight should be given to the patient on which information is shared with whom.

Actions

- Concerning the question whether the action that was performed should influence which information is sent, the opinions differed for a large amount. This is partly due to the fact that the referral to a medical specialist was taken into account by two of the healthcare groups when their opinion was stated, although that is quite a different action in the context of this project. This last part is seen as a limitation of this project.
  They said that currently there already is a difference between the different actions. This is due to the fact that the transfer of main caretakership is done using a different application, which involves a different set of information. If this could be done by VIPlive in the future, a different set for this action would be required as well, but the current situation was considered to be suitable for them.

What should be the role of informed consent in the improved process and authorization model of the Datakluis?

In this project this research question has been researched and useful information has been gathered. However, it is still unclear at the moment how informed consent should be implemented in the improved authorization process and the new authorization model.

During the interviews it turned out this subject was almost unanimously seen as a difficult subject and there was a large amount of disagreement on it. Two of the three healthcare groups thought that patients should not receive more control on which medical information is shared. They thought that patients should have faith in the decisions of the medical professionals. They also mentioned that it's important to keep in mind that the shared medical information should still be useful to the receiving professionals, which could be difficult if important data is left out. One of them said that when a patient does not give consent to parts of the dataset, it would be better not to send a consultation at all.
One of the healthcare groups as well as the interviewees of Topicus however thought otherwise. They claimed it would be better to take into account in the development of systems that patients will probably get more influence on this process in the future.
In four of the five sessions a clear preference was given that the consent of patients should be centrally recorded. In three sessions it was also mentioned that it is important to provide insight to patients into which of their health information is shared with which parties, this came up during three sessions.

Based on the exploratory analysis of the GDPR it is deemed likely that its rules require some form of granular control in the improved authorization process and the new authorization model. However, as this was an explorative analysis, a professional legal assessment is recommended to gather the definitive legal requirements on this matter.
After the legal requirements have been gathered, further research will be needed to develop a proper implementation of informed consent in this case. How this implementation should look like is still unclear at the moment. Considering the large difference in opinion among the interviewees, it is recommended to develop this implementation in consultation with important stakeholders like the healthcare groups.

What would be an appropriate improved version of the authorization approach in the aforementioned process in which medical information is exchanged?

An improved version of the authorization process in the exchange of medical information in which VIPlive and the Datakluis are used is described in the figure below.

