The Implementation of the
Electronic Patient Record:
A Framework Proposal to Create
a Business Case

By: Jelle-Eric de Vries

BSc Science, Business and Innovation – VU 2012
Student Identity number TU/e 0806198

In partial fulfilment of the requirements for the degree of
Master of Science
in Innovation Management

Supervisor:

Dr. C.M. (Claudia) Chituc, TU/e, IS
Dr.ir. R.M (Remco) Dijkman, TU/e, IS
The Implementation of the Electronic Patient Record

Jelle-Eric de Vries

TUE. School of Industrial Engineering.
Series Master Theses Innovation Management

Subject headings: CLOUD COMPUTING, ELECTRONIC PATIENT DOSSIER, COSTS, SECURITY, PRIVACY, BUSINESS CASE, COST STRUCTURE, MEDICAL DATA, HEALTHCARE, INNOVATION MANAGEMENT, INFORMATION SYSTEMS, MASTER THESIS
The Implementation of the Electronic Patient Record:
A Framework Proposal to Create a Business Case
I. Foreword

Writing my thesis and during my studies I have encountered challenges which provided me with valuable knowledge for the rest of my career. Writing a thesis in an area where I had little to no knowledge about, turned out to be a great test for me. I learned a lot about the area of Information systems, which was new to me, and Cloud Computing specifically. I was glad to be able to link the subject to the healthcare industry.

Researching the Electronic Patient Record gave me insights in privacy, security and finance matters that arise from introducing such a system in the Netherlands. Combining this with a cloud computing system and tackling the issues which arose was both interesting and challenging to do. Working with new technologies, trying to find new insights and creating a framework for a new product helped me to use the knowledge learned from years of studying.

I want to thank all the people who agreed to be interviewed and those who helped me to get in contact with these interviewees. I would also like to thank all the people who took the time and filled in the questionnaire. All these people helped me to finish my thesis. In addition, I would like to thank everyone at the Eindhoven University of Technology who helped me with my thesis.

Special thanks go to my parents and Mara for always supporting me during my thesis and for giving advice whenever needed.

Jelle-Eric de Vries
II. Management Summary

The Electronic Patient Record (EPD) has been an ongoing subject of discussion in the Netherlands. The creation of this system is under pressure from different groups in the Dutch community. Where the citizens think that their privacy is at stake, doctors see the need as well as the problems, security experts see security gaps and others object to the financial investment. The Dutch government has attempted different ways of introducing the system in the Netherlands, but thus far every attempt did not succeed and no system was implemented. Every time, obstacles blocked the introduction of the EPD system.

Some obstacles need to be overcome in order to successfully implement an electronic patient record. The aim of this thesis is to create a framework that will ensure successful implementation. To create a framework that will help with the creation of an EPD system, a cloud computing system is used. The system will facilitate the medical community by sharing patient data, in line with the laws and regulations of the Netherlands. The aim of the research is stated as follows:

“To establish a framework that can create a sustainable business case for an EPD cloud computing system.”

The research will be conducted in different phases. In the first phase the research aim will be established (as shown above) and the methodology will be set. This methodology will show that the research will be conducted via a literature study, interviews and a questionnaire. In the second phase a literature study will be conducted. The third phase will show the results of the interviews and questionnaire in combination with the findings from the literature review. In the fourth and final phase, the framework for successful implementation of an EPD cloud computing system will be developed.

Subsequent to the methodology and goals of this study, the literature study identifies three different possible set-ups that might lead to the creation of EPD cloud computing system. The first set-up will be a nationwide SaaS system that uses a private cloud to secure the data. The second set-up will be a full EPD for local hospitals and a concise version of the EPD nationwide. Here, the nationwide version will only contain the necessary data vital for a patient in case of emergency. This version will use a SaaS system and hybrid cloud to be able to share the data. The third set-up will be a PaaS system in combination with a private cloud that all the local EPD systems are linked to.

The literature study describes four main aspects: ‘privacy’, ‘finance’, ‘cloud computing’ and ‘interviews and questionnaire’. These aspects are the cornerstones that the thesis is built on. The privacy issue, concerning the EPD, shows that a state of the art security system is needed to be able to protect the medical data. Different countries (e.g. Portugal, Sweden and South Korea) are setting up EPD systems. However, none of these countries have found the perfect method to create such a system. Literature regarding cloud computing shows promising ideas on how to create a cloud that will facilitate many doctors in delivering the medical data. The financial need for the system turned out to be different than expected. No revenue stream could be identified. The main financial effect of the EPD was the decrease of cost.

From here on phase three starts. In this phase the requirements for the EPD system are examined, both technical factors from the literature and experts and social factors stated by doctors. This provided a list of 23 items that need to be included in the EPD system to create acceptance when the
The implementation of the Electronic Patient Record (EPD) system is implemented. Among others, the EPD needs to be fast, password protected, encrypted, available 24/7 and available on all devices. Every item on the requirement list is categorised as either a high, medium or low level of importance. This level indicates the need for the requirement. This part of the thesis leads to the creation of a need fulfilment system within the framework.

Dutch citizens surveyed show that they have an understanding of what the EPD is. The questionnaire that was filled in by 92 respondents gave an idea of the perception of the Dutch citizens. It was not possible to generalize the questionnaire for the entire Dutch population but valuable insights were gained about acceptance levels and EPD related knowledge. Dutch citizens lack trust in the system, which creates a low acceptance level and halts the implementation. Although the citizens do see the need for the system, they are concerned about their privacy. While the response to the question if privacy will be in danger is around 50 percent yes and 50 percent no, people do see the need for the EPD with 83.13 percent who state that the EPD is needed. This part of the thesis research revealed the needs of the citizens that will raise the acceptance level when an EPD system is introduced.

The cost structure of an EPD cloud computing system is also taken into account. The main cost factors are divided into two groups: the fixed and the variable costs. The cost factors are found through the literature study and via interviews with experts from the IT sector. The study about the cost structure resulted in 14 items that need to be included in the EPD cloud computing system. For example: the soft-ware and hardware, the physical materials, a monitoring system and the security system. Every item in the cost structure list is categorised with a high, medium or low importance level. This level indicates the need for the cost item. This part of the thesis research gave the input for the financial part of the framework.

In phase four, the framework for the implementation of an EPD cloud computing system is developed to incorporate all the different obstacles and elements displayed above. The framework is based on an outcome model. Every step of the outcome model (input, activities, output, outcomes...
and impact) are derived from phase three. The framework is displayed above in figure A. The framework works toward creating an acceptance basis to improve the success of the implementation. The acceptance is built up from different elements: Accessibility, Ease of Use, Trust in the System and Financially Sound. These elements are part of the steps that need to be taken to create the business case.

The final outcomes that need to be created for a successful implementation are acceptance by the doctors using the system and acceptance by the citizens of the Netherlands. If this step is reached, the implementation of the system will be successful. The outputs that will increase the acceptance level of the doctors and citizens are: ‘accessibility’, ‘ease of use’, ‘trust in the system’ and ‘financially sound’. Phase two and phase three have shown that these outputs are essential for the creation of acceptance. Every element of the output must be fulfilled to the fullest extent to ensure an acceptance level that is high enough to facilitate a successful implementation. The activities to establish the outputs are shown in the framework (figure A). These six activities shown, all include steps that need to be executed to be able to create a nationwide EPD cloud computing system. The start of the framework, the input, will be based the four pillar model. This will be the starting point as it covers all the basic elements of a business case. These four pillars need to be covered to include every aspect of the development of new products.

The framework that is produced is tested for its unique characteristic against other frameworks used for the implementation of EPD systems. The adapted TAM (Technology Acceptance Model), the old implementation framework and the success factors framework all have elements that are needed for a successful implementation. These required elements are also portrayed in the framework above. The most common missing element in these frameworks is the element about acceptation by the citizens. These elements are either left out or just partly included. The framework proposed in this thesis has the acceptance by the citizens as the key elements for the success of the implementation.

The validation of the framework was done via a group of interviewees. A face-to-face discussion with every single interviewee delivered a number of elements which were not correctly displayed in the framework. These elements were analyzed and, where needed, improved in the framework.

The final result is a framework that will, when used correctly, lead to the successful implementation of an EPD cloud computing system. When the doctors and patients are satisfied with the set-up of the system, the acceptance level will be high enough to create a sustainable business case with broad basis for acceptance. This business case will be needed in order to successfully implement the system. The framework shows the possibility to create an EPD system business case based on cloud computing that will be successful when implemented in the Dutch healthcare sector.
III. Table of Contents
I. Foreword ................................................................................................................... IV
II. Management Summary ............................................................................................ V
III. Table of Contents .................................................................................................... VIII
IV. Table of Figures ...................................................................................................... XI
V. Table of Tables ....................................................................................................... XIII

Phase I Literature Research and Research Set-up ........................................................... 1
1. Introduction .............................................................................................................. 1
2. Research Question and Aim of the Research ......................................................... 3
   2.1 Aim of the Research ............................................................................................ 3
   2.2 Research question .............................................................................................. 3
3. Methodology ............................................................................................................ 6
   3.1 Step 1: The Four Pillars and the Keywords ......................................................... 6
   3.2 Step 2: Research ................................................................................................ 9
      3.2.1 Literature Study ........................................................................................ 9
      3.2.2 Interviews ................................................................................................ 9
      3.2.3 Questionnaire .......................................................................................... 10
   3.3 Step 3: Creation of the Framework .................................................................... 11
   3.4 Step 4: Validation of the Framework ................................................................ 11

Phase II Literature Research ......................................................................................... 12
4. Literature overview .................................................................................................. 12
   4.1 Privacy .............................................................................................................. 12
   4.2 Finance ............................................................................................................. 16
   4.3 Cloud Computing ............................................................................................... 18
      4.3.1 General Cloud Computing ...................................................................... 18
      4.3.2 Cloud Computing Systems ..................................................................... 19
   4.4 EPD Questionnaires and interviews ................................................................ 23
   4.5 Statements ........................................................................................................ 23

Phase III Research Results .......................................................................................... 24
5. Cloud Computing Systems ....................................................................................... 24
   5.1 Selection criteria .............................................................................................. 24
   5.2 Types of Clouds for the EPD System ................................................................ 24
6. List of requirements .................................................................................................. 26
   6.1 Requirements Theory ....................................................................................... 26

VIII
6.2 The List of Requirements .................................................................................................................. 27
6.3 Review of the requirements ............................................................................................................... 29
7. Preferences of the Dutch citizens ....................................................................................................... 31
  7.1 The Questionnaire ............................................................................................................................ 31
  7.2 Preferences Results ............................................................................................................................ 32
  7.3 Review of the Preferences ................................................................................................................ 32
  7.4 Towards the framework ..................................................................................................................... 33
8. Cost Structure ...................................................................................................................................... 34
  8.1 Cost Structure Definition .................................................................................................................. 34
  8.2 Cost Structure List ............................................................................................................................. 34
  8.3 Review of Cost Structure .................................................................................................................. 36
  8.4 Towards the framework ..................................................................................................................... 36
Phase IV Framework ............................................................................................................................... 38
9. Framework .......................................................................................................................................... 38
  9.1 Theoretical Basis ............................................................................................................................... 38
  9.2 The Framework ................................................................................................................................ 41
     9.2.1 The Framework Model ............................................................................................................. 41
     9.2.2 Framework Example ................................................................................................................ 43
     9.2.3 Uniqueness of the Framework .................................................................................................. 45
  9.3 Validation of the Framework ........................................................................................................... 46
10. Conclusion ......................................................................................................................................... 48
  10.1 Research Question ........................................................................................................................ 48
     10.1.1 Sub-questions .......................................................................................................................... 48
     10.1.2 Research question .................................................................................................................... 49
  10.2 General Concluding Remarks ....................................................................................................... 49
  10.3 Limitations of the research .............................................................................................................. 50
  10.4 Directions for further research ...................................................................................................... 51
  10.5 Personal Reflection ......................................................................................................................... 52
11. Bibliography ....................................................................................................................................... 53
12. Appendix ........................................................................................................................................... 62
    Appendix I Questionnaire ..................................................................................................................... 62
    Part A. Questionnaire ........................................................................................................................... 62
    Part B. Explanations of the questions .................................................................................................. 65
    Appendix II Interviews set-up ............................................................................................................. 68
### IV. Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>The Final Framework</td>
<td>VI</td>
</tr>
<tr>
<td>1</td>
<td>Structure of the research</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Network of Keywords</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Questionnaire set-up; keywords with the questionnaire questions</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Cloud Computing (Armbrust, et al., 2010)</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>Service Sector Cloud Set-ups (Colomina, 2010)</td>
<td>20</td>
</tr>
<tr>
<td>6</td>
<td>SaaS structure (Boniface et al. 2010)</td>
<td>20</td>
</tr>
<tr>
<td>7</td>
<td>PaaS structure (Boniface et al. 2010)</td>
<td>21</td>
</tr>
<tr>
<td>8</td>
<td>IaaS structure (Boniface et al. 2010)</td>
<td>21</td>
</tr>
<tr>
<td>9</td>
<td>Public Clouds (IBM, 2014)</td>
<td>21</td>
</tr>
<tr>
<td>10</td>
<td>Private Clouds (IBM, 2014)</td>
<td>21</td>
</tr>
<tr>
<td>11</td>
<td>Hybrid Cloud (Mather et al, 2009)</td>
<td>22</td>
</tr>
<tr>
<td>12</td>
<td>Requirement process (Hull et al, 2005)</td>
<td>26</td>
</tr>
<tr>
<td>13</td>
<td>Requirements (Sommerville, 2011)</td>
<td>27</td>
</tr>
<tr>
<td>14</td>
<td>The Business Model Canvas (Osterwalder A., 2010)</td>
<td>34</td>
</tr>
<tr>
<td>15</td>
<td>The Business Model Canvas with the nine building blocks (Osterwalder A., 2010)</td>
<td>38</td>
</tr>
<tr>
<td>16</td>
<td>Elements of a Logic Model (Mclaughlin &amp; Jordan, 1999)</td>
<td>39</td>
</tr>
<tr>
<td>17</td>
<td>EPD cloud computing Framework</td>
<td>44</td>
</tr>
<tr>
<td>18</td>
<td>EPD Framework version 1</td>
<td>87</td>
</tr>
<tr>
<td>19</td>
<td>EPD Framework version 2</td>
<td>88</td>
</tr>
<tr>
<td>20</td>
<td>EPD framework version 3</td>
<td>89</td>
</tr>
<tr>
<td>21</td>
<td>Brainstorm Keywords</td>
<td>90</td>
</tr>
<tr>
<td>22</td>
<td>Keywords network</td>
<td>91</td>
</tr>
<tr>
<td>23</td>
<td>UML diagram Accessibility</td>
<td>97</td>
</tr>
</tbody>
</table>
The Implementation of the Electronic Patient Record

Jelle-Eric de Vries

Figure 24 UML diagram Ease of Use ..............................................................97

Figure 25 UML diagram Trust in the System .................................................97

Figure 26 UML diagram Financially Sound ....................................................98

Figure 27 UML diagram Doctors agree with the system..............................98

Figure 28 UML diagram Citizens agree with the system..............................98

Figure 29 UML diagram Successful Implementation .....................................98
V. Table of Tables

Table 1 Outputs of the Steps ........................................................................................................ 6
Table 2 Cost Structure according to Bellil (2014) ........................................................................ 17
Table 3 Cost Structure according to Armbrust et al (2010) ......................................................... 17
Table 4 Articles selected for Requirements .................................................................................. 26
Table 5 Requirements for the EPD system ..................................................................................... 29
Table 6 Articles selected for Cost Structure .................................................................................. 34
Table 7 Cost structure ................................................................................................................... 36
Table 8 EPD cloud computing Logic Model elements .................................................................. 40
Table 9 Relation of Sub Questions to the questionnaire questions and the interview questions ...... 75
Table 10 Overview of the Interviewees .......................................................................................... 76
Table 11 Security Threats and Recommendation ......................................................................... 80
Table 12 Security threats and their Solutions ................................................................................ 82
Table 13 Demographic question; Age group ................................................................................ 83
Table 14 Demographic question; Gender ....................................................................................... 83
Table 15 Demographic question; Education type ......................................................................... 83
Table 16 EPD knowledge; questions 2, 3 and 4 .......................................................................... 83
Table 17 Participation in the EPD; question 5 ............................................................................... 84
Table 18 Access rights; question 6 and 7 ....................................................................................... 84
Table 19 Accessibly; question 9 ..................................................................................................... 84
Table 20 Privacy, cost, implementation and need; questions 9, 10, 11 and 12 .............................. 85
Table 21 Results validation ............................................................................................................ 95
Table 22 Explanation of the Arrows ............................................................................................... 100
The Implementation of the Electronic Patient Record  

Jelle-Eric de Vries

Phase I Literature Research and Research Set-up

In this phase the initial start of the research is made. The phase will start with an introduction followed by the research question and methodology.

1. Introduction

The electronic patient record (the EPD, Elektronisch Patiëntendossier in Dutch) is meant to record every step of a patient’s healthcare (Pyper et al, 2004). Every patient will have a record, as for every treatment a record is made (Hamakers, 2007). These files allow medical personnel to see what the medical history is of a single patient. The information for the records is collected in different places, for example in hospital, by general practitioners and by physiotherapists (Hamakers, 2007).

Patient records have been a problematic subject. According to a survey by Pyper et al. (2004), patients believe that they should have the right to give or withhold consent for medical specialists to look at the patient records. The same survey states that 47% of the patients have concerns about the security of the records. This, quite old, survey shows a problem that patients still have today with the modern EPD. The system that the Dutch government wants to implement connects all the single EPD systems of Dutch patients to create one big system (Bonthuis, 2007), which is accessible from everywhere (Bellil, 2014).

Patients see the potential for the system, but with this, also a number of downsides. They want to secure who sees their information and how much information is visible (Pyper et al, 2004). This makes the EPD a difficult privacy case (Jacobs et al, 2008). As Jacobs et al (2008) show, the issue of privacy was already there in 2008 and is still a pending issue for the system (Bonthuis, 2007). At this point, individuals can only access their information in a decentralized place, sometimes electronically (Jacobs et al, 2008). The new system should ensure that people can access the information from all possible locations within the Netherlands (Bellil, 2014).

Looking at a variety of questionnaires on the topic of the EPD, it becomes clear that indeed, patients are unsure if their privacy will be affected by the new EPD systems (Masman et al, 2012). According to Masman et al (2012), 64% of people are not sure if the information is well-protected and would like to receive more information in order to understand the security measurements. Within this questionnaire it is also shown that the majority of people say they have heard of the EPD (95%) and a large part claims to know what the EPD is (Masman et al, 2012).

Although people do know what the EPD is, a large part of the population refuses to take part in the EPD. One of the reasons for this is that they are not fond of the idea of “big brother watching you” (Dullaert, 2011). Another reason is the costs that come with the construction of the EPD. This thesis will research the possibilities to create an EPD that is publicly accepted at a price that is in comparison with the benefits of the EPD.

An EPD is, as stated above, an Electronic Patient Record. The system that the Dutch government is trying to create is a network of all the EPDs in the Netherlands. Therefore, from now on, when “EPD” or “EPD system” is stated, the entire network of EPDs in the Netherlands is meant (unless stated otherwise). The overall definition of the EPD that is used and applicable for this system is:
The EPD is an electronic network which enables healthcare providers to see medical files of patients from other healthcare providers. This embodies the goal of sharing relevant information in a secure national infrastructure. (Ter Berg & Schothorst, 2010)(Masman et al, 2012)

To create this EPD, a cloud computing system will be used. This technological starting point will be used and researched within the thesis. The aim of the thesis is:

“To establish a framework that can create a sustainable business case for an EPD cloud computing system.”

When following the framework one should be able to create a business case that will be successful on the short run: implementation, but also on the long run: it must be sustainable.

The cloud computing technology that will be used to create a nationwide system shows promise according to a number of different researchers, including Armbrust et al (2010), Bonthuis, (2007) and Hayes (2012). All state that such a system can be used as a nationwide system. For this reason, the cloud computing system is chosen to be used to create a nationwide system for patient healthcare information. This is the system that needs to convince the citizens of the Netherlands to accept and to use the EPD. The system needs to provide the safety to be able to convince the 47% of the people that the data is well-protected (Pyper et al, 2004). A start can be made by providing information, as 64% of the people state that they want more information about the security of the system to take away any doubt they might have (Masman et al, 2012).

The different set-ups of cloud computing will be researched to determine which set-up will be best applicable to the EPD system. The perception of the public and the knowledge of the experts will be taken into account to ensure that the system will function properly, satisfy the needs of everyone and result in a successful implementation. What is meant here by ‘successful’ is that the EPD system satisfies the patients (when a vast majority (95%) of the population of the Netherlands give their consent to store their data in the EPD cloud computing system), lowers the cost and leads to higher efficiency of healthcare.

The thesis is structured as follows: four different phases that each aim at a different part of the research. In phase one, the following three sections are found: section one provides a brief introduction of the EPD and the research. Section two focusses on the aim of the research and the research questions are presented. In section three, the methodology of the research is given. Phase two will be the literature overview phase. This only includes section four, which contains the literature overview. Phase three will give the results of the research: section five will state the results on cloud computing structures, section six will state the requirements of the EPD cloud computing system, section seven will state the results of the questionnaire and section eight will state the cost structure. Phase four is the concluding phase. This will include the following sections: section nine, where the framework is developed. Section ten, which states the conclusions drawn from the research and section eleven, which states the limitations of this research and the directions for further research. Section twelve gives the bibliography and in the last section, section thirteen, the appendix is located.
2. Research Question and Aim of the Research

As the introduction of the EPD system comes closer, more resistance is found among the Dutch citizens. As shown above, a number of different research papers have been written on this topic. As each research paper gives part of the solution to the problems, this thesis will combine their findings, together with new findings to ensure a sustainable solution.

2.1 Aim of the Research

Research has shown, there are a number of obstacles to overcome before implementing an EPD system (Interviewee1, 2014; Leavitt, 2009; Interviewee4, 2015; Grossmann, 2009; Interviewee3, 2014)(Zhang et al, 2010). The main obstacles to overcome are the financial and the security obstacles (Interviewee3, 2014) (Interviewee1, 2014) (Leavitt, 2009). Within these two main obstacles there are a number of different barriers which need to be dealt with to ensure that a cloud computing system will function properly. These barriers are trust in the product, a financially sound product (cost and revenue), legal matters and technical issues (Van Oorschot et al, 2010). According to the literature, these obstacles can be overcome when there is a thorough understanding of each of the different obstacles (Interviewee1, 2014).

This research aims at creating a framework that will generate a business case which will overcome these obstacles and that will lead to a successful implementation of an EPD system can be secured. This EPD system is planned to be reached by introducing a Cloud Computing system. As the research states, the obstacles can be overcome with a thorough understanding of them, thus a deeper understanding of the problems within the EPD cloud computing system is needed to ensure a successful market introduction. The users of the EPD cloud computing system must inevitably gain this deeper understanding of the EPD, to ensure acceptance and be able to create the sustainable business case for an EPD cloud computing system.

