Medical Data flows in the Landelijk Schakelpunt

A research into the digitized electronic health record in the Netherlands analysed from a privacy and security point of view.

Marissa de Beeld
s1698214
Master Thesis
Crisis and Security Management
Leiden University
January 16th 2020

Supervisor: dr. T. van Steen
Second reader: dr. T. Tropina
Words: 18.718

Abstract

Due to the ever-increasing developments in information and communication technologies, more and more processes are being digitized. These include among others processes from the public sector such as education and healthcare. In 2011, the Dutch Senate has withdrawn from the design of the Electronic Health Record (EPD) because the system was found to be insufficient reliable and secure for medical data exchange. However, the advantages of such a system were acknowledged and permission was given for the development of a system with a similar purpose. From January 2012 onwards, the Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) is responsible for the private restart of a system to digitally exchange medical data, which is called the Landelijk Schakelpunt.

This research analyses to what extent the design of the Landelijk Schakelpunt (LSP) is improved in terms of privacy compared to the earlier rejected Electronic Health Record (EPD). The analysis is executed by applying the NIST Cyber Security Framework, which consists of five phases: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover. The application of the conceptual model had a dual function. It created more insight into which privacy elements are already visible in the system. Besides, it displayed weak elements, which offers an opportunity for further incorporation of privacy. After completing the analysis there will be a reflection on the findings and the effects will be outlined. Besides, recommendations will be explicated that reinforce the privacy concept within the LSP's business operations by focusing on the substantive system, the humans that have to deal with the system, and the perspective of patients in which the importance of data control is high. This research will end with suggestions for future research to offer even more insight in the issue that is in scope.

Key words: *Digitization, Healthcare, Landelijk Schakelpunt, Electronic Health Record*

List of Abbreviations

AP	Autoriteit Persoonsgegevens (Dutch Data Protection Authority)
DPIA	Data Protection Impact Assessment
EPD	Elektronisch Patiëntendossier (Electronic Health Record)
EU	European Union
IGJ	Inspectie Gezondheidszorg en Jeugd
ISACA	Information Systems Audit and Control Association
GBZ	Goed Beheerd Zorgsysteem (Well managed care system)
GDPR	General Data Protection Regulation
GZN	Goed Beheerd Zorgnetwerk (Well managed care network)
LSP	Landelijk Schakelpunt
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
RvIG	Rijksdienst voor Identiteitsgegevens
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
WGBO	Wet op Geneeskundige Behandelingsovereenkomst

Table of Contents

1. Introduction

Due to the ever-increasing developments in information and communication technologies, more and more processes are being digitized. These include, among others, processes from the public sector such as education and health care. Zooming in on the healthcare sector, digitization has meant that it is currently possible to take healthcare related information in different formats and deliver these items in the same basic format at high speeds (Dwivedi et al., 2002). It is also possible to combine different formats of information - such as sound, video, animation, text and graphics - and present them in an interactive manner. The advantages of digital processes in the healthcare sector seem endless, but there are also important disadvantages that require more attention. When the information of medical records of patients is being digitized, more sensitive personal data needs to be stored, but meanwhile the security and privacy of these records also need to be guaranteed.

On May 28th 2018 the General Data Protection Regulation (GDPR) entered into force. This regulation describes new requirements regarding the processing of personal data and has been called the toughest privacy and security law in the world (Welford, 2019). Initially, it has been drafted and passed by the European Union (EU), but it imposes obligations onto organizations anywhere as long as data related to people in the EU is targeted or collected. The regulation itself exists of 99 articles and might be experienced as large, far-reaching, and light on specifics, which makes it more difficult for organizations to become GDPR compliant (Welford, 2019). However, there are fines against those who violate the privacy and security standards, with penalties reaching into millions of euros.

To check whether organizations still meet their lawful obligations different institutions have been appointed in European countries. In the Netherlands this institution is called the Autoriteit Persoonsgegevens (AP), which is also the organization where clients can practice their rights such as the right of access, right to rectification and right to erasure, and where data breaches need to be reported. During the first half of 2019, the Dutch Data Protection Authority (AP) received 11,906 reports of data breaches. In case this trend continues, the AP expects an increase of 14 per cent for 2019 compared to 2018 (AP, 2019a). Since the entry into force of the data breach-reporting obligation, the AP receives most reports from the healthcare sector. The largest number of data breach reports within the healthcare sector comes from hospitals (23%) and pharmacies (22%). Most notifications are made after sending personal data

to the wrong recipient. Smaller healthcare institutions such as health and welfare organizations (24%), social services (15%) and dentists (6%) report data leaks due to hacking, malware or phishing more often than larger healthcare institutions (AP, 2019a). To reduce these numbers, the AP provides healthcare institutions with tips to prevent a number of common types of data breaches.

One digital innovation that may increase, instead of decrease, the number of data breach reports is the Landelijk Schakelpunt (LSP). LSP is the successor of the electronic health record (EPD). In this new system medical data of patients is exchanged "anonymised" by identifying patients based on social security numbers. The disadvantage of this system is the danger that these numbers can easily make a link between information from different files (AP, 2019b). Due to the high risks and the number of disadvantages, there has been a difficult introduction of the electronic health record after the first initiation, which also emphasizes the lack of confidence from a political point of view. After the Dutch Senate quit the national EPD it called for a reliable infrastructure to exchange medical data between doctors and other medical specialists (Modderkolk, 2015). Because the Senate had withdrawn, the LSP got a private restart in 2012. The responsible party of this private restart is the ‘Vereniging van Zorgaanbieders voor Zorgcommunicatie’ (VZVZ), which exists of four umbrella organizations for healthcare providers: the umbrella organizations for general practitioners, general practitioner posts, pharmacies and hospitals (VZVZ, 2019).

Meanwhile, the system has been further developed and identification still takes place by inserting the social security number, meaning an easy target for cyber criminals that want to benefit from identity theft. To combat cyber crime, the Central Identity Fraud and Errors Reporting Center (CMI) was established as part of the National Service for Identity Data (RvIG), from the Ministry of Interior (BZK). This institution provides a platform for reporting identity theft, gives tips to prevent it and offers advice and support when an individual has become a victim (RvIG, 2019).

Due to the difficult establishment of the LSP – the withdrawal of the Dutch Senate and the private restart of the VZVZ – it would be expected that the critical remarks that were given throughout the entire process received sufficient attention to guarantee the safety and privacy of this system. This research will assess whether this expectation could be justified.

1.1 Research Question

To address the gap in the existing literature, this research explores how security and privacy of the Landelijk Schakelpunt are arranged. More specifically, this research focuses on the use of social security numbers in the digitized system of providing insight in medical records. On one hand, it is attractive to use a digital system with easy access to medical health records. When there are accidents or other situations where adequate help is needed, there will be little time lost on identification and corresponding personal information. On the other hand, it is necessary to control and guarantee the security and privacy of patients. Therefore, the following explorative research question will guide this research:

To what extent is the design of the Landelijk Schakelpunt (LSP) improved in terms of privacy compared to the earlier rejected Electronic Health Record (EPD), when applying the NIST Cyber Security Framework?

This study will use a case study approach to thoroughly analyse the establishment of the Landelijk Schakelpunt. The research will explore in-depth and by semi-structured interviews how different involved parties experience this system. Therefore, respondents will exist of a mix between the different identified stakeholders. First of all, patients can be identified since they are the ones whose personal data is recorded. Patients are in this research conceptualized as chronically ill people that have to deal with different healthcare institutions. Another identified stakeholder exist of privacy specialists, whom are able to explain how privacy is defined in legislation and what are the patient's rights. Furthermore, IT auditors will be interviewed because of their focus on the IT infrastructure and content of digitized systems. The NIST Cyber Security Framework, which will be explained in detail in section 2.3.2, exists of five different phases that will be analysed based on various standards (Appendix 1). IT auditors are familiar with these kinds of frameworks. Besides privacy specialists and IT auditors, medical specialists also must be identified as stakeholders. Examples of these specialists are general practitioners, nurses and pharmacists. The perspectives of medical specialists are of great importance since they are the ones that actually work with the system and can indicate the role and functioning of the LSP within their daily working activities.

Digital innovations are focused on new combinations of digital and physical components to produce new products (Yoo, Henfridsson & Lyytinen, 2010). Examples are physical products that are made programmable, addressable, communicable, and traceable. The Landelijk Schakelpunt system relies on digitization, but a digital innovation is also susceptible to undesirable purposes of criminals, such as identity theft. Thus, this research attempts to analyse how the successor of the Electronic Health Record (EPD) has been improved to provide a safe and secure new system, the Landelijk Schakelpunt (LSP), in terms of privacy. This will be done by analyzing the privacy concept, in combination with the perspectives from the NIST cyber security framework. The following sub questions will guide this study:

1. *How could the concept 'privacy' be defined?*
2. *How could the NIST Cyber Security Framework be interpreted from a privacy point of view?*
3. *What role did privacy have in the Electronic Health Record (EPD)?*
4. *To what extent are security and privacy measures incorporated in the design of the Landelijk Schakelpunt (LSP) to introduce a more stable system compared to the rejected EPD?*

1.2 Relevance

This research is scientifically relevant because the risks may be underestimated in relation to the benefits that the LSP can offer. With the arguable reliability of identification based on social security numbers, the privacy of every patient may be questioned. Due to the ever-increasing developments of digitization, more and more information is being published on the Internet, which means that cyber criminals are increasingly thinking of new ways to misuse personal data. To prevent this, various legal guidelines and standards have been drawn up, such as the General Data Protection Regulation (GDPR) and the ISO 27001 standard. During the initiation and design of the system, the main focus was laid on how it could be introduced from a legal point of view. However, a legal perspective alone cannot ensure sufficient reliability of a system, because there always remains a dependence on substantive knowledge and application of that knowledge. There are still humans whom will have to learn to deal with the system (Officiële Bekendmakingen, 2011).

This research is socially relevant because it can affect everyone in society. Every patient is forced to make a choice whether they do or do not want to share their

medical data via the LSP. However, there appear to be many consequences to this choice, which reduces the non-committal aspect. A survey by EenVandaag has shown that patients who do not want to share their medical data often have difficulties in receiving their medication, or do not receive medication at all at a random pharmacy (Nu.nl, 2017). The prescriptions that patients obtain from their general practitioner, dentist or specialist sometimes prove to be insufficient to actually obtain the prescribed medication, creating the impression that they must first be affiliated with the LSP before they can receive medication. This research therefore focuses on the design and management of the LSP, and how this system is evolved to guarantee security and privacy compared to the earlier rejected electronic health record (EPD).

1.3 Reading guide

This first chapter has given more insight in the subject, research design and relevance of this thesis. The following chapter will focus on the body of knowledge, including the research object, an exploration of various academic perspectives and the theoretical framework. Chapter three will discuss the methods used in this research, explaining how data will be collected and analyzed, followed by zooming in on the possible limitations in terms of reliability and validity. Chapter four focuses on the analysis of the different findings, followed by the fifth chapter that will address the conclusion and discussion, finalized with recommendations.

2. Body of knowledge

The previous chapter described the cause, research question and relevance of this research. This chapter will focus on the theoretical framework that will be used. First, the research object LSP will be explained followed by an exploration of various academic perspectives. Thereafter, the theoretical concept will be addressed, existing of the NIST cyber security framework and an assessment of how the phases of the NIST framework are applicable in this research.

2.1 Background information

In 2008, the Ministry of Health, Welfare and Sport (VWS) initiated the Electronic Health Record (EPD). At the start three goals have been identified. The first goal concerns the centralization of knowledge transfer, which occurs because all medical information of a patient becomes accessible from any location, while the information is stored scattered at different health care providers. Theoretically, this should reduce the chance of an incorrect diagnosis or treatment. The second goal focuses on increasing efficiency, whereby written documentation is avoided and research is not duplicated. The additional advantage of this goal is the reduction of costs. The third goal focuses on long-term quality improvement. The effect of certain treatment methods can be better monitored and assessed by analysing the data in the electronic patient portal (Kamerstukken, 2006).

However, a major debate has taken place in the Dutch Lower House since the finding that the EPD system would not be sufficiently secure for the exchange of medical data (ZorgNu, 2017). As a result, in 2011 the Senate decided the EPD would not be implemented. However, since then a private restart has been made on developing a similar system that also revolves around the exchange of medical data from patients, called the Landelijk Schakelpunt (LSP). To prevent the LSP from encountering the same difficulties, various studies have been conducted into the risks associated with digitizing the electronic patient portal. First, there is a risk that unauthorized persons will gain access to the system, which may ultimately lead to cyber criminals viewing, changing, copying and publishing patient's personal data. Another risk is the carelessness of authorized users. A small error can have many consequences because all care providers can request the records. In addition, the possible misuse of the stored data is risky because data can be used for a purpose other than for which it was recorded (ZonMw, 2019).

The LSP consists of a network to which healthcare providers can join, a so-called "healthcare infrastructure". This network enables providers to consult medical data of their patients in each other's systems at any time (Volg Je Zorg, 2019a). The earlier discussion about the safety of the EPD is attempted to be resolved because the LSP has been specially developed and secured for this purpose. The Landelijk Schakelpunt therefore does not form a database, because the medical data is not stored (Volg Je Zorg, 2019a). The information about patients can be viewed while the data remains in the files at general practitioners and pharmacies. When a patient has given consent, the medical specialists report the social security number to the reference index in the LSP. By searching for this social security number, other care providers can consult medical information, which may be necessary prior to starting treatment (Volg Je Zorg, 2019a).

Due to the earlier remarks that have been placed with the EPD, it is expected that the LSP has been more responsive with security and privacy matters during the design phase. A number of measures have been taken to achieve a high quality of information security (Volg Je Zorg, 2019b). The first measure concerns the fact that healthcare providers cannot naturally connect to the network. The computer system of the healthcare provider is checked against strict security requirements before receiving access. In addition, a healthcare provider can only log in with a special pass and password. Another measure is the mandatory consent of a patient before a healthcare provider can share the medical data. This is not possible without permission. In addition, only healthcare providers who are in charge of a patient's treatment may view the relevant medical data. An additional component here is that it actually must be necessary for that treatment. To verify this, close supervision takes place. The network keeps track of what healthcare provider has viewed what data and at what amount of time. A patient has the right to check this. In addition, this option is also included in legislation and regulations such as the GDPR and the Dutch Medical Treatment Agreement Act (WGBO) (Volg Je Zorg, 2019b).

The Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) consists of four umbrella organizations of care providers: the umbrella organizations of general practitioners (LHV), general practitioner posts (InEen), pharmacies (KNMP) and hospitals (NVZ). Since January 1st 2012, this party has been designated as responsible for the electronic exchange of medical data via the Landelijk Schakelpunt (VZVZ, 2019). The organization investigates how the system can be optimized. In 2018, the

VZVZ published the report "Effects and benefits of the use of health care infrastructure", which states the LSP has become an important tool for data exchange in Dutch health care (ICT & health, 2018). Measurements in 2015 clearly differ from measurements in 2017 where a significant increase in exchange can be observed. This is partly due to an increase in the number of affiliated general practitioner practices and pharmacies, and more awareness of the aspect of explicitly granting consent. In addition, significantly more information about medication was requested. However, research by the Radar Test Panel shows that a majority of the 35,000 members surveyed do not know the LSP has been introduced (ZorgNu, 2017). It is remarkable that people indicate they do not know whether or not they are connected to the system, since it entails their personal data.

Studies of this kind suggest there is a gap between the intentions and perceptions of policymakers and practitioners on one hand, and patients whose medical data can be viewed through the LSP on the other hand. In order to determine whether this actually entails negative consequences and risks, such as the loss of privacy and the disclosure of personal data, institutions with monitoring and supervisory functions have been set up, such as the Dutch Data Protection Authority (AP) and the Inspectie Gezondheidszorg en Jeugd (IGJ). The AP sets guidelines on, among other things, the use of the social security number and protection of access to medical data. Regarding the use of the social security number, healthcare providers have a legitimate legal basis to use it for the performance of their duties, by being considered as independent administrative bodies. However, consulting social security numbers is only permitted when it is considered necessary (AP, 2019b). The guidelines concerning the protection of access of medical data include for example the method of authorization, such as how it is determined which person in charge has access to which patient records and when. Another example is the method of logging and checking, such as whether there will be recorded who and when a file is consulted. The AP serves the important function of removing concerns about privacy. The IGJ is also concerned with safeguarding privacy by supervising personal care, publishing independent judgments, and openness to improve care (Rijksoverheid, 2019).

2.2 Academic perspectives

Digitization takes place within various parts of the healthcare sector. Different applications have been developed and marketed to assist in the process of diagnosis, but according to Jutel & Lupton (2015) little attention has been paid to the content, claims, potential risks, limitations, or benefits of these apps. The authors identify easy access to medical data and a convenient diagnostic tool for medical specialists as great advantages, but they also acknowledge numerous significant potential harms (Jutel & Lupton, 2015). These harms entail conflict of interest, transparency, ethical and privacy issues, the accuracy of content, healthcare delivery and the doctor-patient relationship. Jutel & Lupton (2015) warn both patients and practitioners to use medical apps with great caution in the context of evidence-based practices.

Abouelmehdi et al. (2017) argue the trend of digitizing healthcare can be explained by the limitless opportunities for big data in health research, knowledge discovery, clinical care, and personal health management. By gaining more insight in processes the quality of healthcare could be improved. However, there are also obstacles and challenges identified. These exist of technical challenges, privacy and security issues, and skilled talent (Abouelmehdi et al., 2017). To reduce risks of these identified obstacles regarding the security and privacy of healthcare data, different technologies have been introduced, such as authentication, encryption, data masking, and access control (Abouelmehdi et al., 2017).

Patil & Seshadri (2014) argue that the ever increasing cost for healthcare and increased healthcare premiums lead to the need for proactive healthcare and wellness. Digitizing medical records result in an increase in sheer volume of data in terms of complexity, diversity and timeliness. Patil & Seshadri (2014) agree with Abouelmehdi et al. (2017) that big data is seen as the solution, but they argue that is because of the cost reducing priority while also wanting to improve the care process, delivery and management. By using big data mechanisms, security and privacy issues continue to grow (Patil & Seshadri, 2014). Patil & Seshadri (2014) argue that this is partly due to the prominence of big data, resulting in hosting companies that become more reluctant to share massive healthcare data for centralized processing.

Schneider et al. (2014) focus on the safety of health information technology, resulting in several dimensions: using health IT to make care safer, ensuring that health IT is safe itself, and ensuring that health IT is used safely. The potential for health IT to improve the safety of health care delivery has been appreciated for decades, but the

role of health IT in introducing safety risks has been recognized for not that long (Schneider et al., 2014). As the use of health IT has grown, users have begun to observe what it could mean for them and their personal data. There are multiple situations that could occur such as hardware and software can malfunction, data can be lost or corrupted during transmission, deploying complex technologies in a complex organizational environment can introduce new hazards and safety risks. According to Schneider et al. (2014) identifying and mitigating health IT safety risks is a relatively new concept for most health care organizations.

When zooming in on the introduction of the Electronic Health Record (EPD) Groothuis (2007) emphasizes in her article that the process of whether or not to implement the EPD has taken a lot of time and the legal framework involves many layers. Rules concerning the use of personal and medical data are laid down at international, European and national levels. A distinction is made between the fundamental right to respect for privacy as laid down in Article 17, paragraph 1 of the International Covenant on Civil and Political Rights (ICCPR); Article 8, paragraph 1, of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR); and Article 10, paragraph 1, of the Dutch Constitution. In addition, there is also Directive 95 / 46l / EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; the Personal Data Protection Act (Wbp) which has been changed to the General Data Protection Regulation (GDPR); the Civil Code and other guidelines as drawn up by the AP.

According to Schulman (2004), despite legislation and regulations being laid down, safety must be seen as an illusion: safe organizations do not exist because results achieved in the past offer no guarantee for future safety of any organization. From this point of view it may never be the case that the Landelijk Schakelpunt could be classified as a safe and secure system.

Privacy lawyer Solove does not agree with Schulman (2004). According to Solove it is not a problem that information about individuals is collected, but the lack of insight into where and how this data is used must be seen as a problem (Martijn & Tokmetzis, 2016). This increases the power of data collecting and sharing governments and institutions. To gain more insight into the handling of data, the system will have to be studied in terms of content.

One way to gain this insight Martijn & Tokmetzis (2016) address is by applying the NIST Cyber Security Framework. This framework consists of five different phases: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. When the phases are combined, the functions provide a high-level, strategic view of the lifecycle of an organization's management of cyber security risk (NIST, 2018). This is partly due to the fact that there is a clear structure, by identifying underlying key categories and subcategories for each function. After considering the various perspectives, this research will be conducted on the basis of the NIST cyber security framework. The choice for this perspective was made because this concept does not only deal with technical measures, but it also focuses on the human aspect of a system. In addition, this framework is applicable to the complex environment in which the Landelijk Schakelpunt is involved. The next section will explain in detail how this framework can be applied.

2.3 Theoretical framework

This section elaborates on the theoretical concept that forms the central point of view in this research, based on analysing the concept of privacy, the NIST Cyber Security Framework and the conceptual framework in which the NIST framework is studied from a privacy perspective.

2.3.1 Privacy

Although the importance of privacy is being discussed and published more often, the concept seems difficult to interpret. According to Cuijpers (2007), privacy is experienced as complex because the concept is difficult to consider on its own, but depends on the context in which it is placed. In this case, privacy is an umbrella term that can be divided into various dimensions, including relational, physical, territorial, and communicative privacy. Because the concept has been broadened over time, there is a growing tendency in which not only the private sphere must be protected, but also privacy in public spaces must be guaranteed (Cuijpers, 2007).

Koops & Vedder (2001) also acknowledge that privacy is a complex concept, and contextual factors such as technical, social, and economic developments are of influence. The authors distinguish three ways in which privacy is given meaning: (1) spatial privacy, (2) intimacy or individual self-determination, and (3) informational privacy. This research focuses on the third category. Informational privacy deals with the protection of personal data. The term privacy is used here as a defence against unwanted disclosure of information about the privacy of an individual, including medical information (Koops & Vedder, 2001). By shaping laws and regulations such as the GDPR, a common core concept is formulated, which can also be specified per domain by taking contextual and functional factors into account. The GDPR protects patients by introducing rules on for example permission and limiting insight by third parties. In addition to the value of freedom or self-determination, there is also a monitoring function with regard to the dissemination of personal information. With this control mechanism, patients themselves are able to determine and maintain relationships with others and institutions (Koops & Vedder, 2001).

This study focuses on the privacy of patients who have given consent to have their medical data requested via the LSP. The automation processes within the healthcare domain include various IT applications whereby connections between different actors are realized (Keizer, 2011). This concerns both doctor-doctor (D2D)

and doctor-patient (D2P) and patient-patient (P2P) connections. Within the health care domain, patients and other stakeholders appear to be more aware of the importance of privacy, which can be explained from their dependent and vulnerable position (Keizer, 2011). Undergoing medical treatment is without exception a violation of personal space and affects physical privacy. In addition, absolute privacy cannot be spoken of, since communication between healthcare provider and healthcare consumer is and will remain necessary. Medical information is about informational privacy, with attention being paid to protecting information and data against unauthorized intruders. However, there are potential risks here, as the rationale behind the LSP focuses on making medical data available as efficiently and effectively as possible, with the challenge of being able to manage and control information flows. To analyse how the information flows of the LSP are managed and controlled, the NIST Cyber Security Framework will be applied. This concept will be explained in the following section.

2.3.2 NIST Cyber Security Framework

The US National Institute of Standards and Technology (NIST) encourages organizations to collaborate on the plans, assessments, plans of action, and milestones to maximize efficiency and reduce duplication of effort. The objective is to ensure that security and privacy requirements derived from laws, executive orders, directives, regulations, policies, standards, or missions and business functions are adequately addressed, and the appropriate controls are selected, implemented, assessed, and monitored on an ongoing basis (NIST, 2018). The Cyber Security Framework consists of five different phases as shown in figure 1: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover.

Figure 1: NIST Cyber Security Framework by Stickman Consulting (2019).

These five phases form the core of the framework and consist of cyber security activities, desired outcomes, and applicable references that are common across sectors

that are dealing with critical infrastructures. The core presents industry standards, guidelines, and practices in a manner that allows for communication of cyber security activities and outcomes across the organization. It also represents the executive level to the implementation/operations level (NIST, 2018). When the five phases are considered together, the functions provide a high-level, strategic view of the lifecycle of an organization's management of cyber security risk. This is partly due to the fact that it identifies underlying key categories and subcategories for each function and that these will be matched with informative references such as existing standards and guidelines (NIST, 2018)

During the first phase identification takes place. The goal of this phase is to develop an organizational understanding to manage cyber security risk to systems, people, assets, data, and capabilities (NIST, 2018). The activities during this phase are foundational for an effective use of the framework, since it forms the basis for the following phases. It is of great importance to understand the business context, the resources that support the critical functions, and the related cyber security risks that enables an organization to define priorities. These priorities will be in alignment with the risk management strategy and business needs (NIST, 2018). Examples of functions that will be focused on during the identification phase entail asset management, business environment, governance, risk assessment, and risk management strategy (NIST, 2018).

After the identification phase, there comes a protection phase. The goal of this phase is to develop and implement appropriate safeguards to ensure delivery of critical services (NIST, 2018). The protection is focused on the ability to limit or contain the impact of a potential cyber security threat. This means that on one hand technical factors of the system need to be ensured in terms of security, and on the other hand human factors that need to work with the system should be trained and learned how to deal with the system. The function is provided with categories as identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology (NIST, 2018).

The protection phase is followed by the detection phase. During this phase the focus lies on developing and implementing appropriate activities to identify the occurrence of a cyber security event (NIST, 2018). Where the protection phase could be seen as a phase focused on prevention, the detection phase must be seen as a possibility to intervene when something goes wrong. The function is provided with

categories as anomalies and events, security continuous monitoring, and detection processes (NIST, 2018).

After the detection phase, a respond phase enters. The goal of this phase is to develop and implement appropriate activities to take actions regarding the earlier detected cyber security incident (NIST, 2018). The respond function supports the ability to contain the impact of a potential cyber security incident. Taking appropriate technical and organizational measures could minimize the consequences of the threat. After these measures are taken, it is of great importance to focus on the crisis communication. The respond function is provided with categories as response planning, communications, analysis, mitigation, and improvements (NIST, 2018).

After the respond phase, there is the last phase that entails recovery. The goal of this phase is to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident (NIST, 2018). After an incident has taken place the organization needs to recover as soon as possible, to continue their services in a more safe and secure manner. Timely recovery to normal operations can reduce the impact from the incident. The recovery function is supported with categories as recovery planning, improvements, and communications (NIST, 2018).

The NIST Cyber Security Framework must be interpreted as more than a set of basic components, since it is also critical how an organization implements the framework (Shackelford et al., 2015). The implementation varies significantly in different industries. Due to the rapidly evolving cyber threats the framework is equipped with critical infrastructure settings (Shackelford et al., 2015). These settings create flexibility and enable organizations to supplement an already existing cyber security management. The Information Systems Audit and Control Association (ISACA) represents over 100,000 cyber security, governance, and assurance professionals working within different domains. ISACA assisted in the development of the NIST Cyber Security Framework, and marketed the framework by the numerous industry associations they represent. Both governments and business leaders see opportunities in public-private partnerships to develop globally workable cyber security policies. As a consequence, more industries such as energy, IT, manufacturing, retailing and other sectors join ISACA and adopt the NIST Cyber Security Framework (Shackelford et al., 2015).

2.3.3 Conceptual framework

In the previous section the NIST Cyber Security Framework is explained. This section will combine the privacy concept with this framework to assess how these phases are relevant with the establishment of the Landelijk Schakelpunt from a privacy perspective.