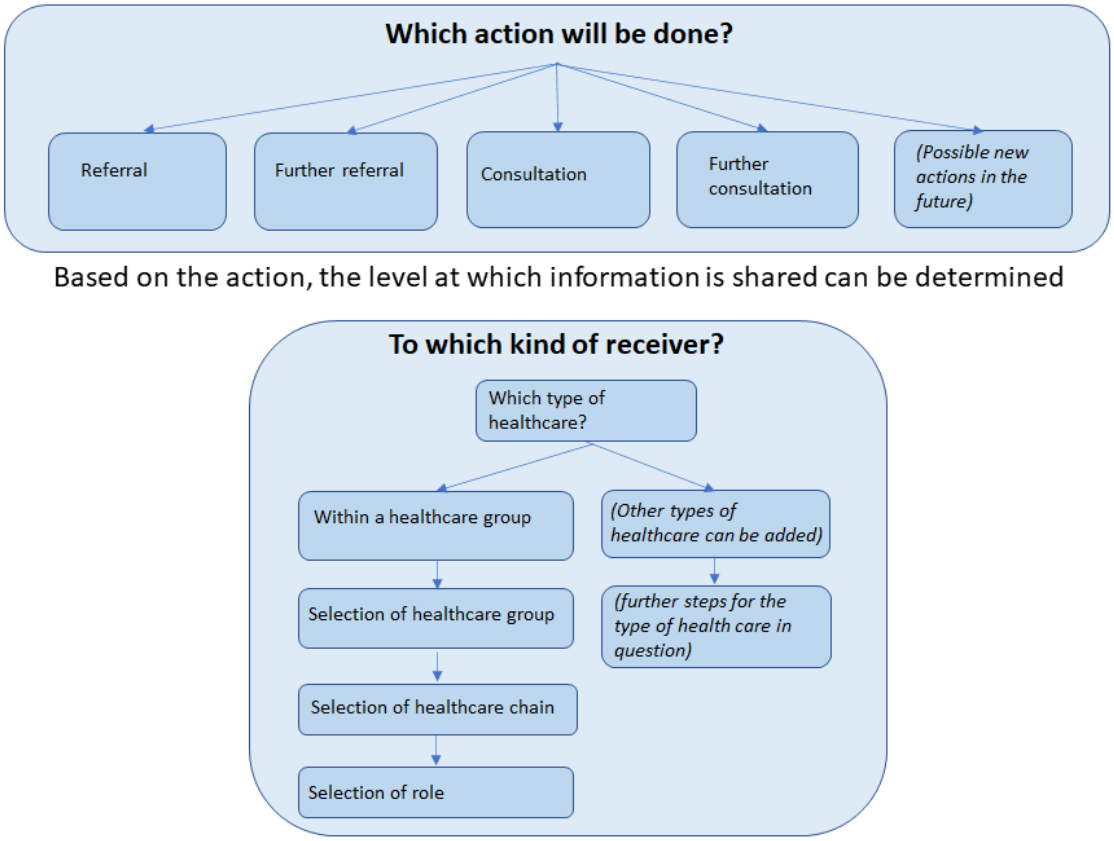


Figure 14; an overview of the improved process

The improved process is still based on the Role Based Access Control approach, in which the role of the receiver is an important factor in which 'standard set' of information is shared to which receiver.

When the data is shared to receivers within healthcare groups, the healthcare group in question and the healthcare chain in question are other factors that determine which standard set is used.
Before this improved process can be implemented entirely, there are several steps that are left for further research. The legal implications for including the measurements from home, how the journal lines should be included, and the proper approach to implement informed consent of patients.

What would be an appropriate authorization model for the case in question which determines which parties are allowed to access which medical information of patients?

Based on the literature review, the preliminary research, the requirements of both Topicus and the three healthcare groups, and finally the improved process a new authorization model has been designed.
This model consists out of two parts: a description of the information concerning authorization that should be stored in the Datakluis when information is shared, as well as the core steps in the storage and the retrieval processes.

The following information elements are advised to store in the Datakluis application when information of patients is shared with others:

1. An identifier for the patient in question
2. Elements that concern the receiver(s) in question. These elements are added in order to properly determine which party and individual is authorized to access the information and to determine which of parts of it he/she can access.
   Identifiers will have to be stored for the organization of the receiver and for the type of healthcare in question (like chain of care, mental health care, regular healthcare etc.
   Secondly at least one 'group' of receivers is defined. Multiple groups of receivers can be added, in which each group is numbered.
   For example, if a patients data is shared in a referral, only group 1 will be filled. An example in which the feature of additional groups would be useful is a consultation, as the data shared in a consultation is accessed by the secretaries/assistants and the medical specialist. In this case the medical specialist could be placed in group 1 and the secretaries in group 2, group 2 would have other access rights to the resulting dataset than group 1 in this case.
   The purpose of these additional groups is that in this way, one action can be used to simultaneously share data with multiple groups who have different access rights to the data that will be sent.
   For each group a separate set of identifiers for multiple elements will be stored: The role of the receiver(s) and/or identifier(s) for the receiving person(s).
   A difference is that the additional groups, (group 2 and further) do not to be added while group 1 needs to be present and have at least one entry; in the action of a referral for example there is no need to use the second group, so no entries will have to be stored for that group.
   In the figure below the additional groups are pictured as group N.
   Elements like the healthcare group and healthcare chain are not added as those only apply to healthcare in healthcare groups, but these elements have to be usable for other types of healthcare as well.
3. The resulting dataset. This concerns the categories/pieces of healthcare information of the patient to which an authorized receiver can gain access. This can be different from the standard set which would normally be sent to a receiver of the role in question, as possible alterations of the set are taken into account. Examples of alterations are additions/omissions

of the GP and changes due to informed consent. As the Datakluis can be used in other types of healthcare in the future, or using other kinds of medical information, the resulting dataset can look similar to those described in 7.1 but can also be totally different. This information element includes a collection of references to *a* resulting dataset, but does not define how exactly such a dataset would look like. The resulting dataset will be stored as a collection of references to parts of the actual dataset of the patient in question.

4. An identifier for the action that is performed, like a referral for example, will be stored. An identifier of the level at which the information is shared with another organization, and thus how many/which persons within the organization can access it, is stored as well. Information can be shared to: a specific individual, to a group within an organization (like the secretaries of the medical specialists) or to an entire organization.
   In the current process for referrals etc. as described before, the level at which information is shared is dependent on the action. In this model the level is also advised to be determined by the choice of action. However, in the future it may be decided that the level of sharing may be determined by other factors. Therefore, in order to make future-proof decisions in which information to store, it is advised to store the level at which the information is shared as well as the action.
5. The last part consists of the overviews of which parts of the resulting dataset the two groups are allowed to access, the access rights.
   For each group a separate overview will be made, based on the rules and agreements that are active at the moment the action is performed. For example, if a consultation is done to a medical specialist, medical information is shared with two groups; the specialist and the secretaries. An overview will be made of which parts of the resulting dataset the specialist can access and a separate one for the parts the secretaries can access. These overviews are made based on the agreements at the moment the action is performed in order to prevent the access rights for this action from changing when the agreements are changed. So if the agreements are changed in the meantime, the access rights in the action are still based on the older agreements. The overviews consist of a collection of the parts of the resulting dataset to which the group in question has access.