As described above, the main objective is the creation of a framework that enables the creation of a sustainable business case for Cloud Computing in the healthcare industry. Aspects that are of vital importance: to store the data safely at an efficient cost to create a sustainable business case (Leavitt, 2009; Interviewee3, 2014). The business case must be shaped in such a way that it will change the perception of people. The citizens of the Netherlands will need to understand that the technology can be safe and sound in order for them to give their consent. They must also understand that an EPD cloud computing system will be of great assistance within the health industry. All this must be achieved within a sustainable amount of financial assets. In other words, the project must not cost an excessive amount of money and create an unhealthy financial situation for medical institutions.

2.2 Research question

The research question proposed in the Research Proposal is the following:

*How can a sustainable business case for storing patient data with Cloud Computing in the healthcare industry be created in the Netherlands, focusing on the aspects of security and cost efficiency?*

The Implementation of the Electronic Patient Record

(Jangerak, 2012). This model covers, according to Langerak, every aspect of a business case. In this research, ‘product’ will be all possible options for the EPD, like a SaaS or PaaS cloud computing system or examples of local EPD systems. ‘Product’ does not stand for the final product. ‘Market’ stands for the needs of the market. ‘Cost’ covers every aspect related to finance. The last pillar, ‘Timing’, covers the aspect of when the product should be implemented.

The choice is made to use these four pillars as the foundation for the business case. This decision is made based on the work of Cooper et al. (2002). This work describes the stage gate approach and the necessary decisions that should be made in each gate. The decisions are based on the information from the business case. In this business case, the four elements are Product, Market, Cost and Timing (Langerak, 2012). A number of different researchers agree with this strategy to channel the product through the stage gate (Onarheim & Christensen, 2012)(Van Oorschot et al, 2010). Through this widely established method, products are able to go faster through the stage gate development process and are more successful (Van Oorschot et al, 2010). Therefore, it is chosen to use the four pillars as cornerstones in the creation of the business case within this research. With this strategy the entire spectrum of essential information for the business case will be covered.

The separation into four pillars has created different categories for the sub-questions. Within every pillar, a number of sub-questions have been created. Through this division the entire spectrum of questions for a successful market implementation can be covered. The following sub-questions are stated:

**Product**
1. Which qualities does the product need to satisfy the customer’s needs?
2. Why is it possible to create a nationwide system in other countries, what stops the Netherlands from creating such a system?

**Market**
3. What are the opportunities and drawbacks of such a nationwide system, according to the citizens of the Netherlands?
4. What can be done to increase the trust of the patients in a Cloud Computing system for the healthcare industry?
5. What are the legal issues that might arise with storing patient data?
6. What is the perception, of the patients, of such a system in The Netherlands at this point? What can be done to change this perception if the perception is negative?

**Cost**
7. Which financial constructs might be used to create a profitable system?
8. What is the main cost factor for storing patient data with cloud computing?
9. What is the main revenue stream that can be found with storing patient data with cloud computing?

**Timing**
10. What are other possible products that might compete with a Cloud Computing system to store patient data? Thus when should the introduction take place?
11. How urgent must the market introduction be on the basis of need for the system?

The sub-questions can be found in Appendix IV (this part will also show the relation between the questionnaire questions and the sub-questions).
The cost pillar and the sub-questions about cost will lead to a cost structure for cloud computing. The final aim is to display all the cost elements within the creation of an EPD cloud computing system. The cost structure will therefore include parts of the cost elements of cloud computing and parts of the cost elements of the healthcare sector.

The questions about the qualities and needs of the system aim to understand the non-functional requirements. In the literature overview, a number of functional requirements are named. These should be fulfilled when creating the system. The non-functional requirements will be researched via answering the sub-questions.

With answering this research question, a framework will be created which ensures a sustainable business case for the nationwide EPD cloud computing system. The implementation of this system will also be a part of the framework, to ensure a fruitful start of the EPD cloud computing system.
3. Methodology

This part will describe the set-up of the research. First, the creation of the keywords and the four pillars will be explained; afterwards the division between the literature overview, questionnaire and interviews will be described. The set-up of the literature study will be stated, followed by an explanation of the questionnaire and concluding with an explanation on how the interviews will be held.

Figure 1 below shows how every step in the research affects the next step and what the output of each step will be. The output of the step will be the input for the next step. In section 3.1 to 3.6 every action will be described.

![Figure 1 Structure of the research](image)

<table>
<thead>
<tr>
<th>Step</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research Question</td>
<td>The research question</td>
</tr>
<tr>
<td>Sub Questions</td>
<td>Sub questions</td>
</tr>
<tr>
<td>Brainstorm</td>
<td>Appendix XI</td>
</tr>
<tr>
<td>Keywords</td>
<td>Section 3.1</td>
</tr>
<tr>
<td>Literature Review</td>
<td>Section 4</td>
</tr>
<tr>
<td>Interviews</td>
<td>Appendix II</td>
</tr>
<tr>
<td>Questionnaire</td>
<td>Appendix I</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Section 6</td>
</tr>
<tr>
<td>Cost Structure</td>
<td>Section 8</td>
</tr>
<tr>
<td>Cloud Computing Systems</td>
<td>Section 5</td>
</tr>
<tr>
<td>Preferences of the Dutch citizens</td>
<td>Section 7</td>
</tr>
<tr>
<td>Framework</td>
<td>Appendix X</td>
</tr>
<tr>
<td>Validation of the Framework</td>
<td>Figure 17</td>
</tr>
</tbody>
</table>

Table 1 Outputs of the Steps

### 3.1 Step 1: The Four Pillars and the Keywords

The research is structured around the Four Pillars; Product, Market, Cost and Timing. The sub-questions that are formed are the basis for a division of the topics into seven different keywords (see appendix IV). These keywords are chosen on the basic pillars that they cover. The keywords are linking the four pillars together to create a network for the questions. Below, the network is shown in figure 2.

The keywords are the result of a brainstorm session around the four initial pillars. This brainstorm session can be found in appendix XI. Below, the motivation behind every keyword is given, as well as their interaction with the other keywords.

- **Quality**: the research questions in the Research Proposal state that the quality of the system is important in order to create acceptance. Therefore, quality is of vital importance (Gollmann, 2010). Within the keyword of quality, the perception of quality plays a major part. When there is...
high quality but the patients do not perceive this quality, the implementation will encounter more obstacles. This part shows the advantages and disadvantages perceived by the patients. The combination of quality and perception will also show the needs of the patients. The need will show which quality the system needs to have and the perception will show if this need is already fulfilled. The keyword of quality refers back to the pillar of product, as it relates to aspects of the product (Byers et al, 2011). The effects of quality are on:

- **Product**: the requirements of the products are the input for the quality needed.
- **Competition**: the quality of the product will affect the successfulness of the competitor’s product.
- **Legal Issues**: the quality of the security is directly linked to what is legally allowed and what thus should be protected with the highest quality of security.

![Network of Keywords](image)

**Legal issues**: within the Research Proposal the issue of laws and privacy is shown. This issue is of major importance to create a sustainable cloud computing system which can be implemented in the market (Groothuis, 2007). These issues form a major obstacle for the implementation, if they are not handled properly (Gollmann, 2010)(Armbrust et al, 2009). The keyword of legal issues refers back to the pillar of product, as it refers back to characteristics that the product must possess in order to be allowed onto the market (Byers et al, 2011). This keyword is also related to the pillar of market, as the market must perceive the product as safe and legally sound (Byers et al, 2011). The effects of legal issues are on:

- **Product**: what is legally possible has an effect on the final form of the product.
- **Cost**: laws and regulations need to be met, which results in an expense.
- **Market**: the legal issues are formed based on the market’s opinion.
- **Trust**: the legal issues need to be met to create trust.
- **Quality**: the quality of the security is directly linked to what is legally allowed and what should be protected with the highest quality of security.

**Trust**: trust represents the overall acceptance of the product. Without trust in the product it will be impossible to implement the structure in the market. With the introduction of any computer system and especially with the implementation of a cloud computing system, the trust in the system needs to be there in order to have a successful implementation (Gollmann, 2010). The
keyword of trust refers back to the pillar of market, as the market must trust the product in order to accept it (Byers et al, 2011). The effects of trust are on:
- Market: trust needs to be created to have market acceptance.
- Timing: the product can only be introduced when the trust in it has been created.
- Introduction speed: the product can only be introduced when the trust has been created.
- Legal issues.
- **Cost Structure**: is proven to be a major part of any product. To create a financially sound product, the cost structure needs to be considered and it needs to be set which different party deals with these costs. As cost structure is also a major part of the Business Canvas, the decision was made to include this as a keyword (Canvas, 2011). The main costs need to be clear in order to understand the cost structure (Canvas, 2011). Cost refers back to the pillar of costs, as this keyword describes the cost structures that need to be in place (Byers et al, 2011). The effects of cost are on:
  - Cost: directly related to the cost of the product.
  - Revenue: is the counterpart of the cost structure.
  - Competition: the cost structure needs to be lower than the cost structure of the competition.
- **Revenue**: next to the cost the revenues need to be considered in order to see if a financially sound product can be made. Will the savings be enough to cover the costs or is the need for the product outweighing the need for revenues. The Business canvas also shows that the revenues are of major importance to create a valuable and successful market introduction (Canvas, 2011). Revenues are related to the pillar costs, as this describes how a profit can be made (Byers et al, 2011). The effects revenue are on:
  - Cost structure; is the counterpart of the revenue.
  - Cost; needs to meet the cost to break even and start making a profit.
  - Timing; when revenue can be made a market introduction can take place.
  - Introduction speed; when revenue can be made the introduction can take place.
- **Competition**: this is shown in the Research Proposal as important, as issues like competitive costs, market timing and monopoly right are caused by possible competition. This part refers to the pillar of time. Knowing the competition is of crucial importance to understand the market and your timeframe (Byers et al, 2011). The effects of competition are on:
  - Quality: the quality of the product will affect the successfulness of the product of the competition.
  - Cost: a higher cost will mean a higher price which will mean a less competitive product.
  - Product: the product standards will set the competitiveness of the product.
- **Introduction Speed**: this point is aimed at the question: how urgent is the necessity of the product? What is the need? Should the product only be implemented when it is sound, or earlier, when it is highly needed? Introduction speed is also linked to the pillar of time and of major importance to the success of the product (Byers et al, 2011). Effects of introduction speed are on:
  - Trust: the product can only be introduced when the trust is created.
  - Revenue: when profit can be made the introduction can take place.
  - Timing: the right timing is needed to guarantee a successful implementation, thus this affects the speed in which the product can be introduced.

A number of connections are not made, for this the following justifications are given:
- Between Quality and Cost: quality and cost are not directly linked, as it is the product that stands between both.
- Between Quality and Revenue: quality and revenue are not directly linked, as it is the product that stands between both.
- Between Competition and Cost: again, not directly linked, because the product stands between both.
- Between Introduction Speed and Competition: as Introduction Speeds focuses on the need of the product and not on gain market share.
- Between Product and Cost & Revenue: not linked because this part is covered within the cost pillar. The cost pillar stands for the revenue and cost of the product.

### 3.2 Step 2: Research

Within this step the choice was made to divide the research into three groups. This decision was made in order to cover the areas where important information might surface. The three different parts will each cover a part of the knowledge that needs to be gained to create the framework. The three parts are: a literature overview, interviews and questionnaires. This division is made based on the keywords described above. They show a variety in areas, for example: the trust keyword shows that citizens need to be involved to be able to measure the trust level, quality shows that experts need to be involved to document the needs for the system while legal issues directs to what is described in the literature.

The literature review will portray the knowledge which is already documented. Scientific articles and journals will be used to create the overview. The interviews will be held to get the experts’ opinions on the matter and to deepen the understanding of the knowledge gained from the literature overview. The last part, the questionnaire, will be held in order to understand the opinion of the citizen of the Netherlands: the people who are supposed to accept the EPD cloud computing system. Thus, it is vital to understand their ground of reasoning.

#### 3.2.1 Literature Study

A literature study will be conducted to find key information elements. The goal of the literature study is to create a scientific base for the framework, which is modelled with the help of the interviews and the questionnaire. A start is made by the literature overview above (see 2. Literature Overview). This part will be extended to find relevant information on all the aspects that are needed to create the framework. Research will be done in the following directions: cloud computing set-ups (to create a system that meets the quality and legal issues), requirements (the qualities that the product must have), and cost structure (of the systems that meet the quality standards, legal issues and have the right requirements). These parts will, together with the background knowledge of the questionnaire, lead to the framework, which needs to be developed to answer the research questions.

#### 3.2.2 Interviews

The interviews will be conducted in order to understand the expert’s opinion on certain aspects of the EPD. The interviews will provide specific knowledge where the questionnaires can only deliver superficial knowledge of the general public. During the interviews, more in-depth questions can be asked, the interview questions can be stated more directly and the answers can be more elaborated (Wengraf, 2001).
For this reason, the interviews will focus on the functional requirements. The aim of the interviews is to create an understanding of how the system can be designed according to experts in their respective fields. The knowledge gained from the literature overview will be deepened, in order to create the framework. For this reason, the technical questions about the cloud computing will be asked during the interviews. Where possible, the interviews will focus on the cost structure and on possible systems that might work to create a nationwide EPD cloud computing system.

The interviews will be semi-structured. The choice for a semi-structured interview is made to cover the entire spectrum of knowledge guided by questions (Wengraf, 2001). This will provide space for additional questions that come up during the interview. Depending on the expert in question, the interviews must be adjusted. The basis of the interview will also be based on the sub-topics named above.

The interview questions are based on the sub-topics within the Research Proposal. The questions of the interview are based on the seven keywords: quality, legal issues, trust, revenue, cost, competition and introduction speed. The different keywords will be used depending on the expert that is interviewed. The interview questions can be found in Appendix II. In this part of the appendix, each question will also be motivated. The data collected from the interviews will be processed and will form the basis of the framework. The data will lead to the answers of the sub-questions and thus to answering the research question.

### 3.2.3 Questionnaire

As stated above, the questionnaire is a part of the process that helps to create the final framework. The questionnaire will be made based on other questionnaires and the information from the literature review. The main topics are finance and security (Gollmann, 2010; Leavitt, 2009; Durkee, 2010; Armbrust, et al., 2010)(Buyya et al., 2008), these parts will be covered in the questionnaire and thus asked to the public. The questions need to be divided among the different topics and all will lead to a better understanding of the sub-topic. The aim was to put at least one keyword with every sub-question of the research proposal. These sub-questions can be seen in figure 3, based on their respective keywords.

![Figure 3 Questionnaire set-up; keywords with the questionnaire questions](image)

The questions considered must have two conditions: the possible answers given must be all clear and the question may not be ambiguous (Mies, 2009). The questionnaire will be available via the internet. With this set-up, it is important that the difference within the group of respondents is equally distributed. Therefore, at the start of the questionnaire a number of different demographic
questions will be asked (Field, 2009). The questionnaire will, in first instance, be given to a small group to see if the questionnaire works and is understandable. After the last revision, the questionnaire will be spread via the internet. The questionnaire should take no longer than 15 minutes to complete, to ensure that people will be focused while answering the questions (Field, 2009).

The questions of the questionnaire are given in Appendix I. Also, the motivation for every question can be found in this part of the appendix. In Appendix IV, a justification is given of which questionnaire question corresponds with which sub-question from the research proposal. The data collected from the questionnaire will be processed and will form the basis of the framework. The data will lead to the answers of the sub-questions and thus to answering the research question.

The sample size for the research needs to be based on the inhabitants of the Netherlands. On 2 October 2014, there were 16.880.870 Dutch citizens (Statistiek, Bevolkingsteller, 2014). From these citizens, there are 1.691.675 people younger than 18 years (Statistiek, Bevolking; geslacht, leeftijd en burgelijke staat, 1 januari, 2014). This leaves 15.189.195 Dutch citizens as the research population. (the people younger than 18 are left out of this research as they are not allowed to choose for themselves if they want to join the EPD and thus do not have an effect on the research. Based on an error of 5% and a confidence interval of 95%, this results in a sample size of 385 people for the research. Therefore, the aim is to reach 385 people.

3.3 Step 3: Creation of the Framework
The output of step 2 will create four different sections with results. These sections cover different parts of the business case.

1. For the product pillar a section will be created with a cloud computing system to use.
2. For the market pillar a section will be created with an outline requirement for the system.
3. For the timing pillar: within this section the preferences of the Dutch citizens will be displayed along with their needs for the system.
4. For the cost pillar: a section will be created with an outline of the cost structure.

These four sections will together deliver the input for the framework. The framework will be created via a logic model. This way, a model will be created that will present a plausible and sensible outcome of how the program will work under certain conditions to solve identified problems (Mclaughlin & Jordan, 1999). The output of the creation of the framework can be found in section 9.

3.4 Step 4: Validation of the Framework
The validation process will be done to understand the correctness of the framework. This evaluation of the framework will be done to improve the framework on the basis of expert opinions. The framework is also compared with other frameworks and tested for its uniqueness.
Phase II Literature Research

4. Literature overview

A number of different studies have been done on the EPD. These studies studied the different aspects of the EPD. Privacy and the financial options are of great importance when trying to make a sustainable EPD. The two points, privacy and financial options, are the result of findings of different researches. Privacy is a main issue within cloud computing and storing data in general. This point is acknowledged by Brokdin (2008); Armbrust et al, (2010); Jansen (2011) and Chen and Zhao (2012).

The creating of a business case comes with creating a financial overview (Osterwalder A., 2010), this financial plan is of great importance for the successfullness of the product (Tripathi & Mishra, 2011). The social point, privacy, will be looked into first. Second, the literature overview will cover the financial options for an EPD. Third, the cloud computing will be covered. Afterwards, a number of surveys will be compared. And finally, a number of conclusions will be drawn from the information above.

The statements are the goal of the literature overview. The statements will serve as a basis to create the questionnaire and the interview questions. The literature overview also indicates what possible solutions there are, which can be offered to the public within the questionnaire. The ultimate goal is to gain deeper understanding of the topic, to fuel the questionnaire and interviews and to create a framework with this knowledge.

The literature overview is created on the basis of scientific articles. The scientific articles are selected on their relevance to the research topics and are found through google scholar and the TU/e online library. The criteria for selection are:

- Relevant to one of the following subjects: privacy, cloud computing finance options, cloud computing in general, cloud computing structures, EPD systems and questionnaire and interviews already done on EPD systems.
- The amount of quotes the articles have: when having more quotes the articles are deemed more important.
- From sources from other articles already found and used in the thesis.

4.1 Privacy

As was said, a number of studies have been conducted on the implementation of a new EPD system. As stated above, 95% of the Dutch population have heard of the EPD and a large proportion claims to know what the EPD is (Masman et al, 2012). While the Dutch law protects (“De Wet Bescherming Persoonsgegevens”, WBP) the information of patients, a large part of the Dutch population is scared that their information will be stolen or miss-used (CBP, 2001). This “Big Brother” feeling stops them from signing up for the EPD. While they do see the advantages of the EPD, they still see the downsides as too threatening (Masman et al, 2012).

The Dutch Law, WBP, (Wet Bescherming Persoonsgegevens) states the privacy laws for the Dutch population. In Article 13 this law shows the rules for the storage of personal information (Hamakers, 2007). The Article states that an institution or person processing the data is the person responsible for the data (CBP, 2001). For this reason, a hospital is obligated to protect that data of their patients adequately.
Next to the WBP, there is the WGBO (de Wet op de geneeskundige behandelovereenkomst). This is the law which states that only the people with a relation to the treatment of the patient may access the information about that particular patient (Hamakers, 2007). A record is made a soon as a patient is in contact with a medical institution, further documentation is made when treating a patient (Hamakers, 2007). The record will show the state of health of the patient, the treatment to be done and any other information that is applicable to the patient and of value for the treatment (Overheid, 2014). From that point onwards, the healthcare provider is responsible for the safety of the record. They may not give the information to a third party without the consent of the patient.

The EPD systems that are in place now, are local EPD systems. They are meant to facilitate one hospital and are not connected to other hospitals within the Netherlands. The plan is now to create a nationwide EPD system which will be subject to the same laws as the local systems. Every user must get a valid identification code to enter the national EPD in order to see the information he or she is entitled to. Different medical personnel will be grouped into different access right groups, nurses will be in a different group than doctors and pharmacists will be yet again in a different group (Hamakers, 2007).

At this point in time, the LSP (Landelijke SchakelPunt) is in place (Consumentenbond, 2015). This structure allows medical personnel to store patient data on their own servers. This can only happen when the patient actively gives his or her consent to join the LSP. When the patient data is linked to the LSP, other medical professionals can request to see the information. They are only allowed to do this when they have a connection to the patient (Sijm, 2008). The LSP is mainly used to connect general practitioners with each other (Sijm, 2008). Hospitals often use their own EPD system, systems, such as EPIC (EPIC, 2014), USER or mijnQuarant (Dorresteijn, 2014).

The problem with this set-up is the access rights for medical specialists are fairly broad. They can access all the information of all the patients. The oath they have taken (KNMG-publicaties, 2003) and the law (WBP) forbids them of doing so, but yet they will be able to access the information of patients they are not treating (Hamakers, 2007). The government admits this set-up is not ideal, but at the beginning of the project it will be hard to know who needs access to the information. At this point, the decision is made that the specialist will receive a notification when accessing a person’s file, when he or she is not entitled to. This notification will also be sent to monitoring group for internal control with the remark of the specialist on why the information was accessed.

Besides the Dutch law WBP, medical personnel have taken an oath that prevents them from sharing information of patients with a third party. This oath of Hippocrates has been used worldwide since 400 BC (Bonthuis, 2007). The oath swears the doctors to secrecy about their patients and their information. The effect of this oath is that doctors cannot share information with any other than the patients themselves. For example: in court a doctor cannot give medical information about the patient according to the oath (Bonthuis, 2007).

In 1878, a variant of the oath of Hippocrates was implemented within the Netherlands. Every medical student has to take the oath to gain the medical rights. This oath states that the students will not give the information they collect about patients to a third party (Bonthuis, 2007). Not fulfilling this oath and violation the oath is punishable by law within the Netherlands (CBP, 2001). The challenge of sharing medical data online when the oath states against sharing is faced by the doctors and needs
The Implementation of the Electronic Patient Record

Jelle-Eric de Vries

to be overcome when the system is completely implemented. This challenge is also seen by the patients, who want their information to be secure.

The plan thus far for the system gives patients the right to refuse the use of the EPD (Jacobs et al, 2008). According to the government, there should be options to partly allow access for certain groups. One should be able to see who has access to one’s files and one should be able to access their own EPD files (Jacobs et al, 2008). The basis for this access is the social security number (Burger Service Nummer; BSN), as every Dutch citizen can be identified by this number.

With this set-up, a decentralized structure must be developed to allow everyone to access the system. People need to be able to access their information when they want to access their information (Jacobs et al, 2008). This gives opportunities for cloud computing to create an EPD system that links the different hospital systems together in one overall system that can be accessed from different locations with an identification and authentication code.

