Caring for security:

an analysis of the security of eHealth services of Dutch General Practitioners

Master Thesis Cyber Security

David Willems (student S1727427)

Supervised by dr. B. van der Berg (1st) and prof. dr. ir. J. van den Berg (2nd)

Abstract

The use of information and communication technology within healthcare is called eHealth. The government and professional organisations within the healthcare sector are stimulating the adoption of modern healthcare services over the internet. General Practitioners (GPs) have adopted eHealth and are providing services for signing up and for requesting repeat prescriptions online. eHealth services of GPs process sensitive personal data and therefore security measures must be implemented to protect this data against malicious actors while transported over computer networks. To protect personal data during transport over untrusted networks the technology HTTPS is used. The support of HTTPS on a website relies on the correct implementation of TLS on the webserver. There are several versions of TLS and a number of these versions are not considered to be secure to protect personal data anymore. TLS implementations must be configured correctly to protect personal data adequately. Guidelines for correctly configuring TLS implementations have been published by the Dutch Cyber Security Centre. The Dutch Privacy Authority has referred to these guidelines in their publications for technical guidance. For this thesis a sample of 368 Dutch GPs has been researched to identify eHealth services for signing up and for requesting repeat prescriptions. The identified services have been tested on 12 TLS implementation aspects with support of internet.nl. This research concludes that 33% of GPs with a website provided the option to sign up online and 56% provided the option to request repeat prescriptions online. Further this research concludes that 2/3 of the eHealth services were hosted by a selection of 7 Application Service Providers and 1/3 by other hosters. Overall the results based on the sample show that ASPs scored high on the TLS tests but there was still room for improvement. The ASPs scored low on supporting HSTS and not supporting client initiated renegotiation. The remaining hosted services within the sample overall scored significantly lower and unfortunately in 2016 over 6% of the eHealth services provided by other hosters did not implement TLS and therefore did not support HTTPS to protect the personal data of patients. Based on several publications of the DPA this thesis concludes that these services violated the Dutch privacy law. Interviews held with a selection of ASPs showed that centralised guidance on cybersecurity within the eHealth sector is lacking and this thesis therefore advices to organise the flow of cyber security related guidelines within the sector.

Acknowledgements

This master thesis is the crown on top of my working and educational life up to now. I could have never achieved this without the help of great people who supported me during this process. My wife, Helene, supported me in my educational and career steps over the last 19 years. She supported me during my career change from electronics to ICT and cyber security and my change from a technical expert to a manager. All the hours I spent away from home and behind my computer she kept our household running like a smooth machine. Her strength and dedication to maintain a healthy life for our family and herself, while also having a fulltime job, is admirable. Many times, she spent a tremendous amount of her time supporting our children with their schoolwork and brought them to their sport clubs while I was studying, writing and working. It would have been impossible for me to achieve all this without her support, personal strength and her reflection on periods in my life. Helene, thank you so much!

I also thank my employer for their support during this study. Without the support of my employer and all the great people that I work with daily, I could have never achieved this goal.

Finally, I want to thank the Cyber Security Academy and specifically Bibi van den Berg and Jan van den Berg for broadening my view on cyber security, the great discussions we had and supervising me during the creation of this thesis.

Thank you all very much for your support!

Table of Contents

Chapter 1

Introduction

1 Introduction

1.1 Introduction

Cyberspace has created new possibilities for people to interact with their friends and organisations all over the world. Cyberspace has made it possible to communicate and exchange information anywhere and anytime. Nowadays people can make use of the possibilities of cyberspace at home, during work and while travelling and waiting. Modern internet devices (such as smartphones, tablets and laptops) can be used to access a broad variety of online services whenever an internet connection is available. The options for making connections to the internet are broad. Internet access is available over wireless networks (such as 4G and Wi-Fi) and over wired network connections. The internet has become commodity. Nowadays people often do not have to pay for internet access. Free internet access is available at hotels, in public transport and at coffee shops. This societal change because of the adoption of cyberspace makes it possible for people to interact with friends and organisations any time and at any place. Cyberspace has widely been adopted by people and organisations. In 2015 only a minority of the Dutch population over 12 years (8%) had never made use of the internet[1]. In 2013 the use of governmental websites by citizens of the Netherlands was higher than the European average. Almost 80% of Dutch citizens used online services of the government and this use had outgrown traditional forms of communication[2]. This strong adoption of the internet has created opportunities for organisations to make use of the internet for their business goals and to provide information about their organisation and their services online. Existing online web services of an organisation can be expanded and can be used to provide products and services to customers directly over the internet. Regular channels for selling products have already partly moved to the internet. People watch television online, buy clothes online and communicate online. Using the internet has become part of our everyday world.

Among the organisations that have adopted cyberspace are healthcare organisations. These organisations provide websites to patients and provide health services over the internet. Health services which are provided online are so called “electronic Health” (eHealth) services. The term eHealth is related to the broad use of Information and Communication Technology (ICT) within healthcare to support and improve health services[3].The Dutch government is stimulating[4] the adoption of eHealth within healthcare and has defined ambitions which are based on the adoption of the internet to provide services to patients. Stimulating the adoption of eHealth has also been part of the European Union ambitions[5] for at least since 2004. The adoption of eHealth however does not only create advantages for healthcare. The use of internet technology as a building block for services also involves adopting cyber security risks, which in this context become relevant to healthcare services. One specific category of cyber security risks are the risks related to the compromise and misuse of personal data. When eHealth services require users to provide personal data for the service, this data then has to travel through many computer systems and networks before it gets delivered at the destination computer

system[6]. The internet is not owned or controlled by a single organisation. Many organisations play a role in keeping the internet infrastructure up and running. Data transported between computers connected to the internet must travel through digital systems of several organisations. This fundamental design of the internet creates opportunities for malicious actors. Information sent over computer networks can be intercepted and misused by malicious actors that have access to parts of this digital infrastructure. The 2016 Cyber Security Assessment of the Dutch National Cyber Security Centre (NCSC)[7] states that theft of personal data Is interesting for several malicious actors. The use of the internet for health services creates (new) opportunities for such malicious actors. Medical and personal data which is exchanged over the internet for eHealth services is interesting for malicious actors because such data is worth money. In 2014 Reuters published an article referring to a FBI article warning healthcare organisations to protect themselves against cyber attackers because their systems are more vulnerable than systems of other companies, the article stated; *"Health data is far more valuable to hackers on the black market than credit card numbers because it tends to contain details that can be used to access bank accounts or obtain prescriptions for controlled substances"* [8, para 2]. The article describes the strong interest for medical data among criminals and states that the digital resilience of the healthcare sector is staying behind. In that same year, a second article on the Reuters website described the value of medical data to criminals. The article stated; *"Your medical information is worth 10 times more than your credit card number on the black market"* [9, para 1]. This article describes that the attacks on the healthcare sector are increasing because of the value of healthcare information. The article further states that systems used in healthcare are outdated and insecure. In August of 2016 an article was published on the website of modern healthcare. This article provides argumentation why healthcare data is so interesting to malicious actors. The article stated; *"Criminals regard healthcare records as more valuable than credit card records because their data elements, such as birth dates, addresses and Social Security numbers, can't be readily changed"* [10, para 15]. These publications illustrate the privacy related risks to digitalized healthcare services and the necessity to adequately protect personal data processed within these systems. The risks related to digitalized healthcare services becomes even more clear when cyber security related incidents occur. The disruption of a network infrastructure of a Dutch eHealth system[11], which was used by 2500 GPs and 900 pharmacies, led to the situation that medical specialists had no access to their patient system and could not administrate their healthcare actions. In 2016 an incorrectly secured webserver[12] resulted in a data breach of patient data of three Dutch hospitals which had to report the incident to the Dutch Privacy Authority (DPA) and risked receiving a fine. These examples illustrate why cyber security within the eHealth domain must be an important field of attention.

General Practitioners (GPs) are part of the healthcare domain. They provide eHealth services to their patients which are mostly used to digitalise the communication between an GP and their patients[13]. The most known eHealth service of GPs in the Netherlands is the service to request repeat prescriptions online[14]. Patients can visit the website of their GP over the internet and request their repeat prescriptions on their internet connected devices. These eHealth services are available 24 hours a day, 7 days a week from any location in the world where

an internet connection is available. As stated in the Dutch eHealth progress report[15] GPs are increasingly providing these services. This report states that 3/4 of Dutch GPs provided the option to request repeat prescriptions online and that 70% of the GPs (which provide this eHealth service) received online repeat prescriptions daily. Such eHealth services can be provided by the GP with the use of web forms[16]. This same technology can also be used to provide an eHealth service to sign up as a new patient online. When patients request repeat prescriptions, or sign up online, they must provide sensitive personal data (such as medical data) over the internet. The Dutch regulation states[17] [18] that this type of personal data (medical data and social security numbers) is considered to be a special category of personal data for which extra strong rules apply. It is forbidden to process this personal data, but an exception is made for healthcare providers who have the legal basis to process this data and also have the responsibility to protect this personal data adequality. When repeat prescriptions are requested online, personal data is transported over the internet from the patient's device to the destination computer system of the GP which hosts the eHealth service. During this transport a malicious actor may try to intercept and misuse this personal data when this is not adequately protected.

The adoption of eHealth services by healthcare providers and patients results in personal data being transported over the internet. This personal data must be protected adequately against malicious actors. GPs have the responsibility to implement adequate technical measures to protect the personal data of their patients. This raises the question to what extent GPs have correctly implemented the technical measures to protect this personal data of their patients online. The research question central in this thesis therefore was;

To what extent do eHealth services of Dutch GPs comply with existing security guidelines and what is a possible strategy to improve security?

The scope of this research

The scope of this research was narrowed down to make the research feasible. The scope was limited to the more than 8000 GPs active in the Dutch healthcare sector[19]. In 2016 75% of these GPs provided[15] the eHealth service to their patients to request repeat prescriptions online. The scope of this research was narrowed down to the webservers which hosted these repeat prescription services and the additional service to sign up online because both of these eHealth services require patients to provide personal data over the internet. Based on the number of GPs in the Netherlands and the adoption of the repeat prescription service, it was expected upfront that thousands of these web forms would be online. In terms of security the scope of the research was also narrowed down. Security is a very broad definition and may refer to a wide scale of technical measures to protect personal data online. The scope of the security research conducted for this thesis was the technology which is used to protect personal data during its transport over the internet between the eHealth system of the GP and the device of the patient. The scope for this thesis therefore was the most used technology to encrypt data

online: Transport Layer Security (TLS)[20]. The correct implementation of TLS on a website enables the use of encryption which enables Hyper Text Transfer Protocol Secure (HTTPS)[21]. The support of HTTPS on a website protects the personal data of patients while transported over the internet against malicious interception and misuse. For this thesis, overall the scope was narrowed down to the correct implementation of TLS on webservers for requesting repeat prescriptions and the webservers used for signing up of GPs in the Netherlands.

1.2 Research Methodology

To answer the research question, several research methods were used. Literature research was conducted to gather information on the definition of eHealth and the ambitions of eHealth adoption. The library of the university of Leiden was used to find recent research on TLS implementations on GP web forms. No previous publications regarding such research was found. For this research, online published information of governmental organisations and professional organisations within the healthcare sector provided most the required input for this thesis. Publications of governmental organisations provided information regarding privacy legislation and guidelines related to implementing TLS correctly. Publications of professional organisations active within the Dutch healthcare sector provided some insight into the guidance on security by professional healthcare organisations which play a role in supporting GPs. Technical publications of organisations such as the Internet Engineering Task Force (IETF) (which is the acting body for the development of TLS) were used as a source of information on the current state of TLS technology.

Online quantitative research was performed to investigate how TLS implementations were configured. Chapter 3 describes the detailed steps that were taken for this quantitative research. The starting point for the online eHealth research was a sample of GP websites. The online list of general practices on the website www.zorgkaartnederland.nl[22] was used to create the required sample for the online research. A sample of 368 GPs was used for the online research. All websites of these GPs were visited with a Google Chrome browser to identify web based services for signing up as a new patient and for requesting repeat prescriptions. All identified data was collected in a spreadsheet for further analysis and was used as the basis for an online TLS scan. This online scan was conducted by internet.nl[23] which was provided the dataset for this scan and tested the TLS configuration of the webservers hosting these web pages. The results were added to the spreadsheet and used for the further quantitative analysis.

To gain information on the governance of the TLS implementations of Application Service Providers (ASPs), 7 ASPs were contacted and asked to contribute to this research. Unfortunately not all organisations participated and in total 4 ASPs provided input during an interview by phone which was structured along 7 questions.

1.3 Document structure

This paragraph describes the structure of this thesis. The 1st chapter, this chapter, introduces the topic eHealth, online services of GPs, the research question, the scope and the methodology used for this research. The 2nd chapter describes the eHealth landscape and further describes the role of TLS in the online security of eHealth services. This 2nd chapter further describes the relevant privacy regulation and guidelines related to TLS. The 3rd chapter describes the methodology which was used for the quantitative online research. The 4th chapter contains the results of the online research and the results from interviews. The final chapter, chapter 5, discusses the research results and answers the research question.

Chapter 2

The eHealth landscape

2 The eHealth landscape

This chapter describes the domain of eHealth and the online eHealth services of a GP. Furthermore this chapter describes the use of websites by GPs for eHealth services and how TLS technology helps to protect personal data online. This chapter also describes relevant Dutch privacy regulation and security guidelines. This chapter ends with a description of the identified problem and introduces a conceptualisation of cyberspace which is used to discuss the results in chapter 5.

What is eHealth?

The term eHealth has been used in relation to health services for several years. Research performed in 2005 by Claudia Pagliari et al. concluded[24] that the term eHealth was used for the first time in the year 2000. The background section of the research paper states that there was; *"Lack of consensus on the meaning of eHealth has led to uncertainty among academics, policymakers, providers and consumers"* [24, para 1]. In that research numerous publications were examined to determine what the term eHealth meant. The research concluded that two definitions used in literature described the term eHealth best. The first definition of eHealth was based of the definition of G. Eysenbach, who stated that; *"e-health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology."* [25, para 4]. The second definition which most resembles the Dutch definition used by Zorginstituut Nederland (ZN)[3], Nictiz[26] and the Royal Dutch Medical Association (KNMG)[27] is the definition of Thomas R. Eng. This definition describes eHealth as; *"e-health is the use of emerging information and communications technology, especially the Internet, to improve or enable health and healthcare"*[24, para 37]. This broad definition of Thomas R. Eng. defines the use of any Information and Communications Technology (ICT) within healthcare, within the scope of the term eHealth. This means that eHealth can relate to a broad scale of digital technology within healthcare. Examples for this definition are patient web portals, digital blood pressure monitors, remote surgery, remote consultation and so on and so forth. A publication of the European Commission (EC) of 2009[28] defines eHealth as "*all medical healthcare services and technology relying on modern information and communication technology (ICT)"*[28, p1] this again resembles the broad definition of the term eHealth. An example of eHealth services mentioned in this EU publication are; *"National and regional healthcare information networks and electronic record systems, including information systems for healthcare professionals and hospitals, online services such as electronic prescriptions, databases used for patient care, research and public health, health related portals and online health promotion services"*[28, p1]. To summarise this exploration of this definition of eHealth; the term eHealth relates to the use of ICT within healthcare which

enables health care services. Providing health services over the internet for requesting repeat prescriptions or for signing up by a GP fit within the scope of this definition.

eHealth within the Netherlands

In 2014 the Dutch minister for health, welfare and sport, defined three eHealth ambitions which rely on the functioning of internet[29] for five years. These three eHealth ambitions have been placed on the agenda of the Convenant Governance eHealth 2014-2019[30] which was ratified by six organisations. These six organisations were; Kwaliteitsinstituut (KI), Nederlandse Consumenten Patiëntenfederatie (NCPF), Nictiz, Vereniging van Zorgaanbieders Voor Zorgcommunicatie (VZVZ) and Zorgverzekeraars Nederland (ZVN). These organisations are further described in APPENDIX I. In June of 2016 the Dutch government announced[31] that 20 million euros would be available for national eHealth initiatives. During the Dutch presidency of the European Union in 2016 the government organised an eHealth week[32] where stakeholders could share their eHealth ambitions and solutions with stakeholders and take notice of funding opportunities of the Dutch government[33]. In 2014 the Dutch government reported[34] about the progress of eHealth adoption within the Netherlands. The publication stated that in 2014, 13% of health care users had the ability to make appointments online with their GP and 30% of health care users had the ability to request repeat prescriptions online. In all eHealth domains described, the adoption of eHealth increased. This publication refers to yearly conducted research by Nictiz[35] which is commissioned by the Dutch Ministry of health, welfare and sport. Their eHealth monitor of 2015 stated[14] that requesting repeat prescriptions online was the most known service which was used by 15% of care users. The eHealth monitor further described that over the period 2014-2015 the use of these services did not increase but also stated 2 out of 5 health care users would like to use such services. This publication advised to focus on three most promising eHealth services (translated by author); "(1)Online services for healthcare users, such as making appointments, e-consulting, requesting repeat prescriptions and access to medical records over the internet (2)Electronic exchange of information between healthcare providers (3)Healthcare services with use of (computer) screens."[14, p13] The first and last of these eHealth services rely on the correct functioning of the internet to transport personal data between patients and health care providers.

Beside the organisations mentioned up to this point, 2 organisations specifically seem to play a role in the domain of GPs providing eHealth services. The adoption of eHealth within the GP practice is stimulated[36] by the Nederlandse Huisartsen Genootschap (NHG) which published[13] an eHealth document for GPs. The NHG defined 4 domains of eHealth services which all relate to the use of internet to exchange information with patients. The position of the NHG also mentions that safeguards for privacy and confidentiality must be part of these eHealth solutions and stated that that general norms for safeguarding privacy must be taken into account. Together with the NHG the Landelijke Huisartsen Vereniging (LHV), which is the professional association for general practitioners in the Netherlands[37], published[38] their future plan for GP care. This plan states that websites of GPs will develop to health portals for patients. A number of eHealth services are mentioned in this

plan. Examples used are eHealth services for making appointments, e-consulting and access to medical lab results which must become accessible over secure connections. This plan however also provides some critique in relation the adoption of eHealth. It states that the actual proof of the advantages as a result of eHealth is staying behind.