In order to generate the necessary information concerning an authorization as described above, the core steps and decisions are described in the figure below:

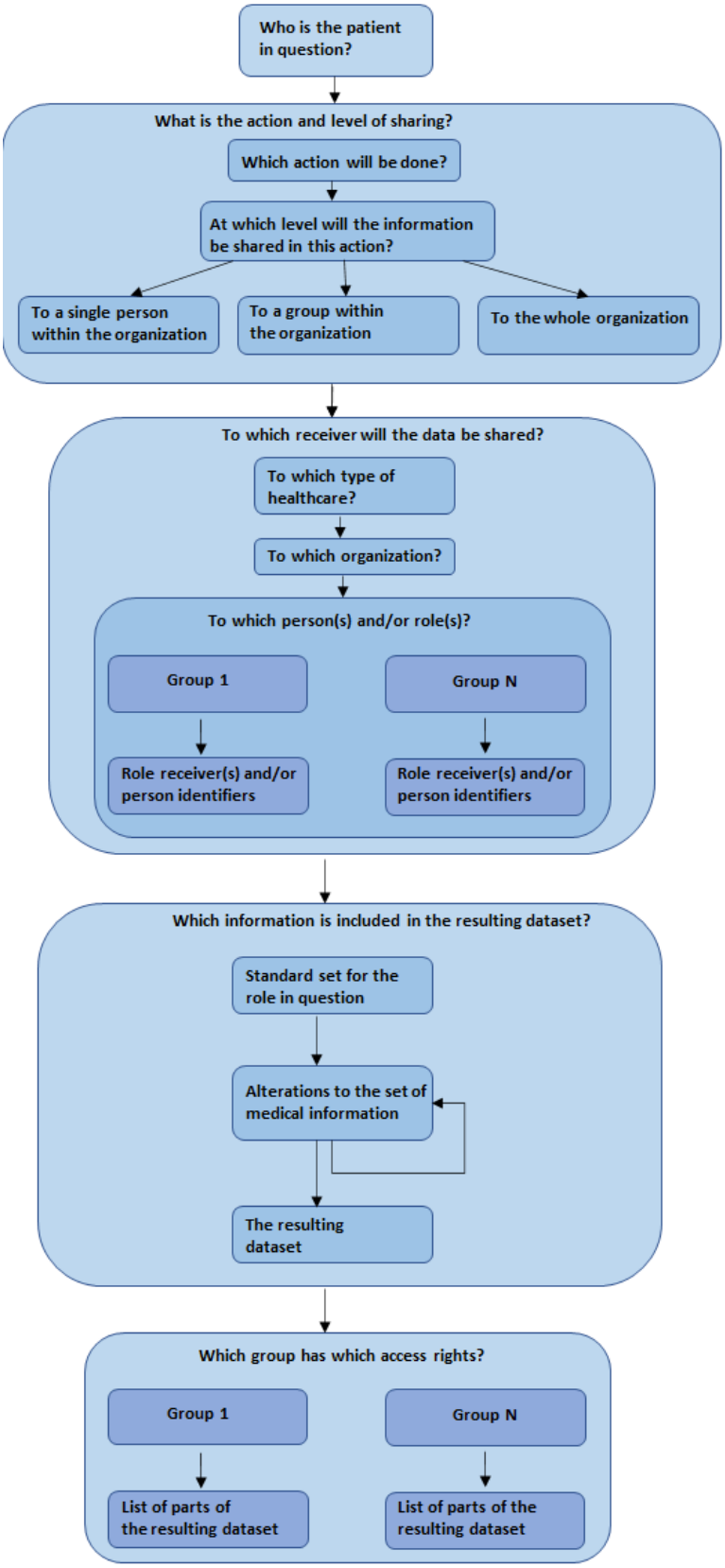


Figure 15; the core steps to generate the information concerning authorization

Using these steps in an authorization process ensures that the described information elements concerning authorization can be generated.

An overview of the steps that should be made when a receiving healthcare professional wants to access this information is shown in the figure below.