This does not mean that the storage cannot be in different places at the same time. The hospital and other medical facilities already have an EPD. These systems need to be linked. This can be done with a decentralized system set-up (Armbrust, et al., 2010). A study by Jacobs et al (2008) classified the system that needs to be made as a high threat system. They state that the privacy might be a problem, but this problem might not be an issue for an ordinary person. The privacy problem might be more relevant to more famous people (Jacobs et al, 2008). They show that the use of private and public keys is only the start of the security measurements that need to be taken to secure this system.

EPD systems are used in different countries, like the United Kingdom and Norway (Christensen & Grimsmo, 2008) (Thiru et al, 2003). While these systems of EPD are being used, the study of Christensen and Grimsmo (2008) also shows that information within the EPD records is not always satisfactory. They state that the systems can be efficient and comprehensive but it can take more time to fill in the files than the paper files. Christensen and Grimsmo (2008) stress that an EPD must be well-designed in order to be an effective clinical tool. When a faulty design is made, the systems might only be a burden.

A study conducted in Norway shows that most medical personnel will fill in the EPD on their computer in their office (93%) (Laerum et al, 2001). As this is an old study, and the researchers indicated a growth, there is reason to believe that nowadays, roughly 100% of doctors have computers in their offices. Laerum et all (2001) stated that similar results can be found in other countries, like the Netherlands. This also indicates that the EPD can be accessed from anywhere within the hospital. Combine these access points with access from anywhere in the country by the patients and millions of access points can be created. This means that every access point needs to be secure in order not to be a threat to the security of the system.

In Portugal, a similar system is being set up. This system is not nationwide yet, but is also in the development stage. Currently, the system covers over 11,000,000 documents for over 35,000 patients in the Aveiro region (LE MAG, 2013). The system uses encryption and digital signatures. “The security mechanism protects the integrity of an electronic document by creating a unique identifier (a hash) for that report that is closely associated with this content” (Ferreira, et al., 2004). This
unique identifier will be made using public key encryption technology. According to the Portuguese, this system is secure enough to use (Ferreira, et al., 2004).

In the Netherlands, the security risk is seen by the patients. However, the depths of the risk are not fully understood by the patients. Surveys that have been conducted show that patients do not have a thorough understanding of the EPD. 65% of the respondents believe that insurance companies can access the information within the EPD about a specific person. However, this is not possible in the current plan (Masman et al, 2012). The survey also shows that people with a higher education level know more about the EPD than people with a lower education level. The majority of the people never search for information about the EPD themselves, although 4 out of 10 would like to have more information about the EPD. Most people state they would like to receive more information about how they can access their information. 3 out of 5 people would like to know which medical professionals have access to their file on the EPD (Masman et al, 2012).

The fear that exists is fuelled by the information stream about hacking. People fear that their record will be hacked and their medical data will be seen by others and used for unintended purposes (Groothuis, 2007). The other fear exists in the form of people. The patients fear that the medical personnel will not protect their information sufficiently. They might be sloppy, or they might not take the necessary precautions. (Groothuis, 2007). This might lead to accidental mistakes in the EPD of a patient. Other medical professionals might not realize a mistake is made and will work with the faulty data with makes treatment more difficult (Groothuis, 2007).

Within the hospital, medical professionals need to cooperate when implementing the system. Surveys in the Netherlands have shown that medical personnel is not always eager to cooperate (Boll, 2006). The survey states that the medical personnel’s motivation to participate is low; they do not want to change the current system. This feeling is often fuelled by the upper management, who make decisions without asking the advice from the personnel who need to use the system (Boll, 2006). Boll (2006) advices hospitals to approach the introduction of the EPD system as an organizational change, not just an IT implementation. When this method is used, a hospital is able to include all the different groups in the implementation process. Boll (2006) also states that the implementation will take time and must not be rushed. In some cases, the old systems might not be compatible with the new EPD and thus must be replaced and this takes time. The implementation of an EPD system must be seen as a dynamic changing process of the organization (Boll, 2006).

The EPD is a chain information system which ensures that everyone, who is entitled to, can see the patient records. As stated above, there is the possibility of failure with such a chain information system. Information can be wrongly processed and this will lead to problems further down the chain. There are a number of steps to increase the functionality of EPD systems (Visser, 2013). These four steps are:

- When implementing, take small steps and keep track of the results of the programs. One step must be completed before moving on to the next step (Visser, 2013).
- Revise any pressure and questions from outside of the organization. In this case, also evaluate the question of the medical personnel and the patients about the EPD (Visser, 2013).
- An abundance of features on a system makes the systems harder to use for non-professionals. The simpler versions often work better (Visser, 2013).
The Implementation of the Electronic Patient Record

- One should not aim at complete unity in opinion. The main problems within the systems should be solved and, later on, individual needs might be taken care of (Visser, 2013).

Research has shown that there might be problems with the implementation of the EPD systems. There is no noticeable difference between EPD users and less intensive EPD users or non-users on the basis of quality of medical treatment (Westert et al, 2002). This old study shows that there was not a big difference twelve years ago. As all the general practitioners have EPD systems now, the general practitioners will now all have similar user intensities. While private clinics often use different systems and thus have a lower intensity. Still, both function perfectly and also without the EPD a clinic can function perfectly.

4.2 Finance

The financial side of the EPD is a big part of implementation (Osterwalder A., 2010) (Tripathi & Mishra, 2011). In a number of different research papers it is claimed that the cost of the healthcare will decrease when the EPD is implemented (Groothuis, 2007). This is one of the main reasons why the system will be implemented. The time-consuming paper files will be replaced with a computer system and thus time and money will be saved. Also, medical professionals can see what kind of medical research has been done on a patient and ensure that they are not doing the same research twice (Groothuis, 2007).

The downside to the system is that new software is required. All medical professionals, or institutions, have to invest in a new system, which is expensive (Maes, 2013). As the system also needs maintenance and updates, the cost of the system is higher than a system consisting of just paper files (Maes, 2013). The introduction costs might be an issue in persuading everyone to start using an EPD system. Within the Netherlands, the general practitioners are already supposed to have a local EPD system for their patients (Khan et al, 2011). That being said, Khan et al (2011) also stated that not all general practitioners have their systems up to standard. This might create extra costs, as when the systems are not all up to the same standard, this will lead to a system that is not functioning properly.

Another reason for higher costs is the failure of government ICT programs. Deira (2014) and Woudt (2014) state in their articles that a large part of the government ICT programs never make it to the market. The same can be said for the development of the EPD. The first development sessions of the EPD have been stopped in 2010 (van Twist et al, 2012). The higher costs that exist arise from restarting the project. With the restart, it is unsure which elements of the former project can be used, thus which costs need to be re-spent (van Twist et al, 2012).

According to Yoon et al. (2012), there are a number of upfront investments to be made. These are: activities, personnel, executive management, human resource and finance, building, supplies, electronic health record and other operating expenses. These costs are matched with savings and possibly some increase revenue. The cost savings consist of eliminating costs of storing paper records and downsizing personnel. The possible increased revenue consists of government incentives for use of health IT and pay-for-performance incentives (Yoon et al, 2012).

Yoon et al. (2012) also state that there is high uncertainty about these investments. Within the Korean market, it is shown that the investment cost is seen as a barrier by 76,3% of the respondents from hospitals without an EPD. For a national system, 53,8% of the respondents from hospitals with
an EPD see the investment cost as a barrier. Also, the return on investment and the concerns about ongoing costs are seen as barriers (Yoon et al., 2012). In the US only 9.1% of hospitals have a form of an electronic record system (Wulsin & Dougherty, 2008). This 9.1% do state that the use of an EPD leads to a reduction of medical errors, thus creating a reduction in the cost. They do see the investment cost as a barrier for the implementation of the system, but have indicated that the upside of the system is worth the investment (Wulsin & Dougherty, 2008).

Bellil (2014) states that in a different form of patient record, there are possible structures to gain revenue from the patient records. These possible structures are mainly applicable on the commercialization of products in the free market. Advertisement, the creation of apps and infomediaries are difficult to introduce in a system that is going to be mandatory throughout the Netherlands. The information is sensitive and the lack of willingness to pay for an app that the patients have no use for, will result in a lack of revenue gained (Bellil, 2014; Groothuis, 2007). The costs described by Bellil (2014) are found in other research articles as well. As stated as well, the costs will consist of: materials, people, teaching, infrastructures and support. The costs of security, monitoring and maintenance are not included in this cost structure (Bellil, 2014). Below an overview of the cost structure is given (table 2).

<table>
<thead>
<tr>
<th>Cost Structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materials</td>
<td>The costs of creating the physical part of the storage system</td>
</tr>
<tr>
<td>Teaching</td>
<td>The costs of instructing people how to use the EPD and how to do maintenance</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>The costs of the software part of the storage systems</td>
</tr>
<tr>
<td>Support</td>
<td>The costs of the support team to help with problems the user may have</td>
</tr>
<tr>
<td>Security</td>
<td>The costs of creating a waterproof system</td>
</tr>
<tr>
<td>Monitoring</td>
<td>The costs of monitoring the system to ensure safety.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>The costs of updating the system, reaper problems and keeping the system running</td>
</tr>
</tbody>
</table>

Table 2 Cost Structure according to Bellil (2014)

The table above shows an outline of the cost structure of the cloud computing system within the healthcare market according to Bellil (2014). Armbrust et al (2010) show part of the cost structure for the EPD. The cost structure for cloud computing is shown. The table below gives an overview of the cost structure for creation of a cloud computing system (table 3). The table gives the elements of the system that require an investment or periodic fee.

<table>
<thead>
<tr>
<th>Cost structure cloud computing</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware system</td>
<td>The physical products needed to create the system. E.g. servers, cables, computers</td>
</tr>
<tr>
<td>Applications software</td>
<td>The software to create the cloud program on location. It probably needs to be scaled up.</td>
</tr>
<tr>
<td>Infrastructure software</td>
<td>The software to link the different systems together</td>
</tr>
<tr>
<td>Electricity</td>
<td>The be able to keep the system running</td>
</tr>
</tbody>
</table>

Table 3 Cost Structure according to Armbrust et al (2010)

The overall cost of introduction is estimated to be around 305.826.211 euro spent between 2002 and 2010 (van Twist, et al., 2012). This estimate was made in 2011 and the costs have risen since. The
money is spent in four categories: ‘Nationwide infrastructure’, ‘Implementation EMD/WDH’, ‘Communication’ and ‘Additional costs’. Around 6,3 million is spent on communication and 5,7 million on additional costs (van Twist, et al., 2012). A total of 217,5 million is used for the creation of a nationwide infrastructure for data exchange. Money was spent on audits, advise, pilot projects, communication, IT development, project management, project subsidies, creation of the basic infrastructure and the development of the LSP (Landelijke SchakelPunt). The implementation of the EMD/WDH has cost 78,5 million. The cost items in the implementation are: hiring of implementation organization, proof of concept, evaluation pilots, subsidies and variable cost of the Uzi-register (van Twist et al 2012). The exact cost items for the infrastructure (e.g. hardware costs, software costs) are not stated in the work of van Twist et all (2012). The costs portrayed in van Twist et al (2012) are the costs of the EPD before the project was stopped. It is unsure which of the expenses can be used in the next attempt to create an EPD. The 305 million spent on an EPD system that failed to be implemented creates a high distrust towards government ICT programs among the Dutch citizens. While there was money spent on communication and advice, it can be concluded, from the failing of the project, that this was not spent the right way. The study of van Twist et al (2012) does not specify on which specific actions the money was spent. The lack of clear structure creates uncertainty about whether every action to spend the money is taken in the best suitable way possible.

The costs above are paid for by the Dutch government to implement the system. Hospitals need to ensure their computers are up for the task of running the system and need to transfer into the EPD systems (Knotnerus & Stegwee, 2010). The benefit of the total system is hard to determine, as this is a combination of different factors. Saving costs will come in the form of there no longer being a need for storage space for the files, as no physical files are needed, a stronger position toward insurance companies, faster delivery of recipes at pharmacies and cheaper medicine (Knotnerus & Stegwee, 2010). Therefore it is difficult to say what the total savings will be when introducing the system. It is safe to say that there will be no profit made, as this system is designed for saving cost and not to generate revenue (Knotnerus & Stegwee, 2010).

The total cost structure will be examined further in section “8. Cost structure”. The information above will be used as a basis for the total cost structure.

4.3 Cloud Computing

4.3.1 General Cloud Computing
The research has shown that cloud computing can be a valuable method to create a national wide linked system (Bonthuis, 2007; Hayes, 2012; Armbrust, et al., 2010), such a system can be used to create an EPD system. The possibility to store information in a decentralized system and the on demand delivery of data will help to support the system. The problem that still remains is the security of the system when storing all the information in different locations (Armbrust et al, 2009). The convenience created by the introduction of the cloud computing system enables medical professionals to access the documents from everywhere (Kundra, 2011). Vaquero et al (2009) also support this statement. Clouds are a large pool of easily usable and accessible virtualized resources (Vaquero et al, 2009).

The full service that cloud computing offers can be used to create a system that facilitates all medical personnel. The main security threats of the cloud computing system need to be revised in order to create a sustainable system. A number of security threats and their solutions can be found in
Appendix VII. These threats and solutions are based on the works of Tripathi & Mishra (2011) and Chen et al (2010). The solutions to the threats form the functional qualities of the EPD. The solution to the problems must be part of the set-up of the system in order to make the system fully functional and safe.

The cloud computing system can be managed as a whole from a remote location (Armbrust et al, 2009). This option will create a central control room where the system will be managed and secured which will give also the possibly for monitoring the system. This is also a functional quality in order to create this system. A control room needs to be set up to create a safe environment. Gollmann (2010) states that the system must be carefully examined before implementation to ensure that the system is reliable. As long as there is human interaction involved, there will be a security threat (Gollmann, 2010).

One of the main obstacles is the level of competence of the EPD users. The security will be as strong as the weakest link (Gollmann, 2010) and thus all the different parties must have the necessary skills and competences (Hayes, 2012). When parties do no acquire the minimum level of competences, the cloud service will not function accordingly (Gollmann, 2010). This will be a risk to the total security of the system. When one part of the cloud computing system is vulnerable, the entire security of the system will be at risk. Therefore the entire system is based on trust. Every part of the information chain must exercise a certain amount of trust in the other parts to ensure a sustainable system which can function to its full extend (Ristov et al, 2012).

This might also be in conflict with the oath the medical professionals have taken as they are forbidden to share information. This must be well arranged within the Dutch law (WBP) to be sure that no conflicts can arise. The law (WBP) above states that medical professionals are responsible for the data of their patients (Overheid, 2014) and it would be problematic when they have to upload the data to a system where they can no longer fully control the situation (Armbrust et al, 2009).

The other parts of the security, Architecture, Identity Management, Software isolation, data protection and availability, are of equal importance (Gollmann, 2010)(Jansen, 2011)(Aymerich et al, 2008)(Jansen & Grance, 2011). These points mostly direct a method to secure the trust in the system. Jansen & Grance (2011) give the basis for a detailed outline of what can be done to fully execute these points to ensure maximum protection of the data. This outline based on the work of Jansen & Grance (2011) is shown in Appendix VI.

The other part of the security outline in the Literature Review shows an outline of what needs to be done on a technical level. Via encryptions, Public Key infrastructure, Rights Management, Digital Signatures and Recovery of Data the data can be protected (Chen & Zhao, 2012) (Gollmann, 2010) (Brodkin, 2008)(Armbrust et al, 2009); (Ellison & Schneier, 2000). These security assets must be utilized to the fullest extent to create a sound system that will gain the trust of the citizen of the Netherlands. With the use of these technical security measurements, it will be possible to create a sound system that will protect the medical data of patients.

4.3.2 Cloud Computing Systems
Different types of clouds can be defined. These even differ in the paradigm one stands in (Colomina, 2010). Looking from the service sector paradigm different cloud options can be seen (Armbrust et al, 2009), but other types of clouds can be identified based on the deployment model (Brodkin, 2008)
and on the access model (Plummer, 2009). The three paradigms including their different cloud types will be explained below.

In general two main models are seen, the service models and the deployment models (Mell & Grance, 2011; Huth & Cebula, 2011; Yang & Chen, 2010; Mahmood & Hill, 2011)(Armbrust et al, 2009). Colomina (2010) shows a third model that is based on an earlier model of deployment but this model is less researched and less developed. Even so, this model will be part of the research as it is deemed important for the construction of an EPD cloud computing system. The third model has an effect on who has access to the cloud, which is a major factor in the security of the EPD cloud.

4.3.2.1 Service Sector
Colomina (2010) states that the paradigm service sector categorizes cloud computing by the service that is being offered. This distinction is often made by other researchers. The different levels of cloud computing can vary in amount of hardware and amount of software (Armbrust et al, 2009) (Vaquero et al, 2009). The researchers categorize the cloud computing in Software-as-a-service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

This service oriented approach disregards all other services that cloud computing facilitates (Colomina, 2010). To limit the possible options it was chosen to use the three main services which are most often stated by research. These are seen as the general services and often able to be used as synonyms for other services (Colomina, 2010). Therefore SaaS, PaaS and IaaS will be used for the service sector paradigm. It is important to note that they are not the only service provided by cloud computing. The main stream research name in general just the three service sector paradigms (Armbrust et al, 2009) (Mell & Grance, 2011)

Figure 4 displays the use of the SaaS system over the internet towards the user of the system. It clarifies the role of the provider of the cloud towards the SaaS user (Armbrust, et al., 2010). The provider of the cloud supplies the hardware and the infrastructure for the cloud. When the provider delivers a SaaS system, the application will also be part of the deliverables.

The level of abstraction increases with the different services (Armbrust, et al., 2010). Flexibility increases in the opposite direction from the level of abstraction. This is shown in figure 5. SaaS offers a set system where the client can enter the data in a set application, thus SaaS has no flexibility in its configuration. SaaS has a high abstraction level. IaaS is the opposite and provides the ability to create one’s own program (Armbrust et al, 2009).
SaaS is the highest level of cloud computing according to Durkee (2010). SaaS gives an entire system with a fully functioning application including hardware (Armbrust, et al., 2010). This gives the user the ability to instantly use the cloud computing set-up. In general it is not possible to write extra code or change the application without the help of the provider (Durkee, 2010). The core principle is that software is deployed as a hosted service and accessed over the internet (Colomina, 2010). SaaS is a well scalable cloud computing option (Chong & Carrao, 2006). Figure 6 gives the SaaS structure.

PaaS is a cloud computing level lower than SaaS (Durkee, 2010). This middle level of abstraction and flexibility enables clients to manage code development and deployment. A PaaS provider generates an environment for the user to create web applications without the back-end knowledge (Boniface, et al., 2010). Figure 7 shows the structure of a PaaS cloud computing set-up. PaaS is scalable like SaaS. PaaS is scalable on a deployment and code development level (Armbrust et al, 2009). In short, a PaaS provider will run your application on their system (Jonas, 2009).

IaaS is seen as the lowest level in service sector cloud computing (Durkee, 2010). The provider of IaaS delivers hardware and the client must create their application themselves. This shows in the fact that IaaS was formerly called Hardware-as-a-Service (Jonas, 2009). Other researchers state that the HaaS level is even below the IaaS level (Yang & Chen, 2010)(Rimal et al, 2009). The IaaS client is empowered to manage the virtual machines the provider facilitates (Armbrust et al, 2009). Figure 8 shows the structure of an IaaS cloud.

4.3.2.2 Deployment Model

The deployment model shows the relation the cloud, and thus the internet, has with the enterprise who uses the cloud (Mather et al, 2009). Four different set-ups are available for the deployment model: Public, Private, Community and Hybrids clouds (Huth & Cebula, 2011). Other research discusses only the Public, Private and Hybrids clouds (Rimal et al, 2009). Public clouds are often referred to as external clouds and private clouds as internal clouds.

Public clouds are clouds hosted, operated and managed by a third party: this can be done from multiple storage locations (Mather et al, 2009). The security and day-to-day operations are also managed by the third party. Yang & Chen (2010) stated that letting the security be handled by the third party creates risks for the company using the cloud. These clouds are seen as easily scalable and cost efficient, while fine-grained control over the data, network and security settings are lacking (Zhang et al, 2010). The public cloud structure is displayed in figure 9.

Private clouds (figure 10) are exclusively used by one organization or by external providers (Zhang et al, 2010). In general it is deployed from the enterprise data center and managed by internal personnel or a service provider (Yang & Chen, 2010). Therefore the security and day-to-day
management are handled by the enterprise: this will create a high degree of control and transparency (Mather et al, 2009). This will increase the customizability, execute security standards, policies and regulatory compliance (Mather et al, 2009).

Hybrid clouds are a combination of private and public clouds. They enable enterprises to run partly in their own private cloud and ask to run in a public cloud for intensive computing resources when peak workloads occur (Yang & Chen, 2010). The main problem with this set-up is the trust barrier that needs to be overcome to share the sensitive information of an enterprise in a public cloud (Mather et al, 2009). This cloud set-up does provide more control over the data and security than a public cloud, but one needs to carefully examine which data to share in which cloud (Zhang et al, 2010). Figure 11 shows the set-up of a Hybrid cloud.

The community cloud uses personal computers to create a cloud that can be used (Marinos & Briscoe, 2009). Thus it can also be that companies that need similar clouds share the same cloud (Huth & Cebula, 2011). The cloud is used specifically by one community. The cloud can be facilitated by a third party or by the community and can be on or off the premises (Mell & Grance, 2011).

4.3.2.3 Access Model

This third model is mentioned in the work of Colomina (2010); the work is also mentioned by Plummer (2009) and Smith (2008). This model is highly linked to the deployment model and refers back to who can access the cloud. The public, private and hybrid clouds all have different access rights and security of access rights (Spinola, 2009). The access model is not widely researched but important to the creation of an EPD cloud computing system as it shows how users can access the cloud (Plummer, 2009).

Public clouds are made in such a manner that multiple members of different organizations can access the cloud from different locations (Armbrust et al, 2009). This makes it easier to access the cloud from different hospitals when needed. This set-up is recommendable when non-critical information is stored in the cloud and when it is not possible to scale the infrastructure because of limitations on-premises (Michelson, 2009).

Private clouds are made to only be accessed by the members of a specific organization (Armbrust et al, 2009). This creates a better secured system, the chances of data flowing out of the system is smaller. Therefore private clouds are better suited for handling sensitive information (Michelson, 2009).

Hybrid clouds are again a combination of both systems. Part of the information is only accessible for members of the organization and part of the information can be stored in a cloud that is accessible for others as well. In a service level agreement (SLA) one can pinpoint who has access rights to the cloud that is being used (Patel et al, 2009).

The information above forms the basis for section 5 “Cloud computing Systems”. There, three main models will be created that can be used to create a cloud computing systems for the EPD. Also a list of requirements for the EPD cloud computing system will be given in section 6 “List of

Figure 11 Hybrid Cloud (Mather et al, 2009)
Requirements". These recommendations and technical measurements will be used together with the data derived from the questionnaire and interviews to create a framework.

4.4 EPD Questionnaires and interviews
A number of questionnaires have been conducted on the introduction of the EPD system. These questionnaires aimed at getting an understanding of the willingness of the public and some aimed more specific at the will of medical professionals. The questionnaires give an indication of what the public opinion on the EPD system is. Van Tiel (2009) gives an overview of the public opinion towards the EPD. Most questionnaires are based on gaining clues about the understanding of the EPD by the Dutch citizens. The information is displayed throughout the thesis and an important part in Appendix IX.

