Het betrouwbaar en veilig inrichten van de digitalisering van medische gegevens

Een onderzoek naar de bedrijfsvoering van het Landelijk Schakelpunt (LSP) ten aanzien van het versterken van de privacy van patiënten door toepassing van het HRO-perspectief.

Master Scriptie
Management van de Publieke Sector
Strategie, Advisering en Verandermanagement
Marissa de Beeld
s1698214
10 januari 2020

Begeleider: dr. J. Reijling
Aantal woorden: 23.802

Voorwoord

Voor u ligt mijn masterscriptie ter afronding van mijn studie Management van de Publieke Sector aan de Universiteit Leiden. Van tevoren ben ik veelvuldig gewaarschuwd voor alle clichés die voorkomen tijdens het schrijven van een scriptie, en gelukkig kan ik stellen dat ik het maar met weinig van die clichés eens ben. Het Landelijk Schakelpunt en het digitaliseren van medische informatie in het algemeen blijf ik fascinerend vinden en ik kan er eindeloos over doorgaan. Toch ben ik ook blij en trots dat dit document nu klaar is, wat nooit in deze vorm was gelukt zonder de hulp en steun van anderen.

Als eerste wil ik graag mijn scriptiebegeleider Jaap Reijling bedanken. Ik ben zeer dankbaar voor alle feedback en suggesties die tijdens het proces zijn aangedragen. De opmerkingen hebben me altijd aan het denken gezet, terwijl het tegelijkertijd geen afbreuk deed aan mijn onderwerp.

Daarnaast wil ik graag alle respondenten die tijd hebben vrijgemaakt om hun perspectieven en ideeën met mij te delen bedanken. De openheid tijdens de gesprekken heeft me meer inzicht gegeven in hoe lastig het is om een goed systeem te ontwerpen terwijl er eigenlijk tegenstrijdige belangen zijn. Mijn enthousiasme om me hier mee bezig te houden is door de gesprekken nog meer aangewakkerd.

Als laatste wil ik graag mijn vrienden en familie bedanken voor alle steun. Bedankt dat jullie mijn eindeloze monologen nooit hebben afgekapt en begrip hebben getoond wanneer ik vooral focus had voor mijn scriptie.

Het zit er nu dan toch echt op, mijn scriptie is af. Ik hoop dat u met het lezen van dit document net zo veel plezier ervaart als ik had met het schrijven!

Samenvatting

Steeds meer organisaties zetten digitale hulpmiddelen in om processen te stroomlijnen. Ook in de zorgsector is deze trend te herkennen. Nadat de Eerste Kamer zich in 2011 heeft gedistantieerd van de optekening van het Elektronisch Patiënten Dossier – omdat het onvoldoende veilig en betrouwbaar werd bevonden – is groen licht gegeven voor het verder ontwikkelen van een soortgelijk systeem. Sinds januari 2012 is de Vereniging van Zorgaanbieders voor Zorgcommunicatie verantwoordelijk voor de private doorstart van het digitale patiëntendossier: het Landelijk Schakelpunt.

Dit onderzoek analyseert in hoeverre het concept privacy naar voren komt in de bedrijfsvoering van het Landelijk Schakelpunt. Dit wordt onderzocht aan de hand van het conceptueel model, bestaande uit een koppeling van kenmerken van de High Reliability Organizations theorie van Weick, Sutcliffe & Obstfeld (2008) en kenmerken vanuit de privacywetgeving. De toepassing van het conceptueel model heeft geleid tot inzicht in de privacy elementen die sterk in het systeem zichtbaar zijn. Daarnaast weergeeft het zwakke elementen, wat een kans biedt voor het verder incorporeren van privacy. Na het analyseren van de bevindingen volgt een aantal aanbevelingen. Deze gaan onder andere in op het inhoudelijke systeem, de rol van menselijke factoren die met het systeem moeten werken, en de visie van patiënten dat zich voornamelijk richt op het hebben van controle over eigen data. Er wordt afgesloten met suggesties voor toekomstig onderzoek, zodat de geschetste problematiek verder inzichtelijk kan worden gemaakt.

Trefwoorden*: Digitalisering, Privacy, Medische Sector, Landelijk Schakelpunt*

Lijst met afkortingen

AVG	Algemene Verordening Gegevensbescherming
BSN	Burgerservicenummer
CBS	Centraal Bureau voor de Statistiek
CMI	Centraal Meldpunt Identiteitsfraude en –fouten
EPD	Elektronisch Patiëntendossier
GBZ	Goed Beheerd Zorgsysteem
GZN	Goed Beheerd Zorgnetwerk
HRO	High Reliability Organization
LSP	Landelijk Schakelpunt
NHG	Nederlands Huisartsen Genootschap
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
PGO	Persoonlijk gezondheidsomgevingen
UZI	Unieke Zorgverlener Indicatie
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
WPISP	Working Party on Information Security and Privacy

Inhoudsopgave

1. Inleiding

Technologie blijft zich verder ontwikkelen waardoor steeds meer organisaties digitale hulpmiddelen inzetten om processen te stroomlijnen. Digitalisering laat zich dan ook kenmerken door een proces van verandering (Rutten, 2007). Vanuit een technisch perspectief wordt digitalisering beschouwd als een nieuwe manier van ontwikkeling, verwerking, verspreiding en consumptie van informatie (Rutten, 2007). Een gecodeerde structuur van nullen en enen zorgt ervoor dat verschillende informatiestromen ontstaan. Iedere gebruiker van het internet kan op deze manier bij verschillende teksten, afbeeldingen, video's, muziek en andere vormen van informatie en uitlatingen, waarvan de herkomst van bronnen, specifieke netwerken, informatie- dragers of apparatuur niet duidelijk hoeft te zijn. Dit heeft tot gevolg dat het produceren, toegankelijk maken en op grote schaal verspreiden van digitale informatie niet altijd betrouwbaar is.

Door deze ontwikkelingen in informatie- en communicatietechnologieën zijn er onder andere nieuwe platformen ontstaan voor sociale media. Voorbeelden van applicaties zijn Facebook en Instagram, welke het mogelijk maken om de 'buitenwereld' meer inzicht te bieden in het leven van een individu. Een onderzoek van het Centraal Bureau voor de Statistiek (CBS) heeft uitgewezen dat steeds meer jongvolwassenen worden bestempeld als 'verslaafd' aan sociale media[1]. Het aantal 18- tot 25-jarigen dat naar eigen zeggen verslaafd is, is van 2015 tot 2017 toegenomen met tien procent. Naast het representeren van de groep die de meeste tijd besteedt aan sociale media, zijn de jongvolwassenen ook het meest angstig om updates te missen. Een gebeurtenis die veelvuldig wordt gedeeld op sociale media is een foto van een pas behaald rijbewijs. Alleen op het platform Instagram stond aan het begin van 2019 een totaal aantal van 3597 berichten onder #rijbewijsgehaald[2].

1.1 Gevaren van digitalisering

Op de digitale zwarte markt, het darkweb, bieden criminelen de gemaakte foto's van jongeren met hun net behaalde rijbewijs inclusief BSN te koop aan

[1] Meer informatie: CBS (2018): Jongvolwassenen vaker verslaafd aan sociale media.
[2] Instagram openbare zoekopdracht: #rijbewijsgehaald

(Privacyzone, 2018). De prijzen die worden gevraagd, variëren van 50 tot 80 euro voor een pakket met meerdere foto's. Voor een enkele foto wordt gemiddeld 2,50 euro gevraagd. De BSN's die de criminelen in handen hebben kunnen voor meerdere doeleinden worden gebruikt. Met behulp van de foto kunnen criminelen onder de naam van het slachtoffer producten aanbieden, zoals smartphones. Eenmaal in gesprek met een potentiele koper, stuurt de crimineel de foto door om het vertrouwen te winnen. Zodra de koper akkoord gaat en betaalt, verdwijnt de crimineel met het geld, met het gevolg dat de persoon op de foto wordt gezien als de oplichter. Een andere manier is het afsluiten van diverse dure abonnementen op naam van het slachtoffer, zodat het slachtoffer de rekening ontvangt en de oplichter het product kan doorverkopen (Privacyzone, 2018). Om deze vorm van cybercriminaliteit tegen te gaan, is het Centraal Meldpunt Identiteitsfraude en –fouten (CMI) opgericht, als onderdeel van de Rijksdienst voor Identiteitsgegevens, Ministerie van Binnenlandse Zaken en Koningsrelaties (BZK). Dit biedt een platform voor meldingen van identiteitsfraude, geeft tips om identiteitsfraude te voorkomen en biedt advies en ondersteuning wanneer een individu slachtoffer is van identiteitsfraude (RvIG, 2019).

Soortgelijke risico's en problematiek zoals hiervoor geschetst doen zich ook voor bij het inzichtelijk maken van medische gegevens. In het nieuwe systeem van het Landelijk Schakelpunt (LSP), de opvolger van het Elektronisch patiëntendossier (EPD), worden medische gegevens van patiënten 'geanonimiseerd' uitgewisseld door patiënten te identificeren aan de hand van burgerservicenummers. Het nadeel van dit systeem is het gevaar dat met het BSN gemakkelijk een koppeling kan worden gemaakt tussen informatie uit verschillende bestanden (AP, 2019a). Door het aantal nadelen is er een moeizame introductie van het elektronisch patiëntendossier geweest, wat ook het gebrek aan vertrouwen vanuit politiek opzicht benadrukt. Nadat de Eerste Kamer zich heeft teruggetrokken van het landelijk Elektronisch Patiëntendossier wegens het onvoldoende kunnen garanderen dat het systeem veilig en betrouwbaar was, werd opgeroepen om te zoeken naar een betrouwbare infrastructuur voor het uitwisselen van medische gegevens tussen artsen (Modderkolk, 2015). Vanwege de terugtrekking van de Eerste Kamer, kreeg het LSP in 2012 een private doorstart.

Na deze gebeurtenissen is het systeem verder ontwikkeld door De Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ). Vanuit juridisch perspectief blijkt dat veel regels zijn vastgelegd op nationaal, Europees en internationaal niveau. Ondanks vastlegging in wet- en regelgeving kan er volgens andere academici niet worden gesteld dat veilige organisaties bestaan doordat in het verleden behaalde resultaten geen garantie bieden voor veiligheid van systemen in de toekomst (Sutcliffe, 2012). Echter zijn er twee stromingen die zich richten op de systeemveiligheid onder complexe omstandigheden, namelijk Normal Accident Theory (NAT) en High Reliability Organizations (HRO). Bij NAT wordt gesteld dat ongeacht de effectiviteit van het beheer of het functioneren, ongelukken bij systemen als 'normaal' of 'onvermijdelijk' moeten worden beschouwd, omdat zij vaak niet kunnen worden voorzien of voorkomen (Sutcliffe, 2012). HRO onderscheidt zich van NAT door zich te richten op mislukking en betrouwbaarheid, om zo tot procesverbetering te komen (Weick, Sutcliffe & Obstfeld, 2008). De prioriteit wordt hierbij gegeven aan het lerend vermogen naar aanleiding van gebeurtenissen, onderzocht aan de hand van vijf thema's: preoccupation with failure, simplify interpretations, sensitivity to operations, commitment to resilience, en underspecification of structures. Om een bijdrage te leveren aan de geschetste problematiek rond beveiliging van privacygevoelige informatie analyseert dit onderzoek de bedrijfsvoering en de bijbehorende risico's van het Landelijk Schakelpunt aan de hand van het HRO perspectief. De centrale vraag die hierbij is geformuleerd, luidt: *In hoeverre kan de bedrijfsvoering van het Landelijk Schakelpunt (LSP) ten aanzien van privacy worden versterkt door toepassing van de High Reliability Organization (HRO) theorie van Weick, Sutcliffe & Obstfeld (2008)?* Hierbij zal worden onderzocht wat het Landelijk Schakelpunt inhoudt, hoe gevoelig het systeem wordt bevonden vanuit een privacy perspectief en wat de risico's van een dergelijk systeem betreffen.

1.2 Relevantie

Dit onderzoek is maatschappelijk relevant doordat het een ieder in de samenleving kan raken. Iedere patiënt wordt gedwongen een keuze te maken tussen het wel of niet delen van medische gegevens via het LSP. Echter, er kleven veel consequenties aan deze keuze, wat de vrijblijvendheid vermindert. Een onderzoek van EenVandaag toont aan dat patiënten die hun medische gegevens niet willen delen vaak moeizaam of helemaal geen medicatie meekrijgen bij een willekeurige apotheek (Nu.nl, 2017). De recepten die de patiënten voorgeschreven krijgen van een huisarts, tandarts of specialist blijken soms onvoldoende om ook daadwerkelijk de voorgeschreven medicijnen te verkrijgen, waardoor de indruk wordt gewekt dat men eerst bij het LSP moet zijn aangesloten voordat ze medicatie kunnen ontvangen.

Dit onderzoek is daarnaast wetenschappelijk relevant doordat de risico's mogelijk worden onderschat ten opzichte van de voordelen die het LSP kan bieden. Met de betwistbare betrouwbaarheid van de identificatie aan de hand van BSN wordt mogelijk de privacy van iedere patiënt in twijfel getrokken. Door de steeds verdergaande ontwikkelingen van digitalisering en het ontstaan van sociale media, wordt steeds meer op het internet gepubliceerd, waardoor cybercriminelen steeds meer manieren bedenken tot het misbruiken van persoonsgegevens. Om dit te voorkomen zijn diverse wettelijke richtlijnen en normenkaders opgesteld, zoals de Algemene Verordening Gegevensbescherming (AVG) en de ISO 27001 standaard. Met het optekenen en de vormgeving van het systeem is de nadruk voornamelijk gelegd op hoe het vanuit een juridisch kader kan worden ingevoerd. Echter kan een juridisch perspectief op zichzelf niet zorgen voor voldoende betrouwbaarheid van een systeem, doordat er altijd een afhankelijkheid blijft bestaan van inhoudelijke kennis en de toepassing daarvan. Er zijn nog steeds menselijke factoren die met het systeem zullen moeten leren omgaan (Officiële Bekendmakingen, 2011). Dit onderzoek focust zich dan ook op de inrichting en bedrijfsvoering van het LSP, waarbij de identificatie van patiënten aan de hand van BSN wordt bestudeerd vanuit een privacy perspectief.

1.3 Leeswijzer

In dit hoofdstuk zijn de aanleiding, centrale onderzoeksvraag en de maatschappelijke en wetenschappelijke relevantie van dit onderzoek uiteengezet. In het volgende hoofdstuk wordt het theoretisch kader toegelicht, waarbij verschillende academische perspectieven en het theoretisch concept aan bod komen. In hoofdstuk 3 wordt ingegaan op de methodologie die wordt gehanteerd, namelijk het research design van dit onderzoek, de manier van dataverzameling en -analyse. Ook worden de betrouwbaarheid en validiteit behandeld. Vervolgens worden in hoofdstuk 4 de resultaten besproken en wordt een conclusie geformuleerd. Tot slot wordt in hoofdstuk 5 afgesloten met de reflectie en discussie van dit onderzoek.

2. Theoretisch kader

In dit hoofdstuk wordt het theoretisch kader uiteengezet. Eerst wordt een verkenning van diverse perspectieven uitgevoerd. Vervolgens wordt ingezoomd op het gekozen theoretisch concept. Allereerst wordt het begrip privacy uiteengezet, daarna wordt, het concept over High Reliability Organizations (HRO) door Weick, Sutcliffe & Obstfeld (2008) gedefinieerd, gevolgd door het conceptueel kader waarin het HRO principe bruikbaar wordt gemaakt voor dit onderzoek, door de theorie te concretiseren naar borging van privacy.

2.1 Verkenning van diverse perspectieven

Groothuis (2007) benadrukt in haar artikel dat het proces omtrent het wel of niet invoeren van het EPD veel tijd heeft ingenomen en dat het juridisch kader veel lagen betreft. Regels omtrent het gebruik van persoons- en medische gegevens zijn vastgelegd op internationaal, Europees en nationaal niveau. Zo wordt onderscheid gemaakt tussen het fundamentele recht op eerbiediging van de persoonlijke levenssfeer zoals vastgelegd in artikel 17, eerste lid van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR); artikel 8, eerste lid, van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM); en artikel 10, eerste lid, van de Grondwet. Daarnaast is er ook nog Richtlijn 95/46lEG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens; de Wet bescherming persoonsgegevens (Wbp) welke inmiddels is vervangen door de Algemene Verordening Gegevensbescherming (AVG); het Burgerlijk Wetboek en andere richtlijnen zoals opgesteld door de AP over het gebruik van BSN. Het wettelijke kader dat van kracht is, kan invloed uitoefenen doordat het de richting bepaalt voor aandachtsgebieden. Dit geldt ook voor het belang van privacy.

Ondanks vastlegging in wet- en regelgeving vormt volgens Schulman (2004) veiligheid een illusie: veilige organisaties bestaan niet omdat in het verleden behaalde resultaten geen garantie bieden voor de toekomstige veiligheid van welke organisatie dan ook. Hierdoor kunnen High Reliability Organizations (HRO) beter worden beschouwd als naar betrouwbaarheid strevende entiteiten dan als betrouwbare entiteiten (Sutcliffe, 2012). Aanvullend benadrukt Sutcliffe (2012) dat

de term ‘high reliability organization’ problematisch kan worden geïnterpreteerd omdat het impliceert dat de beoordeling is gebaseerd op een absolute en statische prestatiemaatstaf in plaats van een relatieve beoordeling. Naar betrouwbaarheid strevende organisaties onderscheiden zich niet door het absolute aantal fouten of mislukkingen maar door effectieve en organisatorische beheersing. Op deze manier kunnen de concepten ‘risicovol’ en ‘zeer effectief’ naast elkaar staan.

Volgens privacy jurist Daniel Solove is het niet problematisch dat zo veel informatie over individuen wordt verzameld, maar vormt het gebrek aan inzicht in waar en op welke manier deze data worden gebruikt het probleem (Martijn & Tokmetzis, 2016). De macht van data verzamelende en delende overheden en instituties wordt hierdoor vergroot. Om meer inzicht te krijgen in de omgang met data zal het systeem inhoudelijk moeten worden bestudeerd. Er kunnen twee stromingen worden geïdentificeerd die zich richten op systeemveiligheid onder complexe omstandigheden, namelijk High Reliability Organizations (HRO) en Normal Accident Theory (NAT). Bij HRO wordt gekeken naar mislukkingen en betrouwbaarheid om tot procesverbetering te kunnen komen. Bij NAT wordt gesteld dat ongeacht de effectiviteit van het beheer of het functioneren, ongelukken bij systemen die worden gekenmerkt door sterke koppelingen en interactieve complexiteit, als ‘normaal’ of ‘onvermijdelijk’ moeten worden beschouwd, omdat zij vaak niet kunnen worden voorzien of voorkomen (Sutcliffe, 2012). Waar HRO vaak wordt gecategoriseerd als optimistisch, wordt NAT omschreven als een pessimistisch perspectief. Ondanks de verschillen, zijn er ook overeenkomsten tussen beide stromingen, zoals de focus op de sociale en organisatorische fundamenten van systeemveiligheid en de oorzaken, gevolgen en preventie van ongevallen. Daarnaast staan de technisch aspecten bij beide theorieën minder hoog geprioriteerd (Sutcliffe, 2012).

Ook Leveson et al. (2009) hebben een blik geworpen op de Normal Accident Theory (NAT). Hierbij is aandacht besteed aan de waarschijnlijk hogere ongevalspercentages bij complexe systemen, doordat de potentiële interacties in dergelijke systemen niet grondig kunnen worden gepland, begrepen, verwacht en bewaakt. Van de interacties wordt verwacht dat ze verder gaan dan het vermogen van ingenieurs om het gedetailleerd te begrijpen en te beheren (Leveson et al,

2009). Doordat ze niet grondig kunnen worden getest en geanalyseerd voor gebruik, hebben zulke complexe systemen meer kans op onopgemerkte ontwerpfouten. Dit gebrek aan inzicht zorgt ervoor dat de systemen waarschijnlijk moeilijker zijn te beheren in crisissituaties. De grondlegger van de theorie NAT beargumenteert dat overtolligheid beperkt effectief is wanneer het gaat om het verminderen van risico's (Leveson et al, 2009). De overtolligheid kan zowel vanuit een technisch als menselijk opzicht ontstaan en is bestempeld tot de minst effectieve en duurste benadering voor het ontwerpen van beveiligingssystemen.