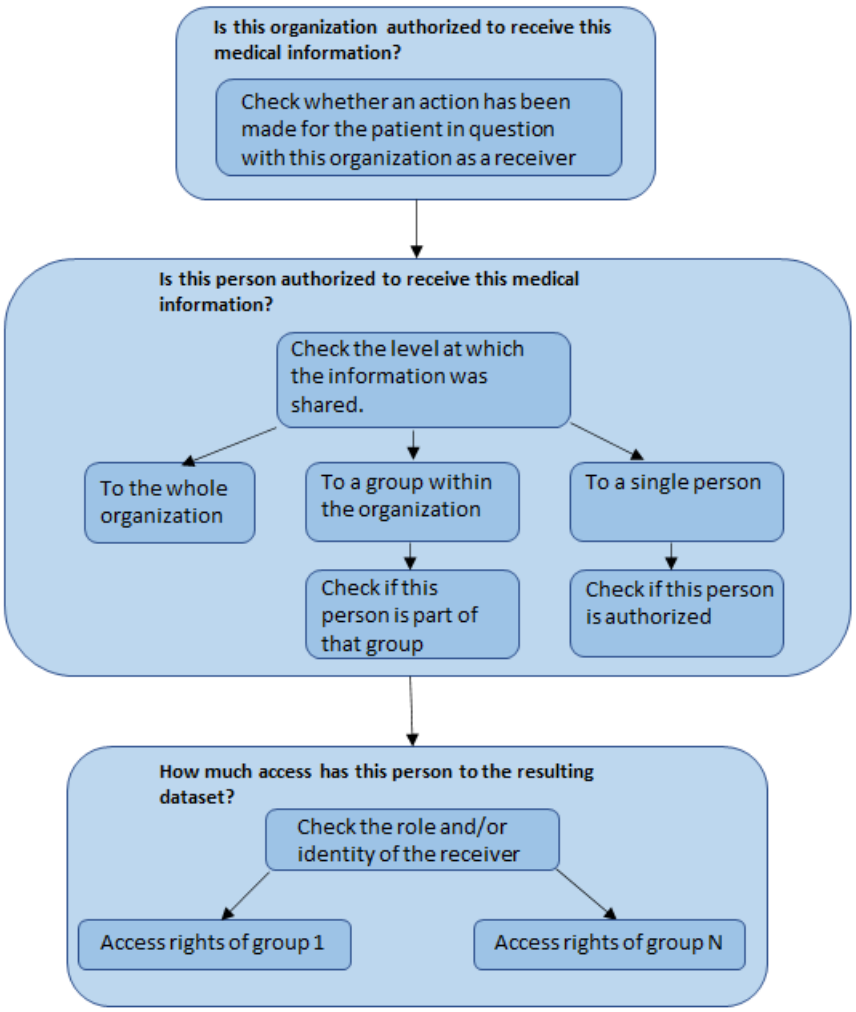


Figure 16; the core steps for when a receiver wants to access shared medical information

When these steps are included or implemented in an authorization process it can not only be checked whether the healthcare professional in question is authorized to access parts of the medical information of the patient. Furthermore, by checking the access rights of the 'group' to which the professional belongs, the access rights can be determined. Using this information, it can be determined which medical information of the patient this medical professional is authorized to access.

9. Discussion and limitations

In this chapter a discussion about this research will be given as well as its limitations and the recommendations for further research.

This research was quite broad in the sense that it concerned many different subjects. Consequently, many of those subjects have been researched but not in depth enough to give definitive answers in how they should be handled or implemented. An example of this is how to implement informed consent. However, this research did yield new information and opinions from the interviews and literature review on these subjects which can be used as input for further research. This input for further research can be seen as one of the main results of this research.

9.1 Limitations

Interviews have been done with employees of healthcare groups, however there are some limitations in this aspect. Firstly, three healthcare groups have been included in this research while there are multiple other healthcare groups in the Netherlands. Therefore, no input of the opinions of these other healthcare groups have been taken into account. Furthermore, from each healthcare group only one person has been interviewed.
Healthcare groups represent many healthcare professionals in their region, but it's important to keep in mind that those professionals are a large and diverse group of people with many different specializations. Their opinions on the subjects in this research may differ for a large amount. The general practitioners themselves for example have not been interviewed, although the results of this research do concern their way of working. The receivers of health information, like dieticians, medical specialists etc. have not been interviewed as well.

As mentioned in the literature review, multiple subjects have been left out of scope for this project, like authentication, the pseudonymization of patient's identity and transmission protection.

Only one source has been used in this research for the exploratory review of the GDPR. In order to obtain a clear picture of the legal requirements on privacy and informed consent, more research is definitely needed.

This research has focused on healthcare for chronic illnesses, like diabetes, which is done in healthcare groups. However, mental health care of care for the elderly has not been researched. The Datakluis may also be used for other kinds of healthcare in the future, but these are not included in this research as well. In 7.1 an assumption has been made concerning these other forms of healthcare and their place in the diagram, but it is important to keep in mind that their workings and processes have not been researched.

Another point of notice is that many of the results of this research, like diagrams in chapter 7, have been made on a conceptual level. No programming or the practical application of (parts of) the new model or process have been done.

The opinions on whether the performed action should influence which medical information is sent were quite different. This is partly due to the fact that the referral to a medical specialist was taken into account by multiple interviewees when their opinion was stated, although that is quite a different action in the context of this project. This last part is seen as a limitation of this project.