The first phase focuses on identification, in which an organizational understanding will be developed to manage cyber risks. This understanding entails a focus on the system, people, assets, data, and capabilities. When it comes to the Landelijk Schakelpunt it is essential to create a stable basis and make sure everyone who is working with the system is aware of how to deal with it. From a privacy perspective, the only way the LSP could be seen as successful is when the security of personal data and medical records of patients is guaranteed. One category of identification is asset management, which focuses on physical devices and software platforms. In addition, communication and data flows will be mapped even as external information systems. Besides resources, a clear structure of cyber security roles and responsibilities is needed. To generate more insight into the domain of the LSP the business environment will be analysed, even as the governance that is applicable. These entail on one hand the legal and regulatory environments, but also dependencies of the critical service. Furthermore, the assessment and documentation of asset vulnerabilities, and internal and external threats may identify possible risks, from which can be learned and developed into a stable risk management strategy.

The second phase focuses on protection, in which appropriate safeguards are developed to ensure the delivery of the critical service. LSP is without doubt a critical service, since it entails sensitive information and operates within a complex environment. From a privacy perspective, implementing the protection phase into the business operations of the LSP is of great importance to guarantee a safe medical health record. This could be done by focusing on identity management and authentication such as the protection of physical access, but also by organizing permissions and network integrity. In addition to technical measures that are taken, human factors also should be trained to work with the system. This could be done by awareness trainings that inform users about their roles and responsibilities. Furthermore, data itself needs to be protected. Ways to do this are by implementing checking mechanisms, information protection procedures, and by periodic maintenance. When measures are taken, it is

also important to keep track of how they evolve, by logging records and communications and control networks.

The third phase focuses on detection, in which appropriate activities to identify the occurrence of a cyber security event is developed and implemented. Even after giving much attention to the identification and protection phase, it is possible that a cyber security incident may happen. In that case it is of great importance to detect the threat as soon as possible, so relevant measures could be taken directly. From a privacy perspective one hopes to never enter the detect phase, because it means a threat is already occurring. However, organizations need to be well prepared in case incidents do occur. To minimize the leakage of personal data and health records of the Landelijk Schakelpunt it is therefore important to react adequately. Focusing on the potential impact an incident entails could do this, by analysing attack targets and methods, and incident alerts. In addition, continuous monitoring is necessary, focusing on both system activity and personnel activity. Besides, also in this phase it remains important that roles and responsibilities are clear to the involved users.

These previous described phases – identify, protect, detect - are all occupied with the prevention of cyber security incidents at the Landelijk Schakelpunt. Phase four and five – respond and recover – are from a privacy perspective phases which an organization hopes will never occur because the risk of losing personal data and medical records is too critical. However, incidents can always happen so an organization must be prepared in order to face and resolve them. When the organization finds itself in the respond phase it needs to have a planning and procedure to coordinate communications, for both internal and external stakeholders. Besides, the situation needs to be analysed to create insight in risks and consequences. After generating a shared understanding of the situation and context improvements should be planned. These may exist of different technical and organizational measures. The planning of improvements evolves into implementation during the fifth phase: recovery. The previously described measures and improvements are during the recovery phase not only executed, but they also need to be communicated. Clear communication is needed so data subjects whose personal data may be lost know what is being done to protect their data against further distribution.

3. Methodology

The previous chapter described the body of knowledge, including the privacy concept and the NIST Cyber Security Framework. This chapter explains which methods will be used in this research, by addressing the research design, the method of data collection, and the method of analysis. In addition, the reliability and validity of this study will be also discussed.

3.1 Research design

The purpose of this research is to assess whether the implementation of the Landelijk Schakelpunt (LSP) is strengthened in terms of privacy in relation to the previously prepared and rejected Electronic Health Record (EPD). More specifically, this research focuses on the use of social security numbers in the digitized system of providing insight in patient's medical data. The contradiction that applies here is the attractiveness to use a digital system with easy access to medical health records, but also the ongoing necessity to control and guarantee the security and privacy. To analyse this from a privacy perspective, the NIST cyber security framework will be applied within a holistic case study approach.

As described earlier, a digital system that contains confidential information such as personal data is a complex process that involves many risks. The LSP is only part of the total range of digital services to which personal data applies. Studying a specific component in detail helps to gain more insight into the entire situation. The approach of a case study is particularly suitable for this type of research because it is possible to focus on a single unit (Gerring, 2004). Moreover, a case study makes it possible to investigate a relatively small number of cases, to collect information about different characteristics, to perform analyses in a 'natural' environment and it is not necessarily a must to create a comparative analysis with other cases (Gomm, Hammersley & Foster, 2009).

The LSP can be considered as an innovative system with a focus on efficiency. The accessibility of medical records is increased because the data of a patient can be viewed in one system. When a patient is involved in a serious accident and is transported to the nearest hospital, doctors can respond immediately when consent is given for the viewing of personal data via the LSP system. As a result, the medical specialists quickly gain insight into the condition of a patient, which theoretically increases the chance of effective treatment. However, at first glance the focus on

efficiency does not automatically appear to promote a system's security. The purpose of this case study is to gain a deeper understanding of the functioning of the Landelijk Schakelpunt and how risks are minimized so a secure application can be offered and privacy can be guaranteed.

3.2 Data collection

In order to collect data, qualitative semi-structured interviews are used as the main source in this study, supplemented by a document study. This research is aimed at analysing the privacy element of the digitized LSP, examining both the substantive aspects and perceptions of patients and stakeholders, so interviewing is the most suitable method to formulate an answer. This approach enables the researcher to gain detailed insight into the analysed object, because subjective ideas, perspectives and feelings can be investigated. Moreover, semi-structured interviews ensure flexibility. This means that "spontaneous" follow-up questions are possible when it seems that a certain topic is important to the respondent during the interview. Also topics that were not identified before the start of the interviews can be given attention with semi-structured interviews. This method of data collection makes it possible for a researcher to delve deeper into the topic and to keep asking questions until it is fully clear what the perspective of the respondent includes, and to be able to place this in the right context (Bryman, 2015). The semi-structured interview is therefore a tool for obtaining in-depth data on perceptions and opinions, which is in line with the purpose of this study.

Illuminating different perspectives, the theoretically established system can be compared with the image of patients and employees who work with the system in practice. The various actors that can be identified as involved include the policy makers who set up the system, and the policy executives such as general practitioners, pharmacists and other medical specialists. In addition, there are patients whose medical data can be viewed. Finally, specialists with substantive knowledge about the safety and risks of such systems can be identified. This includes the chance that unauthorized persons have access to the data and to what extent privacy is guaranteed. The aim is to explain the different sides and experiences of those involved with the Landelijk Schakelpunt.

People from different stakeholder groups have agreed to serve as a respondent for this research. Amongst them are patients, whose personal data have been recorded and are accessible by the LSP. Besides, privacy specialists are identified whom are found to be relevant because they are able to explain how privacy is defined in legislation and what are the patient's rights according to the GDPR. Furthermore, also different IT auditors have agreed on doing an interview for this research. Their focus on the IT infrastructure and content of digitized systems is expected to be relevant in order to generate a detailed understanding of the Landelijk Schakelpunt system. IT auditors are familiar with frameworks like the NIST Cyber Security Framework. Besides privacy specialists and IT auditors, medical specialists are also identified as stakeholders. Examples of these specialists are general practitioners, nurses and pharmacists. Several general practitioners and nurses have already agreed to serve as a respondent for this research. The perspectives of medical specialists are relevant and of great importance since they are the ones that actually work with the system and can indicate the role and functioning of the LSP within their daily working activities.

To provide a complete picture of the situation in scope, a document analysis will be conducted in addition to the interviews. Introducing the electronic portal in which medical data can be viewed by social security number as identification method has taken a lot of time, and more and more risks become visible. The document analysis will focus on both policies of establishing the Electronic Health Record (EPD) and Landelijk Schakelpunt (LSP), since this research analyses to what extent the design of the LSP is improved in terms of privacy compared to the EPD. The prepared policy documents of both EPD and LSP are publicly available, as are the documents of the House of Representatives. These documents from the Dutch Senate indicate the original initiatives, thoughts on electronic health systems, and why there has been a withdrawal from the EPD from a privacy and security perspective. Overall, the documents will mainly represent the theoretical perspective, which will be supplemented by a practical perspective that will be apparent mainly from the interviews.

3.3 Data analysis

Section 2.3.3 addressed the conceptual framework that is applicable in this research. It showed that the three phases – identify, protect and detect – are all occupied with the prevention of cyber security incidents at the Landelijk Schakelpunt. The fourth and fifth phase – respond and recover – are from a privacy perspective phases that

organizations hope to never enter, because the risk on losing personal data and medical records is too critical. However, organizations need to be prepared for each phase in case an incident occurs. The following sections describe the different phases and the corresponding categories and subcategories, which indicate focus points for fulfilling the concerned phase originating from the NIST Cyber Security Framework (NIST, 2018). For full criteria lists see Appendix 1.

3.3.1 Identify

The Identify (ID) phase exists of five different categories: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy. Focusing on Asset Management (AM) the data, personnel, devices, systems and facilities that enable an organization to fulfil its goals are analysed. In addition to resources as physical devices and software platforms, external information systems, communications and cyber security roles and responsibilities are mapped and established. Zooming in on the Business Environment (BE), the organization's mission, objectives, stakeholders, and activities are studied. This means assessing the organization's role in the supply chain, but also its place in the (critical) industry. Furthermore, an understanding of priorities is formed as well as dependencies and resilience requirements. Assessing the Governance (GV) entails policies, procedures, and processes to monitor regulatory, legal, risk, environmental, and operational requirements. Furthermore Risk Assessment (RA) focuses on whether the organization understands the cyber security risk to organizational operations, assets, and individuals. This is done by identifying asset vulnerabilities, cyber threat intelligence and other internal and external threats. After the identification of threats and their potential impacts, the organization's priorities, constraints, risk tolerances and assumptions are established in an organization's Risk Management Strategy (RM). Not only should the processes be established and managed, but also organizational stakeholders should agree with them. The categories of the Identify (ID) phase can be schematically represented as follows:

Function	**Identifier**	**Category**
Identify (ID)	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy

3.3.2 Protect

The Protect (PR) phase exists of six different categories: Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology. Identity Management, Authentication and Access Control (AC) focuses on the access to physical and logical assets by users. This can be done by managing verified identities and credentials, remote access, permissions and authorizations. In addition, the network integrity needs to be protected. Awareness and Training (AT) involves the education of an organization's personnel and partners. All users should be informed so they understand their roles and responsibilities. Data Security (DS) entails the management of information and records, which need to be consistent with the organization's risk strategy. Data in every stage such as in transition, removal, transfers, and disposition need to be secured. This also involves protection against data leakage and integrity checks. The Information Protection Processes and Procedures (IP) addresses security policies to maintain and manage the protection of information systems and assets. Subcategories that complement this category are baseline configuration, system development life cycle, backup policies and deletion procedures. Also, response plans and recovery plans need to be in place and managed. Maintenance (MA) focuses on industrial control and performed information system components, which need to be consistent with policies and procedures. It is important that internal and remote maintenance are logged and controlled. Lastly, Protective Technology (PT) involves technical security solutions to ensure security and resilience of systems and assets. Subcategories are the documentation, implementation and review of audit and log records, the protection of communications and control networks and implemented mechanisms to achieve the resilience requirements. The categories of the Protect (PR) phase can be schematically represented as follows:

Function	**Identifier**	**Category**
Protect (PR)	PR.AC	Identity Management and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology

3.3.3 Detect

The Detect (DE) phase exists of three different categories: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. Anomalies and Events (AE) focuses on the detection of anomalous activity and creates understanding of the potential impact of events. A baseline of network operations and expected data flows for users and systems is established and managed, detected events are analysed to understand attack targets, and event data are collected. In addition, the impact is determined and an incident alert is established. Security Continuous Monitoring (CM) zooms in on monitoring information systems and assets to identify possible cyber security threats and to verify the effectiveness of protective measures. This means that the network, physical environment, and personnel activity are monitored. In addition, when malicious codes, unauthorized codes or external service provider activities are found, they also need to be labelled as detected, so further actions can be taken. During Detection Processes (DP) the focus is laid on maintaining and testing detection procedures and ensuring awareness of anomalous events. Roles and responsibilities for detection need to be well defined, compliance with applicable requirements needs to be assured and event detection information needs to be communicated. Furthermore, continuous improvement is a high priority. The categories of the Detect (DE) phase can be schematically represented as follows:

Function	**Identifier**	**Category**
Detect (DE)	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes

3.3.4 Respond

The Respond (RS) phase is a phase that an organization hopes will never enter from a privacy perspective. However, organizations must be prepared for incidents that may occur. The Respond phase exists of five categories: Response Planning, Communications, Analysis, Mitigation, and Improvements. Response Planning (RP) entails the procedures that are executed and maintained to ensure a quick response to detected cyber security incidents. Communications (CO) zooms in on coordination with internal and external stakeholders. This means that personnel are aware of their roles and the order of operations, incidents are reported, and information is shared. During Analysis (AN) effective response and recovery activities are discussed. In an ideal situation notifications from detection systems are investigated, the impact of incidents

are understood, forensics are performed, and incidents are categorized in consistency with response plans. When it comes to Mitigation (MI) an organization needs to perform activities to prevent expansion of an incident, mitigate its effects and resolve the incident. Also newly identified vulnerabilities need to be mitigated or documented as accepted risks. Finally, Improvements (IM) entails the improved organizational response activities by incorporating lessons from current and previous detection activities. Response strategies need to be regularly updated. The categories of the Response (RS) phase can be schematically represented as follows:

Function	Identifier	Category
Respond (RS)	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements

3.3.5 Recover

The Recover (RC) phase is also a phase that an organization hopes will never enter from a privacy perspective. However, organizations must be prepared for incidents that may occur. The Recover phase exists of three categories: Recovery Planning, Improvements, and Communications. Recovery Planning (RP) involves the execution of recovery processes and procedures. These also need to be maintained to ensure restoration of systems or assets that are affected by cyber security incidents. Improvements (IM) during the recover phase differ from improvements during the response phase. Response improvements entail organizational response activities, and recovery improvements incorporate lessons learned in recovery plans and strategies. Communications (CO) entails the coordination of restoration activities with internal and external parties. These involve the management of both public relations and reputation. The categories of the Recovery (RC) phase can be schematically represented as follows:

Function	Identifier	Category
Recover (RC)	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications

3.4 Reliability

Joppe (2000) defines reliability as the extent to which results are consistent over time and an accurate representation of the total population under study and if the results can be reproduced under a similar methodology, then the research instrument is considered to be reliable (Golafshani, 2003). The policies of the EPD and the LSP are documented and publicly available. Besides, the reports of all discussions of the Dutch Senate are published on their website. These documents do not change over time, it is only possible that new documents will be published, that supplement older documents. Using the methodology of this research, it may occur that subjective answers during interviews differ. However, if the GDPR does not change substantially it is not expected that privacy specialists interpret the law differently. Also IT auditors will be interviewed because of their knowledge of frameworks as the NIST Cyber Security Framework. It is not expected that this framework will change. Using the same method as this research should therefore lead to reliable outcomes.