Na een afweging tussen de verschillende invalshoeken zal dit onderzoek worden uitgevoerd aan de hand van het HRO-concept. De keuze voor dit perspectief is gemaakt omdat dit concept niet alleen ingaat op de technische middelen zelf, maar ook ruimte wordt gecreëerd voor lerend vermogen en bewustzijn. HRO gaat dus verder dan slechts inhoudelijke vormgeving, door ook te focussen op lessen voor de toekomst.

2.2 Theoretisch concept

In deze paragraaf wordt nader ingegaan op het theoretisch concept dat in dit onderzoek centraal staat, aan de hand van het bestuderen van het concept privacy, de theorie over High Reliability Organizations (HRO) van Weick, Sutcliffe & Obstfeld (2008) en het conceptueel kader waarbij het HRO concept wordt toespitst op privacy.

2.2.1 Privacy

Hoewel steeds meer wordt gesproken en gepubliceerd over het belang van privacy, lijkt het begrip moeilijk te duiden. Volgens Cuijpers (2007) wordt privacy als complex ervaren doordat privacy moeilijk alleenstaand kan worden beschouwd en afhankelijk is van de context waarbinnen het wordt geplaatst. In dit geval is privacy een overkoepelende term die kan worden opgedeeld in verschillende dimensies, waaronder relationele, lichamelijke, territoriale en communicatieve privacy. Doordat een verruiming van het begrip heeft plaatsgevonden, heerst er een tendens waarbij niet alleen de privésfeer moet worden beschermd maar ook de privacy in publieke ruimtes moet worden toegekend (Cuijpers, 2007).

Koops & Vedder (2001) hebben evenals Cuijpers (2007) erkend dat privacy een complex begrip is en dat contextuele factoren zoals technische, maatschappelijke en economische ontwikkelingen van invloed zijn. De auteurs onderscheiden drie manieren waarop betekenis wordt gegeven aan privacy: (1) ruimtelijke privacy, (2) intimiteit of individuele zelfbeschikking, en (3) informationele privacy. In dit onderzoek wordt geconcentreerd op de derde categorie. Informationele privacy gaat in op de bescherming van persoonsgegevens. Hierbij wordt het begrip privacy ingezet als een afweermiddel tegen ongewenste openbaarmaking van informatie over de individuele, persoonlijke levenssfeer waaronder medische informatie (Koops & Vedder, 2001). Door het vormgeven van wet- en regelgeving zoals, de AVG, wordt een gemeenschappelijk kernbegrip geformuleerd. Daarnaast kan het kernbegrip worden gespecificeerd per domein door rekening te houden met contextuele en functionele factoren. De AVG beschermt patiënten middels het invoeren van regels over onder andere toestemming en het inzicht door derden te beperken. Naast de waarde van vrijheid of zelfbeschikking is er bij privacy ook een controlerende functie over de verspreiding van persoonlijke informatie. Met deze controle zijn patiënten zelf in staat om relaties met anderen en instituties te bepalen en te onderhouden (Koops & Vedder, 2001).

In dit onderzoek wordt gefocust op de privacy van patiënten, die toestemming hebben gegeven voor inzage in hun medische gegevens via het LSP. De automatiseringsprocessen binnen het domein van de gezondheidszorg omvatten diverse ICT-toepassingen waarbij verbindingen tussen verschillende actoren worden gerealiseerd (Keizer, 2011). Dit betreffen zowel dokter-dokter (D2D), als dokter-patiënt (D2P) en patiënt-patiënt (P2P) verbindingen. Binnen het domein van de gezondheidszorg lijken patiënten en andere betrokkenen meer stil te staan bij het belang van privacy, wat kan worden verklaard door hun afhankelijke en kwetsbare positie (Keizer, 2011). Het ondergaan van medische behandelingen maakt zonder uitzondering inbreuk op de persoonlijke ruimte en tast lichamelijke privacy aan. Daarnaast kan niet worden gesproken van absolute privacy, aangezien communicatie tussen zorgverlener en zorgconsument noodzakelijk blijft. Bij medische informatie gaat het om informationele privacy waarbij aandacht wordt

besteed aan het beschermen van informatie en gegevens ten opzichte van onbevoegden. Echter bevinden zich hier mogelijke risico's, doordat de gedachtegang achter het LSP ingaat op het zo efficiënt en effectief mogelijk beschikbaar maken van medische gegevens. De uitdaging zit in het kunnen beheren en controleren van de informatiestromen.

Kort na de private doorstart van het VZVZ heeft een groep privacy experts van de Working Party on Information Security and Privacy (WPISP) een document gepubliceerd waarin de privacyrichtlijnen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) zijn herzien. Als redenen voor deze herziening worden de veranderende technologieën, markten en gebruikersgedrag en het groeiende belang van digitale identiteiten genoemd(OECD, 2013). De focus heeft hierbij gelegen op de impact van de richtlijnen, de rol van een individu en het economisch perspectief op persoonsgegevens en privacy. Door de veranderende context en omgeving waarin persoonsgegevens worden opgeslagen en gedeeld, ontstaat een groeiende behoefte aan verbetering van privacywetgeving. Hierbij moet meer rekening worden gehouden met onder andere de hoeveelheid persoonsgegevens die wordt verzameld, gebruikt en opgeslagen, de reeks analyses die inzicht geeft in individuele en groepstrends, bewegingen, interesses, en activiteiten, en de waarde van de maatschappelijke en economische voordelen van nieuwe technologieën en verantwoorde gegevenstoepassingen (OECD, 2013). Daarnaast wordt ook geconcentreerd op de omvang van bedreigingen, het aantal en de verscheidenheid aan actoren die privacy in gevaar kunnen brengen of kunnen beschermen, de frequentie en complexiteit van interacties met betrekking tot persoonsgegevens welke van individuen wordt verwacht dat ze begrijpelijk worden bevonden (OECD, 2013). Tot slot wordt ook gefocust op de wereldwijde beschikbaarheid van persoonsgegevens. Nieuwe communicatienetwerken en sociale platforms staan continue met elkaar in verbinding waardoor datastromen steeds sneller worden uitgewisseld. De voorgaande geïdentificeerde focuspunten kunnen tot op zekere hoogte worden teruggevonden in de AVG, die in werking is getreden op 25 mei 2018. Hierin staan regels opgesteld over de omgang met persoonsgegevens met betrekking tot onder andere de toestemming die moet worden verleend voordat gegevens worden uitgewisseld, de beperking om gebruik

te maken van profilering, de verplichte procedures omtrent het melden van beveiligingsincidenten en (mogelijke) datalekken, en de rechten van betrokkenen.

Samenvattend kunnen er vanuit privacywetgeving vijf thema's worden geïdentificeerd die van invloed zijn op het veilig functioneren van het LSP. Dit zijn (1) beleid, (2) authenticatie, (3) kennis, (4) governance, en (5) systeemveiligheid. Onder beleid vallen de procedures die zijn vastgelegd. Dit betreft zowel het beleid dat is opgetekend bij het vormgeven van het Landelijk Schakelpunt, alsmede procedures voor de omgang met onverwachte fouten. Daarnaast bevat het thema beleid ook de verplichte toestemming die patiënten moeten geven voordat medische gegevens inzichtelijk mogen worden gemaakt. Het thema authenticatie gaat in op welke instellingen zijn aangesloten bij het LSP en de wijze waarop ze zijn toegelaten. Dit betreffen onder andere de apotheken en ziekenhuizen. Daarnaast gaat het bij dit thema ook om het instellen van rollenscheidingen en beslissingsbevoegdheden van medewerkers. Bij het thema kennis gaat het om de inhoudelijke kennis die van medewerkers wordt verwacht wanneer zij met het LSP werken. Dit kan op peil worden gehouden door het organiseren van trainingen om het bewustzijn van het systeem en de gevoelige data te vergroten. Het thema governance gaat in op toezicht en controle. Dit betreft onder andere het toezicht en de documentatie van beveiligingsincidenten en de meldplicht voor datalekken. Vanuit de AVG is het verplicht om betrokkenen op de hoogte te stellen wanneer een organisatie de controle op persoonsgegevens (tijdelijk) heeft verloren. De vormgeving van toezicht en controle is mogelijk op intern organisatieniveau, evenals op extern hoger niveau zoals de Autoriteit Persoonsgegevens. Het vijfde thema betreft systeemveiligheid. Het waarborgen van privacy binnen een systeem staat in relatie met de veiligheid van dat systeem. Dit thema kan worden opgevat vanuit een cyber security perspectief, waarbij de gevoeligheid van mogelijke inbreuk op het systeem zo laag mogelijk moet zijn om risico's te beperken. Om te analyseren hoe de informatiestromen van het LSP worden beheerd en gecontroleerd, zal het High Reliability Organization (HRO) concept van Weick, Sutcliffe en Obstfeld (2008) worden gebruikt. Dit concept wordt in de volgende paragraaf uiteengezet.

2.2.2 High Reliability Organization (HRO)

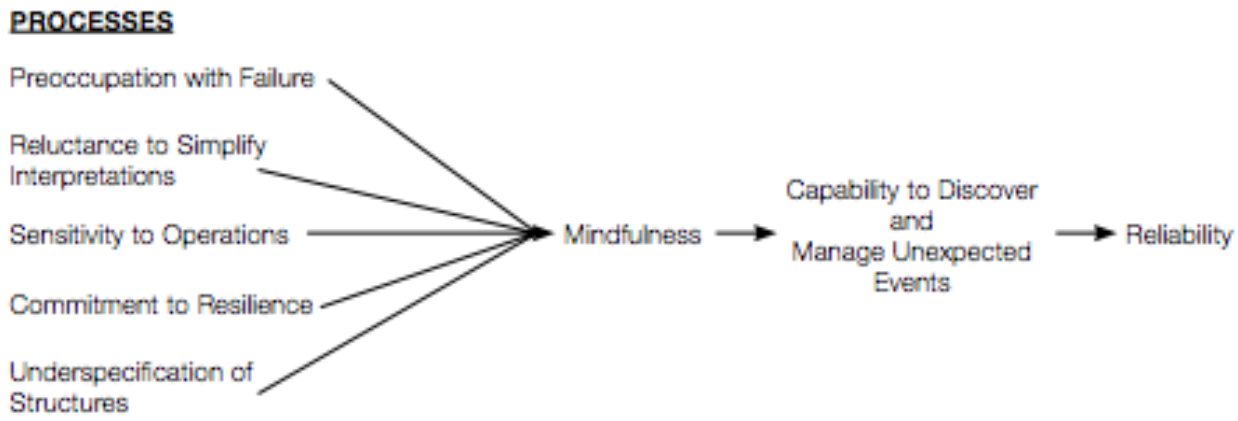
Weick, Sutcliffe & Obstfeld (2008) stellen dat HRO's belangrijk zijn omdat ze een perspectief bieden op een onderscheidende reeks processen die onder moeilijke omstandigheden de effectiviteit bevorderen. Waar bij eerdere organisatietheorieën voornamelijk wordt gefocust op succes en efficiëntie, wordt nu prioriteit gegeven aan mislukking en betrouwbaarheid om op die manier tot procesverbetering te komen. Op deze manier bieden de processen van HRO's een cognitieve infrastructuur dat lerend vermogen en betrouwbare prestaties mogelijk maakt (Weick, Sutcliffe & Obstfeld, 2008). Hierdoor wordt niet alleen gefocust op het preventief voorkomen of adequaat reageren wanneer een situatie zich voordoet, maar wordt meer aandacht besteed aan het anticiperen en creëren van bewustzijn zodat beter kan worden voorbereid op toekomstige situaties.

Het concept van High Reliability Organizations wordt gedefinieerd als organisaties die zich in een meedogenloze sociale en politieke omgeving bevinden, waarin de kans op fouten groot is, waarin het leren van experimenten wordt uitgesloten doordat de omvang van de mogelijke consequenties groot is en waarin mislukkingen worden vermeden om kwetsbaarheid te beperken. Daarnaast worden complexe processen gebruikt om complexe technologie te beheren (Weick, Sutcliffe & Obstfeld, 2008). De bestaande literatuur over HRO's die zich bevinden onder moeilijke omstandigheden betreffen voornamelijk case studies met effectieve actie, beperkte storing, in de buurt van calamiteiten, catastrofale mislukkingen en successen die mislukkingen hadden moeten zijn. Hierbij wordt vooral nadruk gelegd op de structuur en technologie in plaats van op het proces. Analyses van deze cases gaan vaak over activiteiten met anticipatie en vermijding in plaats van activiteiten met veerkracht en insluiting. Ook is er meer aandacht voor macroanalyses op interorganisatorisch niveau dan op microniveau en meer zorg met dodelijke slachtoffers dan met blijvende schade op andere gebieden zoals reputatie, legitimiteit en overleving binnen de sociale sfeer (Weick, Sutcliffe & Obstfeld, 2008).

Sutcliffe (2012) benadrukt dat er twijfel bestaat over de relevantie van HRO's voor andere bedrijven en sectoren, omdat wordt aangenomen dat het concept alleen opgaat voor hoge risico- en zware consequentie sectoren. De auteur noemt deze visie kortzichtig om drie redenen. Ten eerste zijn ook 'gewone' organisaties in

staat om schade aan te richten. Het voorbeeld dat hierbij wordt benoemd, betreft de financiële crisis in de Verenigde Staten. Tijdens de crisis hebben veel inwoners die bijna de pensioengerechtigde leeftijd hadden bereikt, hun spaargeld verloren en hebben veel bedrijven noodzakelijk moeten overgaan tot gedwongen ontslagen met reputatieschade tot gevolg. Ten tweede vormt schaalgrootte een complex concept. In organisaties wordt verwacht dat medewerkers de werkzaamheden naar behoren en op een betrouwbare manier zullen verrichten ook als er een onverwachte gebeurtenis plaatsvindt. Volgens Sutcliffe (2012) hangt het onverwachte af van de context. Wanneer de context wordt begrepen – alsmede de voorzorgsmaatregelen, de vooronderstellingen, de focus van de aandacht en hetgeen is genegeerd – dan volgt de conclusie dat ook organisaties te maken hebben met dreigingen. Ten derde is leren gewenst maar is het lastig te bepalen wat de beste kennisbron hiervoor is. Organisaties die lerend willen zijn, wordt aangeraden niet strak te definiëren hoe en waar het leren zal gebeuren (Sutcliffe, 2012).

Om tot procesverbetering te kunnen komen, eisen HRO's perfectie, maar tegelijkertijd is bekend dat dit niet zal worden behaald. Het proces betreft aanpassing, om continu de betrouwbaarheid te verbeteren en in te grijpen. Dit omvat zowel het voorkomen van fouten, het reageren op fouten en het herstellen van fouten die daadwerkelijk hebben plaatsgevonden (Sutcliffe, 2012). Procesverbetering ontstaat door het creëren van bewustwording (mindfulness) en kan worden onderscheiden in vijf principes. Drie hiervan hangen samen met preventie, namelijk (1) preoccupatie met falen (preoccupation with failure), (2) terughoudendheid om interpretaties te vereenvoudigen (reluctance to simplify interpretations), en (3) gevoeligheid voor activiteiten (sensitivity to operations). De overige twee hangen samen met reactievermogen, namelijk (4) inzet voor veerkracht (commitment to resilience), en (5) onderspecificatie van structuren (underspecification of structures). In figuur 1 is dit proces schematisch weergeven.



Figuur 1: Procesverbetering HRO's door Weick, Sutcliffe & Obstfeld (2008).

2.2.2.1 Preoccupation with failure

Een blijvende zorg over HRO's is dat een analytische fout is ingebed in lopende activiteiten en dat onverwachte mislukkingen en beperkingen van vooruitziendheid die analytische fouten kunnen versterken (Weick, Sutcliffe & Obstfeld, 2008). Dit betekent dat technologie nog steeds voor verrassingen kan zorgen, wat resulteert in terughoudendheid onder het hogere management om besluitvormings- of actiekaders te implementeren die niet gevoelig zijn voor de mogelijkheden van analytische fouten. De zorgen over falen zijn een onderdeel van de onderscheidende kwaliteit van HRO's. Het onderscheidend vermogen vloeit simpelweg voort uit het feit dat fouten zelden voorkomen. Dit betekent dat HRO's zich altijd bezighouden met iets dat ze nagenoeg niet zien.

Wanneer falen wordt beschouwd als een belangrijke voorwaarde voor lerend vermogen, dan zullen veilige HRO's het moeilijk vinden om te leren, doordat er weinig data over falen is. Preoccupation with failure bestaat daarom uit het genoegen nemen met minder dan ideale leeromstandigheden, en deze proberen om te zetten in redenen voor verbetering. Weick, Sutcliffe & Obstfeld (2008) onderscheiden drie manieren om dit te realiseren: door alle fouten te behandelen op systeemniveau, door een grondige analyse van 'bijna mislukkingen' en door te focussen op de verplichtingen van succes. Effectieve HRO's stimuleren het melden van fouten en proberen hier het meeste uit te halen. Een bijkomend gevolg van de verhoogde aandacht voor alle mislukkingen is dat onderhoudsafdelingen in HRO's

centrale locaties worden voor organisatorisch leren, in tegenstelling tot hun inconsequente rol in traditionele organisaties.

Wanneer een organisatie slaagt, schrijven de managers het succes meestal toe aan zichzelf of hun organisatie in plaats van aan geluk. De medewerkers krijgen meer vertrouwen in hun eigen vaardigheden, in de vaardigheden van hun manager en in de bestaande programma's en procedures van hun organisatie. Het vertrouwen in de procedures omvat mogelijkheden voor ontwikkeling. Wanneer wordt aangenomen dat succes voortkomt uit competenties, kunnen medewerkers onoplettend worden en in routines vervallen. Echter vergroot dit patroon de kans op menselijke fouten. In effectieve HRO's wordt zelfgenoegzaamheid geïnterpreteerd als een mislukking van streven, onoplettendheid als gebrek aan waakzaamheid en gewenning als mislukking van voortdurende aanpassing (Weick, Sutcliffe & Obstfeld, 2008). Op deze manier kan huidig succes leiden tot minder succes in de toekomst.

2.2.2.2 Reluctance to simplify interpretations

Medewerkers van organisaties hanteren complexe taken door het vereenvoudigen van de manier waarop een huidige situatie wordt geïnterpreteerd. Deze vereenvoudigingen, welke ook wel worldviews, frameworks, of mindsets worden genoemd, staan medewerkers in principe toe om data te negeren en verder te gaan. De vereenvoudigingen kunnen potentieel gevaarlijk zijn voor HRO's omdat ze zowel de voorzorgsmaatregelen die medewerkers nemen beperken, evenals het aantal ongewenste gevolgen dat ze voorzien (Weick, Sutcliffe & Obstfeld, 2008). De kans op eventuele onvoorziene verrassingen neemt toe doordat anomalieën kunnen accumuleren, intuïties worden genegeerd en ongewenste gevolgen serieuzer worden.

Het probleem van vereenvoudigen is het bepalen of de vereenvoudigde diagnose van de huidige en mogelijk toekomstige situatie nauwkeurig genoeg is om de organisatiedoelstellingen te bereiken zonder onverwachte problemen te ondervinden die mogelijk tot een catastrofe kunnen leiden. De moeilijkheidsgraad ligt hierdoor vooral in het ontdekken welke aspecten wel en niet kunnen worden genegeerd, waar aandacht aan moet worden besteedt en hoe een aanvaardbaar veiligheidsniveau kan worden vastgesteld. Dit zijn dan ook redenen waarom een

minimale mate van overeenstemming en coördinatie is vereist. Door overeenstemming zullen besluitvormers allemaal dezelfde soort aandacht besteden aan beslissingen.