4.5 Statements
A number of different statements and conclusions can be drawn from the text above. These statements can be seen as important conclusions for the successful implementation of an EPD system in the Netherlands. The conclusions are derived from the text. The conclusions will help to create the framework and guide the research purpose of the questionnaire and interviews. Eventually these conclusions will help lead to a successful implementation of the EPD. The conclusions are listed below:

- The main issue and obstacle that needs to be overcome is the security concerns: otherwise this will have an effect on the successfulness of the implementation of a cloud computing system (Gollmann, 2010).
- The reason for the issue in the first bullet point might be that the information towards the citizens of the Netherlands is not clear and there is a lack of knowledge amongst the citizens (Masman et al, 2012).
- The privacy obstacle needs to be overcome before implementing the EPD (Jacobs et al, 2008).
- Trust in the system is required for successful implementation (Ristov et al, 2012).
- Input from all medical personnel who work with the EPD will generate a broad acceptance basis (Boll, 2006).
- Encryption of the data must be done to ensure the safety of patient data (Ferreira, et al., 2004).
- Different data storage locations are possible: central or de-central and on different levels of cloud computing (Armbrust, et al., 2010).
- As long as people are involved there will always be a security risk (Gollmann, 2010).
- The EPD in the current set-up will create possible financial savings. The use of cloud computing will facilitate this cost reduction: it will not necessarily create revenue (Wulsin & Dougherty, 2008).
- The EPD already cost 305 million euros. Costs will rise further (van Twist, et al., 2012).
Phase III Research Results

In this phase the research results will be shown. This is the data found during the research and based on phase II. The presentation of the data will be done in different subgroups corresponding to the research direction based on the sub questions. This information will later be combined in phase IV to create the framework.

5. Cloud Computing Systems

Based on the literature above, a selection will be made of what the best cloud computing systems are to create a nationwide EPD system.

5.1 Selection criteria

Above, a number of different cloud set-up mechanisms are named. Based on these, a combination is made for the EPD. This will be done via selection criteria to ensure the best possible option is chosen. These criteria are shown below:

- Most used cloud computing system – this is chosen to understand the best practice methods and the most common methods used.
- In line with the expectation of the users – this criterion is chosen to understand the need of the end user.

From the information above in section 4.3, the following basic conclusions can be drawn:

- It can be seen that SaaS is the most used system (Yang, et al., 2011; Cusumano, 2010). SaaS is used because the end users usually use a whole application within the Cloud (Armbrust, et al., 2010).
- The four deployment models are all frequently used (Arasaratnam, 2011). All different types are used and have their own opportunities and draw backs (Zhang et al, 2010).

5.2 Types of Clouds for the EPD System

When constructing the EPD cloud computing system, there are a number of different factors that must be considered. The right combination of the models above is essential to create a valuable system. Below, three combinations will be made of which each will be able to form an EPD cloud system. The combinations are made with the use of the selection criteria. These combinations will create systems that can be used depending on the legal rights, demand of the users and other factors. The framework will then show when to use which system.

The following three systems are considered to be appropriate for an EPD cloud computing system (the systems are not ordered in any way):

1. Based on the information above, it is clear that a SaaS system should be used, as it is the most frequent used system (Yang, et al., 2011; Cusumano, 2010). To ensure security and ease of security, a private cloud will be used, as this ensures that no-one else enters the cloud (Mather et al, 2009). Thus the cloud will only be accessible to any person in the healthcare sector. These individuals must be in possession of the right credentials to be able to connect to the server. Servers will be located at a central location in the Netherlands. The
application allows all medical personnel in the Netherlands to consult the information they need, when they need it without asking for consent every time.

2. A nationwide application will be made for the vital information. The interview with Interviewee 3 has shown that it can be of great help to know certain critical information of a patient, like allergies or rare life threatening conditions (Interviewee3, 2014). It also indicates that not all the information should be available for everyone. The system will be a SaaS system with a hybrid cloud. The public part of the cloud can be accessed by everyone to extract the vital information. The private cloud will only be visible for the hospital or collective of hospitals the patient is being treated in. Thus, the servers will be in hospitals and in a central location in the Netherlands.

3. The third system will be a community cloud in which every hospital in the Netherlands can run their own EPD system in (Interviewee3, 2014). This healthcare community can all access the same cloud, but using their own respective systems (Marinos & Briscoe, 2009). This will be done on the level of PaaS. Every hospital must ensure that critical information must be accessible by linking their EPD system with a nationwide “slim” version of the EPD with vital information. Thus, every hospital is storing their information in the same cloud which is located in a central location in the Netherlands. This creates a private cloud on the matter of access as only people from one community can access the cloud, based on a membership model (Marinos & Briscoe, 2009).
6. List of requirements

6.1 Requirements Theory

To implement the EPD cloud computing system, a number of items are needed. These requirements need to be met in order to have a successful implementation in the healthcare sector. The requirements are derived from the literature and from interviews. These two different lists are compared and combined, and one total list is formed. The list indicates the needs for the system, as seen by the researchers and the doctors. For the list, a number of nine articles were used and five experts gave their list with requirements. Later on, the list is validated by the doctors on the importance of the medical factors - the importance of the technical factors is derived from the literature.

The criteria for the selection of the articles are the following:

- Connection with the requirements of the EPD.
- High number of citations or including statements by Dutch law.
- Connection with elements of the EPD, e.g. security, finance, privacy or issues.

<table>
<thead>
<tr>
<th>Number of Article</th>
<th>Name of article</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Article 272, Dutch law</td>
<td>Dutch Government (2003)</td>
</tr>
<tr>
<td>2</td>
<td>A CROSS-COUNTRY STUDY OF CLOUD COMPUTING POLICY AND REGULATION IN HEALTHCARE</td>
<td>Currie &amp; Seddon (2014)</td>
</tr>
<tr>
<td>3</td>
<td>User requirements for cloud computing architecture</td>
<td>Roger (2010)</td>
</tr>
<tr>
<td>4</td>
<td>Cloud Computing - Issues, Research and Implementations</td>
<td>Vouk (2008)</td>
</tr>
<tr>
<td>5</td>
<td>Richtlijn Goed Beheerde Zorgsystemen</td>
<td>NICTIC (2005)</td>
</tr>
<tr>
<td>6</td>
<td>Addressing cloud computing security issues</td>
<td>Zissis &amp; Lekkas (2012)</td>
</tr>
<tr>
<td>7</td>
<td>Business models for an open Personal Health Record platform</td>
<td>Bellil (2014)</td>
</tr>
</tbody>
</table>

Table 4 Articles selected for Requirements
The set-up of this requirement list is derived from the work of Hull et al. (2005). Here, it is described that the starting point is the needs of the stakeholder and from this, the requirements of the systems are made (see figure 12). These steps are combined as stated above. To find the stakeholder requirements the interviews are held, to find the system requirements the literature is reviewed. The final result will be the system requirements which are needed to develop the system (Hull et al, 2005).

Functional and non-functional requirements shall be given. Both will be in the final list. Through the use of literature and experts, most of the spectrum of requirements can be covered. This spectrum of requirements is mentioned by Sommerville (2011). The entire spectrum is shown in figure 13. For time matters and to cover as much of the spectrum as possible, it is chosen to just use the experts and the literate (this part is used to cover the system requirements). Every requirement that is listed must have the ability to be tested (Sommerville, 2011).

The list will be validated via medical personnel and the list of NICTIZ. This list shows a number of requirements an EPD system must have. The NICTIZ ensures that the medical sector acts in line with the “Correct Management of Healthcare Data” guidelines. (Goed beheerde zorgsystemen; GBZ’en) (NICTIZ, 2005). This is an agreement on how to handle e-communication in the healthcare sector. All medical personnel and all hospitals need to act in line with this agreement. Therefore, this agreement is an important tool to validate the information found in the literature and interviews.

### 6.2 The List of Requirements

Below, the list of requirements is given in table 5. The column ‘number’ indicates the number and thus the total amount of requirements. The ‘Demanding group’ shows who named the quality: H stands for Healthcare (and are extracted from the interviews) and T stand for Technical (and are extracted from the literature). ‘Requirements’ shows the actual requirements. ‘Description’ gives a short description of the requirement. ‘Importance’ shows the importance of the requirement by level. This importance level is collected during the interviews, where at the end of the interview the person ranked the entire list on importance. The average importance level of all the interviews is set to be the importance level in this final requirements list. The possible levels are high, medium and low. High indicates that that requirement is needed and without this requirement, the product will fail. Medium indicates the requirement is of importance but the product might still work if the requirement is not executed perfectly. Low indicates that the requirement would give satisfaction to have but it is not necessary for the implementation of the product. The list was verified by interviewee 5.

<table>
<thead>
<tr>
<th>Number</th>
<th>Demanding group</th>
<th>Requirement</th>
<th>Description</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>H</td>
<td>24/7 access</td>
<td>The system should be accessible 24 hours a day (a 99.4 availability percentage. Maximum of 1 malfunction a month must be solved within 15 minutes, maximum of 2 “big” malfunctions per year which need to be</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>H + T</td>
<td>Access logbook</td>
<td>A logbook must be kept, which cannot be altered, to see who has accessed the information of a patient (Interviewee3, 2014)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>H + T</td>
<td>Password protected</td>
<td>The system must only be accessible with a personal password (Interviewee3, 2014) (Interviewee1, 2014)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>H + T</td>
<td>Clusters of information</td>
<td>The EPD system must be accessible from every health provider in a certain cluster (Interviewee3, 2014)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>H</td>
<td>Ability to block certain people or parties</td>
<td>Patients and doctors must be able to block others from seeing the medical file of a certain patient (Interviewee3, 2014)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>T</td>
<td>Encryption</td>
<td>All the data transfers must be encrypted (Zissis &amp; Lekkas, 2012) (Interviewee1, 2014)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>T</td>
<td>Public Key Infrastructure</td>
<td>PKI must be used to transfer the data (Interviewee1, 2014) (Zissis &amp; Lekkas, 2012)</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>H + T</td>
<td>Monitoring</td>
<td>It must be possible to monitor access to files, to see typical and non-typical behaviour (Interviewee1, 2014)</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>T</td>
<td>Certificates</td>
<td>Certificates must be used to secure the cloud (Interviewee1, 2014) (Gollmann, 2010)</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>T</td>
<td>Authentication</td>
<td>The identity of the person asking for access must be checked to see if this person has the right to access the file (Interviewee1, 2014) (Zissis &amp; Lekkas, 2012)</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>H + T</td>
<td>Back-up</td>
<td>Back-ups of the information must be made (Interviewee2, 2014) (Roger, 2010)</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>T</td>
<td>Servers multiple Locations</td>
<td>The back-up servers must be in different locations to ensure information availability is case of crisis (Interviewee1, 2014) (Roger, 2010)</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>H</td>
<td>Access on every location</td>
<td>The necessary information can be accessed from every location via the application (Interviewee4, 2015) (Currie &amp; Seddon, 2014)</td>
<td></td>
</tr>
</tbody>
</table>
### Implementation of the Electronic Patient Record

**Jelle-Eric de Vries**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Importance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>H</td>
<td>Information input size</td>
</tr>
<tr>
<td>15</td>
<td>H</td>
<td>Application must be easy to use</td>
</tr>
<tr>
<td>16</td>
<td>H</td>
<td>Data for medical research</td>
</tr>
<tr>
<td>17</td>
<td>T</td>
<td>Scalability of the application</td>
</tr>
<tr>
<td>18</td>
<td>T</td>
<td>Integrity</td>
</tr>
<tr>
<td>19</td>
<td>H</td>
<td>Support service</td>
</tr>
<tr>
<td>20</td>
<td>T</td>
<td>Fast response when information is asked from the application</td>
</tr>
<tr>
<td>21</td>
<td>T</td>
<td>Know where data is stored</td>
</tr>
<tr>
<td>22</td>
<td>H</td>
<td>Save additional information</td>
</tr>
<tr>
<td>23</td>
<td>H</td>
<td>Communication</td>
</tr>
</tbody>
</table>

Table 5 Requirements for the EPD system.

### 6.3 Review of the requirements

The requirements named above show the division of importance between the technical side and the social side of the EPD. From both groups, a number of requirements are listed, which will result, according to them, in a successful introduction of the EPD cloud computing system. Some of the requirements are seen by both groups.
A number of the requirements are needs and desires from the social side (e.g. support centre), others are technical needs (e.g. authentication) and some are even based on guidelines and laws stated by either the European Union or the Kingdom of the Netherlands (e.g. 24/7 access guidelines).

Both see security as a main factor in the requirements. Where the non-technical group in the interviews name this as a total requirement, the literature names certain aspects. On the list, a number of the security aspects are named which are in the end named by both (when asking the interviewees to specify what they mean by “security”). To compare these findings with the options given in section 5, it shows that all the systems are still possible to be used, based on the requirements which are given by the literature and the interviews.
7. Preferences of the Dutch citizens

7.1 The Questionnaire

The questionnaire that was conducted shows a basis of what the Dutch citizens prefer and what they want. The questionnaire is not a fully equipped research questionnaire. This is due to the fact that not the total number of 385 people filled in the questionnaire. Therefore, any conclusions drawn from the outcomes of the questionnaire cannot be generalised over the entire Dutch population. The total number of people who started filling in the questionnaire is 92 respondents and 83 finished the questionnaire. The questionnaire has been spread via the internet by use of the website thesistools.com. This was done via Facebook and email. The network of acquaintances was used to spread the questionnaire. The questionnaire was available for a month from half December 2014 until half January 2015. The respondents were 66,3% female and 33,7% male. The respondents were spread over the age groups with the largest amount in the groups 18-24 and 45-55. 44,57% of the respondents have a university degree. These results show that the questionnaire has a respondent group that does not reflect the Dutch population. This questionnaire is used to gain insight in the perception of the people but is not used as main source of information for the thesis. Thus it is noted that the group is not representative.

The extent of this problem can be discussed on the basis of other questionnaires. The questionnaire for this research is based on a number of other questionnaires. The results of these can be compared to the questionnaires of van Thiel (2009) and Masman (2012). A number of questions from the questionnaire are, when compared, generalizable. The questions about participation (5), knowledge of the EPD (2, 3 and 4), privacy danger (9) and the need for the EPD (12) have similar results in the questionnaire of Masman (2012) and van Thiel (2009). While these questionnaires were conducted three and six years ago respectively, the results show that the outcome of the questions remains steady. Except for the knowledge question: a steady increase in knowledge is shown between the 2009 questionnaire, the results from the one in 2012 and this thesis’ questionnaire. From these results it can be concluded that the questions about participation, knowledge and need in the questionnaire are generalizable. The questions about cost (10) and implementation speed (11) are in that sense not generalizable. There are no comparable answers for these questions. Thus they cannot be generalized with the help of other questionnaires. For these questions, no statements can be made for the entire population, they will be assumptions with no statistical grounds. The question about accessibility (8) and whom is able to access the EPD (6 and 7) are based on questions in other questionnaires as well. However, the accessibility question was asked in such a manner that it does not correspond to any question answered in other questionnaires. In this extent, the question is not generalizable, but the statements made in that question by the respondents are. Masman (2012) and van Thiel (2009) show similar statements made in their sections about the information needs. The statements show the same need for more information. The question about whom should access the EPD, is asked in the questionnaire of Masman (2012) but the results from both questionnaires differ extensively. Thus this question cannot be generalized over the entire population of the Netherlands.

Below an overview is given of the main results of the questionnaire. A number of statements are made by the respondents about the EPD which are helpful to create the framework, these are given here as well. For a complete overview of the results, see “Appendix VIII Results Questionnaire”.
7.2 Preferences Results

While only half of the respondents know what the abbreviation ‘EPD’ stands for (53.33%), the majority knows what the goal of the EPD is (93.18%). Although most of the respondents know what the EPD is, a large part does not know if they participate (i.e. if their data is stored in the EPD) in the EPD (21.59%). 23.86% are participating in the EPD and 36.36% would like to participate. 17.05% do not participate and 1.14% actively rejected to participate in the EPD. An example of a reason for rejecting to participate is given by respondent 19: “I find that the privacy of information cannot be guaranteed”.

When looking at who the respondents think have access rights and who should have access rights to the EPD, the answers show that 15.12% think that the Dutch government have access rights to the EPD whereas only 4.88% thinks that the Dutch government should have these rights. 100% of the respondents say that general practitioners should have access to the EPD and 97.56% want specialized doctors to have access too. Only a few people think employers have the rights and should have the rights (2.44%). An alternative answer, provided by respondent 44, is that “only on request” access to the EPD should be granted.

The spread in where people want the EPD to be accessed from is large. A difference is made between “Accessible from every location from every device”, “Only be accessible from medical locations from all devices” and “Only be accessible from pc inside medical locations”. The respondents are spread over these three possibilities. The largest group (37.65%) only wants access from medical locations from pc, 30.59% wants access from all devices in medical locations and 23.53% from every location from every device. That the largest group (37.65%) only want access from pc leads to a problem, as interviewee 3 states that it would be practical to be able to access the EPD from tablet or smartphone. Reasons given by respondents who are in the largest group all come from privacy issues and the security of their information. They range from “security” (respondent 3) to “I suppose that computers in medical locations are secure” (respondent 82) and “Less chances of fraud” (respondent 78). For the second largest group, respondents mostly see the usefulness as a main reason. Responses say that “because only there it is useful. And then it can be best protected” (respondent 77), “otherwise too limited” (respondent 42) and “least chance of misuse, but accessible in case of emergency” (respondent 37). For the group who choose every location from every device the reasons where spread among the following: “something can happen everywhere, so EPD should be accessible from everywhere” (respondent 8), “in an emergency, information may be needed before arriving at hospital” (respondent 46) and “A doctor should be able to access the EPD from my home” (respondent 62).

While the responds to the question if privacy will be in danger is around 50% yes and 50% no, people do see the need for the EPD with 83.13% who state that the EPD is needed. They do want a perfect system, as 72.62% is willing to wait and postpone the implementation until the system is perfect.

7.3 Review of the Preferences

One of the most important points the respondents give is that they see the need for the EPD. With 83.13% of all respondents stating that the EPD is needed it becomes clear that when implementing the system, there will be an acceptance. They also clearly state that they want a secure system and different opinions are given on what form of EPD it should be.
A trend can be seen in this questionnaire. There is a group of respondents who are completely against the EPD. These people clearly stated that whatever form of the EPD is introduced, they will be against it. They state that their private medical information needs to stay private. The health benefit is not seen and sharing the information is not worth the risk of their information getting in the wrong hands. Another group show that they can be persuaded into accepting the EPD, but the system needs to be bulletproof. When there are small issues with the system, they will not trust the system and thus not see the EPD as being beneficial. This group indicated that the system is only beneficial if rightly implemented. The last group see all the benefits of the EPD and want the system as soon as possible. They state that the system is needed and will be beneficial to the healthcare sector. In which form the EPD should be introduced differs from respondent to respondent.

To keep the EPD secure, some respondents propose a closed system only to be accessed in hospital, but accessible from outside of hospital in emergencies. Some only want personal computers with the EPD and others see the need for portable access devices. Within every one of the groups mentioned above, respondents differ in what the EPD should look like. The only general opinion that they share is that the system must be safe and private data must be protected. In general it becomes clear the respondents know what the EPD is and have a certain degree of willingness towards the EPD. They need to see that the system is safe and secure before they are able to accept the system. While the respondents know what the EPD is, it shows that they do not have a full understanding of what the system does and how it is designed.

7.4 Towards the framework

The acceptance of the citizens is of critical importance for the success of the EPD cloud computing system. While most people see the need for the system, the acceptance level is still low as only a small percentage (13% (Schellevis, 2014)) of the Dutch citizens have given their consent to the system. The system needs to be a success from the start of the implementation. The questionnaire has indicated two possible options that might be included in the framework, to create this success.

The first option is that more information is to be provided about the EPD to citizens and doctors. This is, as stated above, a generalizable result, as the questionnaires of Masman (2012) and van Thiel (2009) reach the same results. This will result in a better understanding of the system and therefore lead to a higher acceptance level. This means that information needs to be provided to every citizen of the Netherlands that needs to give his or her consent for creating a medical patient file and storing their patient data.

The second option the questionnaire shows is that the locus of control is important to the patients. Their trust level will be lower when they cannot influence their own medical file. This is shown in the question about who should access the EPD. The results of this question are not generalizable as they did not match any other results, but they are similar outcomes of questionnaires where the results of who should have access and who have access differ in the opinion of the responder. As the questionnaire of Masman (2012) shows a difference between the two questions, it can be concluded that to this extent the question is generalizable. The general consensus is that patients should be able to exercise control over their own file. When they are able to exercise this control the locus of control will increase which will result in a higher trust level. This trust level is needed to create acceptance for the system.
8. Cost Structure

8.1 Cost Structure Definition
The cost structure is part of the Business Model Canvas (Osterwalder A., 2010). These nine building blocks form, according to Osterwalder (2010), the building blocks for a business case. The cost structure is the building block responsible for the overall cost set-up (Osterwalder A., 2010). Chesbrough (2010) also states that defining the cost structure is essential for the creation of a business plan. Chesbrough (2010) shows the same structure as Osterwalder (2010) for the creation of a business model (Chesbrough, 2010).

Cost structure is defined as: which costs are essential to let the business model function (Essential, 2010). While the BusinessDictionary defines the cost structure as “a method to determine how much it will cost a company to manufacture a product” (BusinessDictionary, 2014). Chesbrough (2010) and Osterwalder (2010) have similar definitions and state that the cost structure shows the most important costs inherent in the business model (Osterwalder A., 2010).

Cost structure consists of both variable and fixed costs (Osterwalder & Pigneur, 2010). With this it will show all the possible costs that a business model may have when being implemented or later on when the implementation was successful.

Therefore, the last definition of Osterwalder & Pigneur (2010) will be used in the document as definition for the cost structure. Below, in line with the definition, the most important elements of the EPD cloud computing system are listed in table 6. The table is compiled of 3 interviews and 6 articles. The following articles where used:

<table>
<thead>
<tr>
<th>Number of Article</th>
<th>Name of article</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Business models for an open Personal Health Record platform</td>
<td>Bellil (2014)</td>
</tr>
<tr>
<td>3</td>
<td>The cost of doing science on the cloud: the montage example</td>
<td>(Deelman et al, 2008)</td>
</tr>
</tbody>
</table>

Table 6 Articles selected for Cost Structure

8.2 Cost Structure List
The list of the cost structure is compiled from literature and interviews. The two lists are compared and combined into one complete cost structure list. Below the list is given. The column “number” indicates the number and thus the total amount of cost items. The “Demanding group” shows who named the cost item: I stands for Interviews (and are named by interviewees, both working in the healthcare and IT sectors) and T stands for Technical (and are extracted from the literature). “Cost Item” shows the actual cost item. “Description” gives a short description of the cost item.
“Importance” shows the importance of the cost item by level. The levels are high, medium and low. ‘High’ indicates that this cost item is needed and without this cost item the product will fail, ‘medium’ indicates the cost item is of importance, but the product might still work if this item is scraped to reduce costs and ‘low’ indicates that the cost item would give satisfaction to have but is not necessary for the implementation of the product.