An important point of notice is that the new model that has been developed has not been tested in practice. This model is developed based on the interviews and the results have been validated using the results of the literature review. However, how elements like the improved process would work in practice is still unclear at the moment.

9.2 For further research

As mentioned before there was a large difference of opinion among the interviewees on the subject of nationwide implementations. Due to this disagreement, in this model the nation-wide implementations have not yet been added. However, due to the administrative burden of the current system for Topicus, this subject has a relatively high priority among the subjects for further research.
Concerning the journal lines, it was noted that if this would be implemented, a decision should be taken on how to do so. You could choose to only send the last journal line, but you could also choose to send the journal lines that concern the episode of the patient for which he/she is consulted or referred.
During the interviews the possible addition of the health plan has been discussed. However, if this would be implemented, the legal implications of adding the health plan should be researched first. Furthermore, there are multiple different domains within a health plan and not every receiver would require all of them, so how this should be implemented should be looked into.
Measurements from home were seen as a useful addition, however the legal implications concerning the ownership of data should be looked into, as this is information that belongs to the patient. Furthermore a requirement was given that the difference between a normal lab value and measurements from home should be made clear for users, as they both should be stated under measured values.
It is possible that due to the aforementioned additions/omissions feature the workload of GPs would increase, as they are now able to adjust the set of medical information to share. It is advised to look into whether there is a significant increase and if so, how to deal with it. A possible method may be to implement a feature, that would enable a GP to automatically add or remove episodes and/or medication that are linked to other common healthcare conditions. For example, so that the GP can choose to automatically remove the medications and/or episodes that are related to depression while doing a referral, instead of having to remove each individual one individually.
Concerning episodes, it is advised to look into the current system of automatically adding all the episodes which have priority. Which is done despite the fact that some of those episodes may have nothing to do with the reason of the referral/consultation. This research project was too limited to determine whether a different approach for this subject would be more suitable.
It is also advised to redetermine which types of medication are ‘linked’ to each healthcare chain, which determines which types of medication of the patient are automatically added. This should be done by, or in cooperation with, healthcare professionals of the healthcare groups to ensure that relevant lists of medication are sent.

During the interviews it turned out that the healthcare groups did not have a clear picture yet of the needs and wants of all kinds of medical specialists concerning the information they need to receive. Therefore it is advised to look into this in the near future.
The possible addition of a role of medical assistants is also advised for further research, as during two of the three sessions it was mentioned that it could be a valuable addition. In this role it could be defined which medical information they would be able to access, but it is still unclear at the moment which information they should be able to access. Ideas on how roles with partial access to the resulting dataset, like medical assistants, could be implemented are described in 7.3.
Concerning the ideas for partial access; Which factors should determine which parts of the resulting dataset a person with partial access should be able to see is currently still unclear. This is advised to include in further research.

Concerning privacy and informed consent multiple subjects are advised for further research.
Firstly, the legal requirements on these subjects should be researched.
The opinions differed for a large amount on how informed consent should be implemented in this particular case, so more research on this is definitely needed.
A point of notice is that if more control for the patients would be implemented, it is important that the medical information is categorized in a manner that is understandable for patients. Furthermore, patients should have an easy to select option to give consent for the sharing of the information that is relevant and important for his healthcare.
During two of the interview sessions it was mentioned that it is very important that the information that is sent to the receiver is still useful for the receiver. If important information is left out because the patient doesn't give consent to it, the receiving professional may be limited in his/her ability to assess the medical situation of the patient.
Consequently, if it occurs in a consultation that a patient has used the option of informed consent to omit certain important medical information, it might be very difficult for the receiving professional. Certain information is necessary for the healthcare professional to do their job and provide a proper judgement. Therefore an option was discussed that the receiving professional would be able to cancel a consultation if important medical information was omitted.
One of the results of the literature review was that patients who have concerns about the security and privacy of EHR systems tend to disclose less information to the care providers [5]. In a study performed in 2014, 13% of patients have said that they didn't disclose full information to health care providers because of security concerns [13]. In the research on informed consent this may be a factor to keep in mind.
Another relevant outcome of the literature review concerns the influence of informed consent on the relationship between the patient and the healthcare provider. According to the research by Caine et al. [19] a large amount of the researched patients thought that the relationship that a patient has with their health care provider might be influenced by their decision whether or not to give them access to certain information. This may have been one of the reasons why patients choose to not restrict the access of providers to their information.
When more control of patients in informed consent is implemented a choice should be made on the level in which this is done. If the medical information of a patient would be shared with a group of persons in the receiving organization, should the patient be able to limit the access of certain individuals within that group? Or should the patient be able to adjust the information that is shared with the entire group, but not be able to exclude individuals?
In four of the five sessions it was mentioned that it should be recorded centrally for which parties and which medical information the patient gives consent, but how this should be done is still an unanswered question.