Om de verleiding tot het vereenvoudigen van interpretaties te beperken, wordt er bij HRO's vanuit gegaan dat een complexe omgeving alleen kan worden begrepen met een complex systeem. Binnen het systeem kunnen verschillende checks and balances worden ingericht zoals commissies en vergaderingen, frequente beoordelingen, het selecteren van nieuwe medewerkers die geen logische eerdere ervaring hebben, frequente rotatie van specifieke werkzaamheden en herscholing (Weick, Sutcliffe & Obstfeld, 2008). Om hier bewust mee om te gaan wordt vaak een vorm van overtolligheid ingezet zoals een duplicatie of een back-up. Maar met overtolligheid gaat ook scepsis gepaard. Overtolligheid gaat namelijk uit van kruiscontroles, twijfels over of voorzorgsmaatregelen genoeg zijn en heeft zorgen over competentieniveaus. Wanneer mensen zien wat ze geloven, dan zullen ze dingen over het hoofd zien. Scepsis kan dus gelijktijdig ook het vertrouwen verhogen, onderkennen dat mensen feilbaar zijn en de betrouwbaarheid verbeteren.

2.2.2.3 Sensitivity to operations

Gevoeligheid voor activiteiten staat in relatie tot het situationele bewustzijn, dat wordt gedefinieerd als 'de perceptie van de elementen in de omgeving binnen een volume van tijd en ruimte' (Endsley, 1997). Het is van belang om inzicht te hebben in het geïntegreerde geheel van bewerkingen dat op het huidige moment plaatsvindt. Al vormt dit inzicht tegelijkertijd een prestatie die moeilijk te handhaven is. Waar situationele bewustzijn generiek verwijst naar het geheel dat elke activiteit vormt, verwijst het thema gevoeligheid voor activiteiten naar een moeiteloze verwezenlijking van een hoog niveau van het situationele bewustzijn (Weick, Sutcliffe & Obstfeld, 2008). Het belang van gevoeligheid voor de huidige activiteiten wordt weerspiegeld in veel van de terminologie in de literatuur over HRO's. Beschrijvende woorden zoals alertheid, misinterpretatie, overbelasting, afleiding, gemengde signalen, verrassingen, waakzaamheid, afwijkingen, waarschuwingen, aanwijzingen en verwaarlozing wijzen allemaal op de drang om fouten direct te ontdekken op het moment dat ze voorkomen.

Een belemmering voor het behouden van een breed operationeel bewustzijn is het gevaar van productiedruk en overbelasting. Effectieve HRO's zijn over het algemeen meer zelfbewust in het omgaan met druk en overbelasting en hebben meer oog voor de gevoeligheid van medewerkers (Weick, Sutcliffe & Obstfeld, 2008). Door bijvoorbeeld inkrimping en gedwongen ontslagen stijgen de productiedruk en overbelasting, hetgeen doorwerkt in de beoordeling van prestaties. Wanneer een organisatie zich bewust is van de situatie, welke zowel de elementen uit de huidige situatie en de projectie naar een toekomstige situatie omvat, dan is een betere voorbereiding mogelijk. Doordat HRO's vaak te maken hebben met complexe technologieën, is het situationele bewustzijn afhankelijk van het delen van informatie en interpretaties tussen verschillende individuen.

Gevoeligheid voor activiteiten wordt bereikt door een combinatie van gedeelde mentale representaties, collectieve verhaalopbouw, situatiebeoordelingen met voortdurende updates, kennis van fysieke onderlinge verbindingen en parameters van systemen en actieve diagnoses van de beperkingen van vooraf geplande procedures (Weick, Sutcliffe & Obstfeld, 2008). Het zijn de cognitieve activiteiten op hoger niveau, de sociale structuur van samenhangende verklaringen en de kennis van het fysieke systeem welke bijdragen aan het creëren van mindfulness. Het situationele bewustzijn voorkomt dat systemen statisch worden ervaren en niet dynamisch genoeg zijn om continu aan te passen aan de omgeving, terwijl herformuleren en monitoren belangrijk zijn in het proces van een HRO.

2.2.2.4 Commitment to resilience

Uit de voorgaande drie thema's is gebleken dat variatie in plaats van onveranderlijkheid bevorderend is voor de betrouwbaarheid van activiteiten en beter voorbereidt op het onverwachte. Daarnaast is 'management' eveneens belangrijk, omdat management meer inzicht geeft in de omgang van medewerkers met verrassingen. Deze omgang wordt gekenmerkt door anticipatie, welke vaak van tevoren is bepaald, maar ook door veerkracht, welke op het moment van plaatsvinden ontstaat. Om onverwachte gebeurtenissen te kunnen beheren, moeten deze worden beheerd in plaats van geëlimineerd (Weick, Sutcliffe & Obstfeld, 2008).

Er kan gelijktijdig sprake zijn van zowel veerkrachtige insluiting als reactieve terugkoppeling. Geloofwaardigheid, vertrouwen en aandacht liggen hieraan ten grondslag.

Anticipatie verwijst naar ‘de voorspelling en preventie van mogelijke gevaren voordat schade wordt aangericht', terwijl veerkracht verwijst naar ‘het vermogen om met onverwachte gevaren om te gaan nadat ze zich hebben gemanifesteerd, zodat organisaties leren terugveren' (Weick, Sutcliffe & Obstfeld, 2008). In tegenstelling tot effectieve HRO's hebben traditionele organisaties de neiging om de kant van anticipatie te kiezen waarbij ze concentreren op verwachte situaties, risicoaversie en te voorziene risico's. Inzet voor veerkracht omvat meer dan het vermogen om verandering te absorberen. De meest effectieve HRO’s wachten niet op een fout voordat wordt gereageerd en gebruiken de verandering om weerbaarder te worden. De voorbereiding op onvermijdelijke veranderingen kenmerkt zich door uitbreiding van algemene kennis, technische faciliteiten en hulpbronnen.

Daarnaast is de inzet voor veerkracht bij HRO’s ook zichtbaar in de formele steun voor improvisatie. In de eerste plaats lijkt improvisatie samen te gaan met het potentieel voor een catastrofe. Maar organisaties die in staat zijn om op gevaren te reageren, zijn ook in staat om risico’s te kunnen inschatten en erover na te denken zodat ze meer inzichten verwerven. De toevoeging van specifieke acties stelt medewerkers in staat om bewust te worden van nieuwe situaties. Daarnaast zijn effectieve HRO’s ook in staat om acties die voorheen zijn voorgekomen, te koppelen zodat nieuwe combinaties ontstaan. Het proces van recombineren vergroot het repertoire even veel als de toevoeging van specifieke acties (Weick, Sutcliffe & Obstfeld, 2008). Een uitgebreid bereik van acties gaat gepaard met een uitgebreid bereik van percepties over nieuwe risico’s. Tenslotte is er ook een rol voor ambivalentie ten opzichte van de toepasbaarheid van de historische praktijk. HRO’s zijn gelijktijdig in staat om, in tegenstelling tot de meeste organisaties, zowel hun eerdere ervaringen te geloven als te betwijfelen.

2.2.2.5 Underspecification of structures

Het organiseren van hoge betrouwbaarheid kan paradoxaal worden opgevat. De goedkeuring van ordelijke procedures zodat fouten kunnen worden verminderd, verspreiden vaak juist fouten. Effectieve HRO's zijn soms vrij van fouten ongeacht hun ordelijkheid en niet vanwege deze ordelijkheid. Elke hiërarchie kan fouten vergroten, voornamelijk wanneer de misstanden zich aan de bovenkant voordoen (Weick, Sutcliffe & Obstfeld, 2008). Fouten op een hoger niveau hebben de neiging te vermengen met fouten van een lager niveau, waardoor de resulterende combinatie moeilijker wordt te behandelen. Dit werkt door in de mate van betrouwbaarheid die wordt bevorderd door de HRO's. Hierdoor kunnen kleine fouten zich verspreiden, zich opstapelen, op elkaar inwerken en leiden tot ernstige gevolgen.

HRO's richten flexibiliteit in door het organiseren van anarchie. Een manier om dit te doen is uiteengezet door Cohen, March, & Olsen (1972). Zij spreken van een vuilnisbakstructuur. In een vuilnisbak zijn er onafhankelijke stromen van problemen, oplossingen, beslissers en keuzemogelijkheden die door een systeem bewegen. Deze stromen worden verbonden door hun aankomst- en vertrektijden en door eventuele structurele beperkingen die van invloed zijn op welke problemen, oplossingen en besluitvormers toegang hebben tot welke mogelijkheden. In een absolute vuilnisbak zijn geen structurele beperkingen. Hierdoor worden oplossingen gekoppeld aan problemen en worden beslissers verbonden met keuzes, voornamelijk door hun gezamenlijke aanwezigheid op hetzelfde moment. Binnen een systeem waarin sterk de focus ligt op de gevolgen, zal het volgende plaatsvinden: "Wil iets ertoe leiden dat iets wordt gedaan, dan is dat verbonden met de behoefte en iets doen leidt tot consequenties die verband houden met de intentie" (March & Olsen, 1986). In vuilnisbakken heeft co-existentie de neiging om tot probleemoplossende processen te komen in tegenstelling tot rationele intenties of hiërarchische posities.

Effectieve HRO's bereiken zowel flexibiliteit als ordelijkheid door het uitvoeren van gedeeltelijke vuilnisbakken. Dit kan door de toegang te openen naar wat voorheen een hiërarchische autoriteit of beslissingsautoriteit was. Door het flexibiliseren van de aangewezen beslissingsbevoegde, wordt meer ruimte geboden

voor het afstemmen van de besluitvorming op de specifieke problemen. Wanneer problemen en beslissingsrechten niet vaststaan, vergroot dit de kans dat nieuwe mogelijkheden worden gekoppeld aan nieuwe problemen. Hierdoor kan expertise van de onderste laag van de hiërarchie gemakkelijker aan de bovenkant worden ingezet.

Wanneer de effectieve HRO's focussen op falen, wordt elk signaal behandeld alsof het nieuw is. Dit genereert de aandacht die nodig is om expertise te koppelen aan problemen, oplossingen en beslissingen van het moment. Doordat effectieve HRO's zich bewust zijn van het falen, worden ook de gevolgen bewust gevolgd. Mindfulness is dan afgestemd op zowel de timing als de consequenties. Dit betekent dat een opmerkzaam systeem de typische tekortkomingen in de besluitvorming van vuilnisbakken tegen beslissingen gebaseerd op flight en oversight tegengaat. Bij oversight worden snelle beslissingen gemaakt en de flight strategie gaat uit van het steeds overspringen naar nieuwe keuzes (March & Olsen, 1986). Het loslaten van procedures zorgt voor meer aandacht voor inspanning, medewerkers worden gevoeliger voor het leveren van een bijdrage en processen worden meer beïnvloed door tijdelijke verbindingen, welke zullen worden ingericht naar het principe van een anarchie (Weick, Sutcliffe & Obstfeld, 2008).

2.2.2.6 Deelconclusie

Om uiteindelijk tot mindfulness te komen hebben Weick, Sutcliffe & Obstfeld (2008) vijf thema's onderscheiden. Bij 'preoccupation with failure' heerst de gedachte dat geleerd kan worden van falen. Hierbij is het belangrijk om het falen niet te ontlopen, maar er juist naar op zoek te gaan en vroege tekenen van mislukking te ontdekken. Met 'reluctance to simplify interpretations' wordt geconcentreerd op de verleiding tot het vereenvoudigen van interpretaties. Labels en clichés kunnen medewerkers beperken in het gedetailleerd bestuderen van situaties. Bij 'sensitivity to operations' is het van belang om cognitieve activiteiten op hoger niveau, de sociale structuur van samenhangende verklaringen en kennis van het fysieke systeem te hebben. Hierbij zijn volume van tijd en ruimte belangrijke factoren. Met 'commitment to resilience' wordt geconcentreerd op anticipatie en veerkracht. Hoewel er risicovolle situaties en mislukkingen zullen plaatsvinden, is het

belangrijk om spanning te absorberen en te leren van voorgaande gebeurtenissen. Als laatste gaat 'underspecification of structures' in op de rol van ordelijke procedures, waarbij HRO's vaak flexibiliteit inrichten door het organiseren van anarchie. Samenvattend zijn naast percepties ook integratie en extrapolatie van belang. Volgens Weick, Sutcliffe & Obstfeld (2008) zijn dit alle drie producten welke door alle vijf thema's worden gecreëerd. Het gaat om collectieve kennis van mislukkingen, details, mogelijkheden tot herstel en relevante ervaringen uit het verleden. Gezamenlijk vormen ze een bewust proces, waarmee een context wordt geboden waarin de huidige activiteiten zinvol zijn of worden gereconstrueerd om zinvol te kunnen zijn. In paragraaf 3.3 zal door middel van een operationalisering worden bepaald hoe de thema's meetbaar zullen worden gemaakt.

2.2.3 Conceptueel kader

In de voorgaande paragrafen zijn het begrip privacy en het HRO perspectief toegelicht. Uit deze uiteenzetting is gebleken dat het concept privacy kan worden beschouwd aan de hand van de volgende vijf thema's: (1) beleid, (2) authenticatie, (3) kennis, (4) governance, en (5) systeemveiligheid. Het HRO-perspectief bestaat idem uit vijf thema's: (1) preoccupation with failure, (2) reluctance to simplify interpretations, (3) sensitivity to operations, (4) commitment to resilience, en (5) underspecification of structures. In dit onderzoek wordt een koppeling tussen beide concepten gemaakt om daarmee te bezien in hoeverre HRO een bijdrage kan leveren aan de borging van privacy.

Preoccupation with failure bestaat uit het genoegen nemen met minder dan ideale leeromstandigheden en deze proberen om te zetten in redenen voor verbetering (Weick, Sutcliffe & Obstfeld, 2008). Door alle fouten te behandelen op systeemniveau, een grondige analyse van gebeurtenissen die kunnen worden aangeduid als bijna mislukkingen en het focussen op de vereisten van successen kunnen lessen voor toekomstige situaties worden gecreëerd. Vanuit een privacy perspectief zullen zowel interne en externe onderhoudsafdelingen worden ingericht. Deze onderhoudsafdelingen treden op als de centrale locatie voor meldingen en zijn eindverantwoordelijk voor een goede structuur en richtlijnen. Intern is gefocust op

organisatorisch leren. Bij extern kan worden gedacht aan de Autoriteit Persoonsgegevens (AP) of het Centraal Meldpunt Identiteitsfraude en –fouten (CMI). Dit thema betreft ook de manier van documenteren van successen en mislukkingen en aan wie deze gebeurtenissen worden toegeschreven. Vanuit een privacy optiek zal worden gekeken naar de aanwezigheid van rollenscheiding, waarbij diverse taken en verantwoordelijkheden zijn gespecificeerd. Dit is gerelateerd aan het vertrouwen in eigen vaardigheden en vaardigheden van leidinggevenden. Een basis kennisniveau van medewerkers zal aanwezig moeten zijn omdat de omgang met het systeem niet alleen technische functies kent maar ook menselijke handelingen. Dit kennisniveau zal vervolgens moeten worden aangevuld met het leren van gebeurtenissen die worden aangemerkt als fouten om beter voorbereid te zijn op toekomstige situaties. Deze bevindingen kunnen worden gekoppeld aan het geïdentificeerde privacy thema *authenticatie*, omdat wordt gefocust op rollenscheiding met verschillende beslissingsbevoegdheden. Daarnaast komt ook het belang van *kennis* naar voren doordat er wordt verwacht dat er (basis) vaardigheden aanwezig zijn. Verder kan ook het thema *governance* worden herleid door de vormgeving van verschillende onderhouds- en controleafdelingen op intern en extern niveau. Tot slot komt ook het thema *systeemveiligheid* naar voren door de focus op het mogelijk falen op systeemniveau.

Reluctance to simplify interpretations voorziet het potentieel voor problemen wanneer medewerkers eenvoudig over situaties denken. Hierdoor worden maatregelen en risico's onderschat. Vanuit het privacy perspectief is een duidelijke richtlijn of protocol gewenst, zodat de moeilijkheidsgraad in het bepalen wat wel en niet kan wordt gestructureerd. Hierdoor wordt meer nadruk gelegd op overeenstemming en coördinatie. Een andere manier waardoor misinterpretaties kunnen worden voorkomen, is het instellen van checks and balances. Door middel van het reviewen van elkaar, vergaderen en regelmatige beoordelingen kan worden nagegaan hoe medewerkers scherp worden gehouden en kan worden bepaald of nadere scholing nodig is om het kennisniveau op peil te houden. Deze bevindingen kunnen worden gekoppeld aan het geïdentificeerde privacy thema *beleid*, doordat een duidelijke structuur, protocollen en procedures zijn gewenst. Daarnaast komt ook het thema *kennis* naar voren. Overeenstemming en coördinatie kunnen worden

vergroot door te focussen op awareness van medewerkers, alsmede het bevorderen van de samenwerking. Tot slot kan ook het thema *governance* worden herkend aan de hand van het instellen van checks and balances. Toezicht en controle worden vergroot door het periodiek reviewen van werk en regelmatige beoordelingen.

Sensitivity to operations focust op de cognitieve activiteiten op hoger niveau, de sociale structuur van samenhangende verklaringen en de kennis van het fysieke systeem. Hierbij is van belang om de processen in de juiste context te plaatsen om druk en overbelasting te minimaliseren. Er is een afhankelijkheid tussen gedeelde informatie en interpretaties van verschillende individuen. Vanuit een privacy perspectief zal worden beweerd dat medewerkers beter in staat zullen zijn om naar behoren te handelen in complexe situaties wanneer zij zich ervan bewust zijn dat zij zich in deze complexe situatie bevinden. Dit thema heeft oorspronkelijk een preventief karakter. Maar wanneer zich een onverwachte complexe situatie voordoet, wordt er vaak zo snel mogelijk gehandeld. Vanuit privacy is het van belang dat medewerkers hierop worden getraind, zodat zij zich bewust zijn van de systemen waarmee ze werken en dezelfde beoordelingen worden gegeven in gelijke situaties. Systemen zijn niet altijd voorspelbaar maar juist dynamisch, waardoor het trainen op verschillende situaties noodzakelijk is. Deze bevindingen kunnen worden gekoppeld aan het geïdentificeerde privacy thema *beleid*. Bij het optreden van een onverwachte situatie zal in eerste instantie een procedure worden gevolgd om zo snel mogelijk op de gebeurtenis in te spelen. Daarnaast is gebleken dat het bewustzijn van de complexe situatie het naar behoren handelen vergroot. Verder kan ook het thema *kennis* worden geïdentificeerd. Dit gaat zowel in op de kennis van het fysieke systeem als de awareness van medewerkers over de context en gevoeligheid van de persoonsgegevens waarmee wordt gewerkt in het LSP.