<table>
<thead>
<tr>
<th>Number</th>
<th>Demanding group</th>
<th>Cost item</th>
<th>Description</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>T + I</td>
<td>Monitoring system</td>
<td>A system to monitor typical and atypical behaviour to increase security (Interviewee3, 2014) (Gollmann, 2010) (Bellil, 2014)</td>
<td>high</td>
</tr>
<tr>
<td>2</td>
<td>T</td>
<td>Maintenance</td>
<td>A cost post to cover the medium maintenance of the entire system (Bellil, 2014)</td>
<td>medium</td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>Hardware</td>
<td>The physical aspect, such as the servers and computer, cables etc. (Armbrust, et al., 2010)</td>
<td>high</td>
</tr>
<tr>
<td>4</td>
<td>T</td>
<td>Infrastructure</td>
<td>The software to link the different systems together (Armbrust, et al., 2010) (Bellil, 2014) (Sultan, 2010)(Deelman et al, 2008)</td>
<td>high</td>
</tr>
<tr>
<td>5</td>
<td>T + I</td>
<td>Support</td>
<td>A system to aid the users (Interviewee3, 2014) (Bellil, 2014)</td>
<td>medium</td>
</tr>
<tr>
<td>6</td>
<td>T</td>
<td>Electricity</td>
<td>To power the system (Sultan, 2010) (Armbrust, et al., 2010)</td>
<td>high</td>
</tr>
<tr>
<td>7</td>
<td>T</td>
<td>Software</td>
<td>The software system that create the cloud for the EPD (Deelman et al, 2008) (Armbrust, et al., 2010)</td>
<td>High</td>
</tr>
<tr>
<td>8</td>
<td>T</td>
<td>Materials</td>
<td>Any other materials needed next to the hardware (Bellil, 2014) (Armbrust, et al., 2010)</td>
<td>medium</td>
</tr>
<tr>
<td>9</td>
<td>T</td>
<td>Network bandwidth</td>
<td>To ensure that large quantities of the data can be access at the same time (Creeger, 2009)</td>
<td>high</td>
</tr>
<tr>
<td>10</td>
<td>T + I</td>
<td>Storage location</td>
<td>A location of place the servers (Interviewee1, 2014) (Armbrust, et al., 2010) (Gollmann, 2010)</td>
<td>high</td>
</tr>
<tr>
<td>11</td>
<td>T + I</td>
<td>Security</td>
<td>The creations of necessary high protections, software and physical to ensure protection of the data (Gollmann, 2010) (Interviewee1, 2014)</td>
<td>high</td>
</tr>
<tr>
<td>12</td>
<td>T + I</td>
<td>Back-up system</td>
<td>A system to ensure 24/7 access and no loss of data (Interviewee1, 2014)</td>
<td>high</td>
</tr>
</tbody>
</table>
The Implementation of the Electronic Patient Record

Jelle-Eric de Vries

2014) (Interviewee2, 2014)
(Creeger, 2009)

<table>
<thead>
<tr>
<th>13</th>
<th>I</th>
<th>Monitoring employees</th>
<th>Employees who control the high monitoring system and act accordingly (Interviewee1, 2014)</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>T + I</td>
<td>Teaching</td>
<td>A master class to help users understand how the EPD works (Interviewee3, 2014) (Bellil, 2014)</td>
</tr>
</tbody>
</table>

Table 7 Cost structure

8.3 Review of Cost Structure

The list above shows that the technical side will enforce a large number of cost items on the overall budget. The main social items on the list are the teaching cost item and the support cost item in order to help every user to understand and use the EPD. Both groups, technical literature and social demand, see the need for the security, back-up and monitoring system and thus see them as cost items.

The cost items that are listed above can roughly be divided into two groups: the fixed and the variable costs. Fixed costs are independent of the output, the variable cost vary with the output (Berk & DeMarzo, 2007). These two groups will need to be listed on the budget for the EPD cloud computing system.

The list shows a number of differences between the literature and the interviews. These differences arise from the social and technical viewpoints. The interviews gave a number of cost items on a more social aspect: support system, monitoring system and privacy issue (listed as security). The literature indicated more parts of the system as cost items: technical components that apply for any EPD system. These technical cost items are still considered of major importance for the cost structure.

The cost items on the list are broad items, they have sub items. For example, ‘security’ is not just one cost item, rather it consists out of a large number of smaller items. In order to create a comprehensive list, the main cost items are named and not the sub items. When creating the EPD, all broad cost items need to be split up so that all sub items are accounted for in creating the total budget.

8.4 Towards the framework

The cost structure is of vital importance to any business case (Osterwalder & Pigneur, 2010). The questionnaire indicated that a sound cost structure will help raise the acceptance level. The literature also indicates the importance of a sound cost structure for a business case. When the framework is created, every aspect of the cost structure in table 7 needs to be realized in the budget.

When every cost item is displayed in the framework, the cost structure will be overly represented in the framework. Thus a different set-up is chosen to create a clear cost step in the framework. In order to create the framework, the cost aspect needs to be well defined in one single step. In order not to put the entire cost structure in the framework two groups will be created: the fixed and the variable costs. This division will create a clear overview for the framework. Table 7 is split up in the two different groups in the following manner:
The fixed cost group will consist of: storage location, security, back-up system, monitoring system, hardware, software, support, maintenance, monitoring employees and network bandwidth.

The variable cost group consists of: materials, infrastructure, electricity and teaching.

These two groups represent the entire cost spectrum for the business case. When creating the business case the same division will be made on the budget between the fixed cost and the variable cost. The step is made to create a clear overview and it shows which items are part of the fixed cost and will needed to be paid on regular basis and which costs vary on the use of the system. For example, when the use of the system increases, more entry points need to be made which will create a non-recurring cost, while the cost for the security and the monitoring employees will stay the same.

As stated before, the implementation and the use of the EPD will not generate revenue. It is stated in the literature that a cost saving will occur (Yoon et al, 2012). This area is not researched extensively, but a number of researchers have attempted to research the cost saving. Van Luxemburg et al (2009) describe a 10% decrease in cost after implementing a local EPD system in a hospital in Nieuwegein, the Netherlands. Cannaby et al (2004) state that it is possible to reach a cost reduction of 25% with the introduction of electronic referrals. In the United States, a cost saving between $142 and $371 billion can be made when introducing an EPD system (Hilestad et al, 2005). Uslu and Stausberg (2008) stated that there is considerable evidence for a reduction of costs by the use of an EPD.

There are no numbers found that indicate what the total cost savings for a nationwide EPD system in the Netherlands would be. The 305 million that was spent to create a nationwide EPD has been put into a project that was stopped. A future EPD system might be able to use parts of the work that has been done, thus lowering the cost. The total amount of cost savings is hard to determine (van Twist et al, 2012). News articles stated that a big cost reduction might occur when more ICT applications are used in the healthcare sector (ANP, 2013). Most of these saving estimations are based on future projections or small scale EPD systems. Thus it can be concluded that the research community agrees that a cost saving will occur when implementing an EPD system. The height of this cost reduction is yet to be determined.
**Phase IV Framework**

Phase IV will show the final framework which will be made to answer the research question. Conclusions will be drawn from the framework, followed by directions for further research. Phase IV is based on phase II and phase III.

9. Framework

9.1 Theoretical Basis

The stated research question (section 3) aims to develop a framework which will lead to the successful implementation of a cloud computing EPD system. This will create a business case for the introduction of the EPD with a cloud computing system. Throughout the research it has become clear that a number of factors are of great importance.

As stated in the introduction, the social part and the financial part are of major impact on the outcome of the implementation of the framework. Where Brokdin (2008); Armbrust et al, (2010); Jansen (2011) and Chen and Zhao (2012) stated that the privacy factor is of major importance with the creation of a cloud computing system, Osterwalder (2010); Chesbrough (2010) and Tripathi & Mishra (2011) show that the financial overview needs to be perfect to create a valuable product.

The four pillars are deemed important to ensure a successful framework and introduction of the EPD cloud computing system: the product, the market, the costs and the timing are the corner stones of a business case (Langerak, 2012) (Onarheim & Christensen, 2012)(Van Oorschot et al, 2010).

As basis for the framework the framework of Osterwalder (2010) will be used. The business model canvas (see figure 15) is recognized by a number of different researchers as a valid tool for the creation of a business case (Chesbrough, 2010) (Blank, 2013) (Trimi & Berbegal-Mirabent, 2012). As this framework is in line with the four pillar framework, both cover the same aspects within different models. The four pillar framework will be used as the basis for the business case framework for the implementation of the EPD cloud computing system.

The set-up for the framework is found in the outcome models. These models are used to spell out every “detail about how it is believed a program or intervention will lead to improvements in higher-level outcomes” (Duigman, 2009). Duigman (2009) states that the model should represent all the high level intended outcomes and lower-level steps. One of the different outcome models is the Logic Model (Penna & Phillips, 2005). “Logic models, the most widely used of these models, provide a graphic overview of a program, outlining the outcomes to be accomplished along with how they are to be achieved and for what groups.” (Penna & Phillips, 2005). According to them, Logic Models
include target groups, the resources to be used, activities and objectives. Others find that the elements of the Logic Model are resources, activities, outputs, customers reached, short, intermediate and longer term outcomes, and the relevant external influences. (McLaughlin & Jordan, 1999).

In order to create a framework based on the Business Model Canvas and the four pillars the theory of the Logic Model will be used. This will be done to create a model that will present a plausible and sensible model of how the program will work under certain conditions to solve identified problems (McLaughlin & Jordan, 1999).

Figure 16 Elements of a Logic Model (McLaughlin & Jordan, 1999)

To create the framework as a Logic Model, all the different elements, displayed in figure 16, need to be known. The research thus far has shown these different elements. Below, in table 8, these elements are presented. The different elements are selected on the basis of the following criteria:

- Labelled important in phase II or phase III
- Stressed in the interviews
- Concluded from questionnaire

The input for the framework will be the four pillar model. This is the starting point of the research and thus serves as the starting point for the framework. This table will give the activities, output, outcomes and impact found in the research to generate the desired impact of a successful implementation of an EPD cloud computing system. The elements are explained in Appendix XII to clarify what is meant by them. Below, the link between the elements and the categories is explained.

<table>
<thead>
<tr>
<th>Element</th>
<th>Activities</th>
<th>Output</th>
<th>Outcome</th>
<th>Impact</th>
<th>Derived from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful implementation</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Research goal</td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Literature Overview, requirements, Preferences of Dutch citizens</td>
</tr>
<tr>
<td>Trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Literature Overview, requirements, Preferences of Dutch citizens</td>
</tr>
<tr>
<td>Fulfilling Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Literature Overview, List of Requirements,</td>
</tr>
<tr>
<td>Non-physical System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Literature Overview, List of Requirements, Cost Structure</td>
</tr>
</tbody>
</table>

39
The research question is aimed at creating a sustainable EPD cloud computing business case. In order to reach this aim, the output of the framework should be a sustainable EPD cloud computing system. Thus the impact the framework needs to have is a ‘Successful implementation’. What is meant here by ‘successful’ is that the EPD system satisfies the patients (when a vast majority (95%) of the population of the Netherlands give their consent to store their data in the EPD cloud computing system), lowers the cost and leads to higher efficiency of healthcare. ‘Doctors’ agreement with the system’ and ‘citizen’s agreement with the system’ are set as outcomes of the framework. This research has shown that these two groups are the groups that need to be convinced to use the system. The questionnaire and interviews have shown that these two elements are vital for the success of the system. Thus acceptance of doctors and patients are considered the two outcomes to be reached.

To reach these outcomes a number of outputs need to be created. These are: ‘Trust’, ‘Accessibility’, ‘Ease of Use’, ‘Privacy’ and ‘Financially Sound’. The interviews have shown that the accessibility and ease of use are critical to the acceptance of the doctors. Trust and privacy are combined into ‘trust in the system’. This is done to create one general output for two elements aimed at the same goal. Privacy demonstrates the obstacle of sharing medical data, patient need to have enough trust in the system to give consent to use their medical data in the system. Therefore both elements are included in the ‘Trust in the system’ element. The trust has proven to be a fundamental step, by the research, in creating acceptance. The questionnaire and literature research have shown that the element ‘financially sound’ gives a broader acceptance base, as this better justifies the money that was spent.

To come to the outputs a number of activities have been identified. ‘Security’, ‘Own Control’, ‘Fulfilling Requirements’, ‘Trust Campaign’ and ‘Financial Budget’ are regarded as the activities to reach the output above. The element Security is divided into ‘physical security’ and ‘non-physical system’. The literature stressed that for every cloud computing system the security needs to be set properly. The literature also indicated subsets of the security which are also listed in the table. The element of fulfilling requirements was identified in the interviews and the literature. This element focusses on the output’s accessibility and ease of use and aims to fulfil all the needs of the doctors.
Own control and trust campaign were both identified in the questionnaire and the interviews. Both aim to increase the trust level. The Financial Budget was identified in the literature review and the questionnaire and focuses on creating a sound financial structure. The two components of the financial budget are also listed in the table.

9.2 The Framework

In addition to the final framework that will be displayed in this section, seven smaller UML diagrams were made. When these diagrams are combined they form the final framework in figure 17. These smaller and simpler diagrams are displayed in appendix XIV. Every outcome, output and impact will be shown on the basis of the ULM diagrams. Below an explanation of the final framework is given.

9.2.1 The Framework Model

In figure 17 the final framework is shown. A Logic Model requires an input: the input for this framework will be the information collected from the four pillars: Product, Timing, Market and Cost. The information collected in these four categories will be used in the activities. The activities are the steps that need to be taken to reach the necessary outputs. The outputs are targets that need to be reached to set the standard of the EPD. These standards will lead to the outcomes which are of crucial importance to the goal of the framework. The outcomes are considered the two groups that need convincing to use the EPD. Thus these two outcomes guide the framework towards the final goal: a successful implementation of a nationwide EPD system. Below, every step of the framework will be explained. This explanation will be done with the help of the elements of table 8. The arrows between the different elements in the framework indicate the effect between the elements. The effect can be by information input (e.g. knowledge about the needed requirements) or by affecting a feature of the EPD cloud computing system (e.g. the system accessibility due to the security implications). Every arrow is explained in more detail in appendix XV.

The activity ‘Fulfilling the Needs’ is executed with the input from the product pillar and the market pillar. Within this activity, all the needs of the doctors and the citizens are compared to the input from the product pillar to see which of the needs are fulfilled, and what can be done to fulfil the missing needs. This will result in a list of needs that are fulfilled and this will be the input going towards the ‘outcomes’. The list of needs that are fulfilled, should at least contain the requirements that are identified in the literature as important requirements for an EPD, as discussed in section 6.2 ‘List of Requirements’.

The ‘Creation of the Non-physical System’ activity deals with every aspect of the non-physical system. The input from the Four Pillars will help with the decisions for the creation of the non-physical system. The minimum creation decision in this step, as identified in the literature, is listed in section 4.3.2 ‘Cloud Computing Systems’ as well as in section 6.2 ‘List of Requirements’. A number of non-physical security aspects that need to be fulfilled can be found in appendix VI and VII. The input from the four pillars is influenced by the needs that are selected in the ‘Fulfilling the Needs’ activities. If the needs state that the system should be accessible with just entering a password once, the system set-up must be matched accordingly. The output of the activity should be a clear set-up of the non-physical system of the EPD.

This output of ‘Creation of the Non-physical System’ can be used in the ‘Creation of Physical Security’ activity. This separate step determines, based on its input, which physical security steps must be taken to protect the medical data. Every physical security aspect must be considered in this activity.
The section 6.2 ‘List of Requirements’ also states a number of physical security items that at least need to be fulfilled in order to create an EPD system. Within section 4.3.1 ‘General Cloud computing’, a number of physical security items are named that need to be fulfilled, these items can also be found in appendix VI and VII. A number of examples of decisions that need to be made to create the EPD system are: the protection of the servers: is there one location for the servers or does every hospital have servers that need to be protected? Where will the back-up system be located? The output of this activity should be a complete physical security system for the complete non-physical system.

‘Creation of Trust campaign’ aims at creating a campaign that can convince the Dutch citizens to trust the system. This campaign needs to show what is done to secure the medical information, thus the input from the physical security, which also includes the information of the non-physical system. The trust campaign should not only aim at convincing the Dutch, but also at providing information about the EPD system in order for the citizens to make an educated decision about participating in the EPD or not. Thus the campaign should be informative as well as convincing. The campaign should be held on every medium possible, to reach as many citizens as possible. The input from the Four Pillars will show the trust level of the citizens. This information can be used to see if the campaign had any effect. To check this effect, a questionnaire could be used.

The literature showed that a sound financial structure improves the agree-ness level of the citizens. Thus the activity ‘Managing of cost’ is implemented to create a sound financial budget. In this activity, every cost item needs to be placed in the budget to create a cost overview. The input will be the set-up of the system and the Four Pillars, which will provide information about the cost of every item. In section 8.2 ‘Cost Structure List’, the elements are listed that should at least be in the financial overview. The physical security can also influence the cost. No direct link has been made in the framework, because the non-physical system leads to which physical security steps are taken. Also, the information from the Four Pillars can show the cost of physical security. The output of this activity should be a sound budget.

The last activity is the ‘Creation of own control’. The goal of this activity is to establish a locus of control level that matches the needs of the citizens. The input from the market will be the need for own control, this will be influenced by how the non-physical set-up is created. With these two inputs the amount of own control can be establish and created. An example of own control is that a patient is able to block a certain doctor from seeing (part) of their medical data. The output of this step should be a level of own control that can be reached within the proposed EPD system.

The activities above all lead towards four different outputs: ‘Accessibility’, ‘Ease of Use’, ‘Trust in the system’ and ‘Financially sound’. The inputs for these four elements are the outcomes of the activities. The activities will deliver a system that will go through these outputs. Every output needs to be fulfilled to increase the chance of success for the system. For example, the extent to which the needs are fulfilled will create a certain level of accessibility. This level needs to be high in order for the doctors to agree with the system. To understand if the level is high enough a test run with the product must made. When the four outputs are to a satisfactory level, they will result in two outcomes. When, indeed, the level is satisfactory, the doctors and the citizens will agree with the system. When one of the outputs is not satisfactory, one or both groups might not agree with the system. This will have a negative effect on the implementation success.
When both groups, doctors and citizens, agree with the system, then the final impact is reached: a successful implementation of the EPD system. When this is the case, the EPD system can be put in construction. When one of the groups is not in agreement with the proposed system, another set-up must be made. This will result in putting an altered or new product through the framework.

9.2.2 Framework Example
This section will provide a short example for the use of the framework. The will be done with the help of the Epic EPD system (EPIC, 2014). EPIC provides software for hospitals to create an EPD system. This American EPD system is used in a number of Dutch hospitals (Dorresteijn, 2013). Thus doctors have worked with the system and are able to give feedback on the system. Therefore, this EPD system is selected for the example. This EPD system is not linked between the different hospitals. Epic can be seen as a possible set-up for the nationwide EPD system with the help of cloud computing. Thus, the Epic system will be implemented in the product pillar as an input to see if this is indeed a possible system. The EPD system will go to the activity ‘fulfilling the needs’, here the system will be checked versus the needs that are the input form the market pillar. For example, doctors will state their needs, and if they have already used the system, their positive and negative points about the system. This information comes from the market pillar. For Epic, interviewee 6 states that the system is hard to understand the first time. However it is added that, when working with the system for a longer period, the system works fine. Thus the fulfilment of the need ‘teaching’ and ‘support’ (requirements section 6) is not high enough. This will affect the outcome ‘ease of use’ in a negative way. This negative affect will influence the agree-ness level of the doctors. Interviewee 6 also states that the system is only accessible on personal computer. This is fine for doctors in a hospital but unpractical for doctors who work outside of the hospital or have to visit patients in their rooms. This accessibility aspect will have a negative effect on the ‘accessibility’ outcome.

The system is also the input for ‘managing the cost’. In this activity every cost aspect of Epic is documented and a sound budget, following every aspect of the ‘Cost Structure List’, is created with help of the Cost pillar. The timing pillar shows in which timeframe it is possible to implement a nationwide Epic system. This will be the input for the ‘Creation of trust campaign’ together with the information from the system set-up to see which steps must be taken to convince the Dutch citizens to use the system. The Epic set-up has the input from the product pillar and checks if it is possible to upscale the system to a nationwide system. This is the ‘Creation of the non-physical system’ activity. From here the system will also be checked for which physical security precautions should be taken, in the ‘Creation of physical security’ (see section 4.3.1, 4.3.2 and Appendix VI and VII), as well as what the level of own control Epic has in the ‘Creation of own control’ activity, which also has the product pillar as input.

This example shows that it might be possible to create a system that the Dutch citizens will accept but in the case of Epic, the doctors might not. Say the citizens are convinced by the sound financial plan and the trust campaign, but the doctors still have the low levels of ‘accessibility and ‘ease of use’. This will result in a lack of support from the doctors and thus Epic will not reach the final impact that is needed and wanted. The framework shows that either a different EPD system must be used or Epic must be adjusted to fit the needs of the doctors. After this adjustment Epic must be put through the framework again to see if it is now suitable to become the nationwide EPD system.
The Implementation of the Electronic Patient Record

Jelle-Eric de Vries

Figure 17 EPD cloud computing Framework
9.2.3 Uniqueness of the Framework

The framework is the product of theoretical findings combined with the input from experts and citizens of the Netherlands. To understand the value of the framework, it is important to know the added value the framework brings to the literature. The added value can be seen when the framework is compared to other similar frameworks. Three frameworks are selected to be compared to the framework in 9.2.1. These frameworks are selected by goal that the framework is trying to reach. This goal is the implementation of an EPD system.

The first framework for the comparison is the old set-up for the creation and implementation of the EPD system. This old framework has not been displayed or published but can be recognised in the actions taken by the Dutch government. The framework can be identified as a straight line framework. The set-up of the old EPD system is based on a market push strategy, where the Dutch government tries to push the EPD system onto the market. With this push they try to force a need and willingness for the system. This research has shown that no input from the doctors and the patients will lead to a dysfunctional system and resistance from the healthcare sector to use the system. The lack of information supplied to the Dutch citizens leads to little understanding for the system. This little understanding has led to distrust in the old EPD system. The framework takes these the elements and combines them. This methodology creates input from the healthcare sector and the citizens’ trust in the EPD system. This difference between the two set-ups is the gap to the success and failure of the implementation of the framework.