In 2013 the LHV published[39] an article on their website regarding previous conducted security research of repeat prescription services. In this article the LHV referred to research which was performed by the Dutch Privacy Authority (the Autoriteit Persoonsgegevens) (DPA) in 2013[40] which stated that 28 percent of repeat prescription web forms of GPs were not secured with HTTPS and that these GPs violated Dutch privacy legislation. The LHV stated that ICT security was one of the main priorities of the LHV. During the research for this thesis it was however noticed that the service page of the LHV did not mention[41] ICT security as a specific topic on their website. In December of 2015 the LHV published[42] an article on their website related to the Dutch data breach notification which came in effect in 2016. It stated that GPs must comply with this data breach notification law and advised GPs to contact their service provider to check whether they comply with applicable security guidelines. The article refers to the website of the KNMG for guidance on information security. This website mentions that the NEN7510 and NEN7513 provide more detailed information. Further the LHV advised GPs to check their contract in relation to responsibility and accountability. For this thesis the website of the LHV and NHG were further examined for technical information related to cyber security measures but no publications were found which provided technical guidance on securing the eHealth services of GPs. During the eHealth week of 2016 an interesting initiative however was launched called “Medmij”[43] in which the NHG and LHV participate. MedMij is a program which is coordinated by Patiëntenfederatie and the Ministry for health, welfare and sport. Within the steering committee a number of organisations take place, such as the NHG, LHV, ZN and Nictiz. The website of MedMij states that the goal of MedMij is to create guidelines (including information security related guidelines) for the exchange of health care data within personal health care environments which are used by patients. A specific goal of MedMij is to make the security of online health care environments transparent to patients by placing a logo on the website. This exploration of the eHealth domain shows that many organisations have a role in the domain of eHealth. Two organisations specifically seem to have a role in providing guidance to GPs, the LHV and NHG. Finally, the adoption of eHealth is also stimulated by patients. Patients want to make use of such online services[44].

2.1 General Practitioners and eHealth security

In the Netherlands GPs fulfil an important role as the gatekeeper of the healthcare system[45] which is described as one of the underlying factors of the success of the Dutch medical system. When patients need medical advice or treatment they must first consult their GP to get access to other services of the healthcare system. The most recent found publication on GP statistics[19] states that in the Netherlands 8.812 GPs worked at 5.068 general

practices, each general practice served 2.168 patients and provided 8.882 consultations per year. This publication also stated that all citizens (99,9997%) are a registered patient of a GP. Patients often make use of the services of their GP. In 2012 over 70% of Dutch citizens consulted their GP at least once a year[46]. A quick calculation concludes that these GPs together roughly provide 45.000.000 consultations per year. These consultations require the exchange of medical data. The way how patients can interact with their GP has changed over time. Traditionally used channels for their interaction with their GP are not always required anymore because of the abilities of cyberspace. The Council for Health and Society expects[47] that communication between medical professionals and their patients will increasingly take place over other media than telephone and face to face interaction in the future.

In their eHealth monitor of 2015 Nictiz concluded that online services for patients such as requesting repeat prescriptions online was one of the most promising eHealth services. Their 2016[15] report stated that the ability to request repeat prescriptions online at a GP had increased from 66% to 75%. To further increase the adoption among patients the 2016 report of Nictiz advices to stimulate the adoption of eHealth by bringing eHealth services to the attention of patients. To illustrate the magnitude of the domain of medical prescriptions, a publication of Medisch Contact[48] provided some insight. In 2015 the total amount of prescriptions processed by Dutch pharmacies was 240.000.000 of which a part was prescribed by GPs. If the adoption of eHealth increases over time, the amount of repeat prescriptions transported over the internet will also increase. This sensitive information of patients must be secured adequately.

When GPs choose to set up eHealth services for requesting repeat prescriptions and for signing up online, they must choose how to technically provide the digital service. A GP may choose to publish his/her e-mail address online so that patients can send an e-mail with their prescription request. But this solution introduces a security risk. Regular e-mail can be considered to be a digital alternative to a postcard[49] which can be read by anyone who has access to the message during transport. Therefore regular e-mail should not be used to send medical data over the internet. There are secure e-mail alternatives, but adopting encrypted e-mail introduces a new problem. Using secure e-mail is complicated. Research[50] performed by Scott Ruoti et al. (for which people were asked to set up a modern secure e-mail computer program) concluded that the use of encrypted e-mail technology is too complex to be adopted by the general public. A different option to provide eHealth services is with the use of a website. Almost each organisation already has a website online and can be found on the internet with help of a search engine. These websites can be used to provide general information about an organisation and its services, but these websites can also be used to provide services and products to consumers directly over the internet. The adoption of these so called e-shopping services has steadily increased over the past years[51]. When a GP practice (practice) already makes use of a website, this website can be used to provide general information about the practice itself (such as the address information, holiday plans and opening hours), but this same website can also be expanded to provide online eHealth services. This can be realised with the use of web

forms on that same website. Nictiz has stated[49] that the use of web pages for providing such online services is considered to be a more future proof technical solution than the use of secure e-mail. Nictiz stated that the advantages compared to the use of e-mail are the presence of less vulnerabilities and the ability to automatically process the provided information. From a technical perspective, publishing a webform on a website is quite easy and can be set-up by a professional in just a few hours. A search with the Google search engine with the search query “create web form in minutes” provides a long list of results for creating web forms in a short amount of time. However it must be realised that from the perspective of protecting personal data a very large change is made when the functionality of an existing GP web site is expanded to also provide eHealth services. Suddenly the same computer system processes sensitive personal data. With this functional change the system now must be capable of protecting sensitive personal data against interception by malicious actors. With this minor technical change, suddenly privacy legislation for processing personal data online becomes relevant to the system of a GP. This means that technical security measures must be able to protect the personal data processed on that system and secure the transport of data over the internet. This concludes that adding a web form for eHealth services on an existing website of a practice requires cyber security expertise to adequately protect personal data of patients online.

Web forms

So what are web forms and how can these be used by GPs for eHealth services? Looking from a functional perspective a web form is the digital alternative to a paper form which must be filled in to receive a service. A web form is hosted on a web server and can be accessed over the internet with an internet browser. The browser presents the web form to the user who then has to provide the required information. From the perspective of an organisation, the use of web forms is very convenient because it reduces paper administration and labour for entering the information from a paper form into a computer. When a practice provides eHealth services online based on web forms, the patient visits the web page of the practice with a web browser on their device and provides the required information for that health service over the internet. Requesting repeat prescriptions and signing up online requires patients to provide a large amount of sensitive personal data. This is illustrated by the amount of information that is required to provide on the two GP forms in *figure 1* and *figure 2.* In some cases the web form will be only presented after the authentication of the patient. This situation occurs when web portals are used to provide eHealth services.

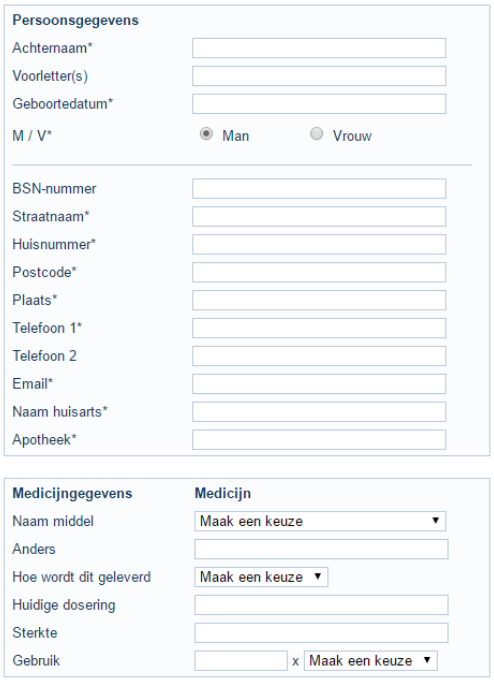


Figure 1; a web form for requesting repeat prescriptions (Source:https://dedrieweg.hvdeb.nl/Online_regelen/Formulieren_Heinkenszand/Herhaalrecepten)

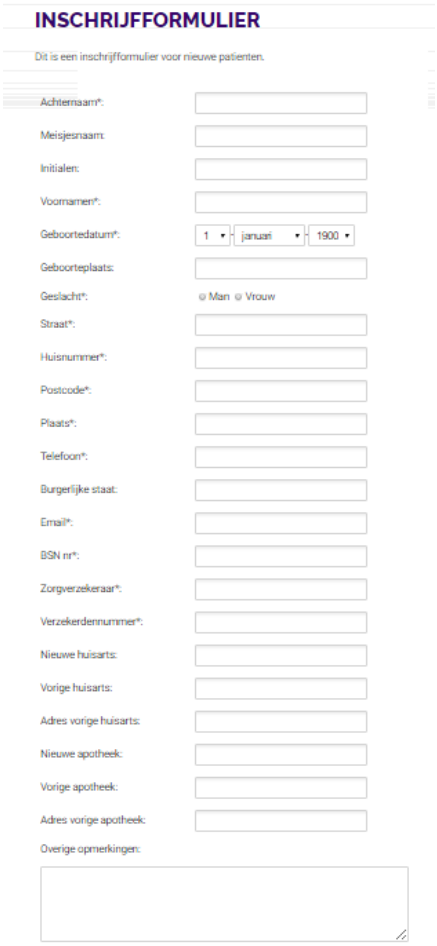


Figure 2; a web form for signing up online (Source: https://huisartsenhelvoirt.praktijkinfo.nl/modules/inschrijfformulier.php)

These two web forms illustrate the amount of personal data which must be provided over the internet to request repeat prescriptions and to sign up online. In addition to the patient's name and address these web forms instruct the patient to provide additional sensitive information such as a medical data, social security information and insurance details. One advantage of the use of web forms by GPs is that the computer system can directly provide feedback on the input when the data is provided by the patient. The system can automatically check if all required information is provided and can reject not correctly filled in forms. The system then notifies the patient what information is missing or is entered in an incorrect format (such as a postal code format which has a specific syntax) and refuses to process the information until all information is provided correctly. This provides an advantage to the GP because only completely correct filled in forms are received. But the use of web forms also introduces a risk. When the web form provides the option to voluntary provide additional data (the entry boxes without the *), such as the pharmacy information in *figure 2*, the patient might just provide all information without thinking of the risks related to sending all this personal information over the internet. When the patient provides the information online, the device of the patient sends the entered information over the internet to the

web server hosting the web forms. To illustrate how personal data is transported from the user's device to the GP practice, a simplified illustration of such a network connection is provided in *figure 3*.

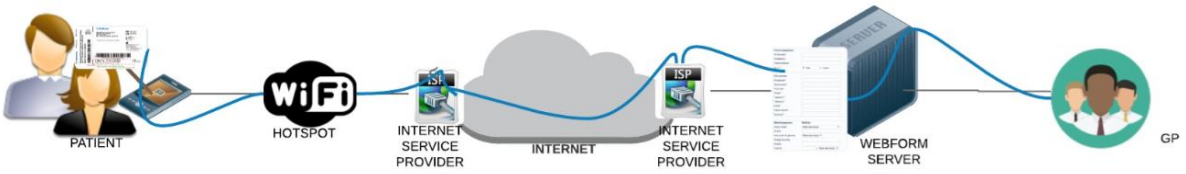


Figure 3; How personal data travels over the internet from a patient to a GP

Figure 3 illustrates how the personal data (the blue line) of a patient travels from the user device to the GP over computer networks. In this scenario the patient uses his/her internet device to connect to the internet via a hotspot and opens the web form or portal of the GP. The patient fills in the web form and the provided data is then transported from the patient's device, via the hotspot, to the internet service provider (ISP). Next the personal data travels over the public internet infrastructure to the ISP of the GP which delivers the data to the web form server. The GP then receives the data and then is able to provide the eHealth service to the patient. Nor the patient or the GP, has control over the internet infrastructure which is used between the patient and the practice. Both make use of (publicly) provided internet services. The internet itself is not an isolated infrastructure, it consists of several systems[6] which are owned and managed by numerous organisations other than the GP and the patient. Because both the GP and the patient have no control over this infrastructure this connection cannot be trusted and the personal data sent from the patient to the GP must be protected against interception and misuse by malicious actors.

Securing web page traffic

Data transport over the internet between a user and a website is not secured by default. The protocol to transport website content over the internet is Hyper Text Transfer Protocol (HTTP), "*HTTP is the foundation of data communication for the World Wide Web*"[52, para 1]. HTTP does not provide any form of confidentiality of transmitted information. Internet browsers which support the HTTP protocol (such as Google Chrome and Mozilla Firefox) send so called HTTP requests to a webserver and receive the webpage content over computer networks[53] (such as the internet) and then present the webpage to the user. There are many protocols and technological devices involved in transporting the data to (and from) a webserver over the internet. How this works in detail is outside the scope of this thesis. When a user wants to access a webpage on their device, the user enters "http://" in their browser, followed by the website address that they would like to access, such as "http://www.csacademy.nl". After entering this so called Uniform Resource Locater (URL)[54] the browser connects to the webserver and presents the website to the user. Modern browsers do not require the user to enter "HTTP://" in their browser anymore. Users can directly enter the website address, such as "www.csacademy.nl", and view the webpage. The browser automatically uses the HTTP protocol to connect to

the webpage server. As stated before; a problem of the HTTP protocol is that it does not provide any form of confidentiality of the information transported over the network. The data within a HTTP session can be read when it is intercepted during transport. In the scenario of a patient using the eHealth service of their GP, this interception may take place anywhere in the communication chain. This personal data could be intercepted at the hotspot, at the ISP, at the GP office and anywhere else within the internet infrastructure. This introduces a privacy risk to personal data of patients. One of the attack vectors for intercepting personal data is described by the NCSC in their factsheet[55] related to the use of public Wi-Fi. The factsheet states that it is very easy to intercept and read Wi-Fi traffic which can lead to the compromise of information (such as login credentials). This attack vector also applies to personal data which is entered in a web form of a GP. This means that personal data sent between a patient and the webserver of GP may be incepted, read and misused by a malicious actor intercepting Wi-Fi signals. *Figure 4* provides a visualisation of an insecure HTTP session between a patient and a GP web server and the interception by a malicious actor.

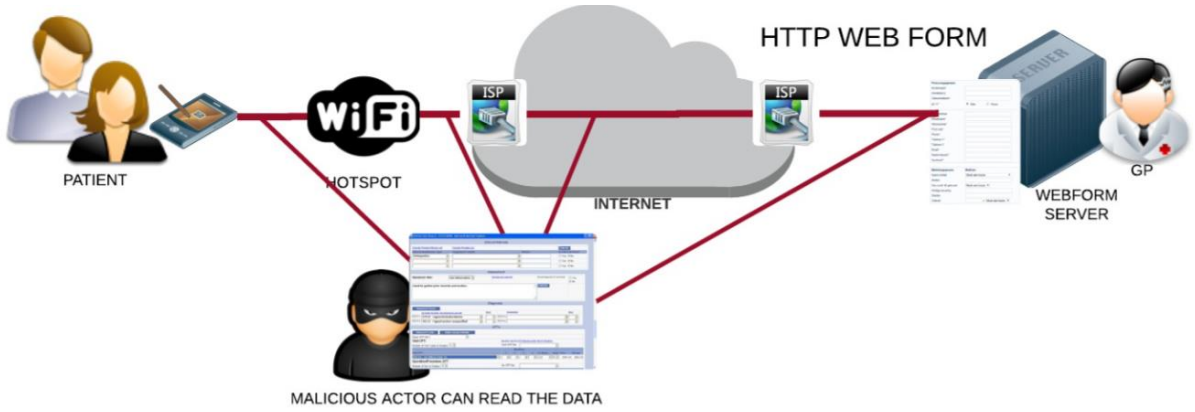


Figure 4; How personal data can be intercepted and read by a malicious actor when HTTP is used

Because there is risk that a malicious actor compromises personal data of patients when HTTP eHealth services are used, this personal data must be protected with security measures which are described next.

Hyper Text Transfer Protocol Secure

The technology used to secure the content of HTTP data is Hyper Text Transfer Protocol Secure (HTTPS)[21]. The use of HTTPS on websites has increased rapidly over the past years, the availability of HTTPS on websites has doubled in the period 2015-2016[56]. To protect personal data sent to web forms of GPs this protocol must be implemented. The importance of the use of HTTPS has been acknowledged by Google. Google announced[57] that (starting from 2017) HTTP pages which collect passwords or credit cards will be marked as “insecure” and users will be notified that the website is “not secure”. This shows the push of large internet organisations to stimulate the adoption of HTTPS on websites which process sensitive information. The technology required for HTTPS support on a website is the most used technology to encrypt traffic over the internet: Transport Layer

Security (TLS)[20]. The correct implementation of TLS on a webserver creates an encrypted tunnel over the internet which can be used by server applications (for example; e-mail and webservers). TLS secures the data transported between the user and the server. TLS will be described next.

Transport Layer Security (TLS)

Encryption technology used to secure transport of data over the internet has been around for a long time. The predecessor of TLS, Secure Sockets Layer (SSL), was invented by Netscape Communications in the early 90s[58]. SSL became the de-facto standard technology to encrypt data sent over the internet. Three versions of SSL have been created over time; Version 1.0, 2.0 and 3.0. From version 3.1 and onward this technology was provided with a new name; Transport Layer Security. The first version of TLS, version 1.0, is identical to SSL version 3.1. The Internet Engineering Task Force (IETF) (who has been responsible for the development of TLS) describes TLS as; "*The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications*"[59, para 1] In other words, TLS protects information sent over computer networks against malicious adversaries reading the data and makes sure that information is not tampered with during transport. The IETF adopted the first version of TLS in 1999 and in 2008 the IETF published[59] the latest version of TLS (version 1.2) in RFC5246. Currently the IETF is working on TLS version 1.3 of which a concept was published[60] in October of 2016. Encryption technology is under continuous development because over time the strength of encryption technology decays. Technological advance and the discovery of vulnerabilities make protocols less strong which then can be more easily be exploited by malicious actors. Therefore, the security community needs to keep improving this technology. The Open Web Application Security Project (OWASP), which is an internationally respected organisation for application security, published their transport layer protection cheat sheet, which states; "*Use TLS, as SSL is no longer considered usable for security"*[61, para 1]. In June of 2015 the IETF announced[62] that SSL version 3.0 was not sufficiently secure anymore to encrypt sensitive information. The versions SSL v1.0, v2.0 and v3.0 therefore should not be used anymore to protect personal data online. The underlying technology of TLS is based on a Public Key Infrastructure (PKI) and requires the implementation of digital certificates. This paper will not describe the technical details of TLS and the underlying PKI technology, there is a lot of literature available which describes the working of PKI and TLS in detail.