As explained in chapter 5, there were mixed opinions on how the further referral and the further consultations should be handled. However, these were only discussed during two sessions so more research could provide answers on what the proper approach should be.
It is also advised to look into a possible maximum duration of a referral and other actions, as a clear preference for this was given in session 2. Furthermore it is advised to look into if and how patients could be more involved in this process. For example so that he/she is also able to close referrals to healthcare providers who aren't relevant anymore for his/her care process.

In picture 10 in 7.1 an extra space was allocated to show where other types of healthcare could possibly be added. However, these types of healthcare were not included in this research so if Topicus would like to add them, it should be researched whether the diagram is suitable for them and if the diagram should be adjusted.

In 7.3 the information concerning authorization that should be stored is described. However, it is at the moment still unclear whether the identifiers should be used directly in the user-interface of these applications or if the applications should determine the identifiers based on the input given by the user. This will also determine whether the identifiers should be known to the users of the system or just within the application itself.

This research has focused on the medical information of patients that is shared with other parties, but personal information like name, address and hometown of patients is also important information. During a referral these types of information are in general shared with the receiving parties. But whether the current approach is adequate for the future has not been researched and is advised to look into in the future.

Healthcare group 2 was quite open to new additions and changes during the interviews, as can be read in chapter 5. It can be considered to contact this healthcare group when it is desirable to test features of the improved process in practice, like the additions and omissions feature.

References

[1] Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., Iqbal, W., Rashid, I., Yaseen, A. (2018). Privacy preservation in e-Healthcare environments: state of the art and future directions. *IEEE Access*, *6*, 464-478. DOI: 10.1109/ACCESS.2017.2767561

[2] Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.T.O., Toval, A. (2013) Security and Privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46 (3)

[3] Meslin, E.M., Alpert, S.A., Carroll, A.E., Odell, J.D., Tierney, W.M., Schwartz, P.H. (2013) Giving patients granular control of personal health information: Using an ethics 'Points to Consider' to inform informatics system designers. *International Journal of Medical Informatics*, 82 (12), pp. 1136-1143

[4] Vimarlund, V. (2016) *E-Health Two-Sided Markets: Implementation and Business Models.* Linköping: Academic Press.

[5] Caine, K., Tierney, W.M. (2015) Point and Counterpoint: Patient Control of Access to Data in Their Electronic Health Records *Journal of General Internal Medicine*, 30 (1), pp. 38-41

[6] Wolfswinkel, J.F., Furtmueller, E., Wilderom, C.P.M (2013) Using grounded theory as a method for rigorously reviewing literature *European Journal of Information Systems*, 22 (1), pp. 45-55

[7] Mamlin, B.W., Tierney, W.M. (2016) The Promise of Information and Communication Technology in Healthcare: Extracting Value from the Chaos *American Journal of the Medical Sciences*, 351 (1), pp. 59-68.

[8] Margulis, T. (2003) Privacy as a Social Issue and Behavorial Concept *Journal of Social Issues,* 59 (2), pp 243-261

[9] Petronio, S. Reierson J. Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory *Uncertainty, Information Management, and Disclosure Decisions: Theories and Applications,* pp 365-383

[10] Westin, A.F. (2003) Social and political dimensions of Privacy. *Journal of Social Issues,* 59 (2), pp. 431-453

[11] Sousa, M. Ferreira, D. Santos-Pereira, C. Bacelar, G. Frade, S. Pestana, O. Cruz-Correia, R. OpenEHR based systems and the general data protection regulation (GDPR) S*tudies in Health Technology and Informatics,* 247 pp 91-95

[12] Helms, E. Williams, L. Evaluating access control of open source electronic health records systems *Proceedings - International Conference on Software Engineering*, pp. 63-70

[13] Bhuyan, SS. Bailey-DeLeeuw, S. Wyant, D.K. Chang, C.F. (2016) Too Much or Too Little? How Much Control Should Patients Have Over HER Data? *Journal of Medical Systems* 40 (7)

[14] Seol, K. Kim, Y.G. Lee, E. Seo, Y.D. Baik, D.K. Privacy-Preserving attribute-based access control model for XML-based electronic health record system *IEEE Access* 6 pp 9114-9128

[15] Peleg, M. Beimel, D. Dori, D. Denekamp, Y. (2008) Situation-Based Access Control: Privacy management via modeling of patient data access scenarios *Journal of Medical Informatics* 41 pp 1028-1040

[16] van der Linden, H. Kalra, D. Hasman, A. Talmon, J. (2009) Inter-organizational future proof EHR systems. A review of the security and privacy related issues. *International Journal of Medical Informatics* 78 (3), pp. 141-160

[17] Caine, K. Hanania, R. (2013) Patients want granular privacy control over health information in electronic medical records *Journal of the American Medical Informatics Association 20(1),* pp. 7-15