Joppe (2000) defines validity as the instrument that determines whether the research truly measures what was intended to measure or how truthful the research results are (Golafshani, 2003). The research question focuses on *to what extent the design of the Landelijk Schakelpunt (LSP) is improved in terms of privacy compared to the Electronic Health Record (EPD)*. This research will be executed by applying the NIST Cyber Security Framework. By creating insight from patients themselves, privacy specialists, the ones that work with the system as medical specialists, and people that focus on these kinds of frameworks this research is expected to be valid.

4. Analysis

The previous chapters described the body of knowledge and methods that guide this research. In section 2.3.3 the privacy concept was combined with the NIST Cyber Security framework. The five different phases, (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover will now be analysed by the conducted interviews and studied documents.

4.1 Identify

The identification phase focuses on developing a shared organizational understanding to manage cyber threats, by managing the system, people, assets, data, and capabilities. From a privacy perspective, the only way the Landelijk Schakelpunt could be seen as successful is when the security of personal data and medical records of patients is guaranteed. To assess whether this criterion is fulfilled, five categories are identified: asset management, business environment, governance, risk assessment and the risk management strategy.

One priority is asset management. Access to physical devices and systems is necessary in all healthcare institutions. VZVZ has set a three-step procedure with criteria that need to be fulfilled in order to receive a connection to the LSP (VZVZ, 2019a). One of these steps addresses how to deal with electronic identities. Theoretically, employees receive a card and in combination with the corresponding PIN code they are authenticated. All interviewed medical specialists confirmed this procedure. Besides, authorization is also important which entails the specific rights of use (VZVZ, 2019a). Dependent of one's specific role, the account has limited access functions. The modules to which no access has been granted cannot be viewed either. In addition to the arrangement of roles VZVZ has set different checks and balances such as a division in cybersecurity tasks and responsibilities.

Besides asset management, focus is laid on the business environment. The Ministry of Health, Welfare and Sport (VWS) set the following objective for the EPD: '*to make (parts of) the patient record integrated and electronically accessible, irrespective of place and time, with a view to patient-oriented care'*. The national implementation started in September 2008, and in order to ensure a smooth realization a number of conditions have been drawn up, including lessons from practical experiences, audits, and the BSN Healthcare Use Act (Wbsn-z). In 2012, the Dutch School for Public Administration published a study concerning an evaluation of crucial

moments in the EPD decision-making process and improvements for IT processes in the healthcare sector (NSOB, 2012). The publication argues the ministry was mainly focused on the realization of the EPD, and conceived it as a planned process to be settled. In retrospect, it seems an emergent strategy would have been more applicable, whereby strategy adjustments can be made during the process, which therefore responds more to current events. VZVZ indicates that during the period 2012 - 2015 focus was set on the commissioning of the national healthcare infrastructure and arranging the associated governance of the LSP (VZVZ, 2015). Period 2016 - 2020 concentrates on intensifying the use of the infrastructure and the development of new functionalities, facilities and new users (VZVZ, 2015). To define and clarify the role of the national healthcare infrastructure in data exchange, an extensive SWOT analysis has been executed, describing opportunities, threats, strengths, vulnerabilities, success factors, barriers and risks. The result is: "*a barrier-free use of the infrastructure throughout the entire chain is the guideline for everything we do*" (VZVZ, 2015). It is recognized that at the same time there are components of the LSP that still need to be solved, the need for data and functionalities continues to increase, and the LSP chain can contribute more to medication monitoring and verification. In addition, the patients are a central point of focus, the pilot regions form examples to follow, and a trust model is active in coordinating the chain (VZVZ, 2015). To continue to meet expectations, focus on research, development and innovation is important. VZVZ decided to continue the path taken in order to achieve optimum use through a robust management organization with regard to technology, architecture and user support. The second focus is on innovation and further improvements. It is defined that these two aspects should not impede each other in priority and staffing, but must be implemented synergistically. Different stakeholders can be identified, such as the patients whom share their data, medical specialists that need to work with the data, the AP and IGJ that control if legal requirements are met.

Focusing on governance, VZVZ states that reports show the availability of healthcare information is good. At the same time, it sometimes seems unclear to stakeholders such as care providers, managers and representatives how to deal with incidents and disruptions (VZVZ, 2019e). The procedure is separated in a description for end users, a description for representatives of end users and a detailed description for administrators. Furthermore, administrators report malfunctions to the service desk of the party where the cause of the malfunction lies. It is only allowed to contact

AORTA support if the cause of the failure cannot be determined (VZVZ, 2019e). AORTA support is the primary point of contact for questions about services from other chain management parties. Contact details of all service desks can be found on the Supportal app. Supportal is the online platform for exchanging management information about disruptions and maintenance for the purpose of cooperation between management organizations in the AORTA chain. Summarized, information about incidents, malfunctions and maintenance can be found, but it is quite unclear and there are many references to different parties. It seems like there is not one central point or person of contact to reach out to in case of incidents. Furthermore, the legal framework has been improved over time. According to GDPR Articles 15 to 20, a patient has the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to the notification obligation regarding rectification or erasure of personal data or restriction of processing, and the right to data portability. In addition, it becomes mandatory for a person to give prior permission when personal data is processed. The data subject must be able to withdraw consent at all times, the so-called "opt-out function" (EUR-Lex, 2016). In addition to the GDPR, the NEN7510 standard focuses specifically on information security in the healthcare sector. The standard was initiated to be able to offer patients the desired level of service. It is therefore necessary that health care providers have access to reliable information at any time. At the same time, it is important that sensitive information does not fall into the hands of unauthorized parties to protect the privacy of the patient (NEN, 2019).

Focusing on risk assessment, VZVZ argues responsibilities are separated: the government sets a framework for the infrastructure, identities and attributes; the public must become aware of dangers and risks; and systems must be designed according to prescribed regulations (VZVZ, 2019f). A way to control whether these criteria are being fulfilled is to execute a Data Protection Impact Assessment (DPIA). A DPIA is a tool used for clarifying needed measures by mapping privacy risks of data processing in advance. A DPIA is mandatory if the data processing is likely to pose a high privacy risk for those involved (AP, 2019c). All EU privacy authorities published criteria about mandatory DPIA's. One of the categories is: large-scale processing of health data (for example, by institutions or provisions for health care or social services, working conditions services, reintegration companies, (special) educational institutions, insurers, and research institutions) including large-scale electronic exchange of health data (AP, 2019c). Although the LSP fits into this category, there is no proof of an

executed DPIA on the system.

To create an overview of the enormous amount of data, it is desirable to set retention periods. VZVZ states that provided contact details will be kept for the time required to answer questions adequately and they will be deleted afterwards (VZVZ, 2019g). When subscribed to the newsletter the e-mail address will be saved until anyone unsubscribes from that service at any time. It is indicated that data will not be used for any other purpose than for the purpose mentioned in the privacy declaration on VZVZ's website. VZVZ works in accordance with NEN 7510, 7512 and 7513 and has set up procedures for deleting, supplementing, correcting or giving access to the data that vzvz.nl collects from a data subject (VZVZ, 2019g). Medical data are not saved in the LSP, but will remain stored in the XIS of the healthcare provider. The reference index includes information about which healthcare provider(s) submit a medical record of what patient, processed based on the social security number (BSN). To react to possible threats it is of great importance to monitor and log the events and flows of data. All IT auditor and privacy specialist respondents address this importance:

'*Access has to be easy and I very much believe - and hope - that every doctor has access to my data. But monitoring is necessary.*' – IT Auditor and Privacy Specialist 2.

'*Logging is mainly reactive, you are able to see if someone did something, but you actually want to be also preventive, by implementing and arranging different roles and responsibilities.*' – IT Auditor 1.

'*In this case, logging is important because you want to know if the procedure is working properly, so I want to see that nothing is being misused. By analysing the logging I can also see if a procedure may or may not work.*' – IT Auditor and Privacy Specialist 3.

The exchanged data are encrypted and every query is logged. Patients can receive notifications by e-mail and get insight into who has requested information via the Volgjezorg.nl website. Attention has been paid to logging and monitoring of the LSP. In 2019, it is decided by senator Bruins that healthcare institutions must set retention periods for logging at the minimum of five years.

The 'Business plan VZVZ 2016 – 2020' describes in detail the identified developments, strengths and challenges, and the upcoming strategy. Vulnerabilities are

not viewed as insurmountable obstacles, but subjects that still need more attention (VZVZ, 2015). These vulnerabilities can be found both at VZVZ as organization, as well as at the LSP as system. The aim of VZVZ and its chain partners is to promote healthcare and patient safety through the establishment of safe exchange of medical data (VZVZ, 2015). The strategic targets include, amongst others, increase of use, connection of new entrants, coordination by VZVZ without a mandate but with partner's commitment, regional support organizations, and focus on co-creation, innovation, and further development of the healthcare infrastructure (VZVZ, 2015). These goals and targets are translated into ambitions and indicators, resulting in agendas for future developments and change management. The specific strategy is therefore based on the identified risks.

Compared to the EPD, there is no difference in the need of physical devices, software and resources. According to senator Hans Franken, the EPD had too many possibilities to gain access to patient's medical records (NOS, 2011). Franken called on Schippers, the senator that initiated the EPD, to come up with an adapted proposal in which matters such as security, privacy and patients' rights were properly arranged. The Senate favoured a smaller, regional set-up of the Electronic Health Record (NOS, 2011). First reactions from associations of medical specialists were that the EPD is collapsed out of fear for the unknown (Van den Elsen, 2011). It is remarkable that they suggest the EPD was safer than the information systems doctors had at that time, when the EPD was already called unsafe. The association of hospitals argued the withdrawal of the Senate is a missed opportunity (Van den Elsen, 2011). The Senate considered the privacy of patients insufficiently guaranteed, but according to the association a national EPD had made it possible to streamline information about complex care processes and would have ensured clear data exchange between healthcare providers. Both the design of the EPD and the LSP included a mission, objectives and stakeholders. In addition, the importance of sensitive data was understood and prioritized. VZVZ is aware of the electronic health record's place in the health sector and its critical function. However, because of the withdrawal of the Dutch Senate the designing phase of the EPD never got as far as the designing phase of the LSP. The legal framework has been improved over time. Both during the designing phase of the EPD and the LSP the WGBO law was applicable, stating the retention period for medical data is 15 years. However, VZVZ states that when the patient withdraws his consent, the social security number will be removed from the reference index. The data is kept for as long as the permission

has not been withdrawn, suggesting the retention period of 15 years can be exceeded. The GDPR is in the interest of data subjects – in this case the patients - even as the sector specific regulations. Like IT auditor and Privacy Specialist 2 states: '*much attention is paid to privacy, and according to me sometimes too much. That might be out of fear because it's about sensitive information, but you don't solve it by locking the door'*. In this sense, risks are reduced, but a system still needs to be workable.

4.2 Protect

The protection phase focuses on how the assets that are in place according to the identification phase are designed substantively. To guarantee a safe and secure exchange of medical data it is of great importance that medical specialists know how to work with the system. To assess whether the LSP complies with the protection phase, there are six categories identified: identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

In order to receive a connection to the Landelijk Schakelpunt VZVZ three steps must be fulfilled. The first step is the presence of a Well Managed Care System (GBZ). An organization appoints a GBZ manager - internal or external - who takes care of the technical management and ensures the system continues to meet the security requirements for data exchange with other GBZs. This manager is also the person of contact in disruptive situations. The list of accepted care information systems is included in Appendix 2. The second step comprises a Well Managed Care Network (GZN) that ensures good and safe communication between the GBZ and the LSP (VZVZ, 2019a). The list of accepted care networks is included in Appendix 3. After these two steps, the third step consists of UZI resources. This includes the UZI server certificate and a UZI healthcare provider card. The purpose of the certificate is to confirm the electronic identity of the system when the healthcare provider logs in to the LSP. The pass contains information about which data can be consulted (VZVZ, 2019a). The above steps can all be submitted online. After access is granted, healthcare institutions must ask patient's consent for the exchange of medical records. Theoretically, when patients give consent it does not necessarily mean these data will be transferred from one system to another. Consent only gives insight in medical records, but the data itself stays in the systems at the healthcare institution where the data is collected. Therefore, data can be stored scattered, leading to potential risks. One of those risks is determining the scope of permission. According to the interviewed patients, it is not clear what the given consent includes.