The technology acceptance model (TAM) is a model to implement new technology in the market (van Ree, 2009). The model has become one of the most frequently used for predicting acceptance behaviours of information technologies (Ku, 2009). The model aims to give the acceptance of the new technology. The model is used by van Ree (2009) to predict the acceptance of an EPD system. The model is aimed at the healthcare sector and how it will accept the EPD system. Personal aspects, cognitive aspects, organizational aspects and social aspects are taken into account to create an adapted version of the TAM. These social aspects are, according to van Ree (2009), the opinions of the patients. Similar as the framework in 9.2.1 the adapted TAM accounts for trust by looking at personal aspects. These two personal aspects are the ICT-age and the willingness to change to a new system. Via this step the adapted TAM predicts the acceptance level of the doctors. This is different from the needs of the healthcare sector. The adapted TAM differs from the framework in 9.2.1 in a number of ways. The first is that the needs are only half fulfilled within the cognitive aspects of the adapted TAM. Other differences are that the adapted TAM does not account for the security standard or for raising the acceptance level of the public, nor does it look at the financial side of the EPD. The adapted TAM of van Ree (2009) gives a good indication of how an EPD is accepted when implemented and names a number of factors that influence the success of the implementation. However, these factors are too limited to ensure a successful implementation. The model is aimed more at acceptance in the healthcare sector than full acceptance including that of the citizens of the Netherlands.

Mies (2009) describes in his framework the success factors for implementing an EPD system. When all the success factors of Mies (2009) are considered, the EPD system should be successfully implemented. Five main areas surface from the meta-analysis of Mies (2009), these areas can be grouped into three overhead areas: People, Processes and Technique. The framework created from
these overhead areas indicates what should be done in the development phase, implementation phase and to maintain the EPD. As the framework displayed in 9.2.1, the framework of Mies (2009) accounts for the healthcare side of an EPD system. The framework includes, among other elements: support of management, teaching, needs and expectation. The part left out by Mies (2009) is the social side of the implementation of an EPD system. Mies (2009) does not consider the trust of the citizens of the Netherlands as a success factor for the implementation of an EPD system. This will lead to a low acceptance level throughout the Netherlands. In turn this will affect the participation degree of the patients. Without the participation of the citizens the EPD system will not reach a successful implementation.

Comparing the framework to other sectors, like for example the banking sector, cannot be done directly. The framework is designed for the healthcare sector and this sector has different processes than other sectors. For example security of the information is in both sectors, healthcare and banking, extremely important. In both cases no one wants their financial or medical data accessible for everyone. The access time for this information is different. Lives might depend on how quick medical data can be accessed where there is not such a critical access drive with financial data (excluding stock change). Another difference between the sectors is that it is possible to choose a different bank if one does not like their data storing system. One cannot change their EPD system. Therefore the framework proposed is better applicable for government IT programs. An example might be the implementation of a new DigiD system. The framework needs to be adapted to fit this implementation process but the same steps would still apply. The citizens still need to trust the system and need to be convinced the system is safe and financially sound. In this case, not the healthcare sector needs to be convinced to use the system, but governmental organizations need to be convinced to use the system. The needs of the organization still need to be fulfilled to ensure ease of use and accessibility. Thus, with minor adaptation, it would be possible to apply the created framework from 9.2.1 to other government related sectors.

9.3 Validation of the Framework

The framework is validated with the help of five interviewees. This group examined the framework and the text. They gave, each separately, their feedback on the framework and the framework was adjusted accordingly. To adjust the system, multiple interviewees should have indicated that a certain aspect of the framework could be improved. In appendix XIII the interviewees are listed, as are the questions asked, the results, the review of the results and actions taken. The following three main points arose from the feedback given to improve the framework:

- The respondents stated that it was unclear why the link between the four pillars and the ‘needs fulfilment step’ was different from the link between the four pillars and all other activities. In a previous version of the framework, this link separated the other links from the pillars. This link was changed so that all lines split at the same point in the framework.
- The link from the ‘physical security’ to the ‘trust in the system’ was found unnecessary as there is already a step in between: ‘the trust campaign’. The information is delivered via the ‘trust campaign’ to the ‘trust in the system’, therefore this link was removed. The security does not have a double effect on the trust in the system.
- According to the interviewees, the different elements are not clear within the framework (e.g. what are activities and what are outcomes?). Therefore the interviewees stated that it would improve the system when the difference between the different elements was well defined.

The validation process indicated more improvements for the framework than there are listed above. Some of the improvements are a direct result of unclear text. The interviewees did not necessarily have trouble understanding the framework but had trouble understanding the written text. The face-to-face feedback session helped in clarifying the text and increasing the readability.

The changes made to the framework itself were the results of overthinking the framework. The aim is to create an understandable framework (e.g. therefore all the links from the ‘the four pillars’ are joined, to ensure that not a maze of links is created). This means that unnecessary links need to be removed and all the links need to be set in the same manner. When working on a project for months at a time it can happen that one overlooks details because they seem self-evident.

The validation indicated that the framework is still not the “perfect” framework. It showed improvements could be made to create a better framework. The interviewees indicated that the initial start and the framework thus far created was good. It would, in their opinion, lead to a successful implementation of a nationwide EPD system. A probable reason why the interviewees in the validation sessions agree with the framework is that the interviews conducted before creating the framework (with people who also work in the healthcare or IT sector) played an important part in the creation of the framework. This led to a wider acceptation as interviewees in the validation sessions stated that the needs of their sector was covered.

Overall, the validation process gave a number of valuable insights on how to improve the framework. Through this it can be concluded the validation process was conducted properly. It can also be said that the framework made improvements to ensure that the framework reaches its goal. The framework displayed in section 9.2.1 is the final framework. This is the framework that will lead to the successful implementation of the EPD.
10. Conclusion

10.1 Research Question
This section gives answers to the proposed research question and the sub-questions proposed. First the sub-questions will be answer and then the research question will be answered.

10.1.1 Sub-questions
The first question proposed in the sub-questions is about the product section: “Which qualities does the product need to satisfy the customer’s needs?” The answer to this question is shown in section 6.2 ‘List of Requirements’. There the distinction is made between technical qualities and social requirements to satisfy the needs. The main point is that the system needs to be secure and trustworthy in every way, yet this security must not limit the ease of use and the accessibility of the system.

The second question is “Why is it possible to create a nationwide system in other countries, what stops the Netherlands from creating such a system?” A number of countries are working on the creation of an EPD system. A few lessons can be learned from their set-ups, but the main issue why the Netherlands does not have a functioning EPD is that citizens of the Netherlands do not trust the proposed EPD system with their private information. The different systems in other countries are described in section 4 ‘the literature overview’, specifically in 4.1 and 4.2.

From the market section the first question is “What are the opportunities and drawbacks of such a nationwide system, according to the citizen of the Netherlands?” The answer to this sub question can be found throughout the thesis. Section 3, ‘Literature Overview’ gives a number of opportunities, such as a more efficient system, better sharing of knowledge, lower cost and faster access. This section also states drawbacks like loss of privacy. Section 7 ‘Preferences of the Dutch citizens’ and the interviews with experts provided similar opportunities and drawbacks.

The second question is “What can be done to increase the trust of the patients in a Cloud Computing system for the healthcare industry?” The framework proposed in section 9 ‘the Framework’ shows what can be done to increase the trust in the system.

The following question is “What are the legal issues that might arise with storing patient data?” The main laws to be followed are the privacy law of the Netherlands. It must be known where the data of the EPD will be stored at all times. This information can be found in section 4.1 in the ‘Literature overview’.

The last question in this section is “What is the perception, of the patients, of such a system in The Netherlands at this point? What can be done to change this perception if the perception is negative?” This question relates to the question about trust. The Dutch citizens do not have a high trust level in an EPD system. To change their perception, the trust level must be increased. The answer to this question can be found in section 7 ‘Preference of the Dutch citizens’.

In the cost section the first sub question is “Which financial constructs might be used to create a profitable system?” The answer to this sub question is that there is no construct to make the EPD system profitable. The system is made to reduce costs and for the doctors to be able to respond better to situations and help patients.

The next question is “What is the main cost factor for storing patient data with cloud computing?” The answer to this question can be found in the section on ‘Cost structure’, section 8.
The third question: “What is the main revenue stream that can be found with storing patient data with cloud computing?” There are no revenue streams to be found as the system will not generate revenue. The system will lower the costs and thus save money in that way.

The last two sub questions are in the section ‘timing’. The first question is “What are other possible products that might compete with a Cloud Computing system to store patient data? Thus when should the introduction take place?” There are at this point no other nationwide systems. Local EPD systems do exist, but they do not form a threat to the introduction of a nationwide EPD cloud computing system. Therefore it is possible to postpone the introduction until the system is closer to being perfect.

The last sub question is “How urgent must the market introduction be on the basis of need for the system?” The main response to this question is: wait with the introduction until the system is perfect. Faults in the system will lead to a lower level of trust and this will jeopardize the success of the system. The answer to this question was found in the interviews and is also displayed in section 7 ‘Preferences of the Dutch citizens’.

10.1.2 Research question
The research question is stated as:

How can a sustainable business case for storing patient data, with Cloud Computing in the healthcare industry, be created in the Netherlands focusing on the aspects of security and cost efficiency?

The question can be answered with the framework displayed in 9.2. A number of different steps need to be taken in order to create this system. As shown within the framework, the aspect of security needs to be well managed to be able to create the trust that is needed to implement the system. Without this trust factor there will not be a successful implementation of the cloud computing system.

The research has shown that to create a cost efficient EPD system a clear cost structure must be made. The research shows that cost reduction will take place with the EPD cloud computing system in place. The problem with the costs reduced is that they are not only the costs of the system documenting the data. The costs of wrong medicine being prescribed will be reduced as well. The creation of faster response time and less waiting time will lead to even more cost reductions. Not all of these reductions will directly come to light, which is why it is difficult to give a definite number of cost reductions.

Thus it will be possible to create an EPD system, with cloud computing, that will be sustainable and successful when implemented. While it will take a great effort to overcome the barriers, the public will see the necessity of the system. A good preparation and a perfect execution will result in a business case that will be accepted by all layers of the community. Concluding, it is possible to create a sustainable business case for storing patient data, with cloud computing.

10.2 General Concluding Remarks
A number of general concluding remarks can be made from the research conducted.

- The first conclusion that can be drawn from the research is the set-up interviewee 3 described. During the interviews it became clear that a number of interviewees agree with a
more restricted set-up of the system. The only information that would be in a national database would be information that would be vital to the treatment of a patient.

- The system can be secure but there will always be a possibility of the system being attacked or other forms of misuse.
- The main focus should be on the creation of a system that the healthcare sector benefits from and this must be done at a reasonable price. The cost structure must be clear but the system is a long term investment.

Applying the three conclusions to the system when developing it will lead to a successful implementation of the EPD system. The framework is designed with the input of the target users and shaped to create a high acceptance level among doctors and patients. Steps must now be taken from the theoretical framework towards the development of the system. The basic knowledge to shape the information in ‘the four pillars’ is already available. Now the start needs to be made with the activities listed in the framework to move forward in creating a nationwide EPD system with the help of cloud computing.

10.3 Limitations of the research

A number of limitations of the research should be mentioned. The research is made from the standpoint that the Dutch government wants to create a system that is accepted by the Dutch citizens. It is entirely possible for the government to create the system without the acceptance of the general public. While the chances are limited that the government will execute the plan without profound proof of the system working, no guarantees can be given.

The second limitation is the small number of interviews. The amount of interviews on the topic is able to give an overview of the general trend and of the popular opinion. Due to the small number of interviews conducted it will not statistically be possible to generalize answers for all medical and technical experts in the Netherlands. This does not have to be a limitation in the larger sense but because the interviewees do not necessarily have an objective view, this might cause a problem. Privacy is the main topic of the interviews and it is shown that privacy is a touchy subject where interviewees might answer questions based on emotions they feel about the EPD instead of the factual knowledge they possess. The interview questions where made to try and ensure that this will not happen. This did not work out completely and some of the answers might still have a basis more on the emotional side than on the factual side.

Another limitation similar to the second limitation is the small number of respondents in the questionnaire compared to the total population of the Netherlands. There should be 385 respondents to generalize the results from the questionnaire. Only one fourth of this amount was reached and thus this could not be generalized. The hundred respondents do give an overview of the opinion in the Netherlands and this did give helpful insights. The same problem is encountered here as above: the respondents are answering questions about their privacy and answer with emotional statements. Some even show that they are, in principle, against anything that has to do with displaying their private information.

The second part of this limitation can be found in the respondents group. The respondents group is not a perfect match for the average Dutch population. The average education level of the respondents group is higher than the Dutch average and the age groups are not spread the same as
the Dutch population age groups. Therefore, the respondents group is not representative of the Dutch population and thus the result cannot be generalized for the Netherlands.

The fourth limitation is the lack of statistical testing to proof the framework. The framework is theoretically sound but has no statistical grounds. As the framework is validated by an expert is it not possible to say with certainty that the general public will allow this set-up and that the framework will reach the intended end result. Therefore the theoretical ground has been covered and results are promising but the added value to the field might seem to have less of an impact.

The last limitation is that the study focuses on the internal forces within the market. The study disregards any external forces (e.g. EU regulations) that might influence the implementation of an EPD cloud computing system. These external factors could make or break the implementation success. To focus the study they were not researched in the study.

10.4 Directions for further research

The main finding of the research is the trust factor. Without this, the research shows that the implementation will not succeed. The research has proven on a theoretical basis that the framework will work. The factors that are listed below are directions for further research, where research could be done to improve the framework or give a better chance of successful implementation.

One of these directions would be to gather more statistical proof. This would be done by enlarging the questionnaire respondent group and the interview group. This will have as result that it will be possible to generalize their input into the framework on a bigger scale.

Another direction would be to test the framework on the general public. The framework is a theoretical set-up where the public had little influence on. It would be good for further research to test the framework with the citizens of the Netherlands to proof its successfulness.

For further research, the possible outside effects on the development of the framework should be considered. Within this research only the effects within the playing field are taken into account. It would be wise to further develop any external effect that might influence the implementation of the EPD cloud computing system. This should be done to ensure a successful implementation of the system.
10.5 Personal Reflection

Every time you start with something new, it is a challenge to understand everything. When I started with my master thesis in the ‘information system’ group I had little knowledge about cloud computing or any other information system that exists. From the start on it was a challenge to learn every new aspect, every new term and every new system. With no prior knowledge this did not always go as smooth as I intended. The term ‘cloud computing’ is used wildly nowadays. You hear the term on the radio, see it in television commercials and on website banners. Many companies promote their services in cloud computing. I had heard the term and had a basic understanding of what cloud computing might be. It turned out to be a complex system full of highly technical elements. It took a while before I understood all the material at hand. The second step was to use my new knowledge and conduct the interviews and create the framework. While going through these steps, it became clear that I still had more to learn about the cloud computing system. This meant that I needed to learn more about cloud computing and repeat the process until my knowledge level was high enough. The framework has been built on the knowledge about the cloud computing systems I gained during the research. Learning about cloud computing also gave me input in how to create an acceptance basis for the citizen: how to create trust in the system.

Getting familiar with the EPD and the healthcare sector was easier than it was with cloud computing. With a number of relatives in the healthcare sector there were always people who could point me in the right direction or even answer my questions. The input was an immense help, but this sector also showed to be harder to understand than expected. The privacy issue and the stubbornness of the citizens where far greater obstacles than anticipated from the start. When this sector was fully understood it was possible to combine the newly acquired knowledge about cloud computing to the EPD and create the framework.

This provided a new problem. Probably most university students will write just one master thesis in their life. I felt like I was thrown in the deep end and was not as well-prepared as I would have liked to be. This in combination with dyslexia results in lower academic writing skills than the average students. Therefore it takes more effort to bring across the message that the thesis is trying to tell. This is not limited to spelling and grammar but also to academic writing in general: using the right words at the right point in the thesis has been challenging. While writing, I learned an enormous amount about how to structure the words, arguments, paragraphs and sentences. Using feedback I received, I tried to improve my writing skills and my academic skills in general. I am proud to say that I have acquired new skills and improved old ones.

New skills in setting up research proposals, doing literature reviews, structuring research findings are among the skills I can now use. From little to no experience in the field and in writing a thesis in general I am proud to say I did my best to create a thesis document that is satisfying. I hope the work will be helpful for the sector and the implementation of the EPD. I will follow the development of the EPD closely.

Jelle-Eric de Vries
11. Bibliography


The Implementation of the Electronic Patient Record

Jelle-Eric de Vries


Interviewee1. (2014, 10 23). Director. (J. De Vries, Interviewer)

Interviewee2. (2014, 10 30). Director . (J. De Vries, Interviewer)


12. Appendix

Appendix I Questionnaire

This appendix will show the questions of the questionnaire and the set-up of this questionnaire. Part A will therefore only state the questions and the possible answers for the questionnaire. In part B the reason why the questions were selected will be discussed. For every question a motivation will be given of why the question is asked.

Part A. Questionnaire

Introduction text (see Appendix III)

----

1. Demographic questions

How old are you?

- 18-24
- 25-34
- 35-44
- 45-55
- 56-64
- 66-74
- 75+

What is your gender?

- Male
- Female

What is the highest form of education you have finished?

- Mavo
- havo
- vwo
- athenum
- hbo
- wo
- lower school
- other,....

What is your current profession?

- Manager
- no job looking
- no job not looking
- healthcare
- engineer
- sales
- customer service
- board member
- other

----

2. Do you know what the abbreviation EPD stands for?

- Yes, namely.....
- No

----

3. Do you know what the purpose of the EPD is?

- Yes
- No
The Electronic Patient Dossier (EPD, Wikipedia, 2014) is planned to be a nationwide medical data transfer system. The EPD is not one big pile of medical information of all the patients in the Netherlands. It is an electronic network which enables healthcare providers to see medical files of patients from other healthcare providers. This embodies the goal of sharing relevant information, like the medical summary of your healthcare that your general practitioner keeps. There will be national laws on what relevant information is. This method enables medical professionals to give a better treatment because, for example, they will not redo tests but simply share the test results. The first aid treatment can also be faster as the patient’s file just needs to be opened to see blood type and possible allergies. The personal medical data will be as secure as possible with the latest technology and systems that monitor who enters the file. All efforts will be made to secure the privacy of a person’s medical data. (Ter Berg & Schothorst, 2010)

A number of security measurements are planned to be taken. These range from encryption to login keys and from public key infrastructure to monitoring. For medical professionals, the transfer of patient information will happen via a closed and secured network. They can only access the information with a personal pin and a card. On this card the information is stored on what a person is allowed to see. A medical professional may only see information that is directly related to the treatment of the patient. This will be checked afterward as every action to see data is stored. Patients will be able to give their consent to medical professionals to look at their data. They can also block medical professionals from seeing their information. They can also partly shield the information for healthcare providers.

4. Did your answer to question 3 correspond with the text above?
   a. yes
   b. no

5. Do you participate in the EPD?
   o Yes
   o No, but I would like to
   o No, I have declined because.....
   o No, I would not because....
   o I don’t know

6. Who do you think have access rights to your healthcare data? (Multiple answers possible)
   □ Doctors  □ general practitioners  □ physiologist  □ you yourself
   □ Nurses  □ pharmacies  □ physiotherapists  □ homecare
   □ Insurance companies  □ first aid  □ employers  □ other, .....
7. Who do you think should have access rights to your healthcare data? (Multiple answers possible)

- Doctors
- general practitioners
- physiologist
- you yourself
- Nurses
- pharmacies
- physiotherapists
- homecare
- Insurance companies
- first aid
- employers
- others, .....

8. 8.1) Do you think the system should be accessible from everywhere? Think about accessing on tablet, pc and phone from hospitals, medical practises, at home and on the road.

- The EPD should be accessible from every location from every device
- The EPD should only be accessible from medical locations from all devices
- The EPD should only be accessible from pc inside medical locations
- The EPD should be accessible from pc and laptops from everywhere.
- Other access places, like....

8.2) You chose: (show answer picked at 7.1) Why do you see this as the best option?

- Open question

9. Do you think your personal medical information would be in danger with the use of the EPD? (see for the security measurements that are being taken: Veiligheid)

- Yes
- no

10. The Dutch government spends around 63150 million on healthcare, the EPD system costs thus far 305 million and costs are still rising. Is this a fair amount to pay for the system compared to the health budget?

- Yes
- no

11. Should the EPD be introduced as soon as possible?

- Yes, even though there might still be a few glitches
- No, wait until the EPD is completely safe and there is no chance of failing

12. Do you think we need the EPD?

- Yes
- no

13. Other comments
Part B. Explanations of the questions
This part of the appendix will give an explanation of why every question was selected for the questionnaire.

1. Demographic questions

This will to show which demographic groups have certain opinions on the matter of the EPD system. This will show on which groups the framework must focus to ensure acceptance within every layer of the society.

2. Do you know what the abbreviation EPD stands for?

This question will be asked to understand what people already know about the EPD. This will give the current knowledge and show how much information about the EPD is already understood by the society. This will show, in combination with the questions later on, if people understand what they have signed up for or what they have refused or what they need to sign/refuse. The deeper understanding of the knowledge basis will help in creating a framework that helps create public acceptance, as it might show that more information needs to be provided to ensure that people are better informed. Thus the main aim of this question will be to understand the perception of the participant.

The question is based on (Masman et al, 2012) and (van Thiel, 2009)

3. Do you know what the purpose of the EPD is?

The question is asked to understand the perception of the EPD of the participants, to understand the qualities and needs to ask from the product. If the participant knows what the purpose of the EPD is, this question can show how these qualities are seen now.

The question is based on (Masman et al, 2012) and (van Thiel, 2009)

4. Did your answer to question 3 correspond with the text above?

To check if the respondents indeed think of the right purpose of the EPD.

5. Do you participate in the EPD?

This question will be asked to see the percentage of people participating in the EPD. This helps to conclude how successful the old EPD set-up is. This question is asked to understand the public opinion of the system and to see if people’s answers correspond (for example someone did not participate but they do see the need). This also combines with the need shown in the two questions above.
The question is based on (Mouw, 2010)

6. Who do you think have access rights to your healthcare data? (BusinessDictionary, 2014)(Multiple answers possible)

This question is asked to check the knowledge of the participants to see if they know who has access. This is done to see if more information needs to be provided about the access rights of the EPD. This question relates back to how the participants perceive the EPD, how they trust the EPD and how they see the safety of the EPD (and with safety they immediately review the privacy they think the EPD covers). The question relates to the legal issues, the perception and the trust of the participant in the system.

This question is based on (NIPO, 2009)

7. Who do you think should have access rights to your healthcare data? (BusinessDictionary, 2014)(Multiple answers possible)

This question is asked to see who should have access according to the patients. This is done to see if more information needs to be provided about the access rights of the EPD. This question relates back to how the participants perceive the EPD, how they trust the EPD and how they see the safety of the EPD (and with safety they immediately review the privacy they think the EPD covers). The question relates to the legal issues, the perception and the trust of the participant in the system.

This question is based on (NIPO, 2009)

8. Do you think the system should be accessible form everywhere? Think about accessing on tablets, pc and phone from hospitals, medical practises, at home and on the road.

In a more dynamic world it is important to know how accessible people want the EPD to be. If they want the system to be accessible from everywhere, which leads to more security measurements and more liabilities in the security chain or just from set locations which are more manageable to secure. The question refers back to the keywords of quality and legal issues.

9. Do you think your personal medical information would be in danger with the use of the EPD? (see for the security measurements that are being taken: Veiligheid) (epd.infozoeker.tk, 2009)

This is a direct question to understand if people have trust in the system and it also relates back to the safety of the system. It will also show directly if there are obstacles within this part of the implementation of the EPD system. It shows the legal matters that interact with the privacy laws of the Netherlands. This combines the issue of trust and the legal matters together. It will show the perception of the systems and the trust the participants have that the legal issues will be dealt with and their information is safe.