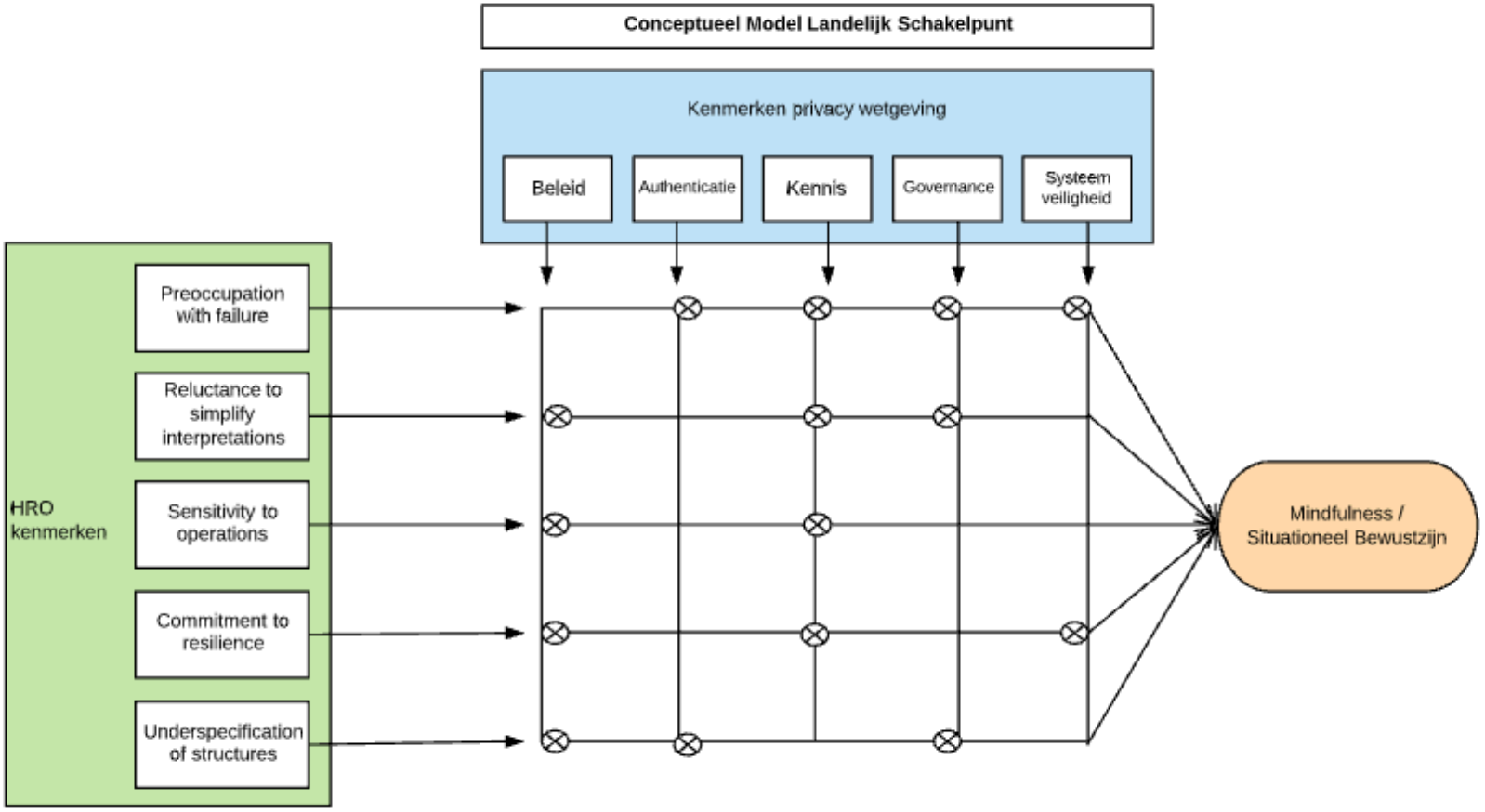
Commitment to resilience gaat in op het vermogen om met onverwachte gebeurtenissen te kunnen omgaan en heeft een reactief karakter. De bewustwording van situaties die hebben plaatsgevonden, vergroot het inschatten van mogelijke nieuwe scenario's waar vervolgens ook van kan worden geleerd. Vanuit het privacy perspectief is het van belang om te bepalen of medewerkers zich bewust zijn van de service die zij bieden, de strategie die wordt gevolgd en hoe het inschatten van nieuwe situaties plaatsvindt. Ook is het van belang hoe het systeem

kan worden hersteld nadat fouten zijn opgetreden, wat in relatie staat met het herstellen van de privacy van personen en persoonsgegevens. Een organisatie zal de complexe gebeurtenis moeten oplossen, ervan moeten leren en daarnaast moeten groeien voor toekomstige gebeurtenissen. Daarbij is het belangrijk dat discreet met de data wordt omgegaan. Deze bevindingen kunnen worden gekoppeld aan het geïdentificeerde privacy thema *beleid* omdat medewerkers op de hoogte dienen te zijn van de strategie van een organisatie en het systeem. Belangrijke principes, zoals de rechten van betrokkenen en bijvoorbeeld het verbod op profilering, zijn aspecten die hierbij naar voren komen. Daarnaast is *kennis* ook hier van belang. Enerzijds zal een basisniveau van kennis aanwezig moeten zijn, anderzijds is kennis nodig om nieuwe situaties te kunnen inschatten en te leren van gebeurtenissen. Verder speelt systeemveiligheid een grote rol vanuit de back-up en herstelmogelijkheden. Wanneer (onverwacht) inbreuk wordt gemaakt op het systeem en de opgeslagen persoonsgegevens die het LSP bezit, is het van belang dat er een manier is om de controle op het systeem terug te krijgen, de veiligheid te waarborgen en de risico's te beperken.

Underspecification of structures gaat in op de rol van de ordelijke procedures die van kracht zijn. Procedures moeten kritisch worden bekeken omdat er structurele fouten in de vooraf beschreven en vaststaande procedure kunnen zitten. Hierdoor zal de fout blijven optreden. Deze fout kan zich vervolgens verspreiden, opstapelen of op andere fouten inwerken. Dit proces kan worden voorkomen door het inrichten van anarchie waardoor er naar balans wordt gezocht tussen vaststaande procedures en flexibiliteit. Vanuit een privacy aspect zal meer waarde worden gehecht aan vastgestelde procedures zodat medewerkers een houvast hebben in de omgang met privacygevoelige data. Hierbij is hiërarchie gewenst en zullen beslissingsbevoegden worden aangesteld. Dit betekent niet dat feedback en suggesties worden afgewezen; deskundigheid staat altijd voorop. Deze bevindingen kunnen worden gekoppeld aan het geïdentificeerde privacy thema *beleid*. De ordelijke procedures hebben een prominente plek binnen het concept privacy doordat deze documenten de medewerkers begeleiden in de omgang met gevoelige persoonsgegevens. Ook het thema *authenticatie* kan worden herleid aan de hand van het onderscheid in rollen en bijbehorende beslissingsbevoegdheden. Tot slot kan

het thema *governance* worden geïdentificeerd, waarbij het herzien van reeds opgestelde procedures aan bod komt. Dit verscherpt de kritische blik op mogelijke fouten in bestaande procedures.

De vijf thema's vanuit zowel het concept privacy als het HRO-perspectief vullen elkaar aan in het proces om meer (situationele) bewustzijn te creëren. De focus ligt hierbij vanuit HRO op de collectieve kennis van mislukkingen, inhoudelijke details, mogelijkheden om te herstellen nadat negatieve gebeurtenissen hebben plaatsgevonden en het kunnen gebruiken van relevante ervaringen uit het verleden. Door het realiseren van mindfulness wordt een bewust proces gevormd, waarmee de context inzichtelijker wordt gemaakt zodat huidige en toekomstige situaties kunnen worden ingeschat. Het inrichten van het LSP heeft veel tijd in beslag genomen en zou moeten hebben geleerd van de fouten waarop eerder het EPD is afgekeurd. Vanuit de privacy thema's houdt dit in dat de vormgeving en het proces van het LSP zijn ingericht met aandacht voor beleid, authenticatie, kennis, governance en systeemveiligheid. Dit kan schematisch worden weergeven als volgt in figuur 2.



Figuur 2: Conceptueel kader

3. Methodologie

In het vorige hoofdstuk is het privacy concept gekoppeld aan het theoretisch concept over High Reliability Organizations van Weick, Sutcliffe & Obstfeld (2008). Dit hoofdstuk beschrijft de methoden die worden gebruikt in aanloop naar het formuleren van een antwoord op de exploratieve onderzoeksvraag. Dit gebeurt door het bespreken van het research design, de manier van gegevensverzameling en de wijze van analyseren. Daarnaast worden ook de betrouwbaarheid, validiteit en beperkingen van dit onderzoek besproken.

3.1 Research design

Het doel van dit onderzoek is te beoordelen in hoeverre de bedrijfsvoering van het Landelijk Schakelpunt (LSP) ten aanzien van privacy kan worden versterkt. In het theoretisch kader is besproken dat dit vraagstuk wordt behandeld vanuit het perspectief over High Reliability Organizations door Weick & Sutcliffe (2008). Dit perspectief wordt gekoppeld aan thema's vanuit privacywetgeving. Om dit inzichtelijk te maken wordt een holistische case study uitgewerkt.

Zoals eerder beschreven, betreft een digitaal systeem met vertrouwelijke informatie zoals persoonsgegevens een complex proces waaraan veel risico's kleven. Het LSP is slechts een onderdeel van het totale aanbod aan digitale diensten waarbij persoonsgegevens van toepassing zijn. Een specifiek onderdeel in detail bestuderen helpt om meer inzicht te krijgen in het geheel. De aanpak van een case study is bijzonder geschikt voor dit soort onderzoek omdat het zich op één enkele eenheid kan richten (Gerring, 2004). Bovendien laat een case study toe om een relatief klein aantal gevallen te onderzoeken, informatie over verschillende kenmerken te verzamelen, analyses uit te voeren in een 'natuurlijke' omgeving en betreft het niet noodzakelijkerwijs een vergelijkende analyse met andere gevallen (Gomm, Hammersley & Foster, 2009).

Bij dit onderzoek is de aanpak van een case study de meest geschikte methode doordat deze is gericht op een diepgaand begrip van een specifiek onderwerp. Case study maakt een grondige analyse van de probleemstelling mogelijk en geeft ruimte om op verschillende perspectieven te concentreren. Deze functies verbeteren de kwaliteit van het gedetailleerd bestuderen. De casus over het

LSP betreft één specifiek geval en wordt geanalyseerd in een niet-experimentele omgeving. Dit betekent dat de omstandigheden en variabelen niet vooraf volledig worden gecontroleerd. Hierdoor kan een probleem worden geanalyseerd zonder dat deze wordt beïnvloed of gemanipuleerd (Gomm, Hammersley & Foster, 2009).

Het LSP kan worden beschouwd als een vernieuwend systeem met een focus op efficiëntie. De bereikbaarheid wordt verhoogd, doordat de gegevens van een patiënt kunnen worden ingezien in één systeem. Wanneer een patiënt betrokken is bij een ernstig ongeluk en naar het dichtstbijzijnde ziekenhuis wordt vervoerd, kunnen artsen direct reageren wanneer via het LSP toestemming is verleend tot het mogen inzien van de persoonlijke gegevens. Hierdoor verkrijgen de medisch specialisten snel inzicht in de gesteldheid van een patiënt, waardoor theoretisch gezien de kans op een effectieve behandeling wordt vergroot. Echter lijkt op het eerste gezicht dat focus op efficiëntie niet vanzelfsprekend bevorderlijk is voor de beveiliging van een systeem. Echter, op het eerste gezicht is de focus op Deze case study heeft tot doel een dieper inzicht te verkrijgen in de bedrijfsvoering van het Landelijk Schakelpunt en hoe risico's worden geminimaliseerd zodat een veilige applicatie kan worden aangeboden.

3.2 Data verzameling

Om data te verzamelen wordt in dit onderzoek gebruik gemaakt van kwalitatieve semigestructureerde interviews als voornaamste bron, aangevuld met documentenstudie. Aangezien dit onderzoek is gericht op het analyseren van het effect van het digitaliseren van het LSP, waarbij zowel de inhoudelijke aspecten als percepties van patiënten en betrokkenen worden onderzocht, is het houden van interviews de meest geschikte methode om een antwoord te kunnen formuleren. Deze benadering stelt de onderzoeker in staat om een gedetailleerd inzicht te krijgen van het geanalyseerde object, doordat subjectieve ideeën, perspectieven en gevoelens kunnen worden onderzocht. Bovendien zorgen semigestructureerde interviews voor flexibiliteit. Dit houdt in dat 'spontane' vervolgvragen mogelijk zijn wanneer tijdens het interview wordt opgemerkt dat een bepaald onderwerp belangrijk is voor de respondent of de respondent zelf begint over een onderwerp

dat niet voorafgaand door de onderzoeker was geïdentificeerd. Deze methode van gegevensverzameling maakt het voor een onderzoeker mogelijk om dieper in te gaan op het onderwerp en vragen te blijven stellen totdat volledig wordt begrepen wat het perspectief van de respondent omvat en dit perspectief in een juiste context kan worden geplaatst (Bryman, 2015). Het semigestructureerde interview is dus een hulpmiddel om diepgaande gegevens over percepties en meningen te verkrijgen, wat overeenkomt met het doel van dit onderzoek.

De diverse actoren die kunnen worden geïdentificeerd als betrokkenen zijn onder andere privacy specialisten, IT-auditors en medisch specialisten. Het interviewen van privacy specialisten is relevant aangezien zij kennis hebben over de definitie van privacy in wetgeving. Daarnaast kunnen IT-auditors aangeven wat de rechten van de patiënten zijn volgens de AVG. De IT-auditors worden relevant bevonden vanwege hun focus op de IT-infrastructuur en de inhoud van gedigitaliseerde systemen. Hierdoor kan een gedetailleerd inzicht in het Landelijk Schakelpunt worden gegenereerd. Naast privacy specialisten en IT-auditors kunnen medische specialisten worden geïdentificeerd als stakeholders. Voorbeelden van deze specialisten zijn huisartsen, verpleegkundigen en apothekers. De perspectieven van medisch specialisten zijn relevant en van groot belang, aangezien zij degenen zijn die daadwerkelijk met het systeem werken en de rol en het functioneren van het LSP binnen hun dagelijkse werkzaamheden kunnen aangeven. Daarnaast bestaat de groep ‘patiënten’, van wie de medische gegevens kunnen worden ingezien. ‘Patiënten’ wordt in dit onderzoek gedefinieerd als chronisch zieken die te maken hebben met verschillende zorginstanties zoals ziekenhuizen en apotheken. Hoewel patiënten toestemming moeten verlenen voor het inzichtelijk maken van hun medische gegevens, kan het zijn dat zij hierin geen keuze voelen zonder (negatieve) consequenties te ervaren. Ook kunnen patiënten toestemming hebben verleend zonder te weten waarvoor ze toestemming geven. Om een juiste weergave van de bedrijfsvoering van het LSP te kunnen geven, wordt gestreefd naar het belichten van de verschillende kanten en ervaringen van betrokkenen. De profielschetsen van de respondenten worden toegelicht in bijlage 1.

Naast interviews wordt ook documentanalyse uitgevoerd. De inrichting van het elektronisch portaal – waarin medische gegevens kunnen worden ingezien aan

de hand van BSN identificatie – heeft veel tijd ingenomen. Bij de inrichting zijn steeds meer risico's zichtbaar geworden. Aangezien dit onderzoek analyseert in hoeverre het ontwerp van het LSP is verbeterd op het gebied van privacy in vergelijking met het EPD, omvatten de documenten zowel het beleid voor het Elektronisch Patiëntendossier (EPD) als het Landelijk Schakelpunt (LSP). De beleidsdocumenten van zowel het EPD als LSP zijn openbaar beschikbaar, evenals de documenten van de Eerste en Tweede Kamer. Deze documenten van de Staten-Generaal geven de oorspronkelijke initiatieven en gedachten over elektronische gezondheidssystemen weer. Daarnaast blijkt uit deze documenten de reden om te stoppen met het EPD vanuit een privacy- en veiligheidsperspectief. De documenten vertegenwoordigen hoofdzakelijk het theoretisch perspectief. Dit perspectief wordt aangevuld met een praktisch perspectief, dat vooral uit de interviews zal blijken.

3.3 Data analyse

Dit onderzoek wordt uitgevoerd aan de hand van het theoretisch concept over High Reliability Organizations van Weick, Sutcliffe en Obstfeld (2008). Dit concept gaat in op het realiseren van procesverbetering door middel van mindfulness en lerend vermogen. In het conceptueel kader zijn de HRO-thema's gekoppeld aan thema's vanuit privacy wetgeving. In deze paragraaf wordt het conceptueel kader meetbaar gemaakt, zodat de functies van deze thema's bij de bedrijfsvoering van het LSP kunnen worden geanalyseerd.

3.3.1 Preoccupation with failure

Bij het thema 'preoccupation with failure' wordt geconcentreerd op falen als voorwaarde voor lerend vermogen, waarbij falen wordt omgezet in redenen voor verbetering. Weick, Sutcliffe & Obstfeld (2008) hebben hierbij een drietal manieren onderscheiden om procesverbetering te realiseren: (1) het behandelen van alle fouten op systeemniveau, (2) het uitvoeren van een analyse van 'bijna mislukkingen', en (3) het focussen op de verplichtingen van succes. De auteurs bestempelen HRO's als effectief wanneer het melden van fouten wordt gestimuleerd, zodat hierop kan worden geanticipeerd. Zonder het streven naar voortdurende ontwikkeling zal zelfgenoegzaamheid worden geïnterpreteerd als een mislukking van streven, onoplettendheid als gebrek aan waakzaamheid en gewenning als mislukking van

voortdurende aanpassing (Weick, Sutcliffe & Obstfeld, 2008). Uit het conceptueel kader is gebleken dat 'preoccupation with failure' de privacy thema's authenticatie, kennis, governance en systeemveiligheid raakt. *Authenticatie* gaat bij dit thema in op rollenscheiding en beslissingsbevoegdheden. Daarnaast gaat *kennis* in op de verwachte basisvaardigheden. Verder kan *governance* worden herleid door de vormgeving van verschillende interne en externe onderhouds- en controle-afdelingen. Tot slot komt *systeemveiligheid* naar voren door de focus op het mogelijk falen op systeemniveau.

Om voorgaande te kunnen analyseren zal worden geconcentreerd op de volgende onderwerpen:

In welke mate worden meldingen van fouten gestimuleerd? Wordt de onderhoudsafdeling gezien als een centrale locatie voor organisatorisch leren (effectieve HRO), of heeft deze een inconsequente rol (traditionele organisatie)? Hoe en aan wie worden successen weggeschreven? Hoeveel vertrouwen heerst er bij medewerkers over eigen vaardigheden en vaardigheden van leidinggevenden? Is er vertrouwen in de geldende programma's en procedures? Zijn er mogelijkheden voor ontwikkeling, of is het werken voornamelijk routinematig? [*De heersende gedachte bij dit thema is, dat falen kan worden voorkomen door er juist naar op zoek te gaan en gevoelig te worden voor de (vroege) tekenen van mogelijke mislukkingen. Op deze manier wordt geleerd van fouten, waardoor een organisatie zich beter kan voorbereiden op toekomstige situaties.*]

3.3.2 Reluctance to simplify interpretations

Bij het thema 'reluctance to simplify interpretations' wordt gefocust op vereenvoudigingen van interpretaties van medewerkers van organisaties. Deze interpretaties worden ook wel worldviews, frameworks of mindsets genoemd. De vereenvoudigingen kunnen potentieel voor problemen zorgen omdat medewerkers te makkelijk over situaties gaan denken. Hierdoor worden voorzorgsmaatregelen genegeerd en de risico's voor ongewenste gevolgen niet voldoende ingeschat. De moeilijkheidsgraad van dit thema is het kunnen bepalen welke aspecten wel en niet kunnen worden genegeerd. Dit kan gedeeltelijk worden beperkt door het realiseren van overeenstemming en coördinatie. Uit het conceptueel kader is gebleken dat 'reluctance to simplify interpretations' de privacy thema's beleid, kennis en governance raakt. *Beleid* komt naar voren door de duidelijke structuur, protocollen en procedures. Daarnaast komt *kennis* naar voren door het belang van

overeenstemming, coördinatie, awareness en samenwerking van medewerkers. Tot slot kan *governance* worden herkend aan de ingestelde checks and balances.

Om voorgaande te kunnen analyseren wordt geconcentreerd op de volgende onderwerpen:

Zijn taken en rollen verdeeld? Is helder wie welke verantwoordelijkheid heeft? Zijn er verschillende checks and balances ingericht? Zijn er bijvoorbeeld verschillende commissies opgericht en vinden er regelmatig vergaderingen plaats? Worden er frequente beoordelingen gegeven? Hoe worden nieuwe medewerkers geselecteerd? Is her- en bijscholing mogelijk? Hoe houden medewerkers elkaar scherp? Is er sprake van overeenstemming en coördinatie over het proces en op welke manier wordt dit vormgegeven? Wordt er gewerkt volgens een protocol? Is er een back-up aanwezig van het systeem? Is er een herstelprocedure voor wanneer zaken fout gaan? Hoe wordt met fouten omgegaan? [*Om situaties juist te kunnen blijven inschatten zal moeten worden voorkomen dat medewerkers vervallen in vereenvoudigde interpretaties*].