Patient 1 states: '*I have asked if I gave permission to a limited group of medical specialists and they told me I did. I believe that, but I have never received more information or anything. I didn't know medical data may be shared nationally'.*

Patient 2 argues that the consent is not a choice, since '*I went to the doctor and arranged that the medical details were transferred to my new doctor. They gave a choice, but suppose I didn't agree to share my medical history then I wouldn't have a new doctor'.*

Because the LSP consists of sensitive data it is important unauthorized people do not have access. Employees are divided into different roles, consisting of a different set of rights, which are aligned with the tasks and responsibilities of the specific employee. Medical Specialist 1 explained the steps that are taken when starting a job at a healthcare institution. At the start one gets a contract and an account. The account is accessible by username and password, even as the healthcare information systems. Dependent of your specific role, the account has limited access functions. The modules to which no access has been granted cannot be viewed either. That restriction seems theoretically logical, however Medical Specialist 1 addresses the following issue:

'*To me, it is not always clear what the different tasks and responsibilities of colleagues are. You do not know what other functions have access to what information. Sometimes others cannot see screens that I can see. Then you have the idea that they are not doing their job as they should, but they simply have no access to it'*. – Medical Specialist 1.

The medical specialists state no insight is offered into the possibilities of other functions. Specialists will gradually have to find out themselves what rights belong to which role. From a practical perspective, it is less desirable that it is not shared what rights belong to which role. As medical specialist 1 argues, this can lead to misinterpretations and less mutual understanding of work performed. However, the separation of roles and functionalities in itself is desirable. A critical classification of what each role needs access to clarifies responsibilities. IT auditor 1 underlines this statement with the following words:

'*Every medical specialist is allowed to perform certain proceedings, which belong to specific profiles. The system really has to support it from the basics, because otherwise you are going to give large groups of specialists information they don't have to see for their work, or even worse, they see information that they are not allowed to see at all.'* – IT Auditor 1.

To guarantee employees' awareness and training VZVZ offers online information for different groups of healthcare providers. Options are ranging between pharmacies, general practitioner practices, general practitioner posts, hospitals, independent clinics, VG institutions, GGZ institutions, VVT institutions, care groups, JGZ organizations, regional organizations, and IT service providers (VZVZ, 2019c). Subsequently, support is offered on various levels and based on the philosophy '*To ensure that you can spend as much time as possible on patient care, we try to take work off your hands wherever possible*'. Employees are trained in requesting permission, informational and promotional materials are available, special consent actions are organized, and information maps have been drawn up. Healthcare institutions are obliged to pass on changes, because this may have consequences for their LSP connection (VZVZ, 2019c). This is partly monitored by means of random selected research into compliance with legislation and regulations and the method of obtaining and recording permission. It is remarkable that there is room for two-way traffic. On one hand, VZVZ offers help to guide employees through the LSP system, while on the other hand questions and suggestions are also welcomed.

VZVZ's documentation about the possibilities of awareness and training of employees seem promising. Medical specialist 1 confirms the following:

'*There are certain trainings you have to follow depending on your role. Over time, different aspects become more important and it's about development. As soon as you see the patients, you do nut want their data to be lost or carelessly treated. You don't want that in case of your own data either'.*

Comparing the design of the EPD with the LSP awareness and training did not become less important, although a shift in focus can be identified. As context, including regulatory environment, changes over time, so are perceptions and identified risks. As medical specialist 1 clarifies: '*there are no special training courses on how to handle sensitive data. That is also fairly new. Five years ago, nobody was interested in what happened to the data, but that has changed because of the privacy legislation'*.

Data security concentrates on the protection of data-at-rest and data-in-transit. Furthermore, subjects as retention periods, removal and disposition are addressed. VZVZ emphasizes that LSP does not store data in its system, but only makes it possible to view data in other healthcare institution's systems. Responsibilities to protect

medical data are hereby passed towards the individual healthcare institutions. Divided responsibilities may lead to more risks, since security is not provided centrally, leading to a variety of procedures, protocols and different ways of processing. Section 4.1.4 Risk Assessment described the retention periods for the healthcare sector.

In addition to the legal framework a system as the LSP has to work with, the 'Wet cliëntenrechten bij elektronische verwerking van gegevens' specifically addresses electronic data exchange. This law sets conditions for secured exchange and insight into the medical data of patients and lists rights (VWS, 2017). This only concerns treatment relationships and it must be strictly necessary. Health insurers, medical examiners, company doctors and insurance doctors are denied access to medical data from the LSP.

From the perspective of clients, the following applies:

Current situation:	From 1 July 2017 also:	From 1 July 2020 also:
Giving permission for the exchange of data.		Giving permission to make all or certain data available for inspection to all or to certain care providers with whom a treatment relationship is in force (or will be).
Getting a copy of your own medical file.		Obtaining an electronic copy of your own medical file (free of charge).
Gain insight into your own medical file.		Get (free) electronic access to your own medical file.
Adding, removing, destroying or shielding medical data.		
Upon request, a client is entitled to an overview of the logging: categories of data that have been processed, the recipients, or categories of recipients that have data and information about the origin of the data.	Upon request, the client receives an overview of who has made certain information available in an electronic exchange system and on which date and who has viewed or requested information and on which date.	

Source: VWS (2017) - Elektronische gegevensuitwisseling in de zorg.

The described risk strategy for the LSP determined by VZVZ addresses different subjects to protect the confidentiality, integrity, and availability of information. Compared to the EPD, the legal framework was mainly constituted of the WGBO. This law also addresses the different categories of data, data subject rights, retention periods, and disposal (Witmer & de Roode, 2004). The term of custody is laid down in Article 454 paragraph 3 of the WGBO. However, there were miscommunications about whether it was intended as a minimum or maximum period

(Witmer & de Roode, 2004). Eventually, the legislator defined it as a maximum period, meaning that ten years after the production of data it must be destroyed. An exception to this period can be made based on appeal to good counselling including substantiation of the need.

The VZVZ security policy includes the applicable conditions for lawful processing of data. They described how the conditions apply within the LSP system and provide evidence to support compliance. According to the GDPR, it is necessary that consent is granted freely, specific and based on sufficient information ('informed consent'). VZVZ states the LSP is based on an opt-in function, and patients have the right to opt-out at any time. When the patient withdraws his consent, the number is removed from the index. The data will be saved as long as the permission is not withdrawn. Compared to the earlier rejected EPD system, one marked change of the LSP is the obligation of informed consent. It is up to a patient to choose whether he wants to share his medical records with other healthcare institutions, without having negative consequences. The design of the EPD did not include the obligation of consent. Although it is documented that patients are free of choice, the interviewed respondents had different experiences. Patient 1 stated:

'*I am not well informed. They could have told me a little more about the system and what limited circle I share my data with. I found out myself. You just give permission and they immediately put it in the computer. I said yes myself, but that is because you are in a process. Your health is first priority, so you admit you need care. It is about your health and later on you might think would it really have been necessary?*'- Patient 1.

There are information leaflets where permission can be given in written form. However, the interviews show permission is often requested during a visit or must be checked directly on the registration form. Patient 2 experienced an unpleasant way of giving consent:

'*I recently moved, so I needed a new doctor. And then they said yes we do need your medical record. They gave a choice but it was not a free one, because if I didn't agree that my details were being transferred I wouldn't have a new doctor. I first wanted to*

do some research, then I actually ignored it a bit, and then they called me a few times that they really needed the information.' – Patient 2.

The remarkable thing about previous situations is that permission is not without obligation, while it should be. Patients have at all times the right to refuse or to withdraw previously granted permission. These experiences reflect the possible consequence that proper care will not be provided if permission has not been given.
To ensure resilience of the LSP system VZVZ emphasizes it forms a secure network for data exchange. Besides social security numbers, no data is stored. Furthermore, the LSP sets strict security and access requirements for participating healthcare institutions. The security measures spoken of seem to entail mostly authentication and authorization. A patient can look into the summary of his data, with details about what type of data, when data is requested, and what medical specialist entered the request. In case a healthcare provider was not entitled to do so, responsibilities must be found externally according to the policy (VZVZ, 2019h). Summarized, VZVZ keeps stating security measures are taken but it is not fully clear what those measures include. The main focus lies at expanding possibilities and innovation, for instance by developing eHealth applications. The characteristics of the LSP addressed by VZVZ are: consent, security, private network, identification, standards for data exchange and proportionality of data, authentication, authorization, no data storage, and logging (VZVZ, 2019h). When comparing the design of the EPD and the LSP the handling of data has not changed much in terms of determining retention periods and data subject rights. However, focus and attention shifted more towards privacy of patients over time.

4.3 Detect

The detection phase concentrates on developing and implementing appropriate activities to identify the occurrence of cybersecurity events. After identification and protection of assets and needs it is important the LSP system is continuously monitored to detect unwanted activities. To assess whether this criterion is fulfilled, three categories are identified: anomalies and events, security continuous monitoring, and detection processes.

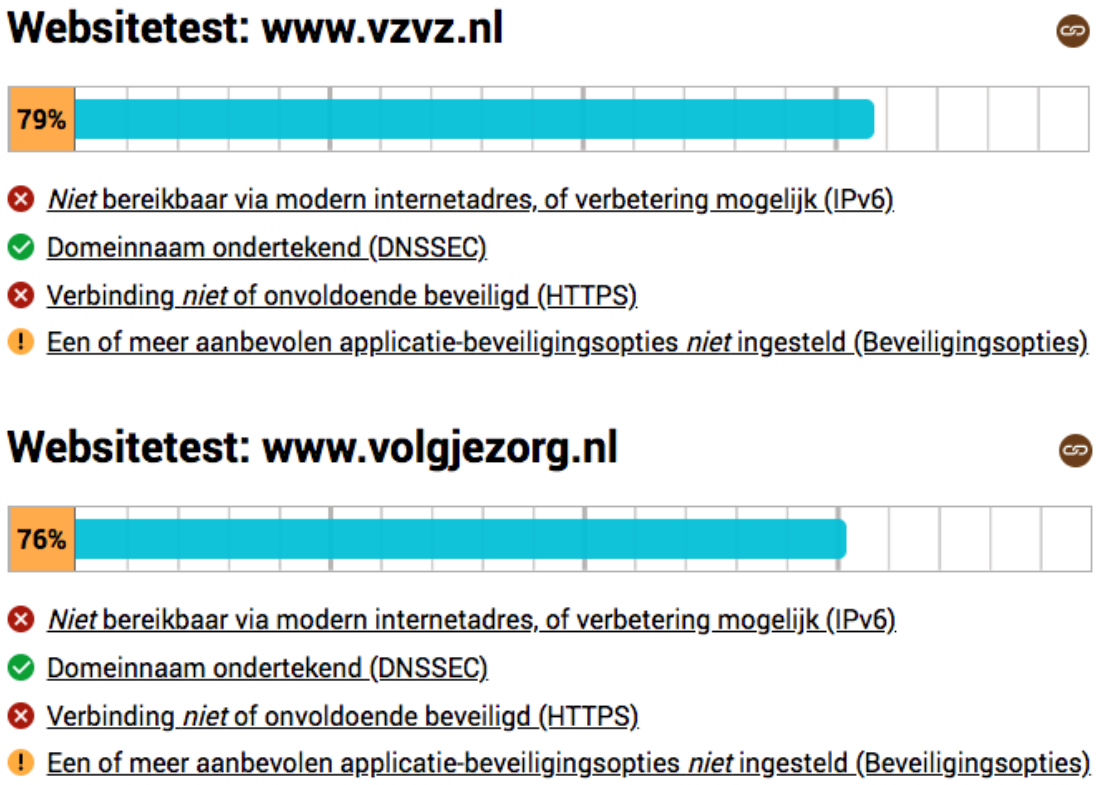
According to VZVZ the LSP and all proceedings on its system are closely monitored to ensure there is no unauthorized, incorrect or deviant use, which could involve abuse (VZVZ, 2019b). All consultations by healthcare providers are recorded in the so-called 'logging'. Logging makes it possible to check whether data is requested on a legal basis. If the healthcare institution does not appear to be entitled to do so, it is up to the regulators – the Dutch Data Protection Authority (AP) and the Health Care Inspectorate (IGZ) – to take further actions (VZVZ, 2019b). From VZVZ's response the monitoring seems to only include requests from medical specialists. Furthermore, VZVZ is reluctant in giving information about maintenance of the LSP system. They continue to emphasize the system does not store (medical) data in itself, but serves as a connector between different healthcare institutions. Responsibilities are shifted towards the creators of data – the specialists.

The medical specialists indicate there is no feeling of being controlled by managers and the system. Medical specialist 1 states: '*in case there is no reason to request data it will be recorded. It is not immediately blocked by the system, you get access to the information, but it is recorded how often someone gives a reason for a wrong file. The manager will appeal this to you.*'

Medical specialist 3 identifies risks and is sceptical about this monitoring:
'*It is just a matter of a click and that is of course registered so it can be traced, but there is no extra security. In a manner of speaking, I could look for you in an EPD in a hospital where you are known if I know your name and date of birth. And that is not allowed, but I could just do that. With an average person, I think that it is never checked who is and who is not looking at that file.*'