When TLS is implemented correctly on a webserver of a GP, the HTTPS protocol is used to protect the personal data of the patient using the eHealth service. Such a HTTPS connection is illustrated in *figure 5*. This figure shows that the browser of the patient contacts the web form server over the internet and a HTTPS connection is set up between the patient's browser and the web form server. The data transported between the locks in this figure (on the patient side and the webserver side) is encrypted with HTTPS. When such a HTTPS session is established, the malicious actor is not able to read the personal data in transit.

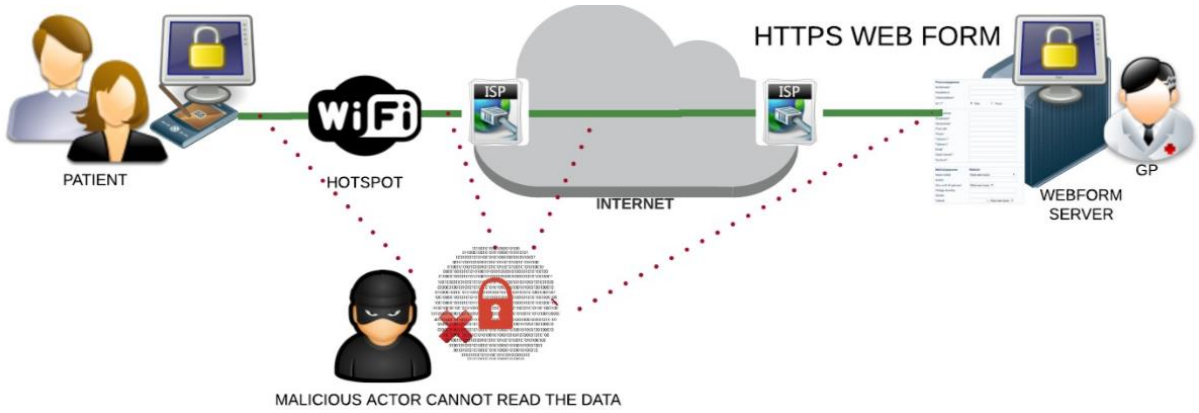


Figure 5; How personal data cannot be intercepted and read by a malicious actor when HTTPS is used

Correctly implementing TLS on a server supports more security measures than the encrypted transport of data alone. An additional advantage of the use of TLS is that it provides a chain of trust based on digital certificates which provides an assurance to a user that they are accessing the legitimate website and not a fake website. This thesis will not go into these technical details but to state it simple; Internet browsers contain a list of trusted certificate providers which are by default trusted. When the GP uses a certificate which is digitally signed by one of these trusted certificate providers, the certificate will be automatically trusted by the browser of the client. A patient visiting a eHealth website will then be provided with a visual notification (such as a green lock in browsers) which notifies the user that the connection is secured and that the website is trusted. Such visual notifications provide a level of assurance to patients that they are using a legitimate and secured website.

Hosting eHealth websites

When a GP decides to provide a website with eHealth services to patients, this website must be created and hosted on a web server. A GP with technical knowledge may choose to install a webserver him or herself and connect this system to the internet connection of their practice. In this case the GP will be responsible for setting up, securing and managing this webserver. This will not be feasible for all GPs. Not all GPs are an ICT specialist or have the time to manage their own eHealth systems. To reduce this overhead, the GP may choose to outsource the hosting of the eHealth website to a third party. Organisations which provides such services are so called Application Service Providers (ASP). ASPs can setup, host, manage and secure the website for the GP. The GP only has to provide the hoster the functional requirements and pay the bill. The adoption of eHealth services within the healthcare sector has therefore created business opportunities for (commercial) organisations. ASPs provide shared platforms for hosting the websites of multiple medical specialists. Such platforms are specifically crafted to provide services to healthcare providers. Sharing computer resources provides financial advantages to both GPs and ASPs. Besides this financial advantage, such a centralised service provides security management advantages because the security measures are also centralised. Centralised services can be secured more easily by the ASPs because measures only have to be correctly configured once for many customers. But at the same

time centralised systems introduce a higher risk when they become compromised[7]. These are incentives to secure such centralised services correctly. Two examples of Dutch ASPs which provide eHealth services for GPs are praktijkinfo.nl and huisarts.info. The website of huisarts.info states[63] that a GP can setup a website in 15 minutes and praktijkinfo.nl states[64] that it is possible to get a website online within two hours. Based on these publications it is therefore concluded that it is easy to setup a webpage with eHealth services by a GP. Because these shared platforms share their security resources this provides an advantage for the correct implementation of TLS. When for example, 100 GPs make use of the same server for their websites, only 1 correct TLS implementation (and one digital certificate) is required to secure the transported personal data of all the patients which connect to each of the 100 websites. When ASPs configure a centralised TLS implementation on their shared platform, the personal data of all patients connecting to the 100 GP websites will be secured with HTTPS. Such a centralised architecture is illustrated in *figure 6.*

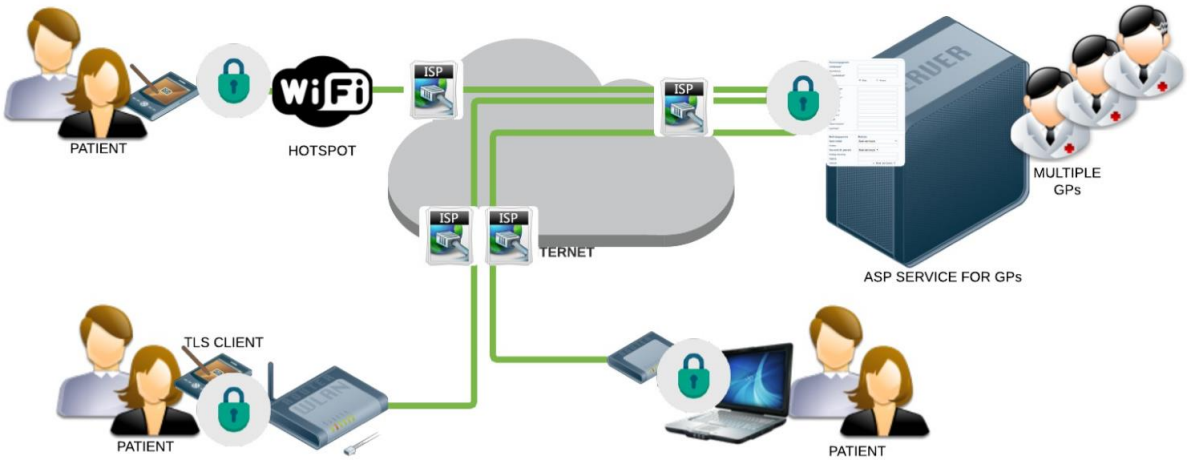


Figure 6; a TLS implementation on a shared platform of an ASP

The role of patients in security

So what is the role of the patient in securing their eHealth sessions? The adoption of mobile devices and mobile internet has rapidly increased over the past years and the use of tablets and smartphones is outgrowing the use of traditional desktop computers[65]. In 2015 91,4% of all Dutch households had access to the internet and 73% owned a mobile phone or smartphone, 72,2% owned a laptop/netbook and 58,1% of people owned a tablet[66]. The adoption of these (mostly wireless supporting) devices provide people the ability to use services whenever an internet connection is available. Internet access has become commodity, as normal as an electricity outlet. Hotels, trains, and restaurants provide internet access to their customers as a complementary service. The use of online shopping, navigation and news websites during travel has become part of people's daily lives. The availability of eHealth services of GPs has created new possibilities for these people. The adoption of mobile devices and the availability of the internet makes it possible for patients to access their GP services whenever

they want. They can make use of their GP services (such as requesting repeat prescriptions, signing up, e-consults etc.) wherever they are. In 2015 15% of healthcare users made use of an online repeat prescription service[67]. As stated before, these services must be secured with HTTPS to protect the personal data transported between a patient and the webserver. Research conducted by telecom paper in 2015[68] concluded that 41% of Dutch citizens make use of free public Wi-Fi. The use of public Wi-Fi for online services which process sensitive data introduces a risk because of the possible interception and misuse of this information. As a comparison, in May of 2014 the Dutch banks warned[69] consumers for risks related to the use of public Wi-Fi for online banking after a demonstrated "man in the middle attack" in a public hotspot environment. The publication of the banks described what measures consumers can take to protect themselves against malicious actors. The banks advised users to avoid online banking over free hotspots and when a browser is used to access the online banking environment to check if the connection is secured by inspecting the "green lock" in the browser. The actual effect of such an advice may however be degraded by actual behaviour of people. Research performed by the Brigham Young University[70] concludes that if security messages on computers pop up at a bad time that almost 90% of people ignore these messages and research performed for the campaign alert online[71] shows that 69% of Dutch people underestimate their chance of becoming a victim of cybercrime. In other words, the actual contribution of patients in securing their online activities may be limited. One of the additional measures banks introduced to improve the security of their online banking environment against "man in the middle attacks" is the implementation of HTTP Strict Transport Security (HSTS) on their webserver. Implementation of HSTS is an effective measure against man in the middle attacks[72] and the NCSC advices to implement[73] this technology to protect sensitive data online. HSTS will be explained in more detail in paragraph 2.2.

To summarise this paragraph; GPs provide eHealth services to patients online. Patients can request repeat prescriptions and sign up by filling in web forms on a server provided by the GP. To secure the personal data transported over the internet between the GP and the patient, HTTPS must be implemented. Otherwise personal data can be intercepted and misused by malicious actors. Implementing HTTPS requires an implementation of TLS on the eHealth webserver. There are many versions of TLS and not all versions are considered to be secure. Demonstrated attacks have revealed the possibility to intercept sensitive data in hotspot environments and banks responded with advice to consumers to preferably not to use public Wi-Fi for online banking and advised consumers to check the security of their internet connection. The role of patients in securing their own internet eHealth activities is expected to be limited. This stipulates the responsibility of a GP to provide secure eHealth services to their patients and to implement TLS on their webserver correctly. When GPs do not manage their webserver themselves, and make use of an ASP, they must ask their ASP to implement TLS correctly

2.2 The Dutch privacy law and security guidelines related to TLS

When GPs provide eHealth services they must comply with law and regulation to protect the personal data of their patients. Dutch GPs must therefore comply with Dutch privacy regulation and take applicable security guidelines into account. This chapter describes the Dutch privacy legislation and describes publications of the DPA which provide insight to guidelines which are applicable for TLS implementations of GPs.

The privacy law

The protection of personal data is regulated by law within the European Union. This is regulated by the European Data Protection Directive 95/46/EC[74] which came into effect in 1995. In the Netherlands this European Directive was transposed into the Wet Bescherming Persoonsgegevens (Wbp)[75]. This law came into effect in 2001 and is the basis for the protection of personal data within the Netherlands. The Wbp is written in Dutch and no formal English translation of this law exists. Hendriks and James Legal Translations has created an English translation of the Wbp[76] which includes the amendments as in force at January 1st of 2016. This translation is line with the terminology used in the European Directive 95/45/EC. This translation by Hendrik and James Legal Translations was used as the source for the Wbp citations in this chapter.

To prevent problems which are the result of interpretations of the law the same definitions must be used by the government and organisations which must comply with the privacy law. Part 1 of the Wpb describes the definitions which are used in the Wbp. The first definition that requires a common understanding is the definition of *personal data*. The Wbp defines *personal data* as " *any information relating to an identified or identifiable natural person*" [75, p7]. This definition states that any piece of information which can be used to identify (directly or indirectly) a single natural person is personal data. An obvious type of personal data is a person's name. Knowledge of a person's name makes it possible to identify that specific natural person. Thus, a person's full name is personal data. The definition of personal data used in the Wbp however also includes a broader scope of information to be personal data because the Wbp states "*any information*" [75, p7]. This definition therefore also includes combinations of information which together can lead to the identification of a single natural person. An example is the combination of a postal code and a street number[77]. This combination of information also makes it possible to identify a single natural person without knowing the person's actual name. Within the perspective of healthcare data, a rare medical condition combined with a city of residence, can make it possible to identify a single natural person. Therefore such a combination of data is considered to be personal data within the context of the Wbp. Within the context of GPs providing eHealth services (such as requesting repeat prescriptions or signing up online) personal information must be provided by a patient which can be used to identify that specific natural person. This concludes that web sites used for requesting repeat prescriptions and for signing up require the patient to provide *personal data* online. A second question regarding the Wbp definitions that raises is; What does *processing* mean? The definition of *processing* is described in article 1 of the

Wbp. Processing personal data is described as; "*any operation or set of operations which is/are performed upon personal data, including in any case the collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data"* [75, p7]. eHealth services of GPs collect, store, disclose, transmit data and so on and so forth. This means that these eHealth services of GPs *process personal data* online.

Not all personal data has the same level of sensitivity. Specific types of personal data are defined to be more sensitive by law. Part 2 of the Wbp describes this type of personal data as "*special personal data*" [75, p12]. Section 16 of the Wbp describes what kind of personal data is considered to be special personal data, the Wbp states "*The processing of personal data relating to a person's religion or belief, race, political affinity, health, sex life and trade union membership is prohibited, subject to the provisions of this Division. The same applies to personal data concerning criminal law matters and personal data on unlawful or objectionable conduct in connection with a prohibition imposed in response to such conduct*." [75, p7]. In other words; medical data is *special personal data* and may not be processed. Section 21 of the Wbp describes exceptions to this restriction to processing *special personal data*. This section states; "*The prohibition on processing personal data relating to a person's health referred to in Section 16 does not apply if the processing is carried out by: a. healthcare providers, institutions or health care or social services facilities in so far as this is necessary for the proper treatment or care of the data subject or the management of the institution or professional practice concerned*" [75, p14]. This concludes that GPs may process personal data when this is necessary for providing their health care services. Another type of special personal data is the Dutch social security number (BSN) which healthcare providers are obliged to use by the government[78] [17].

So who is responsible for taking measures to protect personal data within eHealth services? The Wpb distinguishes two different roles in relation to the processing of personal data. There is a so called *controller*, this is the organisation with the legal basis to process the personal data and there is a *processor*. The *processor* is the entity which does the actual processing of the personal data on behalf of the controller. Within the context of a GP processing personal data; the GP is the *controller* and at the same time may be the *processor*. However, when the processing of personal data is outsourced to a third party (such as an ASP) this third party becomes the *processor*. The next question that raises in relation to the responsibilities while processing personal data online is; What are the required security measures and who is responsible for security when processing is outsourced to a third party, such as an ASP? Section 13 of the Wbp states that; *"The controller implements appropriate technical and organisational measures to protect personal data against loss or any unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures will guarantee a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. These measures also seek to prevent the unnecessary collection and further processing of personal data"* [75, p11]. In relation to outsourcing processing activities to a third party section 14 of the Wbp states that

"If the controller has processing of personal data carried out by a processor on his behalf, he will ensure that the latter provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and in respect of the report of a breach of security, referred to in Section 13, which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data processed by him. The controller will ensure compliance with those measures" [75, p12]. To summarize this analysis of the Wbp in the context of GPs providing eHealth services; a GP may outsource the processing of personal data to an ASP but must ensure that adequate measures are in place to protect the personal data. The GP is responsible that adequate security controls are in place to protect the personal data which is processed on behalf of him. This means that when a GP outsources the services to an ASP the GP must ensure that adequate technical measures are in place.

The Wbp does not describe the details of the actual technical measures which are required to protect personal data online, but describes the required technical measures in general terms. The Wbp states; "*The controller implements appropriate technical and organisational measures to protect personal data against loss or any unlawful forms of processing*" [75, p11]. The technical interpretation of this privacy law has been provided by the DPA. This authority has the task to oversee compliance of the Wpb and has the ability to conduct research related to the protection of personal data[79]. In 2013 the DPA published the "CBP richtsnoeren: Beveiliging van Persoonsgegevens[80] which describes the DPA's "interpretation" of the Wbp. The goal of this document is to function as the connection between the legal domain and the domain of information security. This is the same interpretation the DPA uses when conducting investigations related to compliancy of the Wbp. These guidelines refer to a number of standards such as the NEN 27001, NEN27002 and NEN7510. These DPA guidelines refer to the NCSC ICT security guidelines for web applications for details on securing web applications.

To summarise the Dutch privacy legislation in relation for processing personal data; GPs have a legal basis to process personal data and special personal data (medical data and BSN) for their eHealth services. GPs are responsible for ensuring that adequate security measures are in place to protect this personal data and are responsible for data processing when third parties are used for these services. The guidelines of the DPA refer to the ICT security guidelines for web applications of the NCSC for guidance on securing web applications.