3.3.3 Sensitivity to operations

Bij het thema 'sensitivity to operations' ligt de focus op het situationele bewustzijn, waarbij de perceptie van de elementen in tijd en ruimte worden geplaatst. Een effectieve HRO weet de processen van de organisatie in de juiste context te plaatsen en houdt hiermee rekening. Hierdoor wordt het gevaar van bijvoorbeeld productiedruk of overbelasting geminimaliseerd. Doordat een HRO zich vaak in een complexe omgeving bevindt en zich bezighoudt met complexe technologie, is er sprake van een afhankelijkheid van gedeelde informatie en interpretaties tussen verschillende individuen. Een organisatie kan zich beter voorbereiden wanneer het zich bewust is van de huidige situatie en stilstaat bij mogelijke toekomstige situaties. Er wordt dus veel waarde gehecht aan vooruit kijken. Dit kan worden bevorderd door een combinatie van gedeelde mentale representaties, collectieve verhaalopbouw, situatiebeoordelingen met voortdurende updates, kennis van fysieke onderlinge verbindingen en parameters van systemen en actieve diagnoses van de beperkingen van vooraf geplande procedures (Weick, Sutcliffe & Obstfeld, 2008). Uit het conceptueel kader is gebleken dat 'sensitivity to operations' de privacy thema's beleid en kennis raakt. *Beleid* gaat bij dit thema in op de procedures die worden gevolgd bij onverwachte situaties en het bewustzijn van

complexe situaties. Verder gaat *kennis* in op inhoudelijke kennis van het systeem en awareness van medewerkers.

Om voorgaande te kunnen analyseren zal worden geconcentreerd op de volgende onderwerpen:

Zijn medewerkers zich bewust van de systemen waarmee ze werken? Is er een duidelijke drang naar het direct ontdekken van fouten aanwezig? (Hoe) wordt productiedruk en overbelasting ervaren? Hoe wordt ervoor gezorgd dat medewerkers dezelfde percepties hebben en dezelfde beoordelingen geven in gelijke situaties? Worden de inhoudelijke elementen van het systeem aan medewerkers geleerd? Hoe wordt het systeem ervaren? Wordt er actief gefocust op mogelijke toekomstige scenario's? [*Systemen zijn niet vanzelfsprekend statisch en lineair, maar kunnen ook dynamisch zijn. Wanneer inzichtelijk is hoe het systeem in elkaar zit, kan worden overgegaan tot het analyseren van de beste manier om met het systeem om te gaan*].

3.3.4 Commitment to resilience

Bij het thema 'commitment to resilience' wordt geconcentreerd op het vermogen om met onverwachte gevaren te kunnen omgaan. Daarbij wordt benadrukt dat betrouwbaarheid niet wordt bevorderd door onveranderlijkheid maar juist door variatie. Het omgaan met onverwachte situaties kan door middel van anticipatie, wat vaak van tevoren is bepaald, of door veerkracht, wat op het moment van plaatsvinden ontstaat. Geloofwaardigheid, vertrouwen en aandacht zijn hierbij belangrijke elementen. Door Weick, Sutcliffe en Obstfeld (2008) is geïdentificeerd dat traditionele organisaties vaker vanuit anticipatie reageren en HRO's vanuit de inzet voor veerkracht. Het wachten op een fout voordat wordt gereageerd, is niet effectief. De onverwachte verandering kan ervoor zorgen dat een organisatie meer weerbaar wordt. Bewust zijn van situaties die hebben plaatsgevonden, alsmede situaties die kunnen worden voorkomen in de toekomst, leidt tot het in staat zijn om nieuwe combinaties van mogelijke scenario's te maken en hiervan te leren. Uit het conceptueel kader is gebleken dat 'commitment to resilience' de privacy thema's beleid, kennis en systeemveiligheid raakt. *Beleid* komt naar voren in de strategie van de organisatie en het systeem. Daarnaast gaat *kennis* in op het basisniveau van kennis en lerend vermogen van gebeurtenissen. Tot slot kan systeemveiligheid worden herleid uit de back-up en herstelmogelijkheden.

Om voorgaande te kunnen analyseren zal worden geconcentreerd op de volgende onderwerpen:

Welke strategie wordt vaker gekozen: anticipatie of inzet voor veerkracht? Zijn medewerkers bewust van de service die wordt aangeboden? Kan een systeem terugkeren naar deze service nadat een onverwachte gebeurtenis heeft plaatsgevonden? Wordt er binnen de organisatie nadruk gelegd op het uitbreiden van algemene kennis en technische faciliteiten? Hoe actief wordt omgegaan met het inschatten van situaties en risico's die zich in de toekomst kunnen voordoen? Zijn er verantwoordelijkheden afgestemd over het (her)koppelen van combinaties? Hoe worden eerdere ervaringen gebruikt om te leren in de toekomst? [*Om ervoor te zorgen dat er positief kan worden teruggekeerd naar de aangeboden service, zal een organisatie de ontstane spanning moeten absorberen, moeten leren van de ongewenste gebeurtenissen en moeten groeien uit eerdere ervaringen*].

3.3.5 Underspecification of structures

Bij het thema 'underspecification of structures' ligt de focus op de rol van ordelijke procedures. Op het eerste gezicht lijkt het hanteren van een protocol of procedure bevorderlijk voor de juiste manier van uitvoering van werkzaamheden. Echter, procedures kunnen ook een belemmerende functie hebben. Wanneer er structurele fouten in de vooraf beschreven en vaststaande procedure zitten, dan zal de fout blijven optreden. Deze fout kan zich vervolgens verspreiden, opstapelen of op andere fouten inwerken. Volgens Weick, Sutcliffe en Obstfeld (2008) worden HRO's effectiever wanneer wordt geconcentreerd op het organiseren van anarchie. Hierdoor verdwijnt de van tevoren besloten gelaagdheid en wordt meer ruimte gecreëerd om zonder structurele beperkingen de juiste problemen met de juiste oplossingen te combineren. Dit betekent niet dat protocollen en procedures volledig zullen moeten verdwijnen. Men moet alleen een balans vinden tussen vastgestelde routines en flexibiliteit. Uit het conceptueel kader is gebleken dat 'underspecification of structures' de privacy thema's beleid, authenticatie en governance raakt. *Beleid* komt naar voren door de prominente plek van ordelijke procedures. *Authenticatie* kan worden herleid aan de instelling van rollenscheidingen en beslissingsbevoegdheden. Tot slot kan *governance* worden herkend aan het herzien van bestaande procedures.

Om voorgaande te kunnen analyseren zal worden geconcentreerd op de volgende onderwerpen:

Welke protocollen en procedures zijn van kracht? Is er een duidelijke hiërarchie aanwezig waarvan niet wordt afgeweken? Zijn er beslissingsbevoegden aangesteld? Hoe ervaren medewerkers flexibiliteit? Heerst er het gevoel dat een ieders capaciteiten volledig worden benut? Is er ruimte voor het aandragen van feedback en suggesties? Hoe wordt omgegaan met de signalen van fouten? Wordt er geprobeerd om nieuwe oplossingen aan te dragen, in plaats van teruggrijpen naar een procedure? [*Door niet altijd te reageren vanuit protocollen en procedures, en flexibiliteit een kans te geven, kan er meer worden gereageerd vanuit deskundigheid ongeacht de laag waarin de medewerker in een hiërarchie zou worden geplaatst. Door het creëren van erkenning kunnen medewerkers zich meer betrokken en verantwoordelijk voelen om een bijdrage te leveren*].

Eerder is in het conceptueel kader een koppeling gemaakt tussen het concept privacy – dat bestaat uit de vijf thema's: (1) beleid, (2) authenticatie, (3) kennis, (4) governance, en (5) systeemveiligheid – en het HRO perspectief dat idem bestaat uit vijf thema's: (1) preoccupation with failure, (2) reluctance to simplify interpretations, (3) sensitivity to operations, (4) commitment to resilience, en (5) underspecification of structures. Vervolgens zijn deze concepten meetbaar gemaakt voor data-analyse. In hoofdstuk vier wordt geanalyseerd of deze theoretische invalshoek overeenkomt met de feitelijke bevindingen.

3.4 Betrouwbaarheid en validiteit

Joppe (2000) definieert betrouwbaarheid als de mate waarin resultaten consistent zijn door de tijd heen en een nauwkeurige weergave representeren van de totale populatie die wordt onderzocht. Daarnaast gaat betrouwbaarheid van een onderzoeksinstrument in op de vraag of de resultaten kunnen worden gereproduceerd met een vergelijkbare methode (Golafshani, 2003). Het beleid van het EPD en het LSP zijn gedocumenteerd en openbaar beschikbaar. Bovendien worden de rapporten van alle discussies van de Nederlandse Staten-Generaal gepubliceerd op hun website. Deze documenten veranderen niet in de loop der tijd. Het is wel mogelijk dat nieuwe documenten worden gepubliceerd. Dit zijn bijvoorbeeld nieuwe vergaderingen die een aanvulling vormen op oudere documenten. De methode van dit onderzoek laat toe dat subjectieve antwoorden tijdens interviews kunnen verschillen. Maar wanneer de privacywetgeving, zoals de AVG, niet wezenlijk is veranderd bij een toekomstig onderzoek, wordt niet verwacht dat privacy specialisten de wet anders interpreteren. Ook van IT-auditors, die zullen

worden geïnterviewd wegens hun kennis van IT-infrastructuren en gedetailleerde inzicht in gedigitaliseerde systemen, wordt verwacht dat zij een minimale verandering qua perspectief zullen hebben bij toekomstig onderzoek. Dit omdat de kaders voor het analyseren van IT structuren veranderlijk zijn door veiligheids- en privacywetgeving. Het gebruik van dezelfde methode als in dit onderzoek moeten leiden tot betrouwbare resultaten.

Joppe (2000) definieert validiteit als het instrument dat bepaalt of het onderzoek daadwerkelijk meet wat was bedoeld om te meten. Daarnaast gaat validiteit ook in op de vraag hoe waarheidsgetrouw de onderzoeksresultaten zijn (Golafshani, 2003). De onderzoeksvraag richt zich op de vraag in hoeverre de bedrijfsvoering van het Landelijk Schakelpunt (LSP) is verbeterd vanuit een privacy perspectief. De koppeling tussen thema's vanuit het HRO-perspectief en thema's vanuit privacy zorgt ervoor dat belangrijke kenmerken van privacywetgeving worden geanalyseerd in samenspraak met kenmerken die een systeem als het LSP betrouwbaar zouden moeten maken. De weerspiegeling van de verschillende perspectieven van diverse stakeholders die zijn geïdentificeerd, draagt eraan bij dat wordt stilgestaan bij verschillende theoretische en praktische invalshoeken. Door inzichten van privacy specialisten, IT-auditors, medisch specialisten en patiënten te bundelen, wordt verwacht dat dit onderzoek daadwerkelijk meet wat is beoogd. Hierdoor kan het onderzoek geldig worden bevonden.

Een limitatie van dit onderzoek is dat sommige respondenten mogelijk betere antwoorden op de vragen zullen geven dan de feitelijke situatie. Dit is mogelijk te wijten aan de moeilijke initiatie en introductie van het Landelijk Schakelpunt wegens de terugtrekking van de Eerste Kamer en de private doorstart van VZVZ. De verwachting is dat de voordelen van gemakkelijke toegang tot medische dossiers van dergelijke meerwaarde wordt geacht, waardoor niet iedereen bereid is de nadelen op het gebied van veiligheid en privacy te begrijpen en te erkennen. Verder kunnen respondenten voorzichtig zijn in het vrijuit spreken over hun opvattingen omdat ze een groter belang vertegenwoordigen.

Daarnaast moet de kritische kanttekening worden geplaatst dat dit onderzoek een holistische case study betreft. Dit betekent dat het niet vanzelfsprekend mogelijk is om de bevindingen te generaliseren. Er zullen bevindingen zijn die van toepassing zijn op andere gedigitaliseerde systemen. Maar dit onderzoek focust zich niet op het vergelijken van verschillende gedigitaliseerde systemen. Er wordt gekeken naar de bedrijfsvoering van het aangepaste Landelijk Schakelpunt (LSP) op het gebied van beveiliging en privacy. Om de uitkomsten te kunnen generaliseren, is nader onderzoek van belang.

4. Resultaten

In de vorige hoofdstukken zijn het theoretisch kader en de methode aan de hand waarvan dit onderzoek wordt uitgevoerd, uiteengezet. In dit hoofdstuk komt de analyse aan bod. De analyse wordt verricht op basis van de concepten uit paragraaf 2.2. Dit betekent dat de verschillende elementen van het HRO-perspectief – te weten (1) preoccupation with failure, (2) reluctance to simplify interpretations, (3) sensitivity to operations, (4) commitment to resilience, en (5) underspecification of structures – worden geanalyseerd aan de hand van de elementen die zijn geïdentificeerd bij het concept privacy, namelijk (1) beleid, (2) authenticatie, (3) kennis, (4) governance, en (5) systeemveiligheid. De verschillende elementen worden geanalyseerd aan de hand van de afgenomen interviews en bestudeerde documenten.

4.1 Preoccupation with failure

De heersende gedachte bij het thema 'preoccupation with failure' is dat falen kan worden voorkomen door er juist naar op zoek te gaan en gevoelig te worden voor de (vroege) tekenen van mogelijke mislukkingen. Op deze manier wordt geleerd van fouten en kan een organisatie zich beter voorbereiden op toekomstige situaties. Voorafgaand aan de analyse is in paragraaf 3.3.1 geconcludeerd dat de privacy thema's authenticatie, kennis, governance en systeemveiligheid worden geraakt. Deze thema's worden achtereenvolgend behandeld.

4.1.1 Authenticatie

Wanneer het gaat om authenticatie bij preoccupation with failure komt de invulling van rollenscheiding en beslissingsbevoegdheden aan bod. AORTA is de landelijk beschikbare infrastructuur voor berichtuitwisseling in de zorg in Nederland (VZVZ, 2019c). AORTA speelt een rol bij de authenticatie van zorgverleners en patiënten die via dit systeem gegevens uitwisselen. Zorgverleners hebben hiervoor een UZI-pas nodig. Deze pas bevat hun unieke zorgverlenersidentificatie. Patiënten moeten beschikken over een DigiD, waarna een sms-code wordt verstuurd. Bij beiden is dus een tweestapsverificatie van kracht. Hiernaast regelt AORTA ook de autorisaties van betrokken zorgverleners en patiënten. Daarbij wordt rekening

gehouden met diverse aspecten, zoals de actieve instemming door de patiënt die de keuze moet maken om zijn medische gegevens te delen met andere zorgaanbieders (opt-in) en het bestaan van een behandelrelatie tussen patiënt en zorgaanbieder. Daarnaast gaat het ook om het beroep van de zorgaanbieder en eventueel bezwaar van de patiënt tegen de uitwisseling van zijn gegevens. Verder bestaat op organisatieniveau de mogelijkheid voor de zorgaanbieder om andere medewerkers direct of indirect te mandateren – op basis van een set aan autorisatieregels – waarbij de medewerker gegevens kan uitwisselen onder de verantwoordelijkheid van de zorgverlener (VZVZ, 2019c). Het mandateren van autorisaties brengt risico's met zich mee. Een duidelijke inrichting en structuur van rechtensets kan worden doorbroken wanneer een zorgaanbieder zijn beslissingsbevoegdheid mandateert – ten gevolg van een technische of menselijke fout – naar iemand die deze bevoegdheid niet behoord te hebben. Om dit soort fouten te ondervangen kan een autorisatieprotocol (APT) worden gebruikt (VZVZ, 2019c). Dit is een component die voor alle beroepen en specialisaties van zorgverleners per gegevenssoort of per context vastlegt welke berichtuitwisselingen via AORTA zijn toegestaan. Hierbij worden rolcodes gebruikt door middel van het maken van combinaties van beroepen en specialisaties. Er zijn in het systeem ook rolcodes voor niet-zorgverleners (bijvoorbeeld patiënt, ouder of voogd) vastgelegd. Hierbij is per gegevenssoort of per context ook besloten welke berichtuitwisselingen via AORTA zijn toegestaan. Met zulke protocollen wordt verondersteld dat niet wordt gezocht naar fouten om van te leren, maar dat de fouten liever direct worden vermeden.

4.1.2 Kennis

Bij kennis in relatie tot preoccupation with failure kan worden gedacht aan de verwachte basisvaardigheden en mogelijkheden tot (persoonlijke) ontwikkeling. Het VZVZ biedt online informatie aan. Daarbij wordt een keuze gegeven voor een uitgebreide set aan categorieën, namelijk: apotheken, huisartsenpraktijken, huisartsenposten, ziekenhuizen, zelfstandige klinieken, VG-instellingen, GGZ-instellingen, VVT-instellingen, zorggroepen, JGZ-organisaties, regio-organisaties en ICT-dienstverleners (VZVZ, 2019b). Vervolgens wordt per categorie ondersteuning geboden vanuit het gedachtengoed: '*Om ervoor te zorgen dat u zoveel mogelijk tijd*

kunt besteden aan patiëntenzorg, proberen wij u waar mogelijk werk uit handen te nemen.' Deze ondersteuning raakt verschillende vlakken. Om er voor te zorgen dat assistenten op de juiste manier omgaan met het vragen van toestemming en kunnen werken met het systeem zijn geaccrediteerde trainingen samengesteld. Daarnaast worden verschillende voorlichtings- en promotiematerialen beschikbaar gesteld zodat zorginstellingen patiënten goed kunnen informeren. Dit is een aanvulling op de speciale toestemmingsacties, waarbij wordt betracht het voorlichten van en toestemming vragen aan patiënten te vergemakkelijken voor medisch specialisten. Om inhoudelijk met het systeem overweg te kunnen zijn speciale informatiekaarten over de zorginformatiesystemen opgesteld. Hierin staan uitgebreide stappenplannen beschreven met uitleg over de toepassing van diverse LSP-functionaliteiten. Verder biedt het VZVZ een platform voor het doorgeven van wijzigingen binnen de zorginstellingen, doordat wijzigingen ook mogelijk gevolgen kunnen hebben op de aansluiting op het LSP (VZVZ, 2019b). Dit wordt gedeeltelijk zelf in de gaten gehouden door middel van steekproefsgewijs onderzoek naar het voldoen aan wet- en regelgeving en de manier van toestemming verkrijgen en vastleggen. Opvallend is dat er bij de uitleg over ondersteuning ruimte is voor tweerichtingsverkeer. Enerzijds wordt er vanuit het VZVZ hulp aangeboden om medewerkers te begeleiden in het LSP-systeem. Anderzijds wordt ook gevraagd naar vragen en suggesties. Echter is dit gericht op zo snel mogelijk de onvoorziene en/of onverwachte fouten te corrigeren in plaats van het opzettelijk op zoek gaan naar fouten en gevoelig worden voor mislukkingen. Met dit laatste kan een organisatie zich beter voorbereiden op toekomstige situaties, zoals bij preoccupation with failure het geval is.

4.1.3 Governance

Governance wordt bij preoccupation with failure ingezet voor de vormgeving van verschillende interne en externe onderhouds- en controleafdelingen. Wanneer wordt gefocust op interne toezicht en controle, dan blijkt dat VZVZ monitoring en logging inzet om te controleren welke raadplegingen in het systeem worden verricht. VZVZ benadrukt dat het LSP alleen kan worden bevraagd met een UZI-pas en bijbehorende pincode. Dit zou moeten betekenen dat een persoon geautoriseerd is

om de specifieke opvraging te verrichten. Vervolgens omvat de logging alle raadplegingen van zorgaanbieders zonder registratie van medische inhoud (VZVZ, 2019e). VZVZ vindt deze manier van logging voldoende om te controleren of een zorgverlener rechtmatig gegevens heeft opgevraagd. Informatie dat meer inhoudelijk ingaat op de manier van bijhouden of er sprake is van onbevoegd, verkeerd of afwijkend gebruik blijft uit doordat VZVZ de verantwoordelijkheid bij de aangesloten zorginstellingen legt. De verantwoordelijkheden worden op de volgende manier gesplitst. VZVZ is verantwoordelijk voor de gegevensverwerking via het LSP en voor het beheer en ontwikkeling van het systeem. Daarnaast is de zorgverlener verantwoordelijk voor de inhoud van het medisch dossier van de patiënten en voor het beschikbaar stellen van de gegevens via het systeem. Voorafgaand aan de handelingen dient een zorgverlener de patiënt te informeren over het systeem en actief toestemming te vragen (VZVZ, 2019e). Concluderend is VZVZ de partij die de infrastructuur van het systeem mogelijk maakt en zorgt dat het LSP via een veilige en betrouwbare verbinding tot stand wordt gebracht. Verantwoordelijkheden voor de juistheid en volledigheid van de medische dossiers is bij de aangesloten zorginstellingen zelf geplaatst. De raadplegingen van zorginstellingen worden bijgehouden, zodat achteraf altijd kan worden gecontroleerd of zorgverleners rechtmatig gegevens hebben opgevraagd. Wanneer de uitkomst is dat een niet-gerechtigde opvraging is gedaan, dan is het aan de toezichthouders van de Autoriteit Persoonsgegevens (AP) en de Inspectie voor de Gezondheidszorg (IGZ) om hierover in beraad te gaan (VZVZ, 2019d).