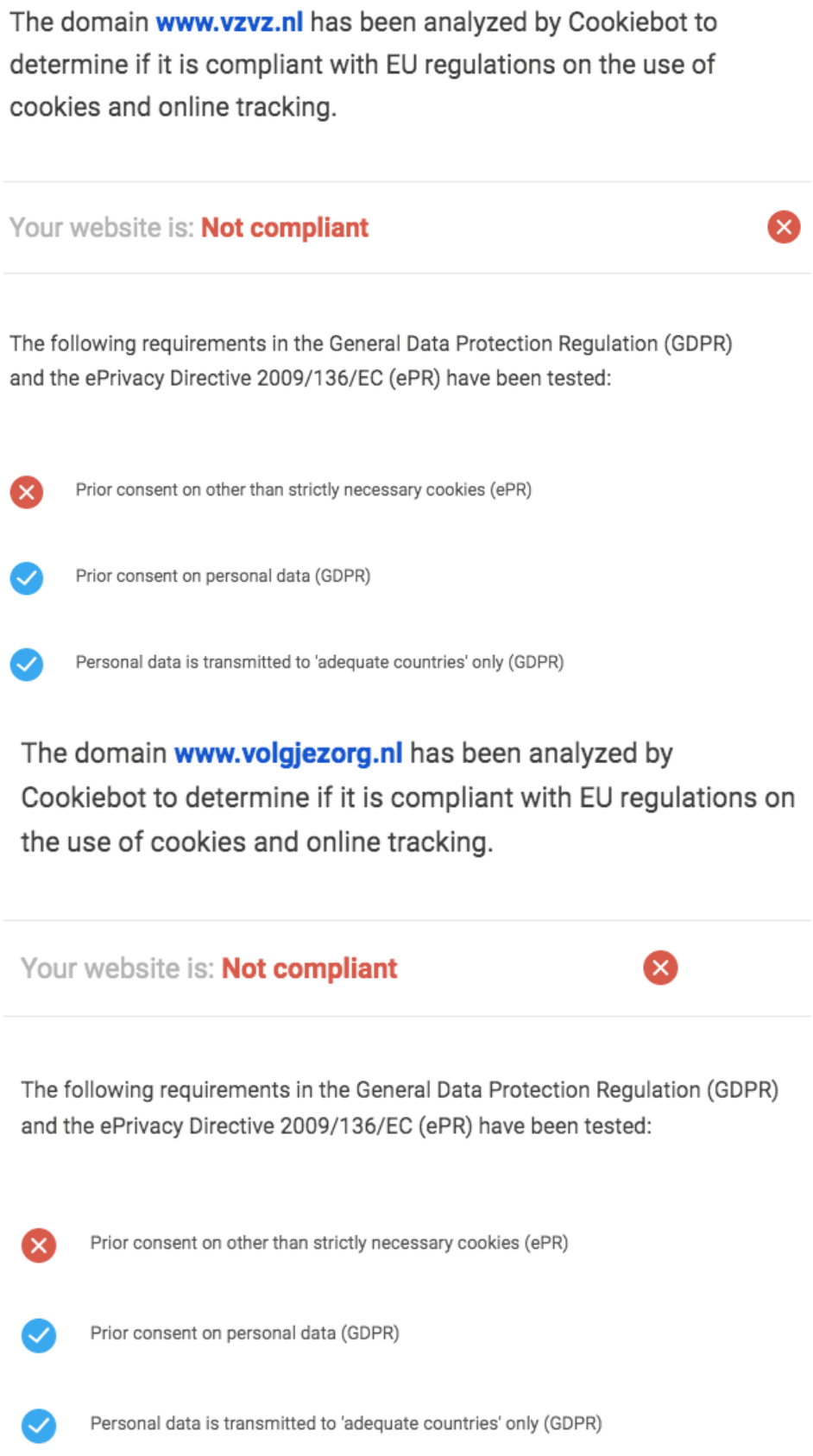
Medical specialist 2 explains the difficulty with an automatic block:
'*You can look at records of all patients in the section. The system does not automatically block because sometimes you have to be able to enter files in an emergency. Because you have different patients per day, there is no check on authorized requests*.' – Medical specialist 2.

Information about the LSP is given on two different websites: vzvz.nl and volgjezorg.nl. The first website entails a platform for healthcare communication and provides information about VZVZ and LSP. The second website mainly provides information for patients. The importance of giving consent and patient's rights are discussed. These two websites are tested on their reliability. Via Internet.nl you can easily test whether a website is up-to-date and compliant. It checks whether the website, e-mail and Internet connection use modern, reliable Internet standards. The checks had the following outcomes:



The website checks show almost the same result. Both are not accessible via a modern Internet address, or improvement is possible. Both connections are not or insufficiently secured. In addition, recommended application security options are not set. However, both have a signed domain name.

In addition to the website checks cookies are analysed. Both outcomes show the websites are not compliant.



The previous checks are executed on the informational websites of VZVZ and the LSP. The results cannot be generalized to the LSP system itself, but it is remarkable these websites are not compliant. From a system that is entirely focused on safe and reliable data exchange you would expect these kinds of principles are met. Logging and monitoring are desirable measures to keep track of what is happening on the system. However, these measures are checking incidents afterwards. As IT auditor 1 states: '*logging is mainly for checking afterwards, you can see if someone did something, but you would actually catch it at the front. It is about the organization of roles and responsibilities, and also the data of the patient*'. VZVZ shifted responsibilities towards the individual healthcare institutions because the LSP does not store medical data but only makes it visible. This means detection responsibilities are also split between different parties.

4.4 Respond

The respond phase consists of developing and implementing appropriate activities to take action regarding detected cybersecurity incidents. The Landelijk Schakelpunt involves personal and medical records. Detecting cybersecurity incidents is an important step, but it is also necessary to ensure a proper follow-up. To assess whether this criterion is fulfilled, five categories are identified: response planning, communications, analysis, mitigation, and improvements.

VZVZ has procedures to offer support in case of incidents. They deliver ICT server providers 1st, 2nd and 3rd line support of ZORG-ID in the web browser environment under certain terms and conditions (VZVZ, 2019d). Furthermore, the 1st, 2nd and 3rd line support to the XIS suppliers and GZNs is intended for disruptions to the ZORG-ID platform. This concerns disruptions to the ZORG-ID server or the hosting environment, and not to the ZORG-ID SDK or the ZORG-ID Client App. The availability of all line support is 24 hours a day 7 days a week, with a rate of 99,982 per cent. The contact details are not shared online publicly, but can be found in the Zorg-ID qualification agreement (VZVZ, 2019d). More general, there is a policy for malfunctions and maintenance. The LSP connections of nearly 6,000 healthcare providers are managed by more than 160 GBZ and GZN management organizations (VZVZ, 2019e).

The medical specialists argue they work according to applicable procedures and protocols. In case an incident is identified medical specialists need to follow procedures to ensure correct follow-up. However, they hardly notice a detailed follow-up because they transfer the data and incident to appointed privacy officers. In case procedures need to be adapted information is given internally so employees know how to handle future incidents. When no adjustments are made information is kept within a select team. One example of awareness of data breaches is the following message that is shared on the internal Internet of a large hospital:

Data breach? Report it as soon as possible

Hospital X processes personal data on a large scale. Most employees come into contact with these data about people on a daily basis. Processing can sometimes go wrong, resulting in a data breach.

Confidential
The law describes a data breach as "personal data breach. In practice, a data breach can be a violation of the confidentiality, availability or integrity of the data. "

Letters, emails
In the past year, there have been data breaches at *Hospital X*. “The Data breach team has found that data breaches are often caused by human error, such as incorrectly sent letters or emails with personal data. A good solution to prevent such a leak is, for example, the use of secure mail or Surf File Sender for e-mailing patient data. "

USB stick
The Data breach team has been dealing with data breaches for a number of years. "For example, until a year ago losing USB sticks were a common data breach." "This has now largely been solved by entering encrypted USB sticks."

To learn
Found a data breach? Always report this to Team Data breach as quickly as possible via a form on the intranet. “As an organization, *Hospital X* can learn a lot from this and take measures to prevent data leaks in the future. Moreover, *Hospital X* is obliged to keep an overview of all data breaches that have occurred. "

There are five golden rules for reporting data breaches.

The five golden rules:
In a security incident, always keep the following Five Golden Rules in mind:
(1) Inform the privacy contact person about the information security incident;
(2) Determine jointly whether there is a processing of personal data and a (possible) data breach. (Determine this independently in the absence of the Privacy Contact Person, so that a possible report to the Dutch Data Protection Authority can take place within 72 hours of discovery);
(3) Immediately inform the head of department or supervisor if there is a (potential) data breach;
(4) Complete the internal data breach reporting form. Indicate what exactly happened, which personal data (possibly) are involved in the incident and what measures have already been / are being taken to limit the consequences and prevent recurrence. Do NOT report the (possible) data breach yourself to the Dutch Data Protection Authority.
(5) Mail the completed form to x and contact the office by telephone about the internal report with the Legal Affairs Office tel. X (office hours).

Furthermore, the LSP uses social security numbers as identification method. When a patient gives permission to make his medical record accessible, he actually gives permission to include his social security number in the reference index of the system (Volg Je Zorg, 2019a). Interviews with patients, IT auditors and privacy specialists have shown that this is not felt or deemed to be the most reliable identification method. All patients did not feel comfortable with the fact that social security numbers are used:

'*I did not know that medical data is viewed on the basis of BSN, and I think it is a bad thing. You think you are reasonably protected and it appears now that this is not the case.*' – Patient 1.

'*A different number might be safer, and maybe you don't have the idea that everyone can just see everything of your entire life, or add information to it. In this way, with BSN someone can take over my identity.*' – Patient 2.

'*You hear more and more about the social security number, also that more and more data can be used, such as requesting all kinds of data. For example, people know where I live, well I think that's pretty intense; that unknown people who have nothing to do with me or don't need anything from me know things about me.*' – Patient 3.

The group of patients indicates they see risks in the use of BSN. This can also be explained by the fact that the social security number is an unique number that is linked to one person. The number is not replaceable and remains for one's entire life. This makes it special and it implies that people need to protect it, or even keep it secret. All patients are open to a different identification method, such as a number that will only be used for medical data. This is not experienced as an extra burden, but rather as extra protection and safety. The IT auditors and privacy specialists also criticize the social security number:

'*The BSN is particularly poorly chosen. It is actually conceived as a primary key by the government, to ensure that all information is collected from 1 citizen. In healthcare I also understand, because you naturally want to make sure you have the right person. I would actually say create a second number, which is linked to the social security number, but is in fact a care number*.' – IT Auditor 1.

'*It is very strange that BSN is used for identification, because the risk is introduced that based on BSN these data can be combined with other data processing that have nothing to do with healthcare. In my opinion, if you do something like this then you should have a sectoral identification number*.' – IT Auditor and Privacy Specialist 3.

IT Auditor and Privacy Specialist 2 has a different opinion: "*If I know your BSN, then I can do something with it. On one hand it can be very safe, but what I notice with a lot of things is that we make it very difficult. It should actually be fun to log in to an application. With a whole bunch of barriers we make everyone think about it. And that sometimes makes it risky again*. "

By designing a digital system as effectively and efficiently as possible, and in particular focusing on the design from a legal perspective, it may have happened that less attention was paid to the risks of using social security numbers as identification method and the mandatory feeling that patients have about having their number recorded because they cannot live without medical care. These concerns are nothing new and have been presented before. Unfortunately there is still no response from VZVZ. The respond phase has become more difficult because of blurred and split responsibilities. Because of the many different stakeholders it is not always clear what can be expected. However, when responsibilities are clear different healthcare institutions take actions. The example of the shared message about data breaches and how to deal with them presented above contributes to this. There is one way that is considered the best way to deal with the system, and the procedures and protocols are designed accordingly. The fact that the LSP system is static and linear does not necessarily have to involve negative consequences, but that is partly depending on communication.

4.5 Recover

The recover phase focuses on developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Landelijk Schakelpunt consists of a critical infrastructure with complex circumstances. Incidents may happen, but preparation to return to a safe and secure system is both necessary and of great importance. To assess whether this criteria is fulfilled, three categories are identified: recovery planning, improvements, and communications.

The possibilities to return to an earlier state of the system after an incident occurred are described by VZVZ. According to their connection policy it is allowed to erase patient's records, but the healthcare institution remains responsible and must ensure the medical data is unambiguous and well registered (VZVZ, 2019a). In addition, it is emphasized that general practitioners follow the ADEPD guideline with the structure and registration in files for an optimal exchange of information (VZVZ, 2019a). ADEPD stands for Adequate File Formation within the Electronic Health Record (NHG, 2019). The Nederlands Huisartsen Genootschap (NHG) – the Dutch General Practitioners Association – has given shape to the ADEPD guideline and is conducting research into the function of the EPD, the social acceptance of the system and the changing role as a result of developments. Besides, lots of attention is paid to data subject rights. In addition, it is stated that the development of Personal Health Environments (PBLs) has impact on the EPD and reporting in general. In a PBL it is possible that a patient can view, use, collect and record file information from multiple healthcare providers (NHG, 2019). The NHG indicates that future developments entail that a patient records data in their PBL and send it to their doctor. There is no denying in the changing function of medical records. It seems patients are getting more individualistic and want to be in control of their data. This corresponds with the perspective of IT auditor and privacy specialist 3:

'I *think the data belongs to me. So I think that these data should actually be under my control somewhere with me. And I determine whether someone has access to it or not. That is my idea and maybe there should be an emergency button somewhere, that if I am no longer able to arrange it, then there will be controlled access for emergencies*.' – IT auditor and privacy specialist 3.

In general, healthcare institutions attach much value to procedures and protocols, but there may be a gap. At first glance, the use of a protocol or procedure seems to be conducive to having work carried out correctly, but there also may be structural errors in the previously described and established procedure. An orderly procedure is a broad concept and can be instituted from different layers such as national politics, an umbrella organization or from an organization itself. With the LSP, a distinction is also made between policy from the government, VZVZ and policy from the healthcare institutions themselves. When the Senate withdrew from EPD's design they set conditions for further development of a similar system. The VZVZ has described a policy for regulating connections. An organization itself focuses on procedures and protocols to streamline work and reach common agreement for handling situations. There is little room for taking your own decision-making powers according to the medical specialists. Flexibility is only expressed by welcoming feedback. With such a system as the LSP it is the question whether flexibility is desirable. Too much space could lead to employees coming up with their own solutions, creating unclear situations and jeopardizing the most suitable way of working. Because of the importance of procedures and protocols it is necessary to periodically and critically assess these documents. When procedures are not regularly reviewed and errors have occurred in the procedure, the errors will continue to repeat. Privacy within the LSP can be promoted by regularly checking whether the policy is still adequate. This concerns compliance with laws and regulations, but also the internal structures that are in force within a healthcare institution.

However, it seems VZVZ's design of the Landelijk Schakelpunt mainly constitutes of preventive measures instead of reactive measures. There is one way that is considered to be the best way to deal with the system, and the procedures and protocols are designed accordingly. The importance of these procedures may lead to possible risks. In case the procedure does not cover every step, these steps will be skipped and forgotten. Also, the focus on the documents may result in a lack of attention for the recovery phase. A tunnel vision may arise in which it is thought that the established policy is sufficient to guarantee safe and secure data exchange. However, this tunnel vision needs to be taken away because incidents can always happen and preparation is key.