Publications of the Dutch Privacy Authority related to securing personal data online

The DPA regularly publishes information on their website. Their yearly report over 2015 starts with an introduction which describes how protecting personal data has rapidly changed over the last five years[81] It states (translated by author) that "*People can impossibly escape from the enormous amount of digital trails of personal data they leave behind*"[81, p5] and "*personal data is becoming the new gold*" [81, p8]. In 2015 the protection of medical personal data was a focus point of the DPA because of the increased use of medical applications. Specifically in relation to GPs processing personal data in 2013 the DPA conducted a research[40]

on 150 websites of GPs and pharmacies which provided the option for requesting online prescriptions. The research concluded that 43 of the 150 researched websites did not make use of a HTTPS connection to protect personal data. The DPA concluded that these organisations which did not secure their connection with HTTPS violated the Wbp in relation to securing special personal data and that potentially 250.000 patients could have been affected. The DPA stated that security measures for protecting medical personal data must comply with the highest standards. This publication of the DPA referred to the NEN7512 and specifically stated that the ICT security guidelines for web applications of the NCSC are applicable[82]. In April of 2014 the DPA published an article which referred to a high impact vulnerability which was found in OpenSSL[83]. The NCSC published a factsheet for this specific vulnerability to which the DPA referred to for technical details[84]. In the article, the DPA stated that if organisations did not update their OpenSSL software to the latest version and did not replace their digital certificates, that they may not comply with Article 13 of the Wbp. In March of 2016 the DPA published an article[85] regarding an letter they had sent to physiotherapists related to securing their online web forms. The DPA stated that whenever the special category of personal data is processed the whole web application provided must be protected with HTTPS and the level of protective measures should be based on the NEN 7512:2015 and the NCSC ICT security guidelines for web applications. In relation to securing online communication these ICT security guidelines for web applications refer to the TLS guidelines of the NCSC for the configuration of TLS. On the first day of March of 2016 a new discovered vulnerability in SSLv2 was published[86]. Only three days later the DPA warned for the use of the vulnerable TLS version (SSLv2) and stated[87] that the TLS guidelines of the NCSC provide guidance for taking appropriate measures. In the same article the DPA stated that if implementations contain known vulnerabilities, these implementations possibly would not comply with article 13 of the Dutch Data Protection Law and stated that more sensitive personal data requires a higher level of protection. All these described DPA publications illustrate the continuous attention of the DPA for the adequate protection of personal data online and their strong advice to implement web applications and TLS configurations accordingly to the ICT security guidelines for web applications and the TLS guidelines of the NCSC.

Not complying to the Wpb can result in large consequences for an organisation. Since the beginning of 2016, The Netherlands has a data breach notification law[88] in place. A data breach may result in a fine of maximum EUR 820.000 or 10% of a company's annual turnover. Whenever a data breach leads to serious negative consequences for the protection of personal data or whenever there is a large change of a breach, companies must file a report to the DPA and risk the chance of receiving a fine. Vulnerabilities in the information infrastructure itself do not have to be reported to the DPA. But an unmitigated vulnerability can lead to a data breach. Based on the publications of the DPA it can also be concluded that using systems which contain known vulnerabilities may be a violation of the law. The policy guidelines of the DPA state[89] that a data breach of the category of special personal data generally must be reported to the DPA and that the persons affected generally must also be informed about the data breach. This means that when personal data processed on an eHealth service for requesting repeat prescriptions or for signing up is leaked, the GP must inform the DPA because these forms

process special personal data. A data breach therefore may result in large implications for a GP and taking adequate security measures upfront is therefore important.

To sum up this chapter to this point; GPs have the legal basis to process (special) personal data and are responsible for taking appropriate technical measures based on the current state of technology. When GPs outsource their services to a third party, they stay responsible for adequately securing their processed personal data. The DPA has shown their attention for processing of medical data online and since the beginning of 2016 a data breach of personal data has to be reported to the DPA which may lead to receiving a fine. In several publications, the DPA has described their interpretation of the Wbp and refers to the NEN7512 and the ICT security guidelines for web applications and TLS guidelines of the NCSC as guidelines for taking appropriate technical measures. Next these specific guidelines are further described.

The NEN7512

The NEN7512[90] is 1 of 3 NEN norms which are specifically created for the healthcare sector (NEN 7510, NEN 7512, NEN 7513). The NEN7512 is the norm which describes the security requirements for the exchange of information within healthcare. The NEN 7512 describes that sensitive personal data exchanged online must be encrypted and that used algorithms and key-lengths must be based on broadly accepted judgments of experts because this is a domain which evolves constantly. In ANNEX A of the NEN7512 some scenarios are described. One of these scenarios is a patient filling in medical questions online as a preparation for a visit to a polyclinic. This scenario is quite similar to a patient requesting repeats prescriptions online because in both cases (special) personal data has to be transmitted over the internet. The NEN7512 states the required assurance level (high/very high) requires the use of encryption technology. Paragraph 6.2.3. of the NEN7512 norm describes that whenever an organisation makes use of a third party, security requirements must be put into the contract and further states that the contract must provide an option for an adjustment during the contractual period because new legal and information security requirements can change over time. This shows that the NEN7512 does not describe the technical details for TLS implementations but states that in such a scenario encryption must be applied and that the technical requirements must be based on broadly accepted judgments of experts.

The NCSC ICT security guidelines for web applications

The ICT security guidelines for web applications of the NCSC provide guidance to organisations that need to "*securely develop, manage and provide web applications and the required infrastructure"*[91, para 1] (translated by author). The domain of these guidelines are not limited to the technical configuration of web applications. They also describe the requirements for secure management of hard- and software required to host web applications. In 2012 the NCSC published their first version of the ICT security guidelines for web applications and in 2015 the second version of these guidelines was published. For the correct configuration of TLS for web applications these guidelines refer to the NCSC TLS guidelines. In relation to online web forms which process

sensitive data and setting up a secure online connection, these ICT security guidelines contain a list of settings which should be taken into account. The following implementation aspects are described in these guidelines (translated by author);

- When a user visits the website, all domains used support HTTPS and the user will always be redirected to the HTTPS website
- When possible, switch off HTTP compression, HTTP compression makes the website vulnerable to the BREACH attack
- Support Http Strict Transport Security (HSTS), HSTS instructs an internet browser to make use of HTTPS whenever the browser visits the website again. This helps to protect against so called "man in the middle attacks"
- Whenever a website makes use of multiple domain names, such as websites which may be reached by using WWW, and without WWW, then support HTTPS on all these domain names by making use of correct certificates and redirecting users to the HTTPS website.
- Prevent providing mixed content on a website, do not mix HTTP and HTTPS within web applications. This decreases the option for an attacker to find confidential parts of the web application.
- Whenever possible, switch of renegotiation, The use of renegotiation is only required whenever large amounts of data (gigabytes) are exchanged between the client and the server or whenever client certificates are used for securing the communication.

These ICT security guidelines for web applications, which the DPA refers to in a number of publications, describe technical measures in relation to securing online communication and these guidelines further refer to the TLS guidelines for setting up TLS configurations, these TLS guidelines are described next.

The NCSC TLS guidelines

The ICT Security guidelines for web applications and the DPA refer to these guidelines for the guidance on the configuration of TLS and therefore are considered to be highly applicable for securing the connection on GP websites. In 2014 the NCSC published[20] their TLS guidelines. These guidelines were created in cooperation with several private and public organisations. The document provides guidance for; *"acquiring, designing and evaluating the security of TLS implementations of computer systems"* [20, para 1] (translated by author). The document provides guidance for organisations to securely implement TLS. The document describes technical details of TLS and describes how TLS configurations should be setup for a secure implementation.

The TLS guidelines consist of 4 chapters. The 1st chapter describes TLS itself, its libraries and the random number generation. The 2nd chapter describes two different scenarios related to TLS implementations and describes

which configuration choices should be made for each scenario. The 3rd chapter describes the technical aspects of TLS and describes the secure configuration of TLS. The 4th chapter provides guidelines and the appendix provides a list of implementation considerations. Throughout the document 3 categories of technical settings are used to categorise the security level of these settings. These 3 categories are; GOOD (*goed*), ENOUGH (*genoeg*) and INADEQUATE (*onvoldoende*). This thesis will not go into all of the technical details of all configuration options and refers to the TLS guidelines itself for this information. In the guidelines: GOOD refers to settings which are considered to be the most secure. ENOUGH refers to settings which are considered to be secure currently, and can be chosen to provide compatibility with older systems. INADEQUATE refers to settings that should not be used because these settings are considered to be insecure. Settings which are considered to be GOOD or ENOUGH today can become INADEQUATE over time because newly discovered vulnerabilities and attack scenarios can devaluate the strength of the security. Therefore, TLS implementations must be evaluated regularly and if required be updated to keep the configuration secure. The NCSC advices to implement GOOD settings and only to use ENOUGH settings when this is necessary to support older software. The NCSC is clear on the use of INADEQUATE settings: <u>These should not be used.</u>

The 2nd chapter of the TLS guidelines describes scenarios related to the span of control of an organisation in relation to the TLS configurations. This chapter describes 2 scenarios. The 1st scenario describes the situation where the organisation has control over both the TLS configuration of the TLS server and the TLS client. This is a typical scenario for an enterprise environment where the ICT department is responsible for managing the client computers and the servers. This is not the scenario of an eHealth website of a GP. A GP only has control over the webserver and client computers are owned by the patient visiting the website. This limits the span of control of the GP in relation to the TLS configuration. The 2nd scenario resembles the eHealth service scenario of a GP. In this scenario the organisation has control over the server and has no control over the client that connects to that server. This 2nd scenario relates to websites of GPs which host eHealth services in which the GP only has control over the webserver and has no control over the devices which connect to the website. For this 2nd scenario the TLS guidelines describe the following; Only GOOD and ENOUGH settings should be used for TLS versions and cypher suites. GOOD settings are advised. But because of backwards compatibility with clients in some cases ENOUGH settings can be used. However, organisations should not implement more cipher suites than needed for the compatibility. The guidelines advice to use ENOUGH for the length of parameters and keys and only to use the GOOD settings when the system owner is sure that all clients support the GOOD versions. For elliptic curves, the use of GOOD configurations is advised and the use of ENOUGH should be used when the clients do not support the GOOD versions. The TLS guidelines advice not to implement more elliptic curves than is necessary for compatibility. For each other setting described in the TLS guidelines, the NCSC advices to use GOOD settings and only to consider ENOUGH settings when there is a major reason to make this choice. The guidelines advice to use a risk analysis to explain deviations from GOOD settings.

The TLS guidelines describe a list of TLS settings and describe which setting must be used to reach the level GOOD, ENOUGH or INADEQUATE. The following aspects of TLS are described (translated by author);

1. *TLS versions*; the GOOD version of TLS is version 1.2, the versions 1.0 and 1.1 are described to be ENOUGH. The versions SSL 1.0, SSL 2.0 and SSL 3.0 are INADEQUATE.
2. *Cypher suites*; the document describes an long list of cipher suites which are described to be either GOOD or ENOUGH
3. *Key length*; the guidelines describe the required key length for a list of different algorithms
4. *Compression*; the guidelines describe that the use of TLS compression combined with many data requests can reveal parts of secret data. This introduces a risk. TLS compression is stated to be hardly used and therefore should not be supported for the level GOOD. Application compression, such as HTTP compression, may be used for the level ENOUGH. When TLS compression itself is supported, the configuration setting is qualified to be INADEQUATE.
5. *Renegotiation*; there are two versions of renegotiation; insecure renegotiation, which is the old version of renegotiation which must be switched off for a GOOD grading. The second type of renegotiation is the client side renegotiation, this must also be switched off for a GOOD grading. Switching renegotiation on makes the TLS implementation vulnerable to DDoS attacks, therefore, switching on insecure renegotiation or client initiated renegotiation is stated to be INADEQUATE.
6. *OCSP stapling*; the validity of a digital certificate used for TLS can be checked by the client that visits the server. For this check the OCSP protocol is used. The client can either check the validity of the certificate at the certificate provider or at the webserver itself. Because checking the validity of the certificate at the certificate providers discloses information about the devices visiting the webserver, the NCSC advices to provide the OCSP service on the webserver itself. When it is provided by the webserver the settings is stated to be GOOD, when the OCSP server of the certificate provider is used, the configuration is stated to be ENOUGH. This setting does not have an inadequate setting.

The NCSC guidelines describe additional settings of TLS in the chapter “other considerations”. These settings can only be switched on- or off. The following list is mentioned in the guidelines;

7. *Forward secrecy*; forward secrecy is a technology which ensures the secrecy of sent data intercepted when the private key of a certificate is stolen in the future. Switching on forward secrecy protects already transported information against a future attack with the private key of the system.
8. *Certificate management*; requesting and managing certificates are not extensively described in the TLS guidelines. A list of important aspects are described. Aspects mentioned are the creation of the private key, the importance of using an trustworthy certificate provider, the correct match between the domain name its subdomains and the certificate, the use of an Extended Validation (EV) certificate to provide

more assurance about the owner of the system, the protection of the private key providing the certificates of the certificate chain on the server. And finally it describes correctly administrating all information regarding certificates and monitoring their expiry date.

9. *Random number generation*; the quality of random numbers for generating certificates and forward secrecy, is important to the security of TLS sessions.
10. *TLS termination*; some organisations terminate TLS sessions on a central point to be able to process the data for specific reasons such as DDoS mitigation solutions. The point of attention is the fact that behind the point of termination, the data is readable to interceptors.
11. *Certificate pinning and DANE*; when an organisation has control over both the webserver and the used clients, a technology called certificate pinning can be implemented to provide protection against maliciously created certificates on a system of a trusted certificate provider. DANE (DNS-Based Authentication of Named Entities) is a technology based on publishing DNS records which can be used to check the authenticity of a certificate. A DNSSEC DNS server must be used to provide the required assurance required for DANE.

To summarize this chapter; The term eHealth relates to a broad scope of medical services which make use of ICT. Within this scope of eHealth are health providers such as GPs. GPs provide eHealth services over the internet for requesting repeat prescriptions and for signing up as a new patient. Recent research concludes that 75% of Dutch GPs provide the option to request repeat prescriptions online. To provide such eHealth services online, GPs can make use of web sites with web forms. GPs do not need to set up the required infrastructure themselves, but can make use of centralised services of an ASP. To secure the transport of personal data over the internet, the HTTPS protocol must be supported by the webserver. This requires the implementation of TLS on this server. Not all versions of TLS are considered to be secure, there are old versions of TLS/SSL which are not considered to be adequate to protect personal data online. Patients can use the eHealth services of a GP 24 hours a day. Therefore their internet devices can make use of trusted and untrusted internet connections. Patients themselves do not seem play a prominent role in securing the online connection and GPs must take the responsibility to implement TLS correctly. The overall eHealth ambitions in the Netherlands are large and it can be expected that the use of eHealth services will increase due to the governmental ambitions and financial support.

To provide eHealth services, GPs process special personal data which require high security measures. GPs must comply with the Wbp and risk receiving a fine when personal data is breached on the computer systems that process their patient data. The DPA has shown their attention for the security of online webforms of GPs, pharmacies and physiotherapists. Publications of the DPA refer to the ICT Security guidelines for web applications and TLS guidelines of the NCSC for technical guidance. These guidelines provide information for correctly implementing TLS and provide technical details for evaluating configurations. The NCSC ICT security guidelines for web applications and NCSC TLS guidelines therefore should be taken into account by GPs and their third

parties (such as ASPs) when they provide eHealth services for requesting repeat prescriptions and for signing up online.

2.3 Description of the identified problem

The majority of GPs provide eHealth services for requesting repeat prescriptions online. Patients can make use of web sites of their GP to request repeat prescriptions or sign up online. When web forms for eHealth services are filled in online, personal data (in this case special personal data) is transported over the internet between the patient's device and the website of the GP. The DPA stated that such web forms must support HTTPS and refers to the ICT security guidelines for web applications and TLS guidelines of the NCSC for implementation guidance. The high use of public Wi-Fi and the ability to make use of eHealth services 24 hours a day. This combined with demonstrated attacks on the interception of Wi-Fi connections illustrates the importance to implement TLS correctly. This analysis raises the question to what extent eHealth services are provided by GPs and to what extent these TLS configurations comply with the NCSC guidelines. Incorrectly configured TLS implementations may introduce privacy and security risks and affect a large part of Dutch society. There is no literature found which provides insight to what extent Dutch GPs comply with these guidelines. By researching the current TLS configurations of the web services of GPs an insight can be gained into a specific part of eHealth security.

2.4 Looking through the Lens of Cyber Space

The domain of cyber security is not limited to technology. A cyber secure society can only exist when elements within the cyber eco system contribute to that security. A lens for looking at cyber space, which is illustrated in *figure7*, is created by Jan van den berg et al.[92].

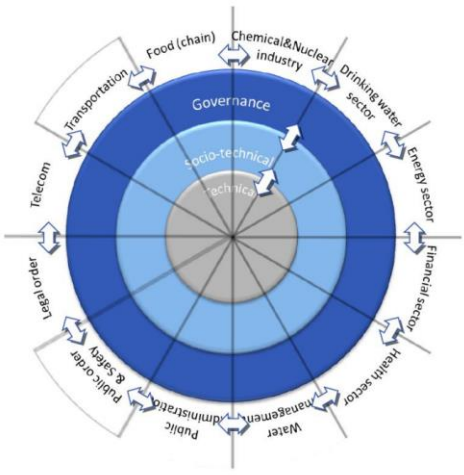


Figure 7; Conceptualisation of cyberspace (source: Jan van den Berg et al)

This model states that cyberspace consists of 3 interacting layers called the cyber sub domains. These 3 layers (the blue and grey rings in figure 7) are the technical layer, the socio-technical and the governance layer which each represent a domain of cyber space. The technical layer consists of the technology used to create the fundament of the internet. This domain consists of hardware such as computers, cables, routers, firewalls and the software which computers and devices run. Of top of that technical layer, the socio-technical layer resides. This is the domain of the key assets of cyber space, the so called cyber activities. The human interaction with technology takes place in this sub domain. Sending e-mails and reading news online are examples of cyber activities which are enabled by cyberspace. Within the context of this thesis; eHealth services are considered to be a collection of cyber activities. The interaction between an GP and patients over the internet with the use of web forms for repeat prescriptions is an example of an eHealth cyber activity. The outer layer of cyberspace is the governance layer which governs the functioning of the technical and socio-technical layers. This is where law and regulation and the role of organisations governing the eHealth domain reside. These three domains together represent cyberspace and each domain must function adequately and be aligned to the other domains to enable the potential of cyberspace. This model is used as the lens for the results of this research.