[18] Leventhal, J.C. Cummins, J.A. Schwartz, P.H. Martin, D.K. Tierney, W.M. (2015) Designing a Systemfor Patients Controlling Providers' Access to their Electronic Health Records: Organizational and Technical Challenges *Journal of General Internal Medicine,* 30(1) pp 17-24

[19] Schwartz, P.H Caine, K. Alpert, S.A. Meslin, E.M. Carroll, A.E. Tierney, W.M. (2015) Patient Preferences in Controlling Access to Their Electronic Health Records: a Prospective Cohort Study in Primary Care *Journal of General Internal Medicine,* 30(1) pp 25-30

[20] Tierney, W.M. Alpert, S.A. Byrket, A. Caine, K. Leventhal, J.C. Meslin, E.M. Schwartz, P.H. Provider Responses to Patients Controlling Access to their Electronic Health Records: A Prospective Cohort Study in Primary Care *Journal of General Internal Medicine,* 30(1) pp 31-37

[21] Regeling multidisciplinaire zorg. (2016, January 1). Retrieved from https://wetten.overheid.nl/BWBR0037368/2016-01-01

[22] Slot, P. Pluut, B. Struijs, A. (2013). Argumentenwijzer over Elektronische Patiënten Dossiers. Retrieved from https://www.ceg.nl/

[23] Croonen, H. (2012, November 28) Landelijk schakelpunt terug van weggeweest. Retrieved from https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/landelijk-schakelpunt-terug-van-weggeweest.htm

[24] Aan opvolger landelijk EPD systeem wordt in betrekkelijke stilte gewerkt. (2017, November 17). Retrieved from https://www.icthealth.nl/nieuws/aan-opvolger-landelijk-epd-systeem-wordt-in-betrekkelijke-stilte-gewerkt/

[25] van der Sloot, B. (2018). *De Algemene Verordening Gegevensbescherming in gewonemensentaal*. Amsterdam: Amsterdam University Press B.V.

[26] Schermer, B.W. Hagenauw, D. Falot, N. (2018) Handleiding Algemene verordening gegevensbescherming. Retrieved from https://autoriteitpersoonsgegevens.nl

[27] EU algemene verordening gegevensbescherming. (2016, May 4). Retrieved from https://www.privacy-regulation.eu/nl/

Appendix A. Interview questions

Interviewvragen voor de zorggroepen

1. Is het huidige proces met betrekking tot het delen van medische gegevens in VIPlive voor u duidelijk?
2. De volgende vragen gaan over de huidige set van medische gegevens en hoe die ingedeeld zou moeten worden (het voorbeeld wordt erbij gegeven)
    a. Wat vind u van de huidige set?
    b. Mist u nog bepaalde categorieën die hieraan toegevoegd zouden moeten worden?
    c. Zou er in de huidige categorieën die aan of uit gevinkt kunnen worden nog meer detailniveau moeten komen? B.v. op dit moment zijn op het gebied van episodes twee categorieën die aan of uit kunnen worden gezet; episodes en niet-relevante episodes.
    d. Op dit moment heeft elke zorggroep dezelfde set van medische gegevens (welke categorieën er aan of uit kunnen worden gezet). Is het van belang dat zorggroepen een keuze hebben in hoe deze set eruit ziet en welke categorieën er hier voor hen worden weergegeven?
3. De volgende vragen gaan over de rollen van ontvangers waarnaar er verwezen kan worden
    a. Wat vind u van de huidige rollen? Zou daar nog meer of minder specificatie in moeten komen?
    b. Wat zou u liever hebben; Dat er in het geval van verwijzen altijd op praktijkniveau wordt verwezen of dat het ook van het beroep van de mensen binnen de praktijk af zou kunnen hangen wie er bij welke gegevens kan? B.v. in het geval van poli assistentes in het ziekenhuis (of een assistente in een dietistenpraktijk)?
4. We zijn aan het onderzoeken hoe we de aanpak voor het delen van medische gegevens toekomstbestendig kunnen maken. Daarom zou ik graag vragen willen stellen over enkele factoren die mee zouden kunnen spelen in de beslissing welke persoon er onder welke omstandigheden toegang zou moeten krijgen tot welke gegevens.
    a. Patiënten kunnen op dit moment bij een verwijzing wel of geen consent geven voor het meesturen van alle gegevens in de set. Wat vind u van deze aanpak? Wat zou naar uw mening de rol van de patiënt moeten zijn in de beslissing wie er welke data zou ontvangen?
    b. Degene die verwijst zou een huisarts of een praktijkondersteuner kunnen zijn. Zou het verschil tussen deze twee rollen invloed moeten hebben op het in kunnen zien en/of het delen van medische gegevens? Dat de een meer gegevens zou kunnen delen dan de andere b.v.?
    (Mogelijk kan ik hier doorvragen over of een praktijkondersteuner in de praktijk van een huisarts bij alle eerdere verwijzingen moeten kunnen die de huisarts heeft ontvangen)
    c. Zou er voor zij die verwijzen een mogelijkheid moeten zijn voor individuele aanpassing welke praktijk er welke gegevens zou ontvangen? B.v. dat de ene diëtist andere gegevens zou ontvangen bij een verwijzing met dezelfde reden als een andere diëtist?