Een vergelijking wat betreft toezicht en controle tussen het EPD en het LSP valt in het voordeel van het LSP uit. Bij het LSP lijkt duidelijker te zijn in welke handen de controle is, terwijl meerdere critici zich hebben uitgesproken over het tekortschieten van het toezicht op toegang bij het EPD. Een van de critici die onderzoek heeft gedaan naar privacy bij het EPD is Brenno de Winter. De documenten over de privacy van het EPD werden opgevraagd bij het College Bescherming Persoonsgegevens (CBP) met een beroep op de Wet openbaarheid van bestuur (Wob). Vervolgens is de informatie geanalyseerd in samenwerking met een medisch tijdschrift (De Winter, 2010). De auteur spreekt over een gebrekkig toezichtsysteem, onder meer omdat de controle op misbruik achteraf wordt

geregeld. Volgens De Winter heeft het Ministerie van VWS dit probleem ook erkend in een toelichting op de Wet die het EPD regelt. Dat probleem omvat het gegeven dat toezicht achteraf goed is vormgegeven. Echter, omdat de gebruiker de gegevens reeds heeft ingezien, is het kwaad al geschied. In principe heeft logging een remmende werking maar het risico kan hiermee niet worden uitgesloten (De Winter, 2010).

4.1.4 Systeemveiligheid

De systeemveiligheid bij preoccupation with failure kan worden opgemaakt uit de focus op het mogelijk falen op systeemniveau. In 2008 werd voor het eerst het Elektronisch Patiëntendossier (EPD) geïntroduceerd door het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Bij de vormgeving is een drietal doelen geïdentificeerd.[3] Het eerste doel betreft de centralisatie van kennisoverdracht. Centralisatie van kennisoverdracht treedt op doordat alle medische informatie van een patiënt toegankelijk wordt vanaf iedere plek, terwijl de informatie verspreid is opgeslagen bij verschillende zorgverleners. Theoretisch zou dit ervoor moeten zorgen dat de kans op een verkeerde diagnose of behandeling wordt verkleind. Het tweede doel focust zich op het verhogen van efficiency, waarbij schriftelijke documentatie wordt vermeden en onderzoek niet dubbel wordt uitgevoerd. Het bijkomend voordeel van dit doel is kostenbesparing. Het derde doel richt zich op kwaliteitsverbetering op de lange termijn. Het effect van bepaalde behandelwijzen kan beter worden gemonitord en beoordeeld door analyse van de gegevens in het elektronisch patiënten portaal.

Echter heeft zich in de Tweede Kamer vanaf het begin een grote discussie voorgedaan omdat het EPD systeem niet voldoende veilig zou zijn voor het uitwisselen van medische gegevens (ZorgNu, 2017). Hierdoor heeft de Eerste Kamer in 2011 besloten dat het EPD niet zou worden doorgezet. Desalniettemin is sinds die tijd een private doorstart gemaakt met de ontwikkeling van een soortgelijk systeem. Dit systeem draait ook om het uitwisselen van medische gegevens van patiënten en wordt het Landelijk Schakelpunt (LSP) genoemd. Om te voorkomen dat het LSP tegen

[3] Meer informatie: Kamerstukken II 2006/07,27529 nr. 29; Programmacommissie Informatie- en Communicatietechnologie in de Zorg

dezelfde moeilijkheden aanloopt zijn diverse onderzoeken uitgevoerd naar de risico's die verbonden zijn aan het digitaliseren van het elektronisch patiënten portaal.[4] Ten eerste bestaat het risico dat onbevoegden toegang krijgen tot het systeem, wat uiteindelijk kan leiden tot het bekijken, wijzigen, kopiëren en publiceren van patiëntgegevens door cybercriminelen. Een ander risico is het onzorgvuldig handelen van bevoegde gebruikers. Een kleine fout kan veel gevolgen hebben doordat het door alle zorgverleners kan worden ingezien. Daarnaast is mogelijk misbruik van de opgeslagen gegevens risicovol omdat gegevens voor een ander doel kunnen worden gebruikt dan waarvoor ze zijn vastgelegd (ZonMw, 2019).

Het LSP bestaat uit een netwerk waarop zorgaanbieders zich kunnen aansluiten, een zogenoemde 'zorginfrastructuur'. Via dit netwerk kunnen de aanbieders op ieder gewenst moment medische gegevens over hun patiënten raadplegen in elkaars systemen (Volg Je Zorg, 2019a). De eerdere discussie omtrent de veiligheid van het EPD wordt getracht te zijn verholpen doordat het LSP speciaal is ontwikkeld en beveiligd voor dit doel. Het Landelijk Schakelpunt vormt dan ook geen database omdat de medische gegevens niet worden opgeslagen (Volg Je Zorg, 2019a). De informatie over patiënten kan worden ingezien terwijl de gegevens blijven staan in de dossiers bij huisartsen en apotheken. Wanneer een patiënt toestemming heeft gegeven, melden de huisartsen en apotheken het BSN aan bij de verwijsindex in het LSP. Andere zorgaanbieders kunnen door middel van het zoeken op dit BSN medische informatie raadplegen, welke nodig kan zijn voorafgaand aan het starten van een behandeling (Volg Je Zorg, 2019a).

4.1.5 Subconclusie

Bij de vormgeving van zowel het EPD als het LSP is rekening gehouden met het mogelijk falen van het systeem. Dit is echter vanuit de gedachtegang om te voorkomen dat er ongewenste situaties, zoals datalekken of beveiligingsincidenten, ontstaan in plaats van een drang naar het leren van fouten. Nadat de Eerste Kamer zich in 2011 heeft teruggetrokken omdat het EPD systeem onvoldoende veilig en

[4] Een elektronisch patiëntenportaal is een online omgeving welke is gekoppeld aan een specifiek zorgverlenerssysteem, waarin persoonlijke gezondheidsdossiers van individuen staan opgeslagen.

betrouwbaar zou zijn, is groen licht gegeven voor een private doorstart van een soortgelijk systeem: het LSP. Echter is bij de optekening van het LSP systeem juist aandacht besteed aan het voorkomen van dezelfde fouten waardoor het EPD is afgewezen. Het leren van fouten komt dus wel naar voren wanneer het ontwerp van het EPD naast het ontwerp van het LSP wordt gelegd. Wanneer evenwel losstaand naar het ontwerp van het LSP wordt gekeken, is het uitgangspunt dat het beleid en het systeem sluitend zijn zodat fouten kunnen worden voorkomen.

Door middel van de ingestelde procedures en protocollen worden meldingen van fouten gestimuleerd. Echter zijn de procedures gericht op het zo snel mogelijk corrigeren van ongewenste situaties zodat wordt voldaan aan wetgeving en de veiligheid van het systeem kan worden gewaarborgd. De fouten worden liever vermeden in plaats van opgezocht om daarvan te leren. Er is ondersteuning aanwezig vanuit het VZVZ zodat accurate kennis van medewerkers op peil blijft. De mogelijkheden voor persoonlijke ontwikkeling worden aangereikt en VZVZ vraagt feedback voor het blijven innoveren van het systeem. Toch kan het werk zelf worden beschouwd als voornamelijk routinematig omdat de prioriteit wordt gegeven aan het volgen van de juiste procedures. De eerdere discussie omtrent de veiligheid van het EPD wordt getracht te zijn verholpen doordat het LSP speciaal is ontwikkeld en beveiligd voor het beschikbaar stellen van medische gegevens. Het Landelijk Schakelpunt vormt geen database, aangezien de medische gegevens niet worden opgeslagen. De infrastructuur zorgt slechts voor een beveiligde toegang tot het raadplegen van medische data in de systemen van andere zorginstellingen. Om te controleren of dit in de praktijk het geval is zowel het interne als externe toezicht verbeterd bij het LSP ten opzichte van de situatie bij het EPD.

Vanuit het High Reliability Organization perspectief van Weick, Sutcliffe & Obstfeld (2008) kan de optekening van het LSP niet direct worden verklaard vanuit het thema preoccupation with failure. Het thema ziet falen en het gevoelig worden voor tekenen van mogelijke mislukkingen als startpunten voor lerend vermogen en een succesvolle voorbereiding op toekomstige situaties. Het Landelijk Schakelpunt is daarentegen juist ingericht op het voorkomen van fouten. Wanneer de optekening van het eerder afgewezen EPD met het LSP wordt vergeleken, dan kan worden geconcludeerd dat de fouten die zijn gemaakt bij het EPD zijn meegenomen in het

ontwerp van het LSP. Op deze manier maakt het LSP niet dezelfde fouten. Het is echter de vraag of de optekening volledig sluitend kan zijn vanuit een privacy perspectief. Het concentreren op fouten zou daar vanuit het HRO-perspectief een bijdrage aan kunnen leveren, zodat lerend vermogen en bewustzijn kan worden gecreëerd.

4.2 Reluctance to simplify interpretations

Om situaties juist te kunnen blijven inschatten moeten worden voorkomen dat medewerkers vervallen in vereenvoudigde interpretaties. Bij het thema 'reluctance to simplify interpretations' wordt gefocust op deze vereenvoudigingen van interpretaties van medewerkers van organisaties. De vereenvoudigingen kunnen potentieel voor problemen zorgen doordat medewerkers te makkelijk over situaties gaan denken. Hierdoor worden voorzorgsmaatregelen genegeerd en de risico's voor ongewenste gevolgen niet voldoende ingeschat. Voorafgaand aan de analyse is in paragraaf 3.3.2 geconcludeerd dat de privacy thema's beleid, kennis, en governance worden geraakt. Deze thema's worden achtereenvolgend behandeld.

4.2.1 Beleid

Bij beleid in relatie tot 'reluctance to simplify interpretations' gaat het om de aanwezigheid van duidelijke structuren, protocollen en procedures en de manier waarop hiermee vervolgens wordt omgegaan. Respondent 7 – medisch specialist – beschrijft dat het volgende het geval is:

'*Ja er moet natuurlijk wel heel veel vastgelegd worden nu, het kan niet meer een soort van in een grijs gebied, want als er iets wordt gemist, dan moeten we allemaal weten waar het fout ging, want dan kan er van worden geleerd*.' – Respondent 7.

Er is vanuit de medisch specialisten begrip voor het feit dat veel moet worden gedocumenteerd, al neemt dit meer tijd in beslag. In situaties met weinig voorbereidingstijd gaat het documenteren af van de resterende tijd van het consult van een patiënt. Er is een spagaat tussen voldoende tijd hebben voor het juist

afwikkelen van de fysieke afspraak en de bijbehorende administratieve werkzaamheden. Dit is volgens Respondent 7 gedeeltelijk ook het gevolg door een verandering in de gezondheidszorg: er zijn steeds meerdere centra, meerdere ziekenhuizen en meerdere artsen betrokken bij een patiënt, de patiënt wordt niet meer vaak gezien door maar één arts door het hele traject heen. Wanneer gegevens minimaal en onzorgvuldig staan beschreven dan dient een zorgaanbieder eigenmatig een schatting te maken van de progressie. Dit moet worden voorkomen. Echter, respondenten spreken de verwachting uit dat de oudere generatie artsen meer moeite heeft met de toename in protocollen over documentatie. De technologische ontwikkelingen bieden kansen en mogelijkheden, maar niet iedereen kan daarmee even goed omgaan. Respondent 7 licht toe dat er een groep artsen bestaat die vastleggen door middel van dicteren omdat dit sneller zou gaan. Hoewel een verschil bestaat in manier van vastleggen – mondeling of schriftelijk – is er geen verschil in de hoeveelheid informatie die wordt gedocumenteerd. Op deze manier wordt uiteindelijk wel voldaan aan het protocol.

Er ligt veel vast wanneer het gaat om structuren, protocollen en procedures. Zo wordt onder andere een verschil gemaakt in werkwijze tussen eerstelijns- en tweedelijnsbehandelingen. Verder is ook merkbaar dat door de tijd heen een verschuiving van focus plaatsvindt. Momenteel wordt meer aandacht besteed aan het belang van de privacywetgeving en de gevolgen die dit heeft voor de werkzaamheden van zorgverleners. Respondent 7 erkent:

'*Je moet wel veel met de privacy wetgeving, zeker in het ziekenhuis omdat mensen heel erg beschermend zijn met hun data. Het is natuurlijk nog redelijk nieuw, maar vijf jaar geleden boeide het eigenlijk helemaal niemand nog wat er met de data gebeurde*.' – Respondent 7.

Ter aanvulling stelt Respondent 7 dat niet alleen nieuwe procedures en protocollen worden beschreven, maar dat ook uitgebreid wordt uitgelegd wat het belang van een dergelijke procedure is. Door toe te lichten wat gaat gebeuren – en daarnaast vooral waarom het op die manier gaat gebeuren – kan meer bewustzijn worden gecreëerd. Het werk van zorginstellingen betreft altijd de medische

gegevens van personen, waardoor een foutieve omgang met gegevens ook vaak resulteert in gevolgen voor de patiënt. Om te voorkomen dat medewerkers vervallen in makkelijk denken over de procedures en het beschouwen als negatieve administratieve handelingen, zetten zowel zorginstellingen als VZVZ middelen in. Dit zijn onder andere (verplichte) trainingen die medewerkers moeten doorlopen, afgestemd naar de verschillende categorieën van specialisten. Ook bestaat hierbij een sleutelrol voor toezicht en controle door te wijzen op fouten van medewerkers en de bijbehorende consequenties voor patiënten. De medisch specialisten geven aan dat in het geval van het onjuist of ongeautoriseerd opzoeken van gegevens het systeem afdwingt dat een reden voor de raadpleging moet worden opgegeven. Wanneer dit frequent gebeurt, grijpt een leidinggevende in en worden de voorvallen besproken. Deze gelaagdheid komt naar voren met meerdere procedures en protocollen. Medewerkers zijn ervan op de hoogte dat bepaalde procedures aanwezig zijn, maar wanneer deze niet nodig zijn voor de eigen werkzaamheden worden deze niet gedeeld. Een voorbeeld hiervan is de back-up en herstelprocedure. VZVZ heeft hier geen landelijk geldende procedure voor opgesteld. De verantwoordelijkheid ligt bij een individueel team van een zorginstelling, waardoor het binnen een specifieke groep wordt gedeeld en verschillen mogelijk kunnen zijn mits het team voldoet aan de geldende wet- en regelgeving. Echter is hierbij van belang dat er duidelijke communicatie is over de aanwezigheid van het verantwoordelijke team en de procedures, zodat medewerkers weten hoe ze moeten handelen in bepaalde situaties.

4.2.2 Kennis

Kennis bij reluctance to simplify interpretations komt tot uiting door te focussen op het belang van overeenstemming, coördinatie, bewustwording en samenwerking van medewerkers. Doordat meerdere medewerkers betrokken zijn bij het uitvoeren van de behandeling van één patiënt, is het belangrijk dat een basisniveau van kennis aanwezig is bij alle betrokken medewerkers. Wanneer de medewerkers zich bewust zijn van de kwetsbaarheid van hun service, is de verwachting dat zij minder terugvallen in het zoeken van de makkelijkste manier waarbij cruciale stappen worden overgeslagen. Een goede samenwerking is

afhankelijk van wederzijds begrip tussen medewerkers. Dit wordt gerealiseerd door het verduidelijken van rollen en functies, zodat kan worden ingeschat voor welke werkzaamheden een medewerker verantwoordelijk kan worden gehouden. Echter lijkt dit niet altijd het geval te zijn volgens de medisch specialisten. Respondent 7 geeft aan:

'Je weet niet van de andere functies hoe hun scherm er uitziet. Dus verpleegkundigen die kunnen bijvoorbeeld niet het volledige scherm zien, zoals ik dat kan zien. Dus dan heb je wel eens het idee dat ze hun werk niet doen zoals het zou moeten, maar dan kunnen ze er gewoon niet bij.'

Het is bekend dat verschillende rollen diverse rechtensets kunnen hebben maar er bestaat onduidelijkheid over de inhoud van die rollen. Het is theoretisch logisch ingericht, maar de respondenten geven aan dat medewerkers er gaandeweg zelf achter moeten komen welke autorisaties bij welke rol horen. Er is niet sprake van een overzicht waarin de verschillende functies worden toegelicht. Het risico van deze onduidelijkheid is dat wederzijdse ergernissen kunnen ontstaan, doordat het lijkt alsof taken niet naar behoren worden uitgevoerd. Respondent 7 heeft aangegeven dit wel eens te hebben nagevraagd, maar dat een standaard reactie wordt teruggekoppeld en dat dit nou eenmaal het beleid is.

4.2.3 Governance

De governance die wordt ingezet bij reluctance to simplify interpretations concentreert zich op de ingestelde checks and balances om te voorkomen dat medewerkers vervallen in vereenvoudigde interpretaties. Door middel van toezicht en controle kan het vertrouwen in het systeem worden vergroot, door meer zekerheid te bieden dat het systeem is ingericht op de manier waarop zou moeten. Door de medisch specialisten is aangegeven dat niet altijd kan worden gesproken van een sluitende afbakening in het systeem. Dit komt tot uiting in onder andere het kunnen inzien van verschillende modules:

'*In principe kun je modules niet zien wanneer je de rechten niet bezit, daarnaast mag je niet in een dossier kijken als jij daar niets mee te maken hebt, maar je kan er wel bij, er zit geen slot op*.' – Respondent 7.

Het gegeven dat er geen slot op zit, maakt het mogelijk dat medewerkers niet gelegitimeerde toegang hebben tot data. Er is geen automatische blokkering van het systeem waardoor toegang direct wordt geweigerd. Wanneer dit vanuit het systeem zelf niet wordt ondersteund, kan het een verschillende uitwerking hebben op de medewerkers. Enerzijds kunnen medewerkers nonchalant worden doordat van hen iets wordt verwacht terwijl het systeem er niet in kan voorzien. Anderzijds kan het mensen motiveren om beter op te letten doordat ze niet worden gecorrigeerd vanuit het systeem en fouten dus niet worden ondervangen.

Het VZVZ lijkt hiervan afstand te nemen door alleen eigen verantwoordelijkheid te nemen voor het aansluitingsbeleid van zorginstellingen op het systeem. De verantwoordelijkheid over hoe vervolgens de inhoudelijke autorisaties worden toegekend aan medewerkers ligt bij de zorginstellingen. VZVZ houdt zich wel bezig met het identificeren van kansen en bedreigingen waarmee het systeem in aanraking komt. In het business plan 2016 – 2020 zijn de volgende bedreigingen door VZVZ beschreven: (1) er is een hoog tempo van (medisch) technologische ontwikkelingen, waardoor potentiële alternatieve infrastructuren en internationale standaarden kunnen leiden tot snelle veroudering, en bilaterale, niet-gestandaardiseerde uitwisselingen; (2) er is een toename van de regeldruk en strenger extern toezicht op onder andere het vragen van toestemming aan patiënten. De focus op privacy leidt tot risicoaversie, administratieve druk en belemmering van innovatie; (3) de impact van verstoringen en gebruiksongemak in de keten kan door de landelijke schaal van de infrastructuur groot zijn op de gebruiksbeleving, het privacy- en veiligheidsimago en het algemene vertrouwen in het systeem; en (4) er zijn fragiele en gefragmenteerde decentrale infrastructuren en configuraties met een sterk wisselende (en vaak meervoudige) organisatiegraad van gebruikers en regio's op ICT-beheer, gebruikersondersteuning, gebruikerstesten en validatie (VZVZ, 2015). Hoewel het VZVZ zich door middel van het businessplan concentreert op de omgeving en context van het systeem en handvatten voor het

vergroten van het bewustzijn, wordt ook van medewerkers zelf verwacht dat zij verantwoordelijkheid nemen.