The question is based on (Masman et al, 2012).
10. The Dutch government spends around 63150 million on healthcare, the EPD systems costs thus far 305 million and costs are still rising. Is this a fair amount to pay for the system compared to the health budget?

The total budget is 63,15 billion. This is derived from the BBP which is 631,5 in 2010 (Vossers, 2014). Around 10% of this was allocated for healthcare (Ministerie van Volksgezondheid, 2012). This question is asked to see how much people are willing to spend on the EPD system. The question relates to the keywords about cost and revenue.

11. Should the EPD be introduced as soon as possible?

This will show the need for the product. It will show if the participants think that the system is ready for its introduction or that the introduction should wait until the system is developed further. This question will show the need for the product and matches this with the introduction speed. Thus, for example, if the system is highly needed and there is need for a high introduction speed or if the introduction can take longer because the need states that the system needs to developed further first.

12. Do you think we need the EPD?

This question is asked to see the clear needs of the participants, if they indeed see the need for an EPD. The focus will be if they see, after reading the intentions of the EPD, the need for the EPD or if they do not. This question relates back to the needs and the qualities the EPD needs to possess to create a successful implementation. The need for the system will be shown directly from this question.

13. Other comments

This last question gives the participants the ability to add information they think is helpful for the questionnaire or other remarks. This might be points the questionnaire has missed or other insights which might be in the scope of the research.
Appendix II Interviews set-up
This appendix will show the questions of the interviews and the motivation behind them. Part A will therefore only state the questions. Part B will state why the questions were selected. For every question a motivation will be given of why the question is asked.

Part A Interview question
In this part of appendix II the interview questions will be given. The interviews are set as a semi-structured interview: the questions proposed are guiding questions. Additional questions may be asked during the interview as they may arise in the conversation.

1: Questions for people that work in healthcare:

1. Do you know what the EPD is?
2. Do you already use the EPD? What is the current method of storing patient data? What is the current method of sharing patient data?
3. Does the system you use now, work well? Do you encounter any problems?
4. Is the EPD, in your opinion, secure? Is the EPD system safe to use?
5. Would you continue working with the EPD if you had the chance?
6. Does the EPD improve the level of healthcare? Will it improve the level of healthcare? Will it take care of the issues there were with the old system?
7. Who should have access to the patient information, to the EPD of a specific person?
8. Should the system be implemented as soon as possible?
9. Should the system be accessible from every location or just from specific locations?

2: Questions for people that work in the IT sector:

1. Do you know what the EPD is?
2. Are you participating in the EPD?
3. Do you think the EPD is secure?
   a. Think about login codes for medical personnel and finding people by using their social security number (Burger service nummer).
4. Do you see risks for the EPD?
5. What would you do to reduce these risks?
6. Do you think privacy is well protected?
7. What would be the best set-up for the system?
   a. Local-, central-, de central- set-up.
   b. Availability from every location or just from specific sites.
   c. Other requirements the interviewee thinks of.

3: Questions for people that work in the finance sector:

1. Do you know what the EPD is?
2. Are you participating in the EPD?
3. What would the cost structure of an EPD cloud computing system look like? What costs are drivers for this system?
4. Would there be profit to be made from such a system?
5. Would this profit outweigh the cost?
6. What would, cost wise, be the best set-up?
7. What would be the best payment method for the EPD?
   a. Pay-as-you go or pay up front

Part B Motivation
In this part of the appendix II a motivation will be given for the questions in the interview.

1: Questions for people that work in the healthcare:

1. Do you know what the EPD is?
   This question is asked to understand the knowledge of the expert about the topic. Without this knowledge the question base might change from the perspective of using an EPD to a perspective of going to use. This question is linked back to the keyword quality.

   This question is based on the works of (Masman et al, 2012).

2. Do you already use the EPD? What is the current method of storing patient data? What is the current method of sharing patient data?
   This question is asked to understand the knowledge of the expert about the topic. The question is asked to understand how the current system works and if the system is sufficient. What are the upsides and what are the downsides of the current system? The question refers back to the quality and legal issues keywords.

3. Does the EPD work well?
   This question is asked to understand the knowledge of the expert about the topic. The question is stated to understand how the current system works and if the system is sufficient. This question refers back to the keyword quality.

4. Do you have the feeling that the EPD is secure? Safe to use?
   This question is asked to understand the opinion of the medical expert about the EPD system, to see if they have the feeling that the system is secure. This knowledge can help determine the problems in the system. When medical personnel does not trust the system this will have a negative effect on the public. When they do trust the system, this will have a positive effect. This question refers back to the keywords trust, legal issues and quality.

   The question is based on (Khan et al, 2011)

5. Would you continue working with the EPD if you had the chance?
   The question is asked to understand if the medical personnel are content with the EPD system they have. This will give an insight in what the medical expert wants. This helps adjust the system. The follow-up question on this might be if they could change something about the system, what would it be. This question intents to see how content they are and thus refers back to the keyword about quality.
The Implementation of the Electronic Patient Record  

Jelle-Eric de Vries

The question is based on (Khan et al, 2011).

6. Does the EPD improve the level of healthcare? Will it improve the level of healthcare?

This question is asked to see if the intended purpose of the EPD has reached its goal and if the proposed system will improve the current system. The goal is to understand where the medical professionals see the improvement in the healthcare and then being able to show these improvements to the public to create a bigger acceptance basis.

The question is based on (Khan et al, 2011).

7. Who should have access to the patient information, to the EPD of a specific person?

This question is asked to see if the medical professional gives answers that match the answers from the same question in the questionnaire. The medical professional has expert knowledge on who might need the access and is therefore able to provide additional knowledge on who needs access rights that the public might not know about.

8. Should the system be implemented as soon as possible?

This question will show the need for the system. If the medical personnel state that the system is needed, the implementation should be as fast as possible. If the system is not currently needed, implementation can take longer. This question refers back to the keyword implementation speed.

9. Should the system be accessible from every location or just from specific locations?

The question is asked to understand the need for access locations within the hospital. Through this question it becomes clear on which devices the EPD should be available.

2: Questions for people that work in the IT sector:

1. Do you know what the EPD is?

This question is asked to understand the knowledge of the expert about the topic. Without this knowledge the question base might change from the perspective of using an EPD to a perspective of going to use. This question is linked back to the keyword quality.

This question is based on the works of (van Thiel, 2009) and (Masman et al, 2012)

2. Are you participating in the EPD?

This question is asked to understand if an IT expert would participate in the EPD while having expert knowledge about the security risk of the system. This question relates back to the keywords trust, legal issues and quality.

The question is based on (Mouw, 2010)
3. Do you think the EPD is secure? Think about login codes for medical personnel and finding people by using their social security number (Burger service nummer). Also general security of severs and access points.

This question is chosen based on the outcome of the literature review. Within the review it is shown that security is one of the main issues with cloud computing and the EPD. Therefore it is important to know what the opinion of an expert is on this point. Comparing the knowledge of the expert with the knowledge of the public, a knowledge gap might become visible. From this gap a strategy can be made to close the gap to implement the system. The question relates back to the keywords legal issues and quality.

This question is based on (Masman et al, 2012) and (van Thiel, 2009)

4. Do you see risks for the EPD?

This question is asked in relation to the question above. To understand why people do or do not participate with the EPD. The expert has the knowledge about the risks and should be able to portray these risks on the EPD system. The question relates back to the keywords legal issue and quality.

The question is based on the work of (Gollmann, 2010)

5. What would you do to reduce these risks?

When understanding these risks it is important to understand how they can be limited. This question is asked to understand how we can reduce the risks in the EPD system. The expert should be able to provide a landscape of options to secure the EPD system in the best way possible. This question relates back to the keyword quality.

The question is based on the work of (Gollmann, 2010)

6. Do you think the privacy is well protected?

This question is aimed at understanding the privacy problems that might occur when introducing the EPD system. Therefore the expert is asked to state his or her opinion on the matter. The outcome of the question can provide a frame of mind that can be applied to what the public thinks about their privacy risk when they participate in the EPD.

This question is based on the work of (Gollmann, 2010)

7. What would be the best set-up for the EPD system?

This question is asked to understand the qualities and requirements an IT specialist names for the EPD. From these qualities a list can be made which shows the needs and must haves for the EPD. The part in the framework that concerns the qualities of the EPD will be based on this list.

3: Questions for people that work in the finance sector:
1. Do you know what the EPD is?

This question is asked to understand the knowledge of the expert about the topic. Without this knowledge the question base might change from the perspective of using an EPD to a perspective of going to use. This question is linked back to the keyword quality.

This question is based on the works of (Masman et al, 2012) and (van Thiel, 2009)

2. Are you participating in the EPD?

This question is asked to understand if a financial expert would participate in the EPD while having expert knowledge about the costs of the system. This question relates back to the keywords trust, legal issues and quality.

The question is based on (Mouw, 2010)

3. What would a nationwide systems cost?

Recently an article was published that government IT projects tend to fail and cost an enormous amount of money (Deira, 2014). This raises the question of what a fully functioning and secure nationwide system costs. How accurate is the budget and what can be done to lower the costs? The question relates back the keyword cost.

4. Would there be profit to be made from such a system?

While the question above states what the cost would be, this question asks if money can be made or if the current cost will be lowered. How long does it take for the system to break even? This question refers back to the keyword revenue.

5. Would this profit outweigh the cost?

This question is asked to understand if the profit outweighs the cost. This question aims at the financial situation. The question refers back to the keywords cost and revenue.

6. What would, cost wise, be the best set-up?

This question aims at understanding what the best cost model would be. It might be possible that the system needs to be free to work properly and thus the cost model needs to be that the costs are as low as possible. The outcome of the question must aim toward a set-up that can be successfully implemented.

7. What would be the best payment method for the EPD?

The answer to this question will give the best method according to the expert for the payment system of the EPD. It will also show if a payment system is needed and what the best method is to make sure the system is always available when needed.
Appendix III Letter to respondents
This is the letter that accompanied the questionnaire to tell the participants what the questionnaire is about.

Dear reader,

I am a student at the Technical University of Eindhoven in the study direction “Innovation Management”. I am currently working on my final thesis.

Participating in the questionnaire is voluntary and anonymous. All the information collected will be used confidentially. Only summarized data will be published. The questionnaire will take about 10 minutes to complete.

I hope you will take the time to help me with finishing my thesis.

With gratitude,

Jelle-Eric de Vries
Appendix IV Mapping of the Questions

The following sub questions have been established from the Literature Review and are listed in the Research Proposal.

Part A Sub Questions

Product
12. Which qualities does the product need to satisfy the customer’s needs?
13. Why is it possible to create a nationwide system in other countries, what stops the Netherlands from creating such a system?

Market
14. What are the opportunities and drawbacks of such a nationwide system, according to the citizen of the Netherlands?
15. What can be done to increase the trust of the patients in a Cloud Computing system for the healthcare industry?
16. What are the legal issues that might arise with storing patient data?
17. What is the perception, of the patients, of such a system in The Netherlands at this point? What can be done to change this perception if the perception is negative?

Cost
18. Which financial constructs might be used to create a profitable system?
19. What is the main cost factor for storing patient data with cloud computing?
20. What is the main revenue stream that can be found with storing patient data with cloud computing?

Timing
21. What are other possible products that might compete with a Cloud Computing system to store patient data? Thus when should the introduction take place?
22. How urgent must the market introduction be on the basis of need for the system?

The following map shows how the sub question will be answered. The sub questions are linked to questions from the questionnaire and the interviews (see Appendix I and Appendix II).
### Part B Map of the Sub Questions

<table>
<thead>
<tr>
<th>Sub Questions</th>
<th>Questionnaire Question</th>
<th>Medical Sector</th>
<th>IT Sector</th>
<th>Finance Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7.1;7.2</td>
<td>9</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4,5,6</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>7</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2,3</td>
<td>1,4</td>
<td>1,2</td>
<td>1,2</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td>5,6</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td></td>
<td>6,8</td>
<td></td>
</tr>
</tbody>
</table>

*Table 9 Relation of Sub Questions to the questionnaire questions and the interview questions*
Appendix V Interviews

Part A Overview of the Interviewees
The table below shows an overview of the interviewees.

<table>
<thead>
<tr>
<th>Interview number</th>
<th>Male/Female</th>
<th>Date</th>
<th>Occupation</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>Male</td>
<td>23-10-2014</td>
<td>Director</td>
<td>Security</td>
</tr>
<tr>
<td>Two</td>
<td>Male</td>
<td>30-10-2014</td>
<td>Director</td>
<td>Telecom/IT</td>
</tr>
<tr>
<td>Three</td>
<td>Female</td>
<td>14-12-2014</td>
<td>Doctor</td>
<td>Healthcare</td>
</tr>
<tr>
<td>Four</td>
<td>Male</td>
<td>08-01-2015</td>
<td>Junior Doctor</td>
<td>Healthcare</td>
</tr>
<tr>
<td>Five</td>
<td>Female</td>
<td>16-01-2015</td>
<td>Doctor</td>
<td>Healthcare</td>
</tr>
</tbody>
</table>

Table 10 Overview of the Interviewees

Part B Outline of the information gained from the interviews

Interview one
Security and cloud  
23-10-2014

A number of key points were kept and thus stand for the entire interview. The main points are listed below:

➢ Security
  • Monitoring
    o Create attacker profiles to be able to detect intruders.
    o Detection of attackers is critical to the safety of the system.
    o Typical and non-typical information should be examined.
    o A group of security personnel should do the different tasks. To be able to do this they should have access to all information.
  • The information must be encrypted.
  • Certificates are needed.
  • Authentication via public and personal keys is a must.
  • The deals that are made with the suppliers of the services must be checked.
  • The location of the cloud is important. It needs to be in the Netherlands to ensure better security and access to the information.

➢ Costs
  • Millions
  • People including security check.
  • Connections.
  • Materials.

➢ Accessibility
  • Only with DSM will the system be vulnerable.
  • Back-up (by use of the 4 hard disk system, if one breaks the other three take over the entire system and thus no information is lost).
  • Multiple locations.
  • Possible needs for a secondary location when the primary location is failing.

Other questions to consider named by the interviewee:
What is the improvement of the system compared to the old system?

What is the damage/effect of (no) using the system?

**Interview two**
Cloud, requirements and security 30-10-2014

Below a summary is given of the points that were discussed during the conversation.

The interviewee states that it should be possible to create a safe EPD system based on the fact that we can secure nuclear power plants. We can secure such dangerous places so we must be able to secure an information system. The question remains how user-friendly the system will become. As it is an everyday used product, the user-friendliness should be high. The information is sensitive and thus must be well protected. The interviewee states that a balance should be found between the user-friendliness and the security level of the product.

The use of encryption, public key infrastructure, back-up and certificates are a must to secure the system. The use of cloud computing should be able to facilitate the system. A close look should be taken at where the information stored. The interviewee says he does not know at this point what the best storage method is, at location in hospital or a number of different remote locations or one remote location.

He states that is a problematic subject and must studied intensively. He also states that it will be possible to create such a system but work must be done. The creation of such a system might be more a political game than a real struggle. When the government really wants to implement the system they would already have done so.

**Interview three**
Healthcare and requirements 14-12-2014

This is a short overview of the main points discussed in the interview with the interviewee, a specialist in Geriatric Medicine.

Requirements for the EPD:

- Password protected but with an ease of use. Now log in on a pc/smartphone/tablet with a password and then on the site/app with a personal password. Not many more security steps than that, otherwise the system will take too long to use. The convenience of the system she uses now is that it is accessible fairly fast and on site. Changes in patients’ records are made in an instant.
- System needs to be accessible on location, thus it is a must to be able to gain access from smartphone or tablet.
- Access needs to be around the clock.
- It needs to be documented who changes what in this system. It must not be possible to alter the logbook in any way.
- It must be possible for doctors and patients to block certain people from the file, e.g. other doctors, nurses etc. this should be possible from the entire file or just from part of the file.
- An instruction must be given to medical personnel on how to use the system.
- The set-up of the information input must be standard but it must be possible to enlarge information input boxes when they are too small or to add boxes if needed.
- Clusters of information are handy (see preference for the system).

Preferences for the system

The interviewee indicates that she is not participating in the EPD. She would rather have a smaller set-up of the EPD. With this she means less information that is stored in the national EPD. She states that an EPD system is necessary and that it is an efficient way for doctors to get the information they need. Hospitals often work in clusters, therefore it is easy for doctors who work in two locations to have access to one system for the information about patients. This system should only be used by the hospitals that work together. A nationwide system should only be used for vital information. Information such as allergies, disease or conditions which are not often seen and where patients often have more knowledge than a non-specialist doctor.

So in this more restricted version of the EPD the interviewee proposes, every doctor can access the system (every time the EPD is accessed should be documented in a logbook which cannot be altered). The information that they can see is only vital information of a patient, needed in case of emergency.

**Interview four**  
Requirements 08-01-2015

The interviewee, who is a junior doctor, names a number of different points which should be in the EPD according to him. The following points are mentioned:

- The EPD system needs to be quick. A long waiting time for the EPD to respond will not be beneficial to the treatment of a patient. The doctor has to wait and so does the patient which prolongs the session time the doctor has.
- The system needs to function 24/7.
- The system needs to be protected by password in order to be secure. But not a lot more than password should be needed in order to log onto the EPD quickly.
- A small lesson should be given to medical personnel on how the EPD works.
- The EPD should offer a clear overview page. In some of the EPD systems that are in use now it is unclear where the information is stored within the patient file. This is not handy and lengthens the time a doctor needs with the patient.
- It would be handy, but not necessary, if every hospital had the same set-up to work with the system, so that there is no need for another lesson on how the EPD works if a doctor should use the EPD in a different hospital.
- It would be handy if the EPD was accessible from every device from every location in order to improve the treatment of the patient.

**Interview five**  
Requirements 16-01-2015
Interviewee number five, who is a paediatrician, verified the list of requirements and added a number of points to the list. The interviewee stated that the list was mostly complete but missed a small number of points. The points she missed are stated below:

- The possibility to store different files of information (information other than text). E.g. attachments like x-rays, lab results etc.
- From the viewpoint that there is no paperwork: how can doctors request tests (for example for x-rays)?
- How does the communication work between doctors? For example between a specialist and a general practitioner?
- The system must be easy and quick to use. It must not be more time consuming than the paper system.

Interview Six
EPD case 13-04-2015

Interviewee number six helped with the EPD case example. The interviewee described the Epic EPD system and what the problems were that the interviewee encountered when using it. The main points are listed below:

- The lack of a good teaching system. This makes it hard to understand and work with the system when you are new to the system.
- When you work with the system for a longer period of time, the system is good to work with.
- The system is only accessible from a computer in the hospital.
Appendix VI Security Threats

<table>
<thead>
<tr>
<th>Security Threat</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architecture</strong></td>
<td>Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.</td>
</tr>
<tr>
<td><strong>Identity and Access management</strong></td>
<td>Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.</td>
</tr>
<tr>
<td><strong>Software isolation</strong></td>
<td>Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.</td>
</tr>
<tr>
<td><strong>Data Protection</strong></td>
<td>Evaluate the suitability of the cloud provider’s data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.</td>
</tr>
<tr>
<td></td>
<td>Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.</td>
</tr>
<tr>
<td></td>
<td>Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization’s continuity and contingency planning requirements.</td>
</tr>
<tr>
<td></td>
<td>Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstited in a timely and organized manner.</td>
</tr>
<tr>
<td><strong>Incident response</strong></td>
<td>Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.</td>
</tr>
</tbody>
</table>

Table 11 Security Threats and Recommendation

The information above is based on the work of (Jansen & Grance, 2011)
### Appendix VII Security threats and their Solutions

<table>
<thead>
<tr>
<th>Possible attacks</th>
<th>Solutions or Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VM-Level attacks</strong></td>
<td>Monitoring the system and implementing firewalls can reduce this problem.</td>
</tr>
<tr>
<td>Faults are made and vulnerabilities appear within the hypervisor. Appear usually because developer overlooks the problem during coding.</td>
<td></td>
</tr>
<tr>
<td><strong>Abuse and Nefarious use of cloud computing</strong></td>
<td>Implement stricter registration and validation process. Detailed inspection of user’s network traffic and monitoring public black lists.</td>
</tr>
<tr>
<td>When not having a perfect authentication and registration system in place, attackers can anonymously gain access to the cloud. All they need from the start is a valid credit to register and use the service.</td>
<td></td>
</tr>
<tr>
<td><strong>Loss of governance</strong></td>
<td>There are no publicly available standards specific to cloud computing security. Thus organizations considering cloud services need to exercise persistent and careful efforts for the execution of Service Level Agreements (SLA).</td>
</tr>
<tr>
<td>The user gives up control to the cloud provider on a number of issues while using the cloud infrastructure. The service Level Agreements (SLA) may not have commitment on the part of cloud provider, to provide such services, thus having a gap in security defences affecting security. This loss of control may lead to a lack of confidentiality, integrity and availability of data.</td>
<td></td>
</tr>
<tr>
<td><strong>Lock-IN</strong></td>
<td>Standardized cloud Application Programming Interface (API) should be used. This standardization will ensure cloud computing to be more fully accepted.</td>
</tr>
<tr>
<td>Lock-IN means inability of the customer to migrate from one cloud service provider to another. This is due to loss of portability of the customer data and programs.</td>
<td></td>
</tr>
<tr>
<td><strong>Insecure Interfaces and APIs</strong></td>
<td>The security model of cloud provider interfaces should be analysed. Strong authentication and access controls should be implemented. Encryption should be used for transmission of content and</td>
</tr>
<tr>
<td>Customers use a set of software Interfaces or APIs to interact with cloud services. If the weak set of interfaces and APIs are used, this may expose organizations to various security threats.</td>
<td></td>
</tr>
<tr>
<td><strong>Isolation Failure</strong></td>
<td>Strong compartmentalization should be employed so that the individual customers do not impact the operations of other customers. This can be enforced by implementing best practices for installation, configuration, monitoring environment for unauthorized changes/activities, promoting strong authentication and access control, patching the vulnerabilities and conducting vulnerability scanning and configuration audits.</td>
</tr>
<tr>
<td>The services are delivered in cloud computing by sharing infrastructure. The hypervisors, that are basic building blocks for cloud computing, have exhibited flaws that enable guest operating system to gain unauthorized control.</td>
<td></td>
</tr>
<tr>
<td><strong>Data loss or leakage</strong></td>
<td>Encrypting and protecting integrity of data in transit, analysing data protection at both design and runtime, implementing strong key generation, storage and management. Contractually demanding provider to wipe</td>
</tr>
<tr>
<td>This data loss or leakage may be due to insufficient authentication, authorization and audit controls, inconsistent use of encryption and software keys, disposal challenges, a data</td>
<td></td>
</tr>
</tbody>
</table>
The implementation of the Electronic Patient Record

<table>
<thead>
<tr>
<th>Security Threat</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centre reliability, and disaster recovery.</td>
<td>Persistent media before it is released in to pool and contractually specifying provider backup and retention strategies.</td>
</tr>
</tbody>
</table>

**Account or service Hijacking**
Phishing, fraud and software vulnerabilities, give attackers opportunity to steal credentials and gain access to critical areas of deployed cloud computing services.