Chapter 3

Online research steps

3 Online Research Steps

This chapter describes steps of the online research conducted for this thesis. The first step of this research was the creation of the sample of GP practices websites. The starting point for the creation of this sample was the website of the Dutch patient federation zorgkaartnederland.nl[22]. This website provides patients the ability to find information on medical specialists and provide feedback on these specialists. The website provided a separate section for general practices on the front page of the website. It was not possible to directly download a complete list of practices for the online research but all information about the practices was spread over more than 200 webpages which were alphabetically ordered. On May 14th 2016 the website had information regarding 4675 GP practices online. The goal was to create a sample size which consisted of 370 practices because academic research[93] showed that this was the required sample size for a population of 4675 practices to gain a confidence level of 95% and a margin of error of 5%.

The first sample of 256 GPs was created in May of 2016. Manually all 224 web pages on zorgkaartnederland.nl were visited with a Google Chrome browser and each first mentioned GP on that web page was registered. This sample was then expanded to 256 samples by adding the last mentioned GP on each 10th page, starting from page 10. During the second round which took place in June (to reach the total of 370 unique samples), starting from page 1 each last GP mentioned on the web page was added to the dataset. This resulted in a total list of 370 GPs and the internet address of their website. When no website for a GP was mentioned on the webpage of zorgkaartnerderland.nl the Google search engine was used to search for a website for that general practice. Unfortunately (in October 2016) two duplicates were found in the sample and the sample size was reduced to 368 unique samples. The collected information was administrated in a Excel spreadsheet which was used for the next steps of the online research for this thesis.

In the period May-June 2016 all collected websites of GPs were visited with the Google Chrome browser and each website was examined for the option to request repeat prescriptions and to sign up online. When a specific web page was found for one of these eHealth services the URL of that page was added to the spreadsheet. During this online research in total 113 web pages for signing up were identified and 191 web pages for requesting repeat prescriptions were identified and added to the spreadsheet. The final step was to test the TLS configurations of the webservers. This was performed with help of an online service (internet.nl) which is described next.

Internet.nl

Internet.nl was launched[23] during the cyber week of 2015. Internet.nl is an initiative of the Internet Standards Platform and the Dutch government. The website provides people the ability to check a website for compliance with the latest internet standards. The website provides a web form where a domain or URL can be entered for

online testing. After entering the information, internet.nl tests the system on a selection of technical settings and presents the results to the user. The standards which are checked are IPv6, DNSSEC, DKIM SPF DMARC and TLS settings. Because the TLS scan and the results of internet.nl are based on the TLS guidelines of the NCSC and two aspects of the ICT security guidelines for web applications, this scan provided information if the TLS configurations were correctly configured for these parts of the guidelines. The services of internet.nl supported the online research for this thesis and provided their service to bulk scan all the collected URLs. If internet.nl would not have provided the service to scan the URLs in bulk, all URLs would have to be scanned one by one manually. This would have taken several days to complete. The actual test of internet.nl is explained next.

The TLS test of internet.nl is capable of testing the TLS settings of the provided GP webservers. The results of the internet.nl scan are based on the GOOD, ENOUGH and INADEQUATE settings of the NCSC TLS guidelines. When a manual scan is started, the results are presented online after the scan. A GOOD result will be presented in green, an ENOUGH result will presented in orange and an INADEQUATE setting will be presented in red. Because a RED result represents an INADEQUATE setting, this means that a TLS implementation with 1 or more INADEQUATE results does not fully comply with the guidelines. In June of 2016 internet.nl changed their scoring system and updated their scanning system[94]. From that moment the test for HSTS and forced HTTPS were added to the total score of the test. This updated version was used to scan the TLS implementations of GP webservers. The TLS scan of internet.nl tested twelve aspects of the TLS implementations. Whenever a setting was tested to be ENOUGH or GOOD, this added 10 points to a total achievable score of 120 points. When a setting was tested to be INADEQUATE, it received 0 points. The twelve aspects of the TLS configurations which were tested by internet.nl are described in the following table;

TEST variable	**Description of test**
cert_pubkey	The length of the public key is checked
cert_trusted	This check is performed to check whether the certificate is signed by a trusted certificate authority to provide a level of assurance that the client if visiting a legitimate website
protocols	This checks the versions of TLS and SSL that are supported by the system.
cert_signature	This test checks whether the used hash functions are secure
fs	This test checks if forward secrecy is supported by the system. This ensures the confidentiality of transported data in the future

ciphers	This tests whether only secure cipher suites (a combination of cryptographic algorithms) are used
client_reneg	This checks whether the webserver allows the client to start a renegotiation. Supporting client initiated renegotiation makes the implementation vulnerable to DDoS attacks
compression	This check is to determine if the webserver supports TLS compression. Whenever a webserver supports TLS compression it may be vulnerable to the CRIME attack
secure_reneg	This checks if the webserver supports secure renegotiation
cert_hostmatch	This checks the match between the domain name in the certificate and the domain name of the website
forced_https	This checks if the website forces the use of https
hsts	This checks if a hsts is supported to ensure the client connects with https for a configured period of time

On June 26th two text files with URLs were created from the spreadsheet and provided to internet.nl. Internet.nl tested the TLS configurations of the all webservers hosting the web pages. On September 1st internet.nl provided the results in a comma delimited file (.csv) for further analysis. This file consisted of 14 columns with the results of the TLS tests. The 1st column of the file contained the domain name which was tested (the URL was stripped to the domain name by internet.nl). The 2nd column contained total score of the individual 12 tests on a specific URL (with a maximum of 120). Column 3 up to 14 contained the results of each individual TLS test. In total this file contained 194 unique domain names that were tested by internet.nl. Together with the results, internet.nl stated that 13 URLs could not be tested by their systems. The advice of internet.nl was to test these URLs manually. Internet.nl stated that the cause of the error could have been a slow internet connection at the moment of scanning. These remaining 13 URLs were scanned manually and when the website internet.nl still resulted in an error, the scan was made with help of Qualys SSL labs[95]. The results were added to the research data.

Chapter 4

Research Results

4 Research Results

This chapter describes the results of the online research. The first part of these results are based on the sample created for the online scanning, these results are described in paragraph 4.1. The results of the online scan conducted by internet.nl are described in paragraph 4.2. The last paragraph of this chapter, paragraph 4.3, describes the results of the interviews which were held with 4 ASPs.

4.1 Results based on the sample

This paragraph describes the data which was collected for the online scanning and provides the results based on the analysis of this sample.

The use of websites by GP practices

The sample of 368 practices which was created from the website zorgkaartnederland.nl was used as the starting point to create the list of the websites of the GP practices. Based on the information published on zorgkaartnederland.nl and additional Google search results in total 344 websites of GP practices were identified. This implies that 93% of these practices had a website on the internet.

Providing online services for signing up and for requesting repeat prescriptions

All 344 websites were visited with the Google Chrome browser and options for requesting repeat prescriptions and for singing up online were identified. In total 113 options for signing up online and 191 options for requesting repeat prescriptions online were identified on these 344 websites. This concludes that 33% of the practices (with a website) provided the option to sign up online and 56% provided the option to request repeat prescriptions on their website.

The use of ASPs for hosting

During the research it was noticed that a number of ASPs provided services to GPs. In total 7 ASPs were selected and administrated during this research to create a distinction between the websites which were hosted by ASPs and by other hosters. In this thesis these two groups of hosters are further mentioned as the "ASPs" and the "other hosters". During this research the identification of the use of an ASP for the online services was not straightforward. In some cases the use of an ASP was visible on the web page because the logo of the ASP was mentioned on the web page. In other cases the URL revealed the use of an ASP because the name of the ASP was part of the URL of the webpage or a specific syntax (the use of a token in the URL) was used. Because the use of an ASP was not always straightforward to identify the following results may contain a minor uncertainty in relation to the distribution between the ASP hosters and the other hosters.

Web pages for requesting repeat prescriptions

Of the 191 web pages for requesting repeat prescriptions, 129 were identified to be hosted by the ASPs. The remaining 62 web pages were hosted by other hosters. This shows that 68% was hosted by the ASPs and 32% was hosted by other hosters. The distributions among the ASPs was as follows; 68 web pages were hosted by praktijkinfo.nl, 29 web pages were hosted by uwartsonline.nl, 13 web pages were hosted by mijngezondheid.net, 5 web pages were hosted by praqtijkplus.nl and huisarts.info and artsenzorg.nl each hosted 3 web pages. The ASP distribution for repeat prescriptions is illustrated in *figure 8.*

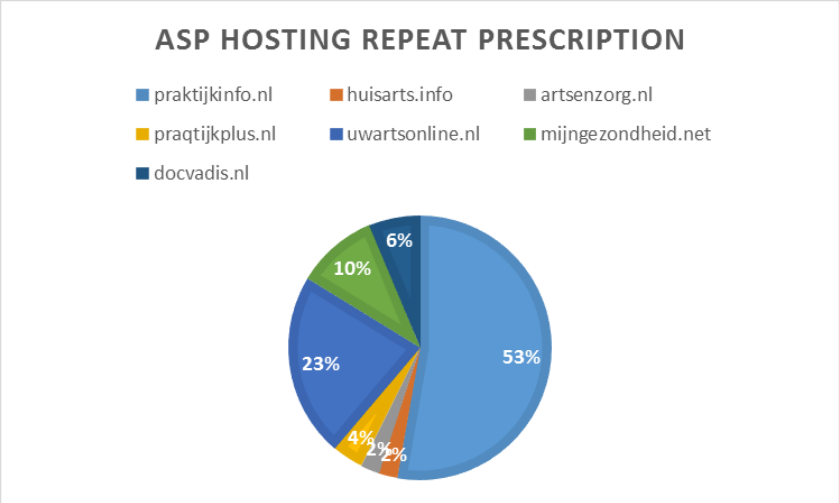


Figure 8; ASP distribution repeat prescriptions

Web pages for signing up

Of the 113 web pages for signing up, 83 were identified to be hosted by the ASPs and the remaining 30 were hosted by other hosters. This shows that 73% was hosted by the ASPs and 27% was hosted by other hosters. Of the 83 hosted by the ASPs, 56 web pages were hosted by praktijkinfo.nl, 19 web pages were hosted by uwartsonline.nl, 4 web pages were hosted by praqtijqplus.nl, 3 web pages were hosted by artsenzorg.nl and 1 web page was hosted by huisarts.info. None of these web pages were hosted by mijngezondheid.net and docvadis.nl. The ASP distribution for signing up is illustrated in *Figure 9*.

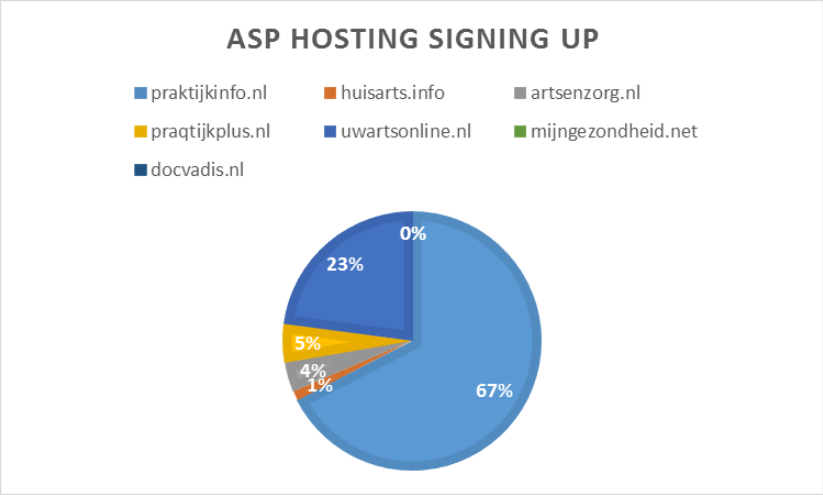


Figure 9; ASP distribution signing up

The use of portals and web forms on the web pages

In October of 2016 all collected web pages were visited again to administrate whether a portal or a web form was presented on the web page. During this online research, it was noticed that since the creation of the sample changes were made to some of the websites of the practices. In total 4 web pages for signing up and 3 web pages for requesting repeat prescriptions were not online anymore. This research showed that all the 109 web pages for signing up which still were online contained a web form which could be directly filled in online. For requesting repeat prescriptions, 106 portal pages were found and 82 web forms were identified. This use of portals and web forms for these eHealth services are illustrated in *Figure 10.*

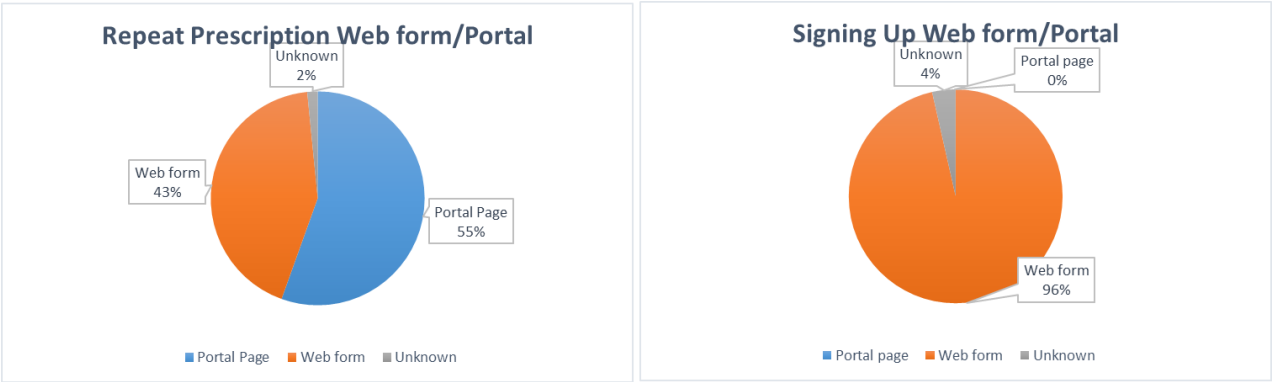


Figure 10; Use of web forms and portals for signing up and for requesting repeat prescriptions

4.2 Results of the TLS scan

This paragraph describes the results of the TLS scan of the webservers performed by internet.nl. It describes the results of the 12 aspects of TLS which were tested on the webservers for signing up and for requesting repeat prescriptions. In this paragraph these results are divided into the results of the ASPs and the results of the other hosters.

Signing up

Scan results of signing up web pages hosted by ASPs

The internet.nl scan results of the 83 ASP hosted web pages for signing up were as follows: 77 of the tests scored 100/120, 5 tests scored 90/120 and 1 scored 110/120. None of the tests achieved the maximum score of 120. These results are illustrated in *Figure 11.* The X axis of this figure presents the total score of the scan from NOHTTPS (0/120) up to 120/120. The Y axis represents the percentage of the ASPs which achieved that score. This visualisation is used to present these TLS scores throughout this chapter.

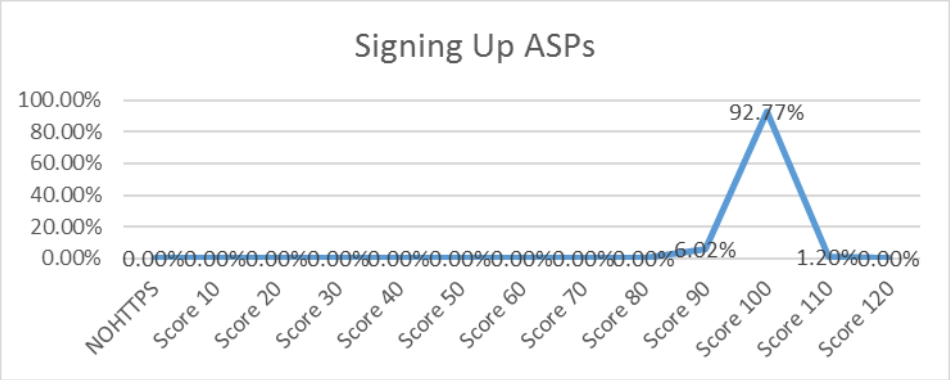


Figure 11; Signing up total scores ASPs

To create an understanding which underlying settings led to these results of ASPs, the individual test results are described next. *Figure 12* shows the score of the ASPs on the 12 individual TLS tests. This visualisation provides insight in the settings of the TLS configurations of the tested signing up webservers of ASPs. The tested settings are stated on the outer ring of *Figure 12.*The level of compliancy of each specific setting in relation to the NCSC guidelines is illustrated by the dots. The position of the dot between the centre of the circle and the outer ring visualises the score from 0 to 100%. This visualisation for these individual results is used throughout this chapter. The scan results showed that 0 out of 83 (0%) of the scanned signing up tests supported HSTS and 79 out of 83 (95%) of the tests supported client initiated renegotiation. The other results were as follows: forced_https 98%, cert_hostmatch 100%, secure_reneg 100%, compression 100%, ciphers 99%, protocols 100%, fs 99%, cert_trusted 100%, cert signature 100% and cert pubkey 100%.