4.2.4 Subconclusie

Om de veiligheid van het systeem te waarborgen is het belangrijk dat overeenstemming bestaat over hoe met het systeem moet worden omgegaan en dat medewerkers hiervan het belang inzien. Deze verantwoordelijkheid ligt bij verschillende groepen, zoals de medewerkers zelf, de zorginstellingen en VZVZ. De zorg is door de tijd heen veranderd. Dit komt onder andere tot uiting in de verschuiving van focus. Het belang van het beschermen van gegevens is binnen enkele jaren steeds meer toegenomen. Daarnaast zijn er verschillen wat betreft de behandelrelatie. Doordat steeds vaker meerdere medewerkers betrokken zijn bij het uitvoeren van de behandeling van één patiënt, is het belangrijk dat een basisniveau van kennis aanwezig is bij alle betrokken medewerkers.

Het wegnemen van de vereenvoudigde interpretaties komt tot uiting in het beleid door de aanwezigheid van duidelijke structuren, protocollen en procedures. Hierbij wordt niet alleen toegelicht *wat* moet gebeuren, maar ook *waarom* het op deze manier moet. Door het aanhalen van het belang van de procedures worden medewerkers bewust gemaakt van de gevoeligheid van hun werkzaamheden en weten zij hun service in de juiste context te plaatsen. Om te voorkomen dat medewerkers vervallen in makkelijk denken over de procedures en het beschouwen als negatieve administratieve handelingen zetten zowel zorginstellingen als VZVZ middelen in. Procedureel zijn taken en rollen verdeeld door middel van authenticatie en autorisatie, maar medewerkers beschikken niet over een overzicht van welke rechten iedere rol bezit. Hierdoor kunnen ergernissen ontstaan en kan het creëren van wederzijds begrip uitblijven. Door middel van toezicht en controle kan het vertrouwen in het systeem worden vergroot door meer zekerheid te bieden dat het systeem is ingericht op de manier waarop zou moeten. Er is geen landelijke back-up en herstelprocedure vanuit VZVZ opgesteld. De verantwoordelijkheid hiervoor is gegeven aan de aangesloten zorginstellingen zelf. Op basis van de afgenomen interviews kan worden gesteld dat een duidelijke gelaagdheid aanwezig is bij zorginstellingen. Dit betekent dat informatie van persoon tot persoon wordt

doorgegeven op hiërarchische volgorde. Deze korte lijnen kunnen er voor zorgen dat medewerkers elkaar eenvoudiger scherp kunnen houden omdat de afstand tussen medewerker en leidinggevende klein wordt ervaren.

Door te concentreren op het thema reluctance to simplify interpretations van het High Reliability Organization perspectief van Weick, Sutcliffe & Obstfeld (2008) kan privacy worden bevorderd in de bedrijfsvoering van het LSP. Het creëren van een technisch stabiel systeem waarbij op een veilige en betrouwbare manier medische gegevens kunnen worden uitgewisseld is de eerste stap. Maar het systeem zal altijd onderhavig blijven aan menselijke factoren. Het zijn de medewerkers die met het systeem moeten kunnen omgaan om op een juiste manier de medische dossiers in te richten en beschikbaar te stellen. Het concentreren op het bewustzijn van medewerkers en het bewerkstelligen van coördinatie en overeenstemming draagt hieraan bij.

4.3 Sensitivity to operations

Bij het thema 'sensitivity to operations' ligt de focus op het situationele bewustzijn, waarbij de perceptie van de elementen in tijd en ruimte worden geplaatst. Systemen zijn niet vanzelfsprekend statisch en lineair, maar kunnen ook dynamisch zijn. Wanneer inzichtelijk is hoe het systeem in elkaar zit, kan worden overgegaan tot het analyseren van de beste manier om met het systeem om te gaan. Voorafgaand aan de analyse is in paragraaf 3.3.3 geconcludeerd dat de privacy thema's beleid en kennis worden geraakt. Deze thema's worden nu achtereenvolgend behandeld.

4.3.1 Beleid

Het beleid bij 'sensitivity to operations' kan bijdragen aan het bewustzijn van medewerkers over hoe het systeem in elkaar zit, hoe zij hier het beste mee kunnen werken en welke mogelijke gevolgen er zijn. Het volgen van de opgestelde protocollen en procedures kan het omgaan met complexe situaties vereenvoudigen.

Door de eerdere vraagtekens die zijn geplaatst bij het EPD, is er bij de opzet van het LSP meer ingespeeld op de veiligheid en privacy van het systeem. Om een hoge kwaliteit van informatiebeveiliging te realiseren is een aantal maatregelen

getroffen (Volg Je Zorg, 2019b). De eerste maatregel betreft het gegeven dat zorgaanbieders zich niet vanzelfsprekend kunnen aansluiten op het netwerk. Voorafgaand wordt het computersysteem van de zorgverlener getoetst aan strenge beveiligingseisen. Daarnaast kan een zorgaanbieder alleen inloggen met een speciale pas en wachtwoord. Nog een maatregel is de verplichte toestemming van een patiënt voordat een zorgaanbieder de medische gegevens mag delen. Zonder toestemming is dit niet mogelijk. Verder mogen alleen zorgaanbieders die een patiënt behandelen de desbetreffende medische gegevens inzien. Een aanvullend component hierbij is dat het daadwerkelijk noodzakelijk moet zijn voor een behandeling. Om dit te verifiëren vindt nauwlettend toezicht plaats. In het netwerk wordt bijgehouden welke zorgaanbieder welke gegevens op welk moment heeft bekeken. Een patiënt heeft het recht om dit te controleren. Daarnaast is deze mogelijkheid ook opgenomen in wet- en regelgeving, zoals de AVG en de Wet op Geneeskundige Behandelingsovereenkomst (Volg Je Zorg, 2019b). Het theoretisch opbouwen van het systeem is de eerste stap. Maar vervolgens moet worden bekeken wat de praktijk uitwijst. Alle ondervraagde respondenten die zijn geclassificeerd als IT-auditor en/of privacy specialist, geven aan dat het een kwestie van tijd is voordat een beveiligingsincident of datalek ontstaat bij een systeem zoals het Landelijk Schakelpunt. Dit kan allerlei verschillende oorzaken hebben: van technische fout tot menselijke fout. Echter, van belang is hoe een beveiligingsincident of datalek wordt opgevolgd en hoe hierover wordt gecommuniceerd. De manier om bij te houden of het systeem werkt zoals wordt beoogd, is het monitoren en loggen van gebeurtenissen en situaties. Volgens de IT-auditors is het proces van monitoren en loggen wat in een systeem gebeurt liever statisch en lineair in plaats van dynamisch. Dit is onder andere op te maken uit volgende citaten:

'Logging is ook een hele belangrijke hier, zie je wie op welk moment een actie heeft uitgevoerd, zij het opvragen van het patiëntdossier, of misschien zelfs het wijzigen.'
- Respondent 4.

‘*Logging is in dit geval belangrijk omdat je wilt weten of de procedure netjes werkt, dus ik wil zien dat er niets misbruikt wordt. Door de logging te analyseren kan ik ook zien of een procedure wel of niet werkt.*’ – Respondent 6.

Opvallend is dat de logging op het systeem door de IT-auditors wordt gezien als een noodzakelijke voorwaarde, terwijl het door medisch specialisten wordt ervaren als een vanzelfsprekendheid. Dit is te verklaren vanuit de onderzoekende en beoordelende rol van een auditor tegenover de uitvoerende rol van een specialist aan wie het beleid wordt opgedragen.

4.3.2 Kennis

Wanneer het gaat over kennis bij sensitivity to operations betreft het de inhoudelijke kennis van het systeem en awareness van medewerkers zodat medewerkers zich bewust zijn van het systeem zelf en de rol die het LSP inneemt. Hoewel bij een digitaal medisch dossier altijd moet worden omgegaan met persoonsgegevens en medische data – zowel in het EPD als in het LSP – zijn er geen speciale trainingen over het omgaan met dit soort gevoelige gegevens. De trainingen zijn vooral gefocust op de omgang met zorginformatiesystemen. Daarnaast zijn trainingen ook afhankelijk van de rol die wordt vervult. VZVZ biedt wel online hulp wanneer medewerkers aangeven dat ze ergens tegen aanlopen, wanneer dit specifiek het LSP systeem betreft. Ook zonder aandacht vanuit VZVZ of de zorginstellingen erkent Respondent 7 bewust om te gaan met gevoelige data:

‘*Zodra je de patiënten ziet dan weet je ook wel van oké dit is iemand zijn data, je wil ook niet dat het voor diegene uitlekt, of dat er onzorgvuldig mee wordt omgegaan. Dat wil je zelf ook niet. Het is een beetje de menselijkheid ervan inzien.*’ – Respondent 7.

Van medewerkers die gaan werken bij zorginstellingen wordt verwacht dat zij hiervoor kiezen omdat ze patiënten die kampen met gezondheidsproblemen willen helpen en begeleiden. Echter mag er niet vanzelfsprekend vanuit worden gegaan dat dit altijd het geval is. Fouten kennen verschillende oorzaken, zoals een technische fout of menselijke fout, per ongeluk of door opzet. Het leren van deze fouten en het

voorbereiden en voorkomen van toekomstige scenario's wordt ondervangen door het opstellen van nieuwe protocollen en procedures. Ook het uitbesteden van controletaken aan externe toezichthouders hoort hierbij.

Een voorbeeld van het creëren van inzicht in de gevoeligheid van het systeem is het plaatsen van berichten met verwijzingen naar protocollen op het interne netwerk. Door deze berichten weten medewerkers hoe ze in een bepaalde situatie moeten handelen. Hieronder volgt een gedeeld bericht via intranet.

Datalek? Meld dit zo snel mogelijk

Ziekenhuis X verwerkt op grote schaal persoonsgegevens. De meeste medewerkers komen dagelijks in aanraking met deze data over mensen. Het verwerken kan dus wel eens misgaan, dan is er een datalek.

Vertrouwelijk
In de wet wordt een datalek beschreven als 'inbreuk in verband met persoonsgegevens. In de praktijk kan een datalek een inbreuk zijn op de vertrouwelijkheid, beschikbaarheid of integriteit van de gegevens'.

Brieven, e-mails
In het afgelopen jaar zijn er in *Ziekenhuis X* datalekken geweest. "Het Team Datalek heeft geconstateerd dat datalekken vaak een menselijke vergissing als oorzaak hebben, zoals verkeerd verzonden brieven of e-mails met persoonsgegevens. Een goede oplossing om zo'n lek te voorkomen is bijvoorbeeld het gebruik van secure mail of Surf File Sender voor het e-mailen van patiëntgegevens."

USB-stick
Het Team Datalek houdt zich al een aantal jaar bezig met de afhandeling van datalekken. "Zo was tot een jaar geleden het verliezen van USB-sticks een veelvoorkomend datalek". "Dit is nu voor een groot deel opgelost door het invoeren van encrypted USB-sticks."

Leren
Een datalek ontdekt? Meld dit dan altijd zo snel mogelijk aan Team Datalek via een formulier op intranet. "Als organisatie kan *Ziekenhuis X* hier veel van leren en onze maatregelen treffen om datalekken in de toekomst te voorkomen. Bovendien is *Ziekenhuis X* verplicht om een overzicht te bewaren van alle datalekken die zich hebben voorgedaan."

Voor het melden van datalekken bestaan vijf gouden regels.

De vijf gouden regels:
Houd bij een beveiligingsincident altijd de volgende Vijf Gouden Regels in gedachten:
(1) Informeer de privacy contactpersoon over het informatiebeveiligingsincident;
(2) Stel gezamenlijk vast of sprake is van een verwerking van persoonsgegevens en van een (mogelijk) datalek. (Stel dit bij afwezigheid van de Privacy Contactpersoon zelfstandig vast, zodat een eventuele melding aan de Autoriteit Persoonsgegevens binnen 72 uur na ontdekking kan plaatsvinden);
(3) Informeer onmiddellijk het afdelingshoofd of de leidinggevende als sprake is van een (mogelijk) datalek;
(4) Vul het interne meldformulier datalek in. Geef daarin aan wat er precies is gebeurd, welke persoonsgegevens (mogelijk) betrokken zijn bij het incident en welke maatregelen er al zijn/worden genomen om de gevolgen in te perken en herhaling te voorkomen. Meld het (mogelijk) datalek NIET zelf bij de Autoriteit Persoonsgegevens.
(5) Mail het ingevulde formulier aan x én neem telefonisch contact op over de interne melding met het secretariaat Juridische Zaken tel. x (kantooruren).

Naast het gegeven dat de medisch specialisten voldoende kennis moeten bezitten om op een goede manier met het systeem om te kunnen gaan, ligt er ook een gedeeltelijke verantwoordelijkheid bij de patiënt zelf. De kennis die van patiënten mag worden verwacht, gaat in op zijn rechten. En van patiënten mag ook worden verwacht dat zij weten hoe bijvoorbeeld de webapplicaties werken waarvan ze gebruikmaken om digitaal inzicht te verkrijgen in het eigen medisch dossier.

4.3.3 Subconclusie

Door middel van een focus op het thema sensitivity to operations kan worden bewerkstelligd dat medewerkers de processen van de organisatie in de juiste context weten te plaatsen. Wanneer een organisatie zich in een complexe omgeving bevindt, zoals bij het LSP het geval is, ontstaan risico's en gevaren. Deze komen onder andere tot uiting bij de afhankelijkheid van gedeelde informatie en interpretaties tussen individuen. Daarnaast is het belangrijk om te identificeren of een systeem statisch en lineair is, of dynamisch.

Het LSP valt in de categorie statisch en lineair. Er is één manier dat wordt beschouwd als de beste manier om met het systeem om te gaan en daar zijn de procedures en protocollen op ingericht. Er wordt onderscheid gemaakt tussen de verschillende categorieën van zorginstellingen, omdat diverse mogelijkheden zijn voor gebruikte informatiesystemen en applicaties. De medewerkers zijn zich bewust

van de plaats die het LSP inneemt in de zorgsector maar er is geen duidelijke drang naar het direct ontdekken van fouten aanwezig. Het beleid, de trainingen en de hulpmiddelen moeten ervoor zorgen dat medewerkers gelijke beoordelingen geven in gelijke situaties. Verder wordt veel naar elkaar verwezen, zoals blijkt uit het bericht in paragraaf 4.3.2. Informatie strekt voor zo ver situaties mogelijk kunnen voorkomen tijdens de werkzaamheden. Daarna wordt direct verwezen naar een andere afdeling die gaat over toezicht en controle. De focus ligt dus meer op het gegeven dat het systeem moet werken in plaats van een ieder op de hoogte stellen van de inhoudelijke elementen van het systeem. Vanuit een privacy perspectief is het belangrijk dat medewerkers de risico's van het werken met gevoelige data kunnen inschatten en dat is gecommuniceerd hoe moet worden omgegaan met bepaalde situaties.

Door te concentreren op het thema sensitivity to operations van het High Reliability Organization perspectief van Weick, Sutcliffe & Obstfeld (2008) kan privacy worden bevorderd in de bedrijfsvoering van het LSP. Wanneer inzichtelijk is gemaakt hoe het systeem in elkaar zit, kan worden overgegaan tot het analyseren van de beste manier om met het systeem om te gaan. Ondertussen kan worden doorgegaan met het aanbrengen van de juiste focus en inzichten. Dit kan onder andere door het stimuleren van het vergaren van kennis, maar het kan ook gedeeltelijk worden opgelegd door het invoeren van beleid. Door middel van het aanscherpen van het belang van het systeem en de mogelijke consequenties die handelingen hebben voor patiënten kan het systeem in de juiste context worden geplaatst en kunnen verantwoordelijkheden worden verduidelijkt.

4.4 Commitment to resilience

De focus bij het thema 'commitment to resilience' ligt op het vermogen om met onverwachte gevaren te kunnen omgaan. Hierbij is het belangrijk om te erkennen dat betrouwbaarheid niet wordt bevorderd door onveranderlijkheid, maar juist door variatie. Om ervoor te zorgen dat positief kan worden teruggekeerd naar de aangeboden service, zal een organisatie de ontstane spanning moeten absorberen, moeten leren van de ongewenste gebeurtenissen en moeten groeien uit

eerdere ervaringen. Voorafgaand aan de analyse is in paragraaf 3.3.4 geconcludeerd dat de privacy thema's beleid, kennis en systeemveiligheid worden geraakt. Deze thema's worden nu achtereenvolgens behandeld.

4.4.1 Beleid

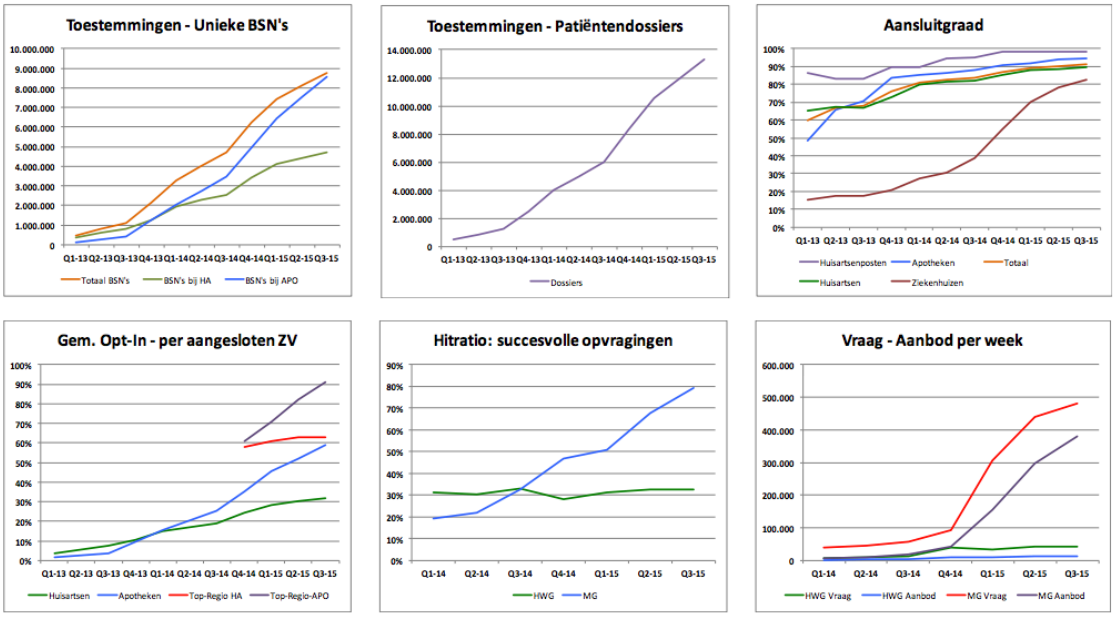
Beleid komt naar voren in de strategische optekening van het EPD en het LSP. Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) heeft invulling aan het EPD proberen te geven vanuit de doelstelling: '*het geïntegreerd en elektronisch toegankelijk maken van (onderdelen) van het patiëntendossier, onafhankelijk van plaats en tijd, met het oog op patiëntgerichte zorg'.* VWS kwam in april 2008 met een stappenplan Landelijke invoering Elektronisch Patiëntendossier (EPD) waarin werd gesteld dat de noodzakelijke voorbereidingen voor de landelijke invoering van de eerste twee toepassingen van het EPD – de uitwisseling van medicatiegegevens en huisartswaarneemgegevens – nagenoeg waren afgerond, waardoor naar verwachting in september 2008 kon worden gestart met de landelijke invoering (VWS, 2008) . Om de implementatie zo goed mogelijk te laten verlopen is een aantal voorwaarden opgesteld, te weten: (1) de praktijkervaringen in de koploperregio's laten zien dat de gegevensuitwisselingen goed werken en dat kinderziekten zijn opgelost, of op korte termijn worden opgelost; (2) een audit op de centrale voorzieningen geeft aan dat deze voorzieningen gereed zijn voor invoering en gebruik op landelijke schaal; (3) de Wet gebruik BSN in de zorg (Wbsn-z) is in werking getreden; (4) een plan voor de voorlichting aan zorgconsumenten op basis van 'geïnformeerde toestemming' kan worden uitgevoerd; (5) zorgaanbieders kunnen in aanmerking komen voor een financiële vergoeding vanwege de aansluiting op het landelijk schakelpunt (LSP); (6) zorgaanbieders kunnen rekenen op adequate voorlichting en ondersteuning (VWS, 2008). Na het voldoen aan deze voorwaarden werd geconcentreerd op elementen betreffende planning en afstemming met ICT-leveranciers, planning van regionale samenwerkingsverbanden van zorgaanbieders en planning en monitoring (VWS, 2008). Hoewel er duidelijke procedures en planningsafspraken zijn gemaakt vanuit het ministerie VWS, heeft de Eerste Kamer uiteindelijk toch besloten het vertrouwen in het EPD-systeem van dat moment op te zeggen, omdat het onvoldoende betrouwbaar en veilig zou zijn.