IT auditor and privacy specialist 2 proposes a solution:

'If you ask me where it goes wrong in the LSP, I think it is typically Dutch and that means that it is being discussed endlessly. I think that the government should just say that this is a minimal data set that I expect and that should just be in every system, and must come into every system, and make it.'

5. Conclusion

The previous chapter discussed the analysis. This chapter addresses the discussion and reflection on the findings. First, there will be a reflection on the analysis, followed by the effects of this study. Subsequently, the limitations of this study will be addressed and suggestions for future research will be proposed. This chapter will be completed by the final conclusion.

5.1 Reflection

Section 2.3.3 addressed the conceptual framework that combined the privacy concept with the NIST Cyber Security Framework. This outcome is used to assess how the NIST phases may contribute to the establishment of the Landelijk Schakelpunt from a privacy perspective. When the five phases are considered together, the functions provide a high-level, strategic view of the lifecycle of an organization's management of cyber security risk. This is partly due to the fact that it identifies underlying key categories and subcategories for each function and it matches these categories with informative references such as existing standards and guidelines. This conceptual framework was helpful in assessing whether the design of the Landelijk Schakelpunt is improved in terms of privacy compared to the earlier rejected Electronic Health Record.

No differences were found between the LSP and EPD when it comes to the need of physical devices, software, and resources. However, there are differences in the amount of procedures and protocols to deal with the system. According to the medical specialists work is handled by following the protocols. There is one way that is considered the best way to deal with the system, and the procedures and protocols are designed accordingly This increases the pressure on having procedures that cover all proceedings and are free from embedded errors. Both the design of the EPD and the LSP established a mission, objectives and stakeholders. In addition, the importance of sensitive data was understood and prioritized. It is important to acknowledge the Senate withdrew from the EPD in an early stage of designing and implementing the system. Because of this decision the EPD never got as far as the designing phase of the LSP. During the development of this new system the legal framework was improved. The changes cover amongst others regulations for data retention and deletion, and the obligation to request prior consent from patients. VZVZ emphasizes the LSP forms a secure network for data exchange and there is no data storage. However, it is remarkable the informative websites were not compliant themselves. VZVZ keeps

stating security measures are taken but it is not fully clear what those measures include. The main focus lies at expanding possibilities and innovations. Responsibilities are split between different parties; meaning detection responsibilities are also split. The respond phase has become more difficult because of these blurred and split responsibilities. Because of the many different stakeholders it is not always clear what can be expected. By designing a digital system as effectively and efficiently as possible from a legal point of view it may have happened that less attention was paid to the risks of using social security numbers as identification method. The LSP can be called static and linear. It seems the system mainly constitutes of preventive measures instead of reactive measures. However, this means that many lessons can still be learned through application and improvement based on the findings of this research.

The conceptual framework had a dual function. The first function is providing insight in how privacy and security are currently incorporated in the design of the LSP. The second function elaborates on the first function, by exposing what lessons can be learned and how the system could be further improved. The application of the NIST phases can be considered as a SWOT analysis. A SWOT analysis lists opportunities and threats in the market, through which strengths and weaknesses of an organization can be identified. Over the years, more and more focus has been paid to privacy, both in the healthcare sector and in other sectors. It has become more important for patients to have control over their own medical records. In addition, more laws and regulations have been developed that organizations must be compliant to. Because the LSP system consists of sensitive information, it is necessary to clarify the context of the system. This concerns the technical characteristics, its function in society, and the control of the system that depends on human factors.

5.2 Effects

In the previous section it was concluded that the conceptual model of this research contributed to clarifying the privacy concept within the operations of the Landelijk Schakelpunt. It provides a representation of subjects that have received much attention when recording the LSP system. An example of this is the informed consent of patients before medical data is made available. A patient is supposed to be free of choice without any negative consequences. However, not all categories of the NIST framework were equally clear in LSP's design. This offers opportunities to learn and adjust the system. An example is the need for clarification of tasks and responsibilities.

The employees indicated that they are briefly informed about the definition of systems, which means that the work carried out is called into question. Improving this understanding can lead to a better mutual understanding. The conceptual model has contributed to clarifying the relationships in the operational management of the Landelijk Schakelpunt and emphasizes which concepts of privacy can be strengthened. These findings have impact on all stakeholders.

There are some recommendations that reinforce the privacy concept within the LSP's business operations, by focusing on the substantive system, the humans that have to deal with the system, and the vision of patients where the importance of data control is high. Due to the sensitivity of data it is important that as few mistakes as possible are made. Errors that will be made in the LSP system always affect patients' medical records. However, IT auditors and privacy specialists have indicated that it is a matter of time before an incident occurs. That is why it is important to pay attention to possible scenarios regarding security incidents. Extensively testing and analysing the system under complex circumstances creates lessons so action can be taken as adequately as possible during an incident. It is striking that medical specialists indicate that the system mainly involves routine work. From a privacy perspective, this is desirable because it provides clarity about the procedures and protocols to be followed. However, it is important that procedures and protocols are regularly reviewed so that embedded design errors can be corrected in time. Furthermore, there is an important role for communication. This concerns sharpening the importance of correct use of the system; clarifying tasks and responsibilities of different stakeholders; and actions to be followed during an incident. Communication should not only be aimed at employees, but also at patients. The respondents indicated that they were insufficiently aware of the LSP system. Providing more information can combat this – for example an information package before deciding whether or not to give permission – and by only using written permission. This guides a patient through the process and removes uncertainties about the scope of the system. Finally, it is recommended to use a different identification method than the social security number. The BSN was originally introduced as the government's identification number. Since the LSP concerns a private restart, this seems to be an illogical method. In addition, BSNs are irreplaceable, it is linked to a person for the rest of his life and a new number is never provided after an incident. Various respondents from the different categories have indicated they are open to a new

identification method in which only medical data are recorded. In case of errors such a number is not traceable to the BSN, so there is a delimitation of data.

5.3 Limitations

In section 3.4 the reliability and validity of this research were discussed. However, there are also limitations. One weakness of this research is that some respondents may display better answers to the questions than the actual situation. This may be the case because the Landelijk Schakelpunt has known a difficult introduction due to the withdrawal of the Dutch Senate and the private restart of VZVZ. The expectation was that the advantages of easy access to medical records is highly appreciated and therefore not everyone may be willing to understand and acknowledge the disadvantages in terms of security and privacy. Furthermore, respondents might have been careful in speaking freely and in all honesty about their views. As the respondents are interviewed as representatives from their respective organization and not as objective individuals, it might be the case that interviewees are restricted in their ability to talk freely. Anonymizing traceable data to the respondents, and emphasizing there will be no judgments about the statements made eliminate this.

The scope of this research entails a comparison between the earlier rejected Electronic Health Record (EPD) and the adjusted Landelijk Schakelpunt (LSP) in terms of security and privacy. Also, because of the single unit of analysis it is not possible to generalize the findings. There are findings that are applicable to other digitized systems, but there is no focus on comparing different digitized systems.

More research will have to be conducted to create more insight in the outlined privacy issues. It is desirable to conduct both comparable and comparative research into the role of privacy in sensitive systems. The healthcare sector represents a major interest because it affects vulnerable people in society. Patients are in a dependent position because they cannot live without proper care. By conducting more research and questioning more respondents, it can be determined whether the findings are broadly applicable and even applicable to other digitized systems under complex circumstances. It is desirable to conduct more research into whether the recording of a (similar) system such as the LSP can be fully conclusive from a privacy perspective. The increasing urge to be in charge of medical data and the growing attention to privacy are recognized, but it also must remain achievable at all times.

Future research could focus on mobile web applications that provide insight in medical data. Via these so-called eHealth applications, patients gain insight into their health via a personal digital health environment (Rijksoverheid, 2020). Saving time is an advantage because people can easily schedule a consultation online with their healthcare provider. In addition, a healthcare provider could start the correct treatment more quickly and in a more targeted manner, because the medical past is stored. Just as with the LSP, the same questions play a role in guaranteeing privacy at eHealth applications. eHealth is also a digitized system that wants to provide insight into sensitive data – medical data of patients – under complex circumstances. It is important that the potential benefits are not prioritized over risks in terms of security and privacy. The same concerns apply to fraud in healthcare. A documentary recently appeared in which an insurer explained how you could register a healthcare institution within five minutes at the Chamber of Commerce without any requirement or check (NOS, 2020). After registering the institution people come up with non-existent patients for whom tens of thousands of euros are declared. The chance of a fraud being caught is very small. In the Netherlands, the Public Prosecution Service does dozens of healthcare fraud cases per year, but the OM states it does not have the capacity to tackle the enormous amount of frauds. It is remarkable it is known that things go wrong, but because of the lack of capacity little can be obviated. The above-mentioned situation is focused on money. When frauds register a healthcare institution and receive a connection to the LSP, fraud can be committed with personal and medical data. This is a worst-case scenario from a privacy perspective, and may have profound effects.

5.4 Final conclusion

The previous chapters analysed to what extent the design of the Landelijk Schakelpunt (LSP) is improved in terms of privacy compared to the earlier rejected Electronic Health Record (EPD). The analysis was executed by applying the NIST Cyber Security Framework, which consists of five phases: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover.

First, defining privacy has reflected the complexity of the concept. The conceptualization showed its meaning is dependent of situational factors. Medical treatment violates without exception the personal space and affects physical privacy. Besides, there is no absolute privacy because of the necessity of communication between medical specialists and patients. Furthermore, medical records classify as informational privacy.

After privacy was conceptualized the NIST Cyber Security Framework is interpreted from a privacy point of view. The only way the LSP could be seen as successful is when the security of personal data and medical records of patients is guaranteed. By aligning and assessing the context of the system, the applicable procedures and identifying how (possible) incidents are handled it is intended to create more insight in the design and reliability of this medical exchange system.

One major difference between the EPD and LSP is that the design of the EPD never got as far as the LSP due to an early withdrawal of the Dutch Senate. Privacy and security were important subjects at both systems but the focus increased over time. It is acknowledged the system entails sensitive data that need to be protected at all times. However, it seems VZVZ's design of the Landelijk Schakelpunt mainly contains preventive measures instead of reactive measures. There is an expectation of one best way to deal with the exchange of medical data, and the procedures and protocols are designed accordingly. This perspective introduces the risk that there is insufficient attention for data breaches and security incidents. By applying the NIST framework the strengths and gaps of the incorporation of privacy in the Landelijk Schakelpunt have become clear. It can be concluded that LSP's design can be improved by focusing on the respond and recover phase of the NIST Cyber Security Framework.

6. Literature

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, 73-80.

AP. (2019a). Zorgsector opnieuw koploper datameldingen bij AP. Retrieved from: https://autoriteitpersoonsgegevens.nl/nl/nieuws/zorgsector-opnieuw-koploper-datalekmeldingen-bij-ap

AP. (2019b). Burgerservicenummer (BSN). Retrieved from: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/burgerservicenummer-bsn?qa=bsn

AP. (2019c). Definitieve DPIA-lijst beschikbaar. Retrieved from: https://autoriteitpersoonsgegevens.nl/nl/nieuws/definitieve-dpia-lijst-beschikbaar

Bryman, A. (2015). Social research methods. Oxford: Oxford University Press.

Cuijpers, C. (2007). Privacy in context. *JMA Berkvens & JEJ Prins.*

Dwivedi, A., Bali, R. K., James, A. E., Naguib, R. N. G., & Johnston, D. (2002, May). Merger of knowledge management and information technology in healthcare: Opportunities and challenges. In *IEEE CCECE2002. Canadian Conference on Electrical and Computer Engineering. Conference Proceedings (Cat. No. 02CH37373)* (Vol. 2, pp. 1194-1199). IEEE.

Eerste Kamer. (2011). Eerste Kamer verwerpt unaniem voorstel landelijk EPD – 31.466. Retrieved from: https://www.eerstekamer.nl/nieuws/20110405/eerste_kamer_verwerpt_unaniem

EUR-Lex. (2016). GDPR 32016R0679.

Gerring, J. (2004). What is a case study and what is it good for? *American political science review,* 98(2), 341-354.

Groothuis, M.M. (2007). Het elektronisch patiëntendossier in een veellagige rechtsorde. Alphen aan den Rijn: Kluwer.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. The qualitative report, 8(4), 597-606.

Gomm, R., Hammersley, M. & Foster, P. (2009). *Case study method.* London: SAGE Publications Ltd doi: 10.4135/9780857024367

ICT&Health. (2018). LSP lanceert publiekscampagne. Retrieved from: https://www.icthealth.nl/nieuws/lsp-lanceert-publiekscampagne/

Jutel, A., & Lupton, D. (2015). Digitizing diagnosis: a review of mobile applications in the diagnostic process. Diagnosis, 2(2), 89-96.

Kamerstukken II 2006/07,27529 nr. 29; Programmacommissie Informatie- en Communicatietechnologie in de Zorg.

Keizer, A.G. (2011). De digitale patiënt centraal – medische informatie in een digitale wereld. In: Wetenschappelijke Raad voor het Regeringsbeleid - De staat van informatie. Amsterdam: Amsterdam University Press.

Koops, B. J. & Vedder, A. (2001). *Opsporing versus privacy: de beleving van burgers*. Sdu Uitgevers.

Martijn, M. & Tokmetzis, D. (2016). Je hebt wel iets te verbergen – over het levensbelang van privacy. Amsterdam: De Correspondent Bv.

Modderkolk, H. (2015). Artsen experimenteren met 'veiliger' patiëntendossier. Retrieved from: https://www.volkskrant.nl/wetenschap/artsen-experimenteren-met-veiliger-patientendossier~baf27b8e/

NEN. (2019). Informatiebeveiliging in de zorg – alles over NEN 7510. Retrieved from: https://www.nen.nl/NEN-Shop/Zorg-Welzijn.htm

NHG. (2019). NHG-Richtlijn – Adequate dossiervorming met het elektronisch patiëntdossier (ADEPD).