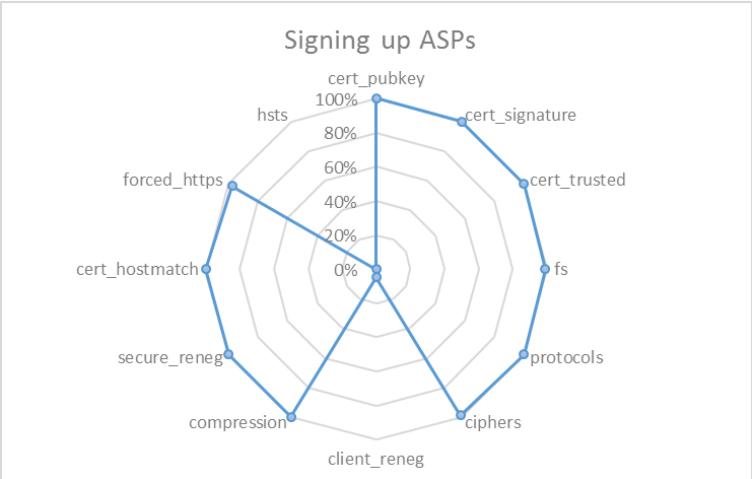


Figure 12; Signing up implementation scores ASPs

Scan results of signing up web pages hosted by other hosters

The results of the 30 web pages hosted by other hosters are as follows: a total of 2 tests (6,67%) did not support HTTPS. The remaining results were as follows: 4 tests scored 50/120, 2 tests scored 60/120, 2 tests scored 70/120, 3 tests scored 80/120, 5 tests scored 90/120, 2 tests scored 100/120 and 10 tests scored 110/120. These scores are illustrated in *Figure 13.*

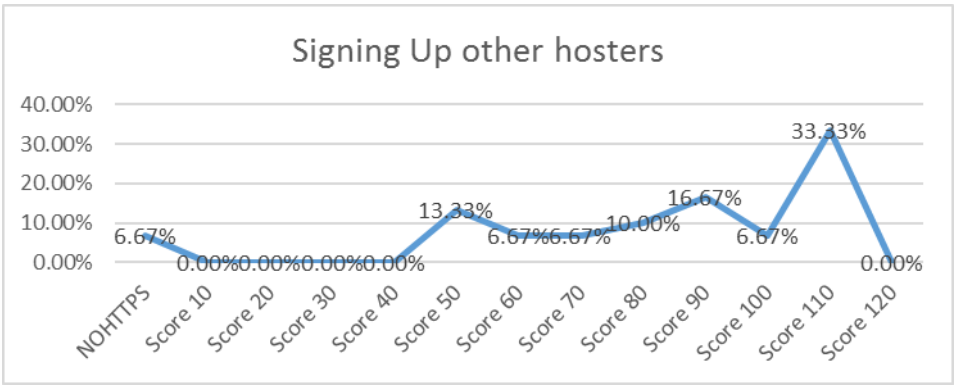


Figure 13; Signing up total scores other hosters

The results of the individual settings of the other hosters were as follows: forced_https 54%, cert_hostmatch 61%, secure_reneg 100%, compression 96%, client_reneg 96%, ciphers 75%, protocols 82%, fs 75%, cert_trusted 71%, cert_signature 79%, cert_pubkey 93%. 0% of the tests supported HSTS. This is shown in *Figure 14.*

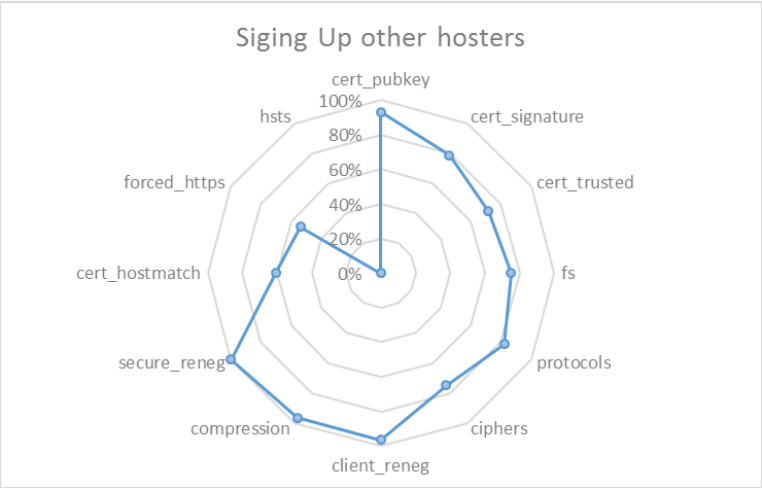


Figure 14; Signing up implementation scores other hosters

Repeat Prescriptions

Next the results of the scan regarding webservers for repeat prescriptions are described. Of the 191 web pages for requesting repeat prescriptions, 129 (68%) were hosted by the ASPs and 62 were hosted by the other hosters.

Scan results of repeat prescription webservers hosted by ASPs

The scores of the webservers hosted by ASPs were as follows: 12 tests scored 90/120, 102 tests scored of 100/120 and 15 scored 110/120. These results are shown in *Figure 15.*

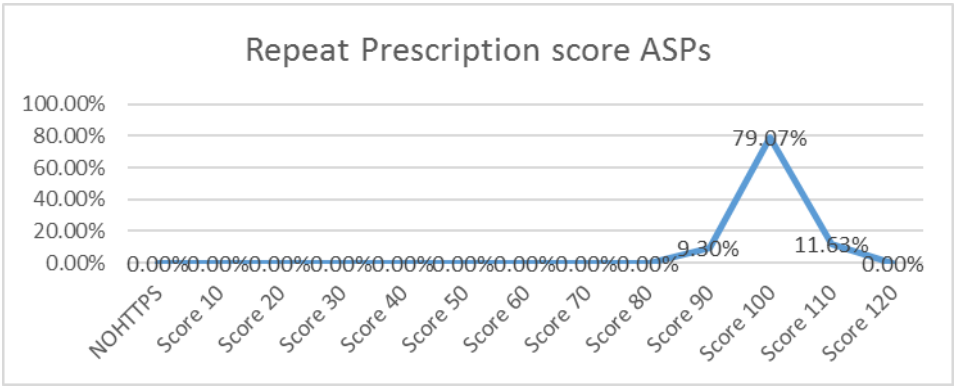


Figure 15; Repeat prescriptions total scores ASPs

On the 12 individual TLS settings the ASPs scored as follows: HSTS 9%, forced_https 92%, cert_hostname 100%, secure_reneg 100%, compression 100%, client_reneg 21%, ciphers 91%, protocols 94%, fs 100%, cert_trusted 100%, cert_signature 100% and cert_pubkey 100%. These results are shown in *Figure 16.*

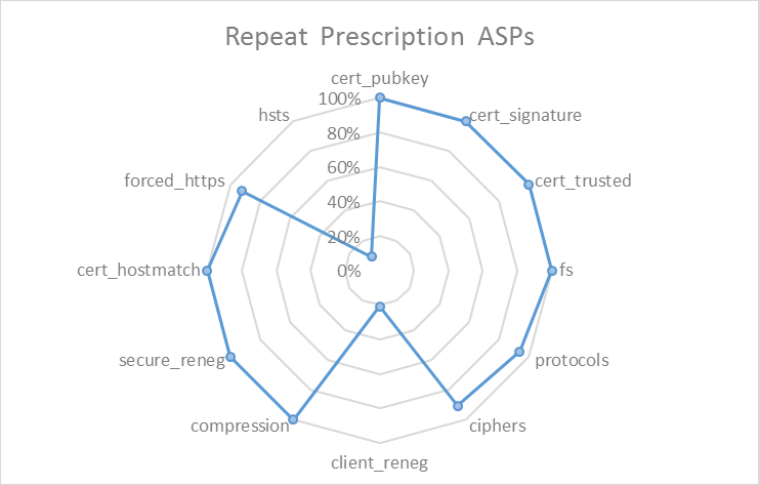


Figure 16; Repeat prescription implementation scores ASPs

Scan results of repeat prescription webservers hosted by other hosters

The scan results of the other hosters for requesting repeat prescription webservers showed a more distributed score. 4 out of 62 tests (6,45%) did not support HTTPS, 1 scored 20/120, 2 scored 30/120, 6 scored 50/120, 4 scored 60/120, 4 scored 70/120, 5 scored 80/120, 7 scored 90/120, 14 scored 100/120 and 15 scored 110/120 (24%). This is shown in *Figure 17.*

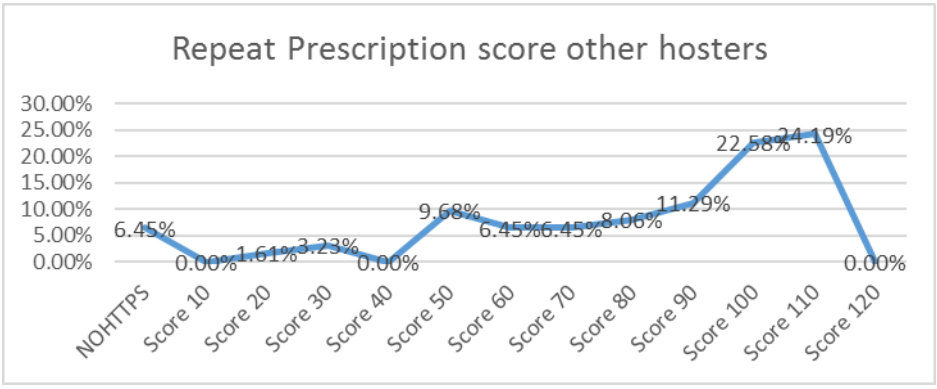


Figure 17; Repeat Prescription total scores other hosters

On the 12 configuration options the other hosters scored as follows; HSTS 0%, forced_https 47%, cert_hostname 66%, secure_reneg 95%, compression 98%, client_reneg 83%, ciphers 71%, protocols 81%, fs 74%, cert_trusted 74%, cert_signature 79% and cert_pubkey 91%. This is illustrated in *Figure 18.*

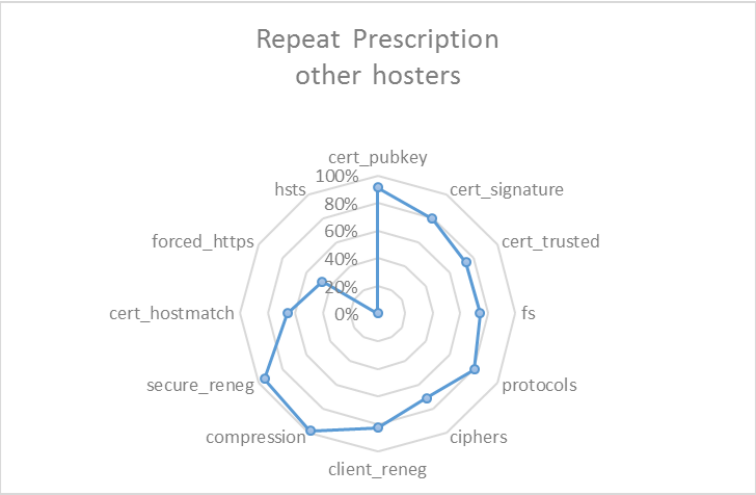


Figure 18; Repeat prescription implementation scores other hosters

4.3 Results of interviews

In the period September-December of 2016 interviews have been held with 4 of 7 ASPs described in this thesis. All 7 ASPs were contacted and asked to provide input for this thesis. Unfortunately 3 of 7 ASPs were not able to provide their input for this research. The goal of each interview was to discuss the scan results of the that specific ASP and to collect information which could provide insight if the ASPs were aware of the NCSC guidelines and the publications of the DPA and how guidance on cyber security was organised within the sector. These interviews were structured along 7 questions (formulated in Dutch) which can be found in ANNEX II. The results of these interviews have been anonymised in this thesis to ensure confidentiality of the information provided. This was agreed on with the representatives of the ASPs so that they could speak freely during the interview. Before the interviews were held, the ASPs had been provided with the results of the internet.nl scan of their platform which was used as input for the discussion.

During the interviews[96][97][98][99] it became clear that none of the ASPs was familiar with the publications of the DPA in relation to securing web forms online. Nor were the ASPs familiar with the guidelines of the NCSC to which the DPA referrers to for guidance for securing such systems. However a single ASP did say that they knew that such guidelines probably existed. The majority of the ASPs however did state that they had to comply with standards such as the ISO27001, NEN7510 and 2 of the ASPs said that they specifically had to comply with requirements for the use of the Dutch authentication system DigiD. These security requirements for DigiD however are based[100] on the ICT security guidelines for web applications.

All ASPs said that professional organisations within the healthcare sector (such as the LHV, NHG, KNMG etc.) did not ask questions regarding the TLS implementations of their platforms. An ASP said that sometimes a single GP asked questions regarding the security of their platform in more general terms. All of the ASPs confirmed that

there is no central organisation within the healthcare sector that provides guidance on cyber security and a single ASP said that the LHV currently probably would not be capable of providing such detailed knowledge. A single ASP mentioned that they must comply with the law, but that the law does not provide the actual information required for technical implementations. The same ASP said that knowledge regarding cyber security is lacking under GPs and that GPs rely on the expertise of the ASPs. Another ASP mentioned that patients do not seem to be interested in information security. In total 3 ASPs said that it should be the task of the government to provide/create guidance on cyber security within the sector. A single ASP said that direct attention of the government would create the incentive to change the TLS configuration of their platform.

In relation to changing the configuration of their own platform, 3 out of 4 ASPs said that they had initiated changing their TLS configurations. 2 ASPs said that recent audits has also revealed that their TLS configuration had to be changed. One ASP said that the research for this thesis had resulted in a change of their internal processes in relation to securing their web systems and a second ASP said that their own discovery created an incentive to change their internal process. In relation to improving cyber security within the eHealth sector, 1 ASP said that measuring the security and publishing the results would be a good methodology to create incentives for the sector to improve security.

To summarise this chapter of results; The sample created for the online scan showed that 93% of the GP practices had a website online of which 56% provided the service to request repeat prescriptions online and 33% provided the option to sign up online. A selection of 7 ASPs hosted 2/3 (68% for repeat prescriptions and 73% for signing up) of these eHealth services. The remaining 1/3 was hosted by other hosters. The online check for the use of web forms and portals showed that these were used in at least 96% of the web pages for signing up and 43% for requesting repeat prescriptions. In total 55% of the web pages for requesting repeat prescriptions were identified to be a portal. The online TLS scan showed that the ASPs for both types of webservers (signing up and repeats prescriptions) scored in the range 90/120-110/120 and the other hosters scored in the range 0/100-110/100. None of the tested webservers scored 120/120 on the TLS scan. The ASPs particularly scored low on their adoption of HSTS, only 1 ASP supported HSTS which resulted in a HSTS score of 9% on the repeat prescription tests and 0% on the signing up tests. The ASP configuration of client initiated renegotiation scored as low as 21% on the repeat prescription tests and 5% on the tests for signing up. The other hosters also scored low on the support of HSTS and overall scored lower on the individual TLS tests. The results show that more than 6% of the other ASP hosted webserver tests still does not support HTTPS and therefore does not protect personal data during transport over computer networks.

The results of the interviews with 4 of the 7 ASPs showed that these ASPs were not actively informed about security requirements by professional organisations such as the LHV or KNMG and that there is no central organisation within the eHealth domain who took the lead on cyber security and provided guidance to the sector.

Chapter 5

Discussion

5 Discussion and Reflection

This chapter discusses the results of this research and provides the answer to the research question. In the Netherlands the government, professional organisations and patients together are stimulating the adoption of electronic health (eHealth) services within the healthcare sector. These health services make use of the internet for the transport of personal data between healthcare providers and patients. The definition of eHealth has a very broad scope and relates to the use of ICT for healthcare services. Among the Dutch healthcare providers are GPs which provided eHealth services to their patients over the internet. For this thesis a selection of eHealth services of 368 GPs were researched. Within the scope of this research were the services to request repeat prescriptions online and to sign up as a new patient online with the use of web based services. These eHealth services process (special) personal data over the internet. GPs must comply with the Dutch privacy regulation which is described in the Wbp. This legislation creates the legal basis for GPs to process personal data and special personal data (such as medical data and social security numbers). Processing special personal data requires the GP to ensure that a high level of security measures are in place to protect this personal data of their patients. GPs may outsource their eHealth services to an ASP but will have to ensure that adequate security measures are in place to protect the personal data of their patients. The Wpb sets the legal boundaries for processing personal data in the Netherlands but does not provide details regarding the technical measures which are required to protect the personal data. Because technology keeps evolving and vulnerabilities in existing technology are discovered over time, security measures must be updated over time. The Dutch Privacy Authority (DPA) published guidelines which describe their “translation” of the legal domain to the technical domain. Publications of the DPA state that the transport of special personal data must be secured with HTTPS. For technical details, in numerous publications the DPA refers to the NEN7512, the NCSC ICT security guidelines for web applications and the NCSC TLS guidelines for technical guidance. The online research conducted for this thesis tested the TLS configurations of eHealth services for requesting repeat prescriptions for and singing up for a selection of 368 GPs in the Netherlands in relation to 12 aspects of these NCSC guidelines.

The results show that 93% of the researched GP practices had a website online. Based on the total of 5.068 general practices it can be concluded that roughly 93%x5068=4713 websites of general practices were online. The results further show that 56% of the practices with a website provided the option to request repeat prescriptions online and 33% provided the option to sign up online. This concludes that roughly 56%x4713=2639 practices provided the service to request repeat prescriptions online and 33%x4713=1555 practices provided the service to sign up online. Over 2/3 (73% for signing up and 68% for repeat prescriptions) of the researched practices made use of the following ASPs to host these eHealth services: praktijkinfo.nl, huisarts.info, artsenzorg.nl, praqtijkplus.nl, uwartsonline.nl, mijngezondheid.net and docvadis.nl. This concludes that the ASPs roughly served 73%x1555=1135 practices with signing up eHealth services and 68%x2639=1795 practices with repeat prescription eHealth services. The remaining services were hosted by other hosters (which may also could

be the GPs themselves). This concludes that roughly 27%x1555=420 Dutch practices used web services for signing up provided by other hosters and roughly 32%x2639=844 practices used repeat prescriptions services from other hosters.

The results further show that all 7 selected ASPs had implemented TLS on their servers to support HTTPS on the eHealth services of their customers. Because the majority of the web pages were hosted by ASPs, this research concludes that if these 7 specific ASPs would fully comply with the applicable guidelines that roughly 2/3 of Dutch GPs automatically would made use of correctly configured TLS configurations. This research further also concludes that not all of the researched eHealth services supported HTTPS. These services were identified to be hosted by the other hosters which served the remaining 1/3 of the sample. The research shows that over 6% of these tests did not support HTTPS (6,45% for repeat prescription services and 6,67% for signing up services). Extrapolated, this related to roughly 6,45%x844=54 practices which served 54x2168=117.000 patients for repeat prescription services. For the signing up services this roughly related to 6,67%x420=28 practices which served 28x2168=61.000 patients. Based on publications of the DPA it can be concluded that these GPs violated the Dutch privacy law. Further this research concludes that the overall adoption of HTTPS by practices increased over the period 2013-2016. This can be concluded based on the results of the research performed by the DPA in 2013 and the research results of this thesis.