d. Zou de inhoud van een waarde in het medisch dossier in bepaalde gevallen invloed moeten hebben op de beslissing of die waarde wel of niet doorgestuurd zou moeten worden? B.v. de reden van verwijzen, zoals hartfalen of atriumfibrilleren bij doorverwijzing naar cardioloog
e. Zou de actie die wordt uitgevoerd (zoals consulteren, verwijzen of anders) verschil moeten maken in welke data er wordt meegestuurd?
f. Zijn er naar uw mening nog factoren die een rol zouden moeten spelen die nog niet genoemd zijn?

Interviewvragen voor binnen Topicus

- De volgende vragen gaan over de set van medische gegevens
    - Zou er nog meer of minder detailniveau in deze set moeten komen?
    - Missen er bepaalde categorieën?
    - Zijn er nog andere behoeftes met betrekking tot de set van medische gegevens waarmee ik rekening zou kunnen houden? Zijn er nog andere dingen nodig om de set toekomstbestendig te maken?

- Role based;
    - Wat vinden jullie van de RBAC aanpak?
    - Een bekend kritiekpunt uit de literatuur op een aanpak gebaseerd op rollen is dat deze erg inflexibel kan zijn. Vinden jullie dat er in de huidige aanpak van autorisatie sprake is van inflexibiliteit waardoor hinder wordt ervaren?
    - Zou er nog meer of minder specificatie in de huidige rollen moeten komen?
    - Welke rollen worden er binnenkort nog toegevoegd?
    - Zijn er nog nieuwe zorgketens die binnenkort toegevoegd worden?
    - Op dit moment is verwijzen op praktijkniveau en consulteren op individueel niveau. Zou het mogelijk moeten zijn om ook op individueel niveau te kunnen verwijzen? (Voorbeelden van poli assistentes in het ziekenhuis en assistenten in een diëtistenpraktijk noemen)
      Vervolgvraag: Zou dat alleen in bepaalde gevallen mogelijk moeten zijn of is dat überhaupt een handige optie?
- Patiëntconsent en de mogelijke invloed van patiënten op welke medische gegevens er wel of niet gedeeld worden
    - Wat vinden jullie van de huidige aanpak?
    - Wat zouden jullie ervan vinden als patiënten een zekere controle zouden krijgen over welke medische gegevens er gedeeld zouden worden? (voorbeeld op scherm; dat in principe de afgesproken set aan gegevens afhankelijk van de ontvanger verstuurd wordt, maar dat de patiënt ervoor kan kiezen dat bepaalde gebieden niet gedeeld wordt) Wat zijn jullie behoeftes op dit gebied?
- Een aantal specifieke cases binnen het verwijzen
    - Bij sommige klanten kan het volgende voorkomen: Dat een patiënt van een huisarts naar een podotherapeut wordt verwezen en dat deze podotherapeut de patiënt vervolgens doorverwijst naar een pedicurist. In dit geval wordt is het dus niet de huisarts die naar de pedicurist verwijst maar de podotherapeut.
    - Wanneer een kaderarts een consultatie ontvangt dan kan deze vervolgens een medisch specialist inschakelen om de consultatie samen te bekijken. De consultatie wordt als het ware geforward om nog meer expertise in te schakelen. Vaak is de huisarts die de consultatie deed hier niet van op de hoogte.

    - Hoe lang zou een verwijzing open moeten blijven staan bij een huisarts, waarbij de medische gegevens in de doorgestuurde set dus geüpdatet worden?
    - Wat als een praktijk overgenomen wordt of veranderd, zou de nieuwe praktijk dan nog steeds dezelfde gegevens van doorverwijzingen in kunnen zien als de oude praktijk?
- Wat vind u van deze mogelijke andere factoren vanuit de literatuur die een rol zouden kunnen spelen in de autorisatie?
    - Inhoud van het dossier; b.v. de reden van verwijzen
    - Rol van verstuurder; praktijkondersteuner of huisarts
    - Individuele aanpassing (kan ook voor specifieke rollen gelden)
    - De actie die wordt uitgevoerd (consulteren, verwijzen of anders)

Appendix B. Index of translations

1.	Ketenzorg	Chain of care
2.	Zorggroep	Healthcare group
3.	Verwijzing	Referral
4.	Consultatie	Consultation
5.	Doorverwijzing	Further referral
6.	Doorconsultatie	Further consultation