**Management Interface Compromise**
One of the strengths of Cloud Computing is the remote access through internet. This may pose a serious threat if web browser vulnerabilities are present.

**Compliance Risks**
This threat arises due to lack of governance over audits and industry standard assessments. Due to this, customers of cloud services do not have a view into the processes, procedures and practices of the provider in the areas of access, identity management and segregation of duties.

**Malicious Insiders**
Malicious insiders’ impact on organization is considerable. Given their level of access, they can infiltrate organizations and assets and do brand damage, financial losses and productivity losses.

Vendors’ internal audit process should be reviewed. How often it is audited by external agencies and, whether or not, it is open to being audited for compliance.

Secure protocol should be used to provide access. Also, web browser vulnerabilities should be completely patched before providing remote access.

Specifying human resources requirements as part of legal contracts, conducting a comprehensive supplier assessment, providing transparency into overall information security and management practices, as well as compliance reporting and determining security breach notification processes.

Table 12 Security threats and their Solutions

The information above is based on the works of (Tripathi & Mishra, 2011) and (Chen et al, 2010).
Appendix VIII Results Questionnaire

This appendix will give the results for the questions asked in the questionnaire.

Question 1

Demographic questions.

<table>
<thead>
<tr>
<th>Age group</th>
<th>Age (1.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>27.17%</td>
</tr>
<tr>
<td>25-34</td>
<td>11.96%</td>
</tr>
<tr>
<td>35-44</td>
<td>4.35%</td>
</tr>
<tr>
<td>45-55</td>
<td>30.43%</td>
</tr>
<tr>
<td>56-64</td>
<td>16%</td>
</tr>
<tr>
<td>65-74</td>
<td>6.52%</td>
</tr>
<tr>
<td>75+</td>
<td>3.26%</td>
</tr>
</tbody>
</table>

Table 13 Demographic question; Age group

<table>
<thead>
<tr>
<th>Gender</th>
<th>(1.2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>33.7%</td>
</tr>
<tr>
<td>Female</td>
<td>66.3%</td>
</tr>
</tbody>
</table>

Table 14 Demographic question; Gender

<table>
<thead>
<tr>
<th>Education type</th>
<th>(1.3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower school</td>
<td>0%</td>
</tr>
<tr>
<td>Mavo</td>
<td>2.17%</td>
</tr>
<tr>
<td>Havo</td>
<td>5.43%</td>
</tr>
<tr>
<td>Vwo</td>
<td>9.78%</td>
</tr>
<tr>
<td>HBO</td>
<td>29.35%</td>
</tr>
<tr>
<td>Wo</td>
<td>44.57%</td>
</tr>
<tr>
<td>Other</td>
<td>8.7%</td>
</tr>
</tbody>
</table>

Table 15 Demographic question; Education type

The occupations were too spread among the respondents to make a statement about them.

Question 2, 3 & 4

Do you know what the abbreviation EPD stands for?, Do you know what the purpose of the EPD is?, Did your answer to question 3 correspond with the text above?

<table>
<thead>
<tr>
<th>Answers</th>
<th>EPD stand for (2)</th>
<th>Goal EPD (3)</th>
<th>Correct on goal EPD (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>53.33%</td>
<td>95.56%</td>
<td>93.18%</td>
</tr>
<tr>
<td>No</td>
<td>46.67%</td>
<td>4.44%</td>
<td>6.82%</td>
</tr>
</tbody>
</table>

Table 16 EPD knowledge; questions 2, 3 and 4

Question 5
Do you participate in the EPD?

<table>
<thead>
<tr>
<th>Answers</th>
<th>Participation in the EPD (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>23.86%</td>
</tr>
<tr>
<td>No but I would like to</td>
<td>36.36%</td>
</tr>
<tr>
<td>No, I have declined</td>
<td>17.05%</td>
</tr>
<tr>
<td>No, I would not because</td>
<td>1.14%</td>
</tr>
<tr>
<td>I don’t know</td>
<td>21.59%</td>
</tr>
</tbody>
</table>

Table 17 Participation in the EPD; question 5

*Question 6 & 7*

Who do you think have access rights to your healthcare data?”, “Who do you think should have access rights to your healthcare data?”

<table>
<thead>
<tr>
<th>Group</th>
<th>Have the rights (6)</th>
<th>Should have the rights (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>15.12%</td>
<td>4.88%</td>
</tr>
<tr>
<td>Doctors</td>
<td>96.51%</td>
<td>97.56%</td>
</tr>
<tr>
<td>Nurses</td>
<td>50%</td>
<td>43.9%</td>
</tr>
<tr>
<td>General practitioners</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Pharmacies</td>
<td>73.25%</td>
<td>70.73%</td>
</tr>
<tr>
<td>Insurance companies</td>
<td>18.6%</td>
<td>7.32%</td>
</tr>
<tr>
<td>First aid</td>
<td>93.02%</td>
<td>93.9%</td>
</tr>
<tr>
<td>Physiologist</td>
<td>33.72%</td>
<td>29.27%</td>
</tr>
<tr>
<td>Homecare</td>
<td>15.12%</td>
<td>15.85%</td>
</tr>
<tr>
<td>Employers</td>
<td>2.33%</td>
<td>2.44%</td>
</tr>
<tr>
<td>Company doctor</td>
<td>26.74%</td>
<td>21.95%</td>
</tr>
<tr>
<td>Other</td>
<td>1.16%</td>
<td>1.22%</td>
</tr>
</tbody>
</table>

Table 18 Access rights; question 6 and 7

*Question 8.1*

“Do you think the system should be accessible from everywhere? Think about accessing on tablet, pc and phone from hospitals, medical practises, at home and on the road.”

<table>
<thead>
<tr>
<th>Answer</th>
<th>Accessibly (8.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible from every location from every device</td>
<td>23.53%</td>
</tr>
<tr>
<td>Only be accessible from medical locations from all devices</td>
<td>30.59%</td>
</tr>
<tr>
<td>Only be accessible from pc inside medical locations</td>
<td>37.65%</td>
</tr>
<tr>
<td>Accessible from pc and laptops from everywhere</td>
<td>2.35%</td>
</tr>
<tr>
<td>Other access places</td>
<td>5.88%</td>
</tr>
</tbody>
</table>

Table 19 Accessibly; question 9

*Question 8.2*

“You chose: (show answer picked at 7.1) Why do you see this as the best option?”
Open question

Answers will be discussed in section 7, “Preferences of the Dutch citizens”, where the answers are valuable to use.

**Questions 9, 10, 11 & 12**

Do you think your personal medical information would be in danger with the use of the EPD? (see for the security measurements that are being taken: Veiligheid), The Dutch government spends around 63150 million on healthcare, the EPD systems costs thus far 305 million and costs are still rising. Is this a fair amount to pay for the system compared to the health budget?, Should the EPD be introduced as soon as possible?, Do you think we need the EPD?

<table>
<thead>
<tr>
<th>Answer</th>
<th>Danger Privacy (9)</th>
<th>Cost (10)</th>
<th>Implementation (11)</th>
<th>Need EPD (12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>47,06%</td>
<td>67,86%</td>
<td>27,38%</td>
<td>83,13%</td>
</tr>
<tr>
<td>No</td>
<td>52,94%</td>
<td>32,14%</td>
<td>72,62%</td>
<td>16,87%</td>
</tr>
</tbody>
</table>

Table 20 Privacy, cost, implementation and need; questions 9, 10, 11 and 12
Appendix IX Information from questionnaires on the EPD

Van Tiel (2009) focuses on the citizens, Khan et al (2011) and Mies (2009) focus more on the medical professional’s side of the EPD. All see the need for the electronic records, but they see the problems as well. Mies (2009) states the success factors for a successful implementation of the medical professional side. He says that doctors are not unanimously agreeing with the implementation of the EPD. Also, hospital managers have doubts with the implementation sequence (Mies, 2009). Khan et al (2011) stress the importance of the EPD. They mention the same thing as Mies (2009) does: the EPD increases in importance when multiple medical professionals are working with the same patient, as the EPD enables them to easily share information (Khan et al, 2011).

The distrust in the implementation can also be seen in the work of Mies (2009), here it is indicated that a large number of the participants would like more information about the EPD. The three studies all concluded that information is the key to successful implementation. This concurs with the statements of Gollmann (2010) about involving all parties and creating a uniform knowledge basis for all participants.

Thus the questionnaires create an understanding of the needs and knowledge of the participants but do not lead to a framework to create acceptance among the Dutch citizens. Mies (2009) suggest using best practice methods to introduce the system. Van Tiel (2009) does not support or reject this suggestion. The main conclusion and direction of Van Tiel (2009) rest on the information streams towards the Dutch citizens and improving this stream to fill the knowledge gaps. This is stated as: “the negative feelings towards the EPD are create by the lack of knowledge and the supply of negative information via the media”.

86
Appendix X Versions of the Framework
Version 1. The first version of the framework based on the findings of the thesis. It was used until 18-01-2015.

Figure 18 EPD Framework version 1
Version 2. This version is based on the feedback and was used until 12-02-2015
The Implementation of the Electronic Patient Record

Jelle-Eric de Vries

This version is based on the feedback after the validation session. The version was used until 10-04-2015

Figure 20 EPD framework version 3
Appendix XI Results of the Brainstorm session

Figure 21 Brainstorm Keywords
Figure 22 Keywords network
Appendix XII Clarification of Framework Elements

Trust (output): The factor is considered as the literature review showed that trust is an obstacle to be overcome when creating a cloud computing system.

Privacy (output): Privacy is a major factor as the literature review showed. The questionnaire showed as well that the citizens are concerned about their privacy. The interviews showed the same result: privacy is a major factor in the creation of an EPD cloud computing system.

Fulfilling the needs (activities): every aspect that has to do with the requirements for the system and which of these requirements must be fulfilled in order to reach the intended outcomes

Security (activities): As the literature review showed, the security needs to be perfect in order to implement the system. This is an important factor in creating the trust in the system. The system needs to be secure when implemented to be accepted by the citizens.

- Non-physical system: every aspect that deals with the software of the system
- Physical security: every aspect that deals with hardware protection

Ease of use (output): The system needs to be easy to use as was stated throughout the interviews. Without this ease of use the doctors will not accept the system.

Accessibility (output): The system needs to be easily accessible as was stated throughout the interviews. Without this accessibility it will take too long to enter the EPD and the doctors will not accept the system.

Trust campaign (activities): The questionnaire indicated that the citizens understood the need for the EPD but do not trust the system. In order to create the trust basis that is needed, a trust campaign needs to be created to convince people that the system is safe and secure.

Financially sound (output): The literature overview shows that a sound financial set-up is needed to create an acceptance basis among the citizens.

Financial budget (activity): The literature overview shows that the creation of a sound budget is needed to create a financially sound product.

Own control (output): The interviews and the questionnaire have indicated that there is a need for the patient to be able to control his/her data. This need comes from the citizens and from the doctors, for example to be able to block people from the EPD.

Doctors’ agreement with the system (outcome): The interviews have shown that the doctors is one of the two groups that needs to be convinced to use the EPD cloud computing system in order to implement it.

Citizens’ agreement with the system (outcome): The questionnaire has shown that the citizens is one of the two groups that need to be convinced to use the EPD cloud computing system in order to implement it.
Appendix XIII Validation Process

The validation of the framework was done by a group of new interviewees. They reviewed the framework (appendix X, version 2) and the explanation of the framework. In additions they also answered a number of questions. Below the process is described:

**Interviewees:** the group of interviewees needed to consist of experts of the different sectors that are part of the framework. Therefore interviewees were needed from: IT, finance, healthcare and from the general public. Finding these different people was more difficult than expected in the short amount of time. Therefore the financial sector spot is filled by a more global expert. The following people were selected for the validation:

- **Doctor**, who has the knowledge of the old paper patient record system and who can say how this is improving (or not) with the EPD cloud computing system framework.
- **Junior Doctor**, for a new and unbiased view of the system as this doctor has not worked with the paper patient record system.
- **IT expert**, for the knowledge about the IT side of the framework and for the knowledge about the security.
- **Manager of a global company**, responsible for the European part of the company and with an extensive knowledge of finance.
- **A citizen** with no background in any of the sectors involved in the framework, to see the patient side of the framework and how their acceptance level is changed by the framework.

**Questions:** three questions were asked to all interviewees before they started to examine the framework. There three question were:

- Is it clear what the goal of the framework is?
- According to you, is this goal reached if the framework is followed?
- According to you, what is missing or should be changed in the framework?

**Method:** All interviewees get the three questions on paper. They also get a printed version of the framework and the explanation of the framework that they can make notes on. The framework in this paper can be found in appendix X, version 2. Every interviewee is asked to evaluate the section. From there on the evaluation of framework and the explanation text are discussed individually with every interviewee. This individual evaluation is done in order to make a distinction between the answers of the respondents. When evaluation would be done in a group there is a chance that the interviewees will follow each other’s answers.

During the evaluation the questions will be discussed and any other possible questions that arise from the evaluation. The interviewee will indicate which changes should be made according to him or her to improve the framework.

All the different comments are listed and examined afterwards. When the same comments are mentioned by different interviewees the comments will be marked in the framework for later examination. Any grammar and spelling remarks are immediately updated.
The remarks of the interviewees were examined and when multiple remarks were about the same issue the framework was changed accordingly. If there was a single remark about a change in the structure of the framework this remark was examined and only changed when deemed necessary.

**Results:** the following comments were made about the framework. The table will show the number of the comment, the comment that was made and how many interviewees have stated the comment.

<table>
<thead>
<tr>
<th>Number of comment</th>
<th>Comment</th>
<th>Amount stated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Why is the line from the four pillars to the ‘fulfillment step’ different from the other lines from the four pillars?</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Why does security have a double effect on trust? (direct effect and via the trust campaign)</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>It is unclear what the different elements are/I would use different colors for different elements (e.g. outcomes, outputs, activities).</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Why are some lines thicker than other lines?</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Why do the two lines join from the pillars and from the ‘the creation of SaaS etc.’ to creation of own control? Other lines do not join.</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>Why do all the lines from the pillars first join and then split again?</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>Are these all the needs?</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>Are these all the non-physical security steps?</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>Why is one of the elements named ‘the creation of the physical security’ and the other</td>
<td>1</td>
</tr>
</tbody>
</table>
The Implementation of the Electronic Patient Record

Jelle-Eric de Vries

Table 21 Results validation

<table>
<thead>
<tr>
<th>Question</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are ‘creation of trust campaign’ and ‘develop knowledge EPD of citizens’ really two different things that need to be done?</td>
<td>2</td>
</tr>
<tr>
<td>What is meant by own control options?</td>
<td>1</td>
</tr>
</tbody>
</table>

Review of comments: Below every comment is discussed and it is stated what should be done with the comment:

1. This is a logical point. The link is supposed to be the same level link as the other links from the pillars. Thus this needs to be changed.
2. The double effect on the ‘trust in the system’ element is unjust. The physical security only once has an effect on the ‘trust in the system’ element. This effect is not a direct effect but an indirect effect via the ‘trust campaign’ element. This element used the security as input to show the public what is done to protect their information. The double effect was removed.
3. The different elements are displayed in italics, in bold, underlined and with circles. As this was understood not to be enough, use of colours is added and the categories will be named above the framework.
4. Some lines are thicker as there are double lines. This has nothing to do with importance. This will be adjusted as well as possible. It will also be stated in the text that there is no difference in importance level of the linkage between the elements.
5. This is indeed a mistake made. This link should indicate that it has an effect on the other line and thus should be an arrow towards the line. This will be changed.
6. The lines of the pillars first join and then split because they are all deemed to be of equal importance. The four pillars are grouped in one model. Therefore, the four pillars are grouped in the framework as one. The decision is made to show which pillars have effect on which elements in the written text.
7. Not all the needs are listed in the framework to keep the framework understandable. This will be stated in the text with a reference to where all the needs can be found.
8. Not all the non-physical or physical security steps are listed in the framework to keep the framework understandable. This will be stated in the text with a reference to where all the security steps can be found.
9. This is done with physical security to stress the need for security in the form of wall and fences. Within the text the distinction is further explained. It is chosen not to change this in the framework.
10. These two parts of the elements are indeed different as one tries to convince people to join the EPD and the other one aims at supplying information about the EPD to inform the citizen what the EPD is. It is chosen not to change this in the framework.
11. The meaning of this will be explained within the text.
After the validation session it was decided to remove the examples from the framework. This was done in order to create a more comprehensive framework. Thus version 3 in appendix X was the outcome of the validation session.
Appendix XIV Buildup of the Framework
The final framework (section 9.2.1, figure 17) consists of the following seven, smaller and easier to read, ULM diagrams:

Figure 23 UML diagram Accessibility

Figure 24 UML diagram Ease of Use

Figure 25 UML diagram Trust in the System
The Implementation of the Electronic Patient Record

Figure 26 UML diagram
Financially Sound

Figure 27 UML diagram
Doctors agree with the system

Trust in the System
Ease of Use
Accessibility

Figure 28 UML diagram
Citizens agree with the system

Figure 29 UML diagram
Successful Implementation
## Appendix XV Explanation of the Arrows

The following table will explain every arrow in the final framework (section 9.2.1, figure 17). All arrows indicate the influence one element has on another.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Influence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Four Pillars - Product</strong></td>
<td>Fulfiling Needs</td>
<td>The product provides the basic knowledge of what is needed (and what is possible) for the creation of an EPD cloud computing system.</td>
</tr>
<tr>
<td><strong>Four Pillars - Market</strong></td>
<td>Fulfiling Needs</td>
<td>The market provides the needs that should be fulfilled.</td>
</tr>
<tr>
<td><strong>Four Pillars - Product</strong></td>
<td>Creation of the Non-physical System</td>
<td>The product provides the security qualifications that are needed for SaaS/PaaS etc.</td>
</tr>
<tr>
<td><strong>Four Pillars - Cost</strong></td>
<td>Creation of the Non-physical System</td>
<td>The cost provides the basic knowledge of what is financially possible for the creation of security.</td>
</tr>
<tr>
<td><strong>Fulfilling the Needs</strong></td>
<td>Creation of the Non-physical System</td>
<td>Every need must be communicated to this security step, in order to adapt the security to the needs.</td>
</tr>
<tr>
<td><strong>Four Pillars - Product</strong></td>
<td>Creation of Trust Campaign</td>
<td>The product provides the basic knowledge of what is needed (and what is possible) for the creation of an EPD cloud computing system.</td>
</tr>
<tr>
<td><strong>Four Pillars - Timing</strong></td>
<td>Creation of Trust Campaign</td>
<td>The timing provides the right moment for the introduction of the EPD system and thus a starting moment for the trust campaign.</td>
</tr>
<tr>
<td><strong>Creation of Physical Security</strong></td>
<td>Creation of Trust Campaign</td>
<td>Every decision taken in the creation of the physical security must be communicated to the citizens in the trust campaign.</td>
</tr>
<tr>
<td><strong>Four Pillars - Market</strong></td>
<td>Creation of Own Control</td>
<td>The market will provide the basic knowledge about the needs of the patients concerning the level of locus of control.</td>
</tr>
<tr>
<td><strong>Creation of the Non-physical System</strong></td>
<td>Creation of Own Control</td>
<td>The level of security within the cloud computing system will provide the input for what is possible for the level of control of the patients.</td>
</tr>
<tr>
<td><strong>Four Pillars - Cost</strong></td>
<td>Managing the Cost</td>
<td>The cost pillar will provide the cost structure to be managed.</td>
</tr>
<tr>
<td><strong>Creation of the Non-physical System</strong></td>
<td>Creation of Physical Security</td>
<td>The steps taken in the creation of SaaS/PaaS etc. will provide the input for specifications needed for physical security.</td>
</tr>
<tr>
<td><strong>Fulfilling the Needs</strong></td>
<td>Accessibility</td>
<td>If all needs concerning accessibility are sufficiently fulfilled, the accessibility level of the EPD cloud computing system will be high. If not sufficiently fulfilled, the accessibility level will be lower.</td>
</tr>
<tr>
<td><strong>Creation of physical accessibility</strong></td>
<td>Accessibility</td>
<td>In which manner the security is arranged will indicate how high the accessibility level of the EPD cloud computing system is.</td>
</tr>
</tbody>
</table>
### The Implementation of the Electronic Patient Record

#### Jelle-Eric de Vries

<table>
<thead>
<tr>
<th>Security</th>
<th>Fulfilling the Needs</th>
<th>Ease of Use</th>
<th>To which extent the needs are fulfilled will influence the level of ease of use.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation of Physical Security</td>
<td>Fulfilling the Needs</td>
<td>Trust in the System</td>
<td>The higher the amount of needs fulfilled, the higher the trust in the system will be. When a low amount of needs is fulfilled, the trust level will be lower.</td>
</tr>
<tr>
<td>Creation of Trust Campaign</td>
<td>Trust in the System</td>
<td>The trust campaign needs to convince the doctors and citizens to use the system by raising the trust level.</td>
<td></td>
</tr>
<tr>
<td>Creation of Own Control</td>
<td>Trust in the System</td>
<td>When there is a high locus of control, the trust in the system will be high. When there is a lower locus of control, the trust level will be lower.</td>
<td></td>
</tr>
<tr>
<td>Managing the Costs</td>
<td>Financially Sound</td>
<td>When the costs are rightly managed, a financially sound product will be delivered.</td>
<td></td>
</tr>
<tr>
<td>Accessibility</td>
<td>Doctors agree with the system</td>
<td>When the doctors can access the system relatively easy they will accept the system better. With a longer accessibility time the acceptance will be lower.</td>
<td></td>
</tr>
<tr>
<td>Ease of Use</td>
<td>Doctors agree with the system</td>
<td>When the system is easy to use for the doctors the acceptance level will be higher. When the system is difficult to use, the acceptance level will be lower.</td>
<td></td>
</tr>
<tr>
<td>Trust in the System</td>
<td>Doctors agree with the system</td>
<td>When the doctors trust the system, they will use it. When there is no trust in the system, the doctors will not use the system.</td>
<td></td>
</tr>
<tr>
<td>Trust in the System</td>
<td>Citizens agree with the system</td>
<td>When the citizens trust the system they will participate in the system. When they do not trust the system they will not participate.</td>
<td></td>
</tr>
<tr>
<td>Financially Sound</td>
<td>Citizens agree with the system</td>
<td>When the system is financially sound, the citizens accept the system better. When the system is not financially sound they will have a lower acceptance level.</td>
<td></td>
</tr>
<tr>
<td>Doctors agree with the system</td>
<td>Successful implementation</td>
<td>When the doctors agree with the system, a successful implementation is possible. When they do not agree, no successful implementation is possible as the doctors will not use the system.</td>
<td></td>
</tr>
<tr>
<td>Citizens agree with the system</td>
<td>Successful implementation</td>
<td>When the citizens agree with the system, a successful implementation is possible. When they do not agree, no successful implementation is possible as they will not participate.</td>
<td></td>
</tr>
</tbody>
</table>

*Table 22 Explanation of the Arrows*