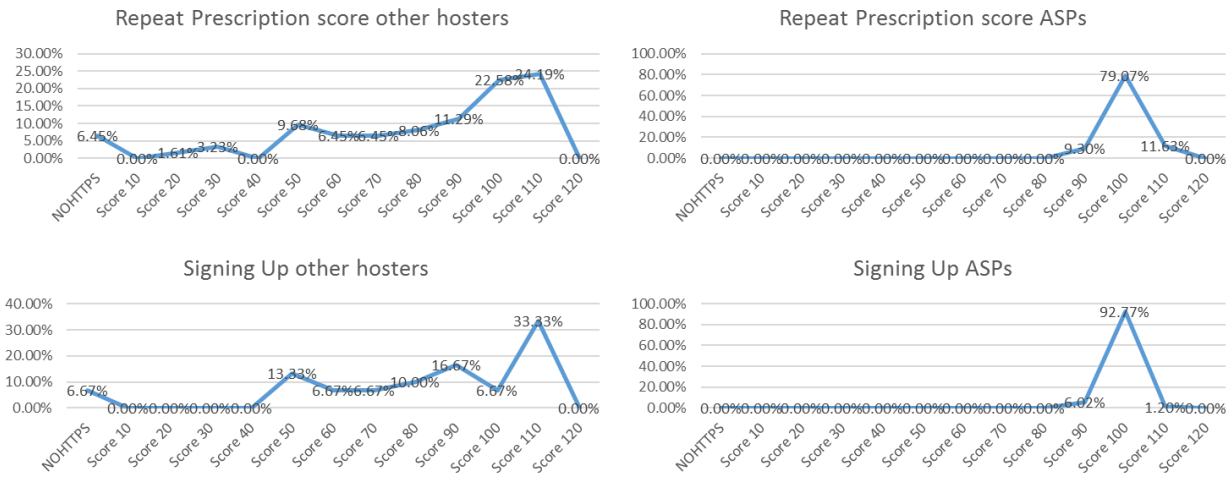
The online scan conducted by internet.nl provided detailed information regarding the settings of the TLS configurations. The scan results show that none of all tested TLS configurations fully complied with the 12 tested TLS configuration aspects (which are based on the NCSC guidelines). Not one single tested TLS configuration achieved the maximum score of 120/120. It is concluded that the services of ASPs overall scored in the range between 90/120 and 110/120. The other hosters scored in the range between 0/120 (no HTTPS) and 110/120. The results further show that specifically 2 settings overall scored low in the TLS tests. These were the support of HSTS and the configuration of client initiated renegotiation. HSTS was hardly supported by the ASPs (1 of 7 ASPs supported HSTS) and the other hosters. The ASPs also specifically scored low on switching off client initiated renegotiation. In relation to the applicable guidelines, supporting HSTS is described in the NCSC ICT security guidelines for web applications and the advice to not support client initiated renegotiation is described in the NCSC TLS guidelines. The implementation of HSTS helps to protect against man in the middle attacks and supporting client initiated renegotiation introduces a DDoS risk. Based on the detailed scan results as presented in *figure* 12,14,16 and 18 it can be concluded that the ASPs overall scored higher on the TLS test than the other hosters.

Next the research question central for this research is answered. The research question central in thesis research was;

To what extent do eHealth services of Dutch GPs comply with existing security guidelines and what is a possible strategy to improve security?

Taking into account the scope of this eHealth research, the answer to the first part of this this question is as follows;

For this research 12 aspects of TLS implementations of eHealth services for singing up and for requesting repeat prescriptions have been tested for a sample of 368 GPs. A number of 7 ASPs which provide 2/3 of these Dutch GP eHealth services showed scores in the range from 90-110/120 on the TLS tests and other hoster scored in the range from 0-110/120. This research further shows that more than 6% of the eHealth services hosted by other hosters did not support HTTPS which is a violation of the Dutch law. The total scores are shown in *figure 19*.



Figure; 19 TLS scores Dutch GPs eHealth services ASPs/ other hosters

The second part of the research question, the question for a possible strategy for improving security is described next. This research concludes that the eHealth services provided by ASPs scored high on the TLS test. The information from the interviews however showed that ASPs were not fully aware of publications of the DPA and the NCSC guidelines. If these ASPs would be actively instructed to fully comply with these guidelines this could create an incentive for them to configure their TLS configurations accordingly to these guidelines. The other hosters were not interviewed for this research but it is assumed that these have the same level of knowledge of the DPA publications and the NCSC guidelines. When the lens of the conceptualisation of cyberspace, as described in paragraph 2.4, is used to look at this problem, an observation arises. To further elaborate on this,

Figure 20 shows how elements of the researched eHealth domain such as; organisations, regulation and technology can be placed within this model.

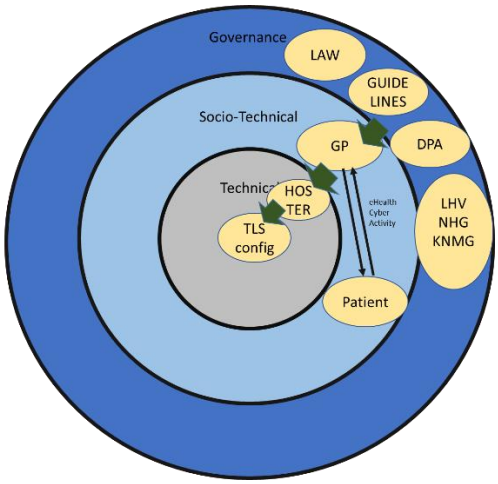


Figure 20; eHealth elements placed within the conceptualisation of cyberspace

In this model the TLS configurations and the hosters responsible for this implementation are placed in the technical domain of cyberspace. In the socio technical layer the GP and the patient reside and the arrows between the patient and the GP illustrate the eHealth cyber activities (the services for requesting repeat prescriptions and for signing up online). In the outer domain, law and regulation are placed together with a selection of organisations which play a role in the governance of the eHealth security domain. So if all these elements are in place, why are the TLS configurations not configured conform the guidelines? The author of this paper argues that there is an important element in cyberspace which is the “oil” of cyberspace and which keeps the cyber space domain secure. This is the flow of information between the domains of cyberspace. The elements of cyber space together function as an eco-system. Components influence each other by the exchange of information. To reach an optimised secure eco system, necessary information must flow between these components in cyberspace. This means that law and regulation will have an influence on the technical implementations by information flow. A technical configuration will only change if required information for such a change enters the technical domain of cyber space. Without this information flow between the domains of cyber space, the technology will not be effectively changed as required by law, regulators and guidelines. Within the context of this research this means that organisations responsible for the technical implementations of TLS must receive or retrieve the necessary information to configure their TLS configurations correctly. If GPs or professional organisations do not actively instruct hosters to comply with specific guidelines, the hosters may not be aware of this information and will not act. But when the GPs are not aware of the guidelines or do not understand the importance of such requirements, they will not be able to instruct their hosters. This blocks the necessary information flow. The lack of this flow of information was identified during the interviews with the ASPs. They were not aware of the guidelines and said that nor GPs or professional organisations instructed them

which guidelines were applicable to their TLS configurations. Therefore this paper argues that correctly securing eHealth services strongly relies on information flow between the domains and components of cyberspace. As an idea, the conceptualisation model of cyber space therefore could make this more explicit by visualising this important fundament such as illustrated in *figure 21.*

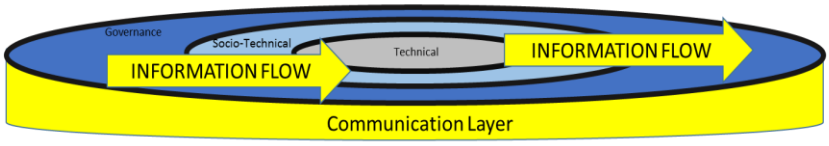


Figure 21; the Information layer of cyber space

During this research no centralised organisation was identified which actively facilitates or ensures the information flow in the eHealth eco system. Based on the interviews with ASPs it may be concluded that the security of eHealth systems could be improved if an organisation with cyber security expertise would provide guidance within this eHealth domain. During the interviews it was mentioned that measuring security and publishing the results would help to improve cyber security in this domain. A solution for this may a collaboration between internet.nl and a professional organisation within the realm of GPs, such as the LHV. By adding a TLS test page to the website of the LHV, (which uses the services of internet.nl) GPs can be stimulated to test their TLS settings on the LHV website which further refers to the NCSC guidelines for technical guidance. Such a professional organisation could also publish the accumulated and anonymised scores to create incentives to update the configurations. Another observation within this research is related to the transparency of security to patients. During this research it was further noticed that it was hard to distinguish the websites which were hosted by ASPs from other hosters. From the perspective of a patient it could be useful to be able to distinguish websites which provide good security from other websites. Currently security of the researched eHealth services is not transparent to patients. In the Netherlands web shops make use of quality labels which help consumers to gain trust in an online web shop. Currently there is not such a label for eHealth services which help patients to become aware of security when they make use of eHealth services. The initiative MedMij might have the potential to solve this transparency problem. The initiative is aimed at introducing a label for patient portals. If MedMij would also stimulate the flow of information, this can further contribute to the security of patient data.

The overarching conclusion of this research is the following; This research has shown that since the research of the DPA in 2013 that still a number of GPs have not implemented HTTPS on their eHealth services and that GPs which make use of ASPs for their services score higher on TLS tests than the GPs which make use of other hosters. The other hosters specifically must be stimulated to change their TLS configurations to the level stated in the guidelines. The low adoption of HSTS and support off client initiated renegotiation are the two main reasons the ASPs did not score maximum on the TLS tests. Stimulating the adoption of HSTS within the sector contributes to the protection of personal data when untrusted networks (such as hotspots) are used. The eHealth push, the adoption of mobile devices and the attention of the DPA for online security stipulates the importance to configure TLS correctly. This research has shown that centralised security guidance within the sector is lacking and is needed to stimulate the flow of information within the eHealth domain. Because the eHealth ambitions will further stimulate the adoption of ICT within healthcare, creating this guidance should be a high priority. The ASPs would like the government to take a lead in this guidance. However, the author of this thesis argues that the healthcare sector does not have to wait for guidance. Professional organisations, such as the LHV, and the MedMij initiative can already take the lead in ensuring the flow of already available cyber security information towards the hosters. Guidelines created by the government and the interpretation of the DPA are available and can actively be communicated by professional organisations. Last, but not least, it is important to realise that this research only looked at a very specific part of the eHealth domain and concludes that there is space to improve this specific part of cyber security within this domain. Adequately securing eHealth services encompasses more than only implementing TLS correctly on webservers. The vulnerability of web forms for SQL injection attacks is a small example of interesting research which can be performed on the sample used for this TLS research. Many new research questions can be defined for new research regarding the level of security of the eHealth domain.

References

[1] Centraal Bureau voor de Statistiek, “Acht procent van de Nederlanders nooit op internet,” 2016. [Online]. Available: https://www.cbs.nl/nl-nl/nieuws/2016/22/acht-procent-van-de-nederlanders-nooit-op-internet. [Accessed: 25-Oct-2016].

[2] Centraal Bureau voor de Statistiek, “Overheidswebsites veel gebruikt: Nederland in top van EU,” 2014. [Online]. Available: https://www.cbs.nl/nl-nl/nieuws/2014/10/overheidswebsites-veel-gebruikt-nederland-in-top-van-eu. [Accessed: 25-Oct-2016].

[3] Zorginstituut Nederland, “eHealth.” n.d. [Online]. Available: https://www.zorginstituutnederland.nl/kwaliteit/projecten/ehealth. [Accessed: 11-Oct-2016].

[4] Rijksoverheid, “Schippers en Van Rijn: door e-health betere zorg en meer eigen regie,” 2014. [Online]. Available: https://www.rijksoverheid.nl/actueel/nieuws/2014/07/03/schippers-en-van-rijn-door-e-health-betere-zorg-en-meer-eigen-regie. [Accessed: 03-Nov-2016].

[5] COMMISSION OF THE EUROPEAN COMMUNITIES, “e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area,” 2004.

[6] L. Gamio, “How data travels across the Internet,” 2015. [Online]. Available: https://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp/. [Accessed: 21-Oct-2015].

[7] Nationaal Cyber Security Centrum (NCSC), “Cyber Security Assessment Netherlands 2016,” 2016.

[8] J. Finkle, “FBI warns healthcare sector vulnerable to cyber attacks,” 2014. [Online]. Available: http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423. [Accessed: 11-Oct-2016].

[9] J. Finkle, “Your medical record is worth more to hackers than your credit card,” 2014. [Online]. Available: http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924. [Accessed: 11-Oct-2016].

[10] J. Conn, “Health systems are a candy shop of personal information,” 2016. [Online]. Available: http://www.modernhealthcare.com/article/20160804/NEWS/160809945. [Accessed: 11-Oct-2016].

[11] Classity Informatiebeveiliging, “Huisartsen Zonder ICT Door Storing In Netwerk Pharma Partners.” n.d. [Online]. Available: https://www.classity.nl/beschikbaarheid/KPN-storing/Pharma-Partners/ICT-huisartsen-onbeschikbaar. [Accessed: 20-Oct-2016].

[12] S. Paauw, “Datalek bij drie ziekenhuizen,” 2016. [Online]. Available: https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/datalek-bij-drie-ziekenhuizen.htm. [Accessed: 03-Nov-2016].

[13] J. van Duivenboden, “Huisarts, patiënt en e-health,” 2015.

[14] Johan Krijgsman et al., “Tussen vonk en vlam - eHealth-monitor 2015,” 2015.

[15] Johan Krijgsman et al., “eHealth Monitor 2016,” 2016.

[16] Wikipedia, “Form (HTML).” n.d. [Online]. Available: https://en.wikipedia.org/wiki/Form_(HTML). [Accessed: 11-Nov-2016].

[17] Autoriteit Persoonsgegevens, “Burgerservicenummer (BSN).” n.d. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/burgerservicenummer-bsn. [Accessed: 25-Apr-2016].

[18] Autoriteit Persoonsgegevens, “Gebruik van medische gegevens.” n.d. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/gebruik-van-medische-gegevens. [Accessed: 20-Oct-2016].

[19] Landelijke Huisartsen Vereniging (LHV), “Feiten en cijfers huisartsenzorg | LHV,” 2016. [Online]. Available: https://www.lhv.nl/uw-beroep/over-de-huisarts/kerncijfers-huisartsenzorg. [Accessed: 18-Sep-2016].

[20] Nationaal Cyber Security Centrum (NCSC), “ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS),” 2014. [Online]. Available: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html. [Accessed: 29-Apr-2016].

[21] Wikipedia, “HTTPS.” n.d. [Online]. Available: https://en.wikipedia.org/wiki/HTTPS. [Accessed: 17-Oct-2016].

[22] Patiëntenfederatie Nederland, “Zorgkaart Nederland.” n.d. [Online]. Available: https://www.zorgkaartnederland.nl/. [Accessed: 01-May-2016].

[23] Internet.nl, “Lancering Internet.nl tijdens Cyber Week 2015,” 2015. [Online]. Available: https://internet.nl/news/lancering-internet-nl-tijdens-cyber-week-2015/. [Accessed: 08-May-2016].

[24] C. Pagliari, D. Sloan, P. Gregor, F. Sullivan, D. Detmer, J. P. Kahan, W. Oortwijn, and S. MacGillivray, “What is eHealth (4): a scoping exercise to map the field.,” *J. Med. Internet Res.*, vol. 7, no. 1, p. e9, Mar. 2005.

[25] G. Eysenbach, “What is e-health?,” *J. Med. Internet Res.*, vol. 3, no. 2, p. E20, Jan. .

[26] Johan Krijgsman et al., “Ordening in de wereld van eHealth,” 2012.

[27] The Royal Dutch Medical Association (KNMG), “KNMG eHealth.” n.d. [Online]. Available: https://www.knmg.nl/advies-richtlijnen/dossiers/ehealth.htm. [Accessed: 21-Oct-2016].

[28] European Commission, “eHealth in Europe,” 2009.

[29] Rijksoverheid, “Rijksoverheid stimuleert gebruik e-health.” [Online]. Available: https://www.rijksoverheid.nl/onderwerpen/e-health/inhoud/overheid-stimuleert-e-health.

[30] College voor Zorgverzekeringen et al., “Convenant Governance eHealth,” 2013.

[31] Rijksoverheid, “20 miljoen voor e-health initiatieven van Nederlandse bodem,” 2016. [Online]. Available: https://www.rijksoverheid.nl/actueel/nieuws/2016/06/07/schippers-20-miljoen-voor-e-health-initiatieven-van-nederlandse-bodem. [Accessed: 18-Sep-2016].

[32] W. and S. Ministry of Health, “eHealth Week 2016,” 2016. [Online]. Available: http://www.e-healthweek.eu/. [Accessed: 20-Oct-2016].

[33] Zorg voor Innoveren, “EHealth financiering,” 2016. [Online]. Available: http://www.zorgvoorinnoveren.nl/kennisbank/ehealth-financiering/. [Accessed: 12-Oct-2016].

[34] Rijksoverheid, “Gebruik e-health in Nederland gestegen,” 2014. [Online]. Available: https://www.rijksoverheid.nl/actueel/nieuws/2014/10/10/gebruik-e-health-in-nederland-gestegen.

[35] Nictiz, “Nictiz, over ons.” n.d. [Online]. Available: https://www.nictiz.nl/over-nictiz/english. [Accessed: 12-Oct-2016].

[36] Nederlands Huisarsten Genootschap (NHG), “NHG-Standpunt: e-health voor huisarts en patiënt.” n.d. [Online]. Available: https://www.nhg.org/nhg-e-health.

[37] Landelijke Huisartsen Vereniging (LHV), “Leden over de LHV.” n.d. [Online]. Available: https://www.lhv.nl/vereniging/lidmaatschap/leden-over-de-lhv. [Accessed: 28-Oct-2016].