NIST. (2018). Cyber Security Framework - Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1

Nu.nl (2017). Patiënt zonder elektronisch patiëntendossier krijgt medicatie moeilijk mee. Retrieved from: https://www.nu.nl/gezondheid/4688850/patient-zonder-elektronisch-patientendossier-krijgt-medicatie-moeilijk-mee.html

NOS. (2011). Eerste Kamer verwerpt EPD – Video. Retrieved from: https://nos.nl

NOS. (2020). Controle zorgfraude faalt, OM en verzekeraars luiden noodklok. Retrieved from: https://nos.nl/nieuwsuur/artikel/2317099-controle-zorgfraude-faalt-om-en-verzekeraars-luiden-noodklok.html

NSOB. (2012). Het EPD voorbij? Evaluatie Besluitvormingsproces Kaderwet Elektronische Zorginformatie-uitwisseling.

Officiële Bekendmakingen. (2011). Kamerstuk: 31466 nr AB.

Patil, H. K., & Seshadri, R. (2014, June). Big data security and privacy issues in healthcare. In 2014 IEEE international congress on big data (pp. 762-765). IEEE.

Rijksoverheid. (2019). Inspectie Gezondheidszorg en Jeugd. Retrieved from https://www.igj.nl/over-ons

Rijksoverheid. (2020). E-Health – digitale zorg. Retrieved from: https://www.rijksoverheid.nl/onderwerpen/e-health

RvIG. (2019). Centraal Meldpunt Identiteitsfraude en –fouten. Retrieved from: https://www.rvig.nl/fraudebestrijding/centraal-meldpunt-identiteitsfraude-en--fouten

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int'l LJ, 50, 305.

Schneider, E. C., Ridgely, M. S., Meeker, D., Hunter, L. E., Khodyakov, D., & Rudin, R. S. (2014). Promoting patient safety through effective health information technology risk management. Rand health quarterly, 4(3).

Schulman, P.R. (2004). General attributes of safe organizations. BMJ Quality & Safety, 13(suppl 2), ii39-ii44

Stickman Consulting. (2019). Develop a whole of company approach to managing risk with the NIST Cyber Security Framework. Retrieved from: https://www.stickman.com.au

Van den Elsen, W. (2011). NVZ: privacy hindert uitwisseling zorginformatie. Retrieved from: https://www.zorgvisie.nl/nvz-privacy-hindert-uitwisseling-zorginformatie-zvs012528w/

Volg Je Zorg. (2019a). Hoe werkt het Landelijk Schakelpunt? Retrieved from: https://www.volgjezorg.nl/het-lsp

Volg Je Zorg. (2019b). Veiligheid en Privacy van het Landelijk Schakelpunt. Retrieved from: https://www.volgjezorg.nl/het-lsp/veiligheid-en-privacy

VWS. (2008). Stappenplan Landelijke invoering Elektronisch Patiëntendossier.

VWS. (2017). Elektronische gegevensuitwisseling in de zorg – de Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg.

VZVZ. (2015). Businessplan 2016 – 2020.

VZVZ. (2019). Over VZVZ. Retrieved from: https://www.vzvz.nl/over-vzvz

VZVZ. (2019a). Over het LSP – aansluiten. Retrieved from: https://www.vzvz.nl/over-het-lsp/aansluiten

VZVZ. (2019b). Wie houdt toezicht op het rechtmatig gebruik van het Landelijk Schakelpunt? Retrieved from: https://www.vzvz.nl/veelgestelde-vragen

VZVZ. (2019c). VZVZ en het LSP. Retrieved from: https://www.vzvz.nl

VZVZ. (2019d). 1e, 2e, en 3e lijn ondersteuning bij incidenten. Retrieved from: https://www.vzvz.nl/ict-dienstverleners/zorg-id/support/1e-2e-en-3e-lijn-ondersteuning-bij-incidenten

VZVZ. (2019 e). Storing en onderhoud. Retrieved from: https://www.vzvz.nl/ict-dienstverleners/beheerorganisaties/storing-en-onderhoud

VZVZ. (2019f). Terugblik VZVZ-dagen: De patient en de zorg, een toekomstbestendige digitale relatie? Retrieved from: https://www.vzvz.nl/actueel/terugblik-vzvz-dagen-de-patient-en-de-zorg-een-toekomstbestendige-digitale-relatie

VZVZ. (2019g). Privacy verklaring. Retrieved from: https://www.vzvz.nl/privacy-verklaring

VZVZ. (2019h). Het LSP en de nieuwe privacywetgeving; een stand van zaken. Retrieved from: https://vzvz.nl

Welford, B. (2019). What is GDPR, the EU's new data protection law? Retrieved from https://gdpr.eu

Witmer, J.M. & de Roode, R.P. (2004). Van wet naar praktijk. Implementatie van de WGBO. Den Haag: Rooduijn.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. *Information systems research*, *21*(4), 724-735.

ZonMw. (2019). Informatie- en Communicatietechnologie in de Zorg. Retrieved from https://www.zonmw.nl

ZorgNu. (2017). Patiënten slecht op de hoogte van 'het nieuwe EPD'. Retrieved from https://zorgnu.avrotros.nl/uitzendingen/achtergrondartikelen/item/patienten-slecht-op-de-hoogte-van-het-nieuwe-epd/

Appendix 1: Data analysis schedules

These schedules represent the NIST Cyber Security Framework.

1. Identify

Function	Category	Subcategory
Identify (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	ID.AM-1: Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk.	ID.GV-1: Organizational cyber security policy is established and communicated
		ID.GV-2: Cyber security roles and responsibilities are coordinated and aligned with internal roles and external partners
		ID.GV-3: Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed
		ID.GV-4: Governance and risk management processes address cyber security risks
	Risk Assessment (ID.RA): The organization understands the cyber security risk to organizational operations (including mission,	ID.RA-1: Asset vulnerabilities are identified and documented
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
		ID.RA-3: Threats, both internal and external, are identified and documented

	functions, image, or reputation), organizational assets, and individuals.	ID.RA-4: Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

2. Protect

Function	Category	Subcategory
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained
		PR.AT-2: Privileged users understand their roles and responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
		PR.AT-4: Senior executives understand their roles and responsibilities
		PR.AT-5: Physical and cyber security personnel understand their roles and responsibilities
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity,	PR.DS-1: Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained

	and availability of information.	PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
		PR.IP-2: A System Development Life Cycle to manage systems is implemented
		PR.IP-3: Configuration change control processes are in place
		PR.IP-4: Backups of information are conducted, maintained, and tested
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
		PR.IP-6: Data is destroyed according to policy
		PR.IP-7: Protection processes are improved
		PR.IP-8: Effectiveness of protection technologies is shared
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10: Response and recovery plans are tested
		PR.IP-11: Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: A vulnerability management plan is developed and implemented
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
		PR.PT-2: Removable media is protected and its use restricted according to policy
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
		PR.PT-4: Communications and control networks are protected
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

3. Detect

Function	Category	Subcategory
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
		DE.AE-2: Detected events are analyzed to understand attack targets and methods
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors
		DE.AE-4: Impact of events is determined
		DE.AE-5: Incident alert thresholds are established
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cyber security events
		DE.CM-2: The physical environment is monitored to detect potential cyber security events
		DE.CM-3: Personnel activity is monitored to detect potential cyber security events
		DE.CM-4: Malicious code is detected
		DE.CM-5: Unauthorized mobile code is detected
		DE.CM-6: External service provider activity is monitored to detect potential cyber security events
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
		DE.CM-8: Vulnerability scans are performed
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-2: Detection activities comply with all applicable requirements
		DE.DP-3: Detection processes are tested
		DE.DP-4: Event detection information is communicated
		DE.DP-5: Detection processes are continuously improved

4. Respond

Function	Category	Subcategory
Respond (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed
		RS.CO-2: Incidents are reported consistent with established criteria
		RS.CO-3: Information is shared consistent with response plans
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated
		RS.AN-2: The impact of the incident is understood
		RS.AN-3: Forensics are performed
		RS.AN-4: Incidents are categorized consistent with response plans
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained
		RS.MI-2: Incidents are mitigated
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned
		RS.IM-2: Response strategies are updated

5. Recover

Function	Category	Subcategory
Recover (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned
		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-1: Public relations are managed
		RC.CO-2: Reputation is repaired after an incident
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Appendix 2 – List of accepted healthcare information systems

The following XIS-applications are accepted by VZVZ:

Leverancier	Applicatie	Applicatieversie	AORTA-versie
Advanced	Adastra (HAPIS)	3.16	6.12.0.0
Allegro Sultum	MLCAS (JGZ)	2.0.1	6.12.0.0
Asterisque	Asterisque (MV)	V19Q1	6.12.0.0
Brightfish (i.c.m. Zorgdoc)	EMR (MV)	V1.83	6.12.0.0
Caresharing	cKIS (KIS Ketenzorg)	P.2019.1.02	8.0.1.0
CareSoft	FarmaSys (AIS)	2018-01	6.12.0.0
Centric	OpenCare (JGZ)	6.4.0	6.12.0.0
ChipSoft	CS-EZIS (MV)	5.2	6.12.0.0
	HiX (MV)	6.1	6.12.0.0
	HiX (AIS)	6.1	6.12.0.0
	HiX (HAPIS)	6.1	6.12.0.0
	HiX (HIS)	6.2	6.12.0.0
CNS connect	CNS connect (MV)	V20190228	6.12.0.0
CompuGroup Medical	CGM APOTHEEK (AIS)	2.3	6.12.0.0
	CGM HUISARTS (HIS)	2.3	6.12.15.0
	CGM HUISARTS (HIS Ketenzorg)	2.13	8.0.1.0
Curasoft (i.c.m. Zorgdoc)	Curasoft (MV)	2.25	6.12.0.0
Diasoft	Diamant 2 (MV)	3.13	6.12.15.0
Dixis (i.c.m. Zorgdoc)	DiSy	V14.0	6.12.0.0

Drimpy (i.c.m. Dixis)	Drimpy	V1.01	6.12.0.0
DXC	Transmurale Medicatie Viewer (MV)	6.30	6.12.0.0
	MicroHIS (HIS)	13.6	6.12.15.0
	MicroHIS (HIS Ketenzorg)	14.5	8.0.1.0
Eljakim Information Technology	Iuvenelis	1.17.0	6.12.0.0
Enovation	LSP Connect Viewer (MV)	1.1	6.12.0.0
Epic	Epic (MV)	V83.0	6.12.0.0
FarmedVisie	FarMedRX (ZIS)	2018_11	6.12.0.0
Finalist	GGiD (JGZ)	1.0.0	6.12.0.0
Forcare	ForLSP (MV)	1.0	6.12.0.0
Gino	Kidos (JGZ)	28.0.9	6.12.0.0
Heart for Health	MedicalPortal (ZIS/MV)	12.23	6.12.0.0
HI-Systems	Zamicom/Klinicom (MV)	2018-3	6.12.0.0
	ViPharma (ZIS)	17.1	6.12.0.0
Isala	EriDanos (MV)	7.0	6.12.0.0
Labelsoft (CGM)	WebHIS Call Manager (HAPIS)	4.1.14	6.12.0.0
	WebHIS Zorgdossier (HIS)	2.5	6.12.0.0
Medicore (i.c.m. FarmedVisie)	MC EPD (MV)	V2018.5	6.12.0.0
Medicore (i.c.m. Medimo)	MC EPD (MV)	V2019.2	6.12.0.0
Medimo	Medimo (AIS)	2019-2	6.12.0.0

MI Consultancy (i.c.m. Zorgdoc)	Neo-ZIS | EPD (MV)	v9.6.4.32328	6.12.0.0
NEXUS	NEXUS / EPD (medicatie) (MV)	2019.01	6.12.0.0
OmniHis	Scipio (HIS)	7.3	6.12.0.0
	Scipio (HIS Ketenzorg)	4.3.7.3	8.0.1.0
Ordina (RIVM)	Praeventis	1.6	6.12.0.0
Orfeus	TransHIS (HIS)	8.0	6.12.0.0
PharmaPartners	Hapicom (HAPIS)	498	6.12.0.0
	Medicom (HIS)	498	6.12.0.0
	Pharmacom (AIS)	498	6.12.0.0
Promedico	ASP (HIS)	2018.1.1	6.12.0.0
	ASP (HIS Ketenzorg)	2019.4	8.0.1.0
	VDF (HIS+AIS)	10.3.5	6.12.0.0
	VDF (HIS Ketenzorg)	10.6.4	8.0.1.0
	Apro (AIS)	1.1	6.12.15.0
SmartMed	SmartMed (MV)	3.1	6.12.0.0
Tetra	Bricks Huisarts (HIS)	8.2019	8.0.1.0
	Bricks Apotheek (voorheen VidiVici) (AIS)	20.20	6.12.0.0
TIMEFF	Emma	V19	6.12.0.0
Topicus	Topicus HAP (HAP)	7.2	6.12.0.0
	Topicus Teleview (MV)	1.4.X	6.12.0.0
	KD+ (JGZ)	4.23.0	6.12.0.0
	GBP Portaal	1.0	6.12.0.0
Vertimart	Exquise (MV)	V4.7	6.12.0.0

VIR E-Care solutions (i.c.m. DXC)	Ecaris (MV)	V3.3.6	6.12.0.0
VitalHealth	VitalHealth (KIS)	3.2	6.12.15.0
Zorgdoc	Medver	1.0.2	6.12.0.0

Source: VZVZ, 2019.

Appendix 3 – Goed Beheerd Zorgnetwerk (GZN)

GZN'en (well-managed care networks) establish a secure connection between well-managed care systems of care providers and the Landelijk Schakelpunt. The network suppliers below have been accepted by VZVZ as GZN:

- Cobbler
- Enovation B.V.
- E-Zorg B.V.
- FuTec Systems B.V.
- GERRIT Diensten (Stichting GERRIT)
- ITPcare (IT-Pros B.V.)
- iunxi B.V.
- KPN ZorgConnect
- NetSourcing.nl
- Previder B.V.
- RAM Infotechnology
- Stichting RijnmondNet
- Stichting Zorgring Noord-Holland Noord
- Systemec B.V.
- Vancis B.V.
- VoiceWorks

Source: VZVZ, 2019.