[38] NHG and LHV, “Toekomstvisie Huisartsenzorg,” 2012. [Online]. Available: http://www.tkv2022.nl/wp-content/uploads/2012/11/LHV001-37-Toekomstvisie-Totaal-Binnenwerk_021112_WWW.pdf. [Accessed: 09-Dec-2016].

[39] Landelijke Huisartsen Vereniging (LHV), “Online aanvraag herhaalrecept niet altijd beveiligd,” 2013. [Online]. Available: https://www.lhv.nl/actueel/nieuws/online-aanvraag-herhaalrecept-niet-altijd-beveiligd. [Accessed: 05-May-2016].

[40] Autoriteit Persoonsgegevens, “CBP: herhaalrecepten vaak via onbeveiligde verbinding,” 2013. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-herhaalrecepten-vaak-onbeveiligde-verbinding. [Accessed: 20-Oct-2016].

[41] Landelijke Huisartsen Vereniging (LHV), “LHV Service.” n.d. [Online]. Available: https://www.lhv.nl/service.

[42] Landelijke Huisartsen Vereniging (LHV), “Ook huisartsen moeten per 1 januari voldoen aan meldplicht datalekken,” 2015. [Online]. Available: https://www.lhv.nl/actueel/nieuws/ook-huisartsen-moeten-1-januari-voldoen-aan-meldplicht-datalekken. [Accessed: 27-Oct-2016].

[43] MedMij, “Wat is MedMij? | MedMij,” 2016. [Online]. Available: http://www.medmij.nl/wat-is-medmij/. [Accessed: 30-Oct-2016].

[44] Nictiz, “NEDERLANDSE PATIËNTEN WILLEN ZORG ONLINE REGELEN,” 2015. [Online]. Available: https://www.nictiz.nl/nieuws/nederlandse-patienten-willen-zorg-online-regelen.

[45] H. Croonen, “Nederland weer beste zorg van Europa,” *Medisch Contact*, 2015. [Online]. Available: http://www.medischcontact.nl/Nieuws/Laatste-nieuws/Nieuwsbericht/148196/Nederland-weer-beste-zorg-van-Europa.htm. [Accessed: 05-May-2016].

[46] Centraal Bureau voor de Statistiek, “Ongeveer drie kwart bezoekt jaarlijks huisarts en tandarts,” 2013. [Online]. Available: https://www.cbs.nl/nl-nl/nieuws/2013/27/ongeveer-drie-kwart-bezoekt-jaarlijks-huisarts-en-tandarts. [Accessed: 20-Oct-2016].

[47] D.C. Duchatteau et al., “Medisch-technologische ontwikkelingen zorg 20/20,” 2011.

[48] S. Paauw, “Apothekers passen 10 miljoen recepten per jaar aan,” 2016. [Online]. Available: https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/apothekers-passen-10-miljoen-recepten-per-jaar-aan.htm. [Accessed: 02-Oct-2016].

[49] Jan Jongenelen et al., “Veilig omgaan met e-mail in de zorg,” 2015.

[50] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons, “Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client,” *Cornell Univ. Libr.*, Oct. 2015.

[51] Centraal Bureau voor de Statistiek, “Ruim 10 miljoen online shoppers,” 2015. [Online]. Available: https://www.cbs.nl/nl-nl/nieuws/2015/30/ruim-10-miljoen-online-shoppers. [Accessed: 16-Oct-2016].

[52] Wikipedia, “HTTP.” n.d. [Online]. Available: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol. [Accessed: 11-Oct-2016].

[53] W3C, “How does the Internet work - W3C Wiki.” n.d. [Online]. Available: https://www.w3.org/wiki/How_does_the_Internet_work. [Accessed: 03-Nov-2016].

[54] Wikipedia, “Uniform Resource Locator - Wikipedia.” n.d. [Online]. Available: https://nl.wikipedia.org/wiki/Uniform_Resource_Locator. [Accessed: 03-Nov-2016].

[55] Nationaal Cyber Security Centrum (NCSC), “Wifi onderweg: gebruik een VPN, Wifi thuis: gebruik WPA2,” 2015.

[56] G. Podjarny, “HTTPS Adoption *doubled* this year,” 2016. [Online]. Available: https://snyk.io/blog/https-breaking-through/.

[57] Chromium Blog, “Moving Towards a More Secure Web,” 2016. [Online]. Available: http://blog.chromium.org/2016/09/moving-towards-more-secure-web.html. [Accessed: 20-Oct-2016].

[58] Wikipedia, “Transport Layer Security.” n.d. [Online]. Available: https://en.wikipedia.org/wiki/Transport_Layer_Security. [Accessed: 12-Nov-2016].

[59] The Internet Engineering Task Force, “The Transport Layer Security (TLS) Protocol Version 1.2,” 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246. [Accessed: 21-Oct-2016].

[60] The Internet Engineering Task Force, “The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-tls13-10,” 2015. [Online]. Available: https://tools.ietf.org/html/draft-ietf-tls-tls13-10. [Accessed: 28-Oct-2016].

[61] OWASP, “Transport Layer Protection Cheat Sheet - OWASP,” 2016. [Online]. Available: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet. [Accessed: 28-Oct-2016].

[62] The Internet Engineering Task Force, “Deprecating Secure Sockets Layer Version 3.0,” 2015. [Online]. Available: https://tools.ietf.org/html/rfc7568. [Accessed: 21-Oct-2016].

[63] Huisarts.info, “Welkom.” n.d. [Online]. Available: https://www.huisarts.info/pagina/welkom.

[64] Praktijkinfo.nl, “Praktijkinfo.nl.” n.d. [Online]. Available: https://www.praktijkinfo.nl/. [Accessed: 03-Nov-2016].

[65] K. Dreyer, “Mobile Internet Usage Skyrockets in Past 4 Years to Overtake Desktop as Most Used Digital Platform,” 2015. [Online]. Available: https://www.comscore.com/Insights/Blog/Mobile-Internet-Usage-Skyrockets-in-Past-4-Years-to-Overtake-Desktop-as-Most-Used-Digital-Platform. [Accessed: 20-Oct-2016].

[66] Centraal Bureau voor de Statistiek, “Internet faciliteiten; particuliere huishoudens,” 2016. [Online]. Available: http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83291NED&D1=a&D2=0-5&D3=0&D4=a&VW=T. [Accessed: 20-Oct-2016].

[67] Nictiz, “eHealth monitor2015 Infografhic,” 2015. [Online]. Available: https://www.nictiz.nl/SiteCollectionDocuments/Infographics/Infographic_eHealth_monitor2015.pdf. [Accessed: 05-May-2016].

[68] M. Kregting, “Slechts een vijfde Nederlanders gebruikt WiFi alleen thuis,” 2015.

[69] B. Nederland, “Internetbankieren via WiFi-hotspots: doe het veilig,” 2014. [Online]. Available: https://www.betaalvereniging.nl/nieuws/internetbankieren-via-wifi-hotspots/. [Accessed: 23-Oct-2016].

[70] T. Hollingshead, “People disregard security warnings on computers because they come at bad times,” 2016. [Online]. Available: https://news.byu.edu/news/most-people-disregard-security-warnings-when-they-pop-our-computer-screen-why-they-come-bad.

[71] Aertonline.nl, “Nederlanders niet voorbereid op cybercrime,” 2016. [Online]. Available: https://www.alertonline.nl/nieuws/2016/nederlanders-niet-voorbereid-op-cybercrime. [Accessed: 05-Dec-2016].

[72] S. Helme, “HSTS - The missing link in Transport Layer Security,” 2013. [Online]. Available: https://scotthelme.co.uk/hsts-the-missing-link-in-tls/. [Accessed: 18-Nov-2016].

[73] Nationaal Cyber Security Centrum (NCSC), “Factsheet HTTPS kan een stuk veiliger,” 2014. [Online]. Available: https://www.ncsc.nl/actueel/factsheets/factsheet-https-kan-een-stuk-veiliger.html. [Accessed: 05-Dec-2016].

[74] European Parliament and of the Council, *European data protection Directive 95/46/EC*. 1995.

[75] Dutch Government, “Wet bescherming persoonsgegevens,” 2000. [Online]. Available: http://wetten.overheid.nl/BWBR0011468/2016-01-01. [Accessed: 25-Apr-2016].

[76] Hendrik and James Legal Translations, “THE PERSONAL DATA PROTECTION ACT,” 2016.

[77] Autoriteit Persoonsgegevens, “Wat zijn persoonsgegevens?” n.d. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens. [Accessed: 20-Oct-2016].

[78] Rijksoverheid, “Burgerservicenummer (BSN).” n.d. [Online]. Available: https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/inhoud/burgerservicenummer-bsn. [Accessed: 12-Oct-2016].

[79] Autoriteit Persoonsgegevens, “Taken en bevoegdheden.” n.d. [Online]. Available:

https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/taken-en-bevoegdheden. [Accessed: 20-Oct-2016].

[80] Autoriteit Persoonsgegevens, “CBP Richtsnoeren BEVEILIGING van persoonsgegevens,” 2013.

[81] Autoriteit Persoonsgegevens, “Jaarverslag 2015,” 2016.

[82] College Bescherming Persoonsgegevens, “Onderzoek naar de beveiliging van het online aanvragen van herhaalrecepten bij huisarts en apotheek,” 2013. [Online]. Available: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2013-beveiliging-online-herhaalrecepten.pdf. [Accessed: 20-Oct-2016].

[83] Autoriteit Persoonsgegevens, “Verscherpte aandacht CBP voor OpenSSL,” 2014. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/nieuws/verscherpte-aandacht-cbp-voor-openssl. [Accessed: 20-Oct-2016].

[84] Nationaal Cyber Security Centrum (NCSC), “Factsheet Heartbleed: Ernstige kwetsbaarheid in OpenSSL,” 2014.

[85] Autoriteit Persoonsgegevens, “Beveiliging contactformulier op websites fysiotherapeuten,” 2016. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/nieuws/beveiliging-contactformulier-op-websites-fysiotherapeuten. [Accessed: 20-Oct-2016].

[86] Nimrod Aviram et al., “DROWN: Breaking TLS using SSLv2,” in *Proceedings of the 25th USENIX Security Symposium, August 2016*, 2016.

[87] Autoriteit Persoonsgegevens, “Verscherpte aandacht AP voor verouderd beveiligingsprotocol SSLv2,” 2016. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/nieuws/verscherpte-aandacht-ap-voor-verouderd-beveiligingsprotocol-sslv2. [Accessed: 20-Oct-2016].

[88] Autoriteit Persoonsgegevens, “Meldpicht Datalekken,” 2016. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken. [Accessed: 20-Oct-2016].

[89] Autoriteit Persoonsgegevens, “Beleidsregels voor toepassing van artikel 34a van de Wbp,” 2015. [Online]. Available: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf. [Accessed: 06-May-2016].

[90] NEN, “NEN 7512:2015,” 2015.

[91] Nationaal Cyber Security Centrum (NCSC), “ICT-Beveiligingsrichtlijnen voor Webapplicaties,” 2015. [Online]. Available: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html. [Accessed: 22-May-2016].

[92] Jan van den Berg et al., “On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education,” 2014.

[93] Glenn D. Israel, “Determining Sample Size,” *University of Florida IFAS Extension*, 2009. [Online]. Available: http://www.sut.ac.th/im/data/read6.pdf. [Accessed: 21-Oct-2016].

[94] Internet.nl, “Internet.nl vernieuwd: ‘HSTS’ en ‘afgedwongen HTTPS’ tellen mee,” 2016. [Online].

Available: https://internet.nl/news/internetnl-vernieuwd-hsts-en-afgedwongen-https-tellen-mee/. [Accessed: 20-Nov-2016].

[95] Qualys, "Qualys SSL Labs." n.d. [Online]. Available: https://www.ssllabs.com/ssltest/. [Accessed: 26-May-2016].

[96] ASP1, "Thesis Interview," 2016.

[97] ASP2, "Thesis Interview," 2016.

[98] ASP3, "Thesis Interview," 2016.

[99] ASP4, "Thesis Interview," 2016.

[100] Logius, "ICT-beveiligingsassessments," 2012. [Online]. Available: https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/. [Accessed: 08-Dec-2016].

[101] The Royal Dutch Medical Association (KNMG), "The Royal Dutch Medical Association (KNMG)." n.d. [Online]. Available: https://www.knmg.nl/over-knmg/contact/about-knmg.htm. [Accessed: 12-Oct-2016].

[102] KNMG, "Privacywetgeving en omgaan met patiëntengegevens," 2002. [Online]. Available: http://www.knmg.nl/Publicaties/KNMGpublicatie/62836/Privacywetgeving-en-omgaan-met-patientengegevens-2001.htm. [Accessed: 05-May-2016].

[103] S. Nouwt, "Beveiligen van patiëntgegevens: Why should I?," 2013. [Online]. Available: https://www.knmg.nl/actualiteit-opinie/columns/column/beveiligen-van-patientgegevens-why-should-i.htm. [Accessed: 02-Oct-2016].

[104] Zorginstituut Nederland, "Kwaliteitsinstituut." n.d. [Online]. Available: https://www.zorginstituutnederland.nl/kwaliteit. [Accessed: 27-Oct-2016].

[105] Patiëntenfederatie Nederland, "Patientenfederatie." n.d. [Online]. Available: https://www.patientenfederatie.nl/. [Accessed: 04-Oct-2016].

[106] Patiëntenfederatie Nederland, "KNMG, NPCF en ZN slaan handen ineen om eHealth te stimuleren," 2012. [Online]. Available: https://www.patientenfederatie.nl/nieuws/knmg-npcf-en-zn-slaan-handen-ineen-om-ehealth-te-stimuleren. [Accessed: 12-Oct-2016].

[107] Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ), "VZVZ, over VZVZ." n.d. [Online]. Available: https://www.vzvz.nl/page/Zorgconsument/Over-VZVZ. [Accessed: 12-Oct-2016].

[108] Zorgverzekeraars Nederland (ZN), "Zorgverzekeraars Nederland." n.d. [Online]. Available: https://www.zn.nl/1483931648/English.

Appendix

APPENDIX I

The Royal Dutch Medical Association (KNMG) – 'The KNMG is the professional organisation for physicians in the Netherlands'[101], which was established in 1849. The organisation has the mission to improve healthcare. To achieve this the KNMG provides services to their members. The organisations therefore create and publishes guidelines and policies. The KNMG stimulates eHealth and focusses on the legal, ethical and preventive aspects of eHealth in relation to the functioning and education of physicians[27]. In 2002 the KNMG published a document in relation to the Dutch privacy legislation and the processing of patient data.[102] Appendix 8 of this document describes the requirements for the electronic exchange of information regarding patients. One of the requirements described is the full encryption of this data during storage and in transit. In 2013 an online article on the website of the KNMG repeated this requirement.[103]

Kwaliteitsinstituut (KI) has the mission to help improve the quality of healthcare and make health care quality information accessible to anyone.[104] KI is part of Zorginstituut Nederland (ZN) which is a governmental organisation which serves the interest of all people who have the right to healthcare within the Netherlands. ZN supports and encourages organisations within the healthcare sector in creating standards for their sectors and helps creating instruments which measure the quality of healthcare. They support patients in making healthcare choices by providing insight into this information. KI has the goal to make sure that new quality guidelines encourage the use of eHealth.

Nederlandse Consumenten Patiëntenfederatie (NPCF) – NCPF is the old name of Patiëntenfederatie Nederland (PN). PN represents 160 consumer and patient organisations.[105] PN want to represent Dutch patients within the waiting room, within the politics, at insurance companies and in the media. One of the focus points of the PN is digital care. PN is responsible for the Zorgkaart website (www.zorgkaartnederland.nl) which facilitates consumers in finding healthcare providers and provides the option to post and read reviews regarding these providers.[22] PN wants to increase the acceptance of eHealth among patients and brings back the eHealth experience of these patients as input for the creation of standards and the procurement of healthcare.[106]

Nictiz – "Nictiz is the centre of expertise for standardisation and eHealth".[35] "Nictiz works towards better healthcare through better information. We support the healthcare sector in the use of IT to improve quality and efficiency within healthcare." Nictiz conducts research into the state of eHealth within Netherlands. The results are published in their yearly eHealth monitor, which has been published from the year 2013 and onward.

Vereniging van Zorgaanbieders Voor Zorgcommunicatie (VZVZ) - VZVZ is responsible for the exchange of medical data through the healthcare infrastructure called "Landelijk Schakelpunt" (LSP). VZVZ develops and manages this infrastructure which is used by healthcare providers to exchange healthcare information.[107]

Zorgverzekeraars Nederland (ZVN) - ZVN is "is the umbrella organization of nine health insurers in The Netherlands. They are: a.s.r., CZ, Eno, DSW, ONVZ, Menzis, VGZ, Zilveren Kruis, en Zorg en Zekerheid. ZN supports its members by fulfilling the mission of the Dutch health insurers: to arrange health care of good quality for their insured, that is affordable and accessible at the same time and aimed at promoting the well-being of their insured". [108]

APPENDIX II

1. Kunt u een schatting geven van het aantal huisartsen in Nederland dat deze online dienst bij u afneemt?
2. Bent u op de hoogte van de huidige interpretatie van de Autoriteit Persoonsgegevens in relatie tot het beveiligen van webformulieren waarop bijzondere persoonsgegevens worden verwerkt?
3. Worden er door huisartsen en/of huisartsenverenigingen wel eens aan u vragen gesteld over de TLS implementatie op hun websites of hebben deze u gewezen op de richtlijnen?
4. U voldoet niet helemaal aan de richtlijnen (zie de scanresultaten), zou u kunnen aangeven waarom dat het geval is?
5. Bent u voornemens, en in staat om uw configuratie conform de richtlijnen aan te passen, zo ja op welke termijn, zo nee wat zijn de belemmeringen daarvoor?
6. Vind u dat een organisatie een taak op zich zou moeten nemen om ASPs werkzaam voor huisartsen te ondersteunen en informeren over dit soort zaken? zo ja welke organisatie zou dat moeten zijn, en wat zou deze organisatie moeten doen?
7. Is er informatie die u verder nog zou willen delen?