In 2012 is een onderzoek gepubliceerd door de Nederlandse School voor Openbaar Bestuur. Het onderzoek betreft een evaluatie van de cruciale momenten in het EPD besluitvormingsproces en de leerpunten voor ICT-trajecten in de zorgsector (NSOB, 2012). Het VWS heeft hun eigen beleidsstrategie omschreven als 'faciliteren, stimuleren en wettelijk verankeren'. De publicatie van het NSOB beargumenteert dat in de praktijk is vast te stellen dat het ministerie vooral gericht is geweest op de realisatie van het EPD en dat dit is opgevat als een planmatig af te wikkelen proces. Achteraf gezien lijkt het erop dat de praktijk zich minder heeft laten herleiden naar een vooraf vastgesteld en bedacht gegeven. Een emergente strategie is in dat geval meer toepasselijk, waarbij tijdens het proces aanpassingen aan de strategie kunnen worden verricht, wat daardoor meer inspeelt op de actualiteit.

Wat betreft het LSP, geeft het VZVZ aan dat in de periode van 2012 – 2015 de focus lag op het in gebruik nemen van de landelijke zorginfrastructuur en het inregelen van de bijbehorende governance (VZVZ, 2015). In het businessplan 'Gebruik landelijke zorginfrastructuur 2016 – 2020' is opgenomen dat deze periode in het teken zal staan van het intensiveren van het gebruik van de infrastructuur en de ontwikkeling van nieuwe functionaliteiten, voorzieningen en nieuwe gebruikers (VZVZ, 2015). Om de rol te definiëren en te verhelderen die de landelijke zorginfrastructuur wil hebben bij gegevensuitwisseling in de zorgsector is een uitgebreide SWOT-analyse uitgevoerd. In de SWOT-analyse zijn kansen, bedreigingen, sterktes, kwetsbaarheden, succesfactoren, barrières en risico's beschreven. De uitkomst hiervan is: '*een drempelloos gebruik van de infrastructuur over de gehele keten is de leidraad voor alles wat we doen*' (VZVZ, 2015). Het gebruik van de beschikbare basisfunctionaliteiten wordt voorop gesteld. Hierbij wordt onderkent dat het gebruik en de stabiliteit van de gehele LSP-keten nog op te lossen punten kent, de behoefte aan gegevens en functionaliteiten verder toeneemt en dat de LSP-keten meer kan bijdragen aan medicatiebewaking en -verificatie. Daarnaast staan de gebruikers centraal, vormen de regio's ankerpunten en is een vertrouwensmodel actief bij de coördinatie van de keten (VZVZ, 2015). Om aan de verwachtingen te blijven voldoen is focus op research, ontwikkeling en innovatie van belang, en moet de organisatie continu worden geprofessionaliseerd. Deze ingezette koers zorgt voor een tweedelige focus van VZVZ. Ten eerste zal de ingeslagen weg

moeten worden voortgezet ter realisatie van een optimaal gebruik, via een robuuste beheerorganisatie met betrekking tot techniek, architectuur en gebruikersondersteuning. De tweede focus omvat het innoveren en verder ontwikkelen op basis van de trends en ontwikkelingen voorkomend uit de behoeftes die in de zorgsector bestaan of ontstaan (VZVZ, 2015). Er is gedefinieerd dat deze twee aspecten elkaar niet mogen belemmeren in prioriteit en bemensing, maar synergetisch moeten worden ingevuld.

In het document wordt aangehaald dat inmiddels een fundament voor veilige uitwisseling van medische gegevens is gelegd. Dit is te danken aan de hoeveelheid energie die is gestoken in het realiseren van aansluitingen, toestemmingen en basisfunctionaliteiten. Volgens het VZVZ kan worden geconcludeerd dat op alle fronten een duidelijke voortgang is bereikt, met name op essentiële onderdelen voor breed gebruik van de landelijke zorginfrastructuur voor medische gegevensuitwisseling. Dit hebben zij als volgt schematisch weergeven:



Bron: Businessplan 'Gebruik landelijke zorginfrastructuur 2016 – 2020'.

4.4.2 Kennis

Kennis bij commitment to resilience betreft het basisniveau van kennis van medewerkers en het lerend vermogen van gebeurtenissen. In 2018 heeft de VZVZ het rapport 'Effecten en baten gebruik zorginfrastructuur' gepubliceerd, waarin wordt gesteld dat het LSP een belangrijk hulpmiddel is geworden voor

gegevensuitwisseling in de Nederlandse gezondheidszorg (ICT&health, 2018). Metingen in 2015 verschillen duidelijk van metingen in 2017 waarbij een significante toename in uitwisseling kan worden geconstateerd. Dit komt mede door een stijging in het aantal aangesloten huisartsenpraktijken en apotheken en meer bewustwording van het aspect omtrent het expliciet verlenen van toestemming. Daarnaast zijn beduidend meer medicatiegegevens opgevraagd. Echter blijkt uit onderzoek van het Radar Testpanel dat een meerderheid van de 35.000 ondervraagde leden niet weet dat het LSP is ingevoerd (ZorgNu, 2017). Opmerkelijk is dat mensen aangeven niet te weten of ze wel of niet op het systeem zijn aangesloten en dat nauwelijks kan worden aangegeven wat het LSP precies inhoudt. Dit soort onderzoeken suggereren dat een kloof bestaat tussen enerzijds de intenties en percepties van de beleidsmakers en -uitvoerders en anderzijds de patiënten waarvan de medische gegevens kunnen worden ingezien via het LSP.

Respondent 7 geeft aan wel eens een incident te hebben meegemaakt. De situatie deed zich voor waarin een brief naar het verkeerde adres is verstuurd door een verschrijving in het adres. In de brief stonden beperkte details, maar wel gegevens waaraan kon worden afgeleid dat de betreffende patiënt een bepaalde ziekte heeft. De fout is achterhaald doordat de verkeerd geadresseerde persoon die de brief had gekregen, had gebeld om hiervan melding te maken. Door de medisch specialisten is toen verzocht om de brief te verbranden. Daarnaast is de daadwerkelijke patiënt in kwestie ingelicht over het voorval. Respondent 7 geeft aan dat prioriteit werd gegeven aan het zorgvuldig en transparant afhandelen van het incident. Na het contact met de betrokkenen is een melding opgemaakt in het logboek, waarin de datalekken en beveiligingsincidenten worden bijgehouden. De medisch specialist geeft aan dat dit een formulier betreft dat wordt opgestuurd naar een andere afdeling. Die interne afdeling verwerkt de melding en zorgt voor de opvolging. Vanaf het moment dat de melding is verstuurd kan een melder niet meer bij de opgegeven informatie. Wanneer de afdeling na de opvolging van het incident concludeert dat lering kan en moet worden getrokken uit het incident, worden medewerkers via artikelen op het interne netwerk op de hoogte gesteld van de veranderde procedures.

4.4.3 Systeemveiligheid

De systeemveiligheid in relatie tot commitment to resilience gaat in op de mogelijkheden om terug te keren naar een eerdere staat van het systeem, nadat bijvoorbeeld een incident zich heeft voorgedaan. VZVZ heeft bij de optekening van het aansluitbeleid vermeld dat patiëntendossiers kunnen worden opgeschoond (VZVZ, 2019a). Hierbij wordt benadrukt dat een zorginstelling die is aangesloten op het LSP moet zorgdragen voor een eenduidige en goede registratie van de patiëntendossiers. Indien noodzakelijk, zullen bestanden moeten worden opgeschoond zodat de gegevens die worden uitgewisseld volledig en juist worden bevonden. Daarnaast wordt benadrukt dat huisartsen met de opbouw en registratie in dossiers de ADEPD-richtlijn volgen voor een optimale informatie-uitwisseling (VZVZ, 2019a). ADEPD staat voor Adequate Dossiervorming met het Elektronisch PatiëntenDossier (NHG, 2019). Het Nederlands Huisartsen Genootschap (NHG) heeft de ADEPD-richtlijn vormgegeven en doet onder andere onderzoek naar de functie van het EPD, de maatschappelijke acceptatie van het systeem en de veranderende rol als gevolg van ontwikkelingen. Ook wordt veel aandacht besteed aan de plaats en rechten van patiënten. Zo wordt benadrukt dat de patiënt de regie heeft over zijn zorg en dat de patiënt een actieve actor en een gelijkwaardige gesprekspartner vormt van de verschillende zorgverleners waarmee hij te maken heeft (NHG, 2019). Daarnaast wordt aangegeven dat de ontwikkeling van Persoonlijke gezondheidsomgevingen (PGO) impact heeft op het EPD en de verslaglegging in het algemeen. In een PGO is het mogelijk dat een patiënt dossierinformatie van meerdere zorgverleners kan inzien, gebruiken en eigen gegevens kan verzamelen en vastleggen (NHG, 2019). Het NHG geeft aan dat een toekomstige ontwikkeling zou kunnen zijn dat patiënten gegevens vastleggen in hun PGO en deze naar hun huisarts opsturen. Dit komt overeen met het perspectief van Respondent 6, uit de categorie IT-auditor en privacy specialist:

"*Ik vind dat de gegevens bij mij horen. Dus ik vind dat die gegevens eigenlijk ergens bij mij onder mijn beheer moeten vallen. En ik bepaal of iemand daartoe toegang heeft of niet. Dat is mijn idee en misschien moet er ergens een noodknop zitten, dat*

als ik niet meer in staat ben om dat te regelen, dat er dan een gecontroleerde toegang is voor noodgevallen." – Respondent 6.

Bovenstaand citaat raakt de discussie over welke van deze informatie in het EPD van de zorgverleners moeten worden opgeslagen. Daarover zullen afspraken moeten worden gemaakt. Vragen die daarbij spelen zijn: over welke informatie gaat het? Welke informatie is nodig voor goede zorg? Wat moet daarvan in het EPD terechtkomen? Moeten hierover landelijke afspraken of juist individuele (persoonsgerichte) afspraken worden gemaakt? Op dit moment is het nog onduidelijk hoe deze zaken de omgang met het EPD zullen beïnvloeden (NHG, 2019). Het NHG vindt het een kwestie van gezamenlijk kleine stappen ondernemen en steeds opnieuw het belang van bepaalde informatie voor de zorg te formuleren. Het uitgangspunt moet daarbij zijn: omdat het nodig is en niet alleen maar omdat het kan (NHG, 2019).

Naast het focussen op de benodigdheden in plaats van op mogelijkheden is van belang aandacht te besteden aan de back-up en herstelmogelijkheden van het systeem. Wanneer het systeem wordt aangetast, is het noodzakelijk dat hiernaar kan worden teruggekeerd zonder dat er fouten zitten in de medische gegevens van patiënten. De verantwoordelijkheden hiervoor zijn gesplitst tussen VZVZ en de aangesloten zorginstellingen. VZVZ is de verantwoordelijke partij voor het beschikbaar stellen van de infrastructuur en de verbindingen tussen het LSP en de zorginstellingen, waardoor een veilige en betrouwbare uitwisseling van medische gegevens kan plaatsvinden. De zorginstellingen zijn zelf verantwoordelijk voor de juistheid en de volledigheid van de medische dossiers. Fouten in medische gegevens zullen dus worden teruggeleid naar de zorginstellingen.

4.4.4 Subconclusie

Door het focussen op commitment to resilience kan in geval van datalekken of beveiligingsincidenten positief worden teruggekeerd naar de aangeboden service. Dit wordt mogelijk gemaakt door het absorberen van ontstane spanningen, het leren van de ongewenste gebeurtenissen en het groeien uit eerdere ervaringen. Door deze

focus kan steeds beter worden omgegaan met risicovolle situaties en kan met meer zekerheid snel worden geacteerd op voorkomende gebeurtenissen. De eerdere ervaringen kunnen dan worden gebruikt voor een betere voorbereiding op toekomstige situaties.

Een eerste stap is het vormgeven van beleid. Hierin worden strategische keuzes vastgelegd. Wanneer een incident zich voordoet bij het LSP zal altijd worden gekozen voor het zo snel mogelijk oplossen van de fout in plaats van een directe focus op lessen voor de toekomst. Er wordt geen nadruk gelegd op het uitbreiden van de technische faciliteiten. Dit is te verklaren vanuit het gegeven dat een zorginstelling wel of niet voldoet aan de vereisten om te mogen aansluiten op het systeem. Er bestaat geen grijs gebied, doordat exacte vereisten zijn opgesteld. Het uitbreiden van (algemene) kennis wordt daarentegen wel benadrukt. VZVZ stelt middelen beschikbaar die focussen op de omgang met het LSP systeem. Verder zijn het inschatten van mogelijke risico's, het voorbereiden op toekomstige scenario's en de opvolging van incidenten gedecentraliseerd naar de verschillende zorginstellingen. Op het niveau van medische dossiers is het begrijpelijk dat de zorginstellingen zelf verantwoordelijk zijn voor de juistheid en volledigheid. Echter blijft VZVZ verantwoordelijk voor het verzorgen van een veilige en betrouwbare infrastructuur. Uit de beschikbare documenten is op te maken dat wordt gefocust op de verschillende bepalingen vanuit wet- en regelgeving en geldende normen en standaarden. Maar de manier waarop kan worden teruggekeerd naar een werkend systeem nadat datalekken en beveiligingsincidenten zicht hebben voorgedaan, blijft uit. Het vertrouwen in het huidige systeem is echter geen garantie voor het blijven behouden van een veilig en betrouwbaar systeem.

Het thema commitment to resilience van het High Reliability Organization perspectief van Weick, Sutcliffe & Obstfeld (2008) komt tot op heden gematigd naar voren in de bedrijfsvoering van het LSP. Door meer focus op dit thema kan de privacy van het systeem worden versterkt. Bij de bedrijfsvoering van het LSP heerst de tendens dat het perfect ingericht moet zijn, waarin geen ruimte bestaat voor het maken van fouten. Dit wordt ook benadrukt in het businessplan waarin wordt gesteld dat inmiddels een fundament voor veilige uitwisseling van medische gegevens is gelegd. Uiteindelijk kan geen volledige garantie worden gewaarborgd.

Het lijkt een kwestie van tijd voordat incidenten zich voordoen. De gelaagdheid die aanwezig is bij zorginstellingen vermoeilijkt het oplossen van incidenten. Ook de gesplitste verantwoordelijkheden in back-up en herstelprocedures kunnen het moeilijker maken om terug te keren naar een veilig en betrouwbaar systeem.

4.5 Underspecification of structures

Bij het thema 'underspecification of structures' ligt de focus op de rol van ordelijke procedures. Ordelijke protocollen of procedures kunnen zowel een bevorderlijke als een belemmerende werking hebben. Indien niet altijd wordt gereageerd vanuit protocollen en procedures en flexibiliteit een kans wordt gegeven, kan meer worden gereageerd vanuit deskundigheid ongeacht de laag waarin de medewerker in een hiërarchie zou worden geplaatst. Door het creëren van erkenning kunnen medewerkers zich meer betrokken en verantwoordelijk voelen om een bijdrage te leveren aan het geheel. Voorafgaand aan de analyse in paragraaf 3.3.5 is geconcludeerd dat de privacy thema's beleid, authenticatie en governance worden geraakt. Deze thema's worden achtereenvolgend behandeld.

4.5.1 Beleid

Een ordelijke procedure is een breed concept en kan worden geïnterpreteerd vanuit verschillende lagen. Procedures kunnen worden opgelegd vanuit landelijke politiek (i.e.) de overheid) of op organisatieniveau. Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) ziet grote kansen voor elektronische gegevensuitwisseling in de zorg. Zij stellen dat zorgverleners beter, sneller en met minder fouten de juiste gegevens over patiënten kunnen uitwisselen en gebruiken bij een behandeling (VWS, 2017). Daarnaast krijgt een burger met elektronische gegevensuitwisseling de regie over het zelf bijhouden en delen van gegevens met huisartsen, ziekenhuizen en behandelaars. Maar het VWS erkent ook dat deze kansen het belang van de waarborging van veiligheid van persoonlijke gegevens versterken. In mei 2017 heeft het VWS 'de Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg' gepubliceerd. In deze wet wordt uitgelegd dat bestaande wetgeving – de Wet bescherming persoonsgegevens en de Wet

Geneeskundige Behandelovereenkomst – zorgverleners verplicht om zorgvuldig met medische gegevens om te gaan (VWS, 2017). Maar deze wetten gaan niet specifiek in op elektronische gegevenswisseling, terwijl de Wet cliëntenrechten bij elektronische verwerking van gegevens wel hierop ingaat.

De Wet cliëntenrechten bij elektronische verwerking van gegevens stelt voorwaarden waarvoor medische gegevens veilig en elektronisch kunnen worden uitgewisseld en ingezien (VWS, 2017). Daarbij komen ook de rechten van cliënten aan bod. Vanaf juli 2017 wordt aan cliënten gevraagd of ze akkoord gaan met raadplegingen van hun medische gegevens door andere zorgverleners. Het is voorgenomen dat vanaf juli 2020 cliënten kunnen aangeven welke gegevens door welke (categorieën van) zorgverleners mogen worden ingezien (VWS, 2017). Hierbij gaat het uitsluitend over behandelrelaties en blijft de voorwaarde dat het noodzakelijk moet zijn voor een juiste behandeling geldig. Onder andere zorgverzekeraars, keuringsartsen, bedrijfsartsen en verzekeringsartsen wordt toegang tot medische gegevens van het LSP geweigerd.

Vanuit het perspectief van cliënten geldt het volgende:

Huidige situatie:	Vanaf 1 juli 2017 ook:	Vanaf 1 juli 2020 ook:
Het geven van toestemming voor het uitwisselen van gegevens.		Het geven van toestemming om alle of bepaalde gegevens voor inzage beschikbaar te stellen aan alle of aan bepaalde zorgverleners met wie een behandelrelatie van kracht is (of krijgt).
Het krijgen van een afschrift van het eigen medisch dossier.		Het (kosteloos) krijgen van een elektronisch afschrift van het eigen medisch dossier.
Het inzicht krijgen in het eigen medisch dossier.		Het (kosteloos) elektronisch inzage krijgen in het eigen medisch dossier.
Het (laten) toevoegen, verwijderen, vernietigen of afschermen van medische gegevens.		
Op verzoek heeft een cliënt recht op een overzicht van de logging: categorieën van gegevens die zijn verwerkt, de ontvangers of categorieën van ontvangers die gegevens en informatie over de herkomst van de gegevens.	Op verzoek krijgt de cliënt een overzicht van instanties die bepaalde informatie in een elektronisch uitwisselingssysteem beschikbaar heeft gesteld en op welke datum en wie informatie heeft ingezien of opgevraagd en op welke datum.	

Bron: VWS - Elektronische gegevensuitwisseling in de zorg.

Inmiddels is de Wet bescherming persoonsgegevens opgegaan in de AVG, een Europese wetgeving die ook in Nederland van kracht is. Ook de AVG kan worden gezien als een ordelijke procedure. Organisaties – zo ook zorginstellingen – worden verplicht om verzoeken van betrokkenen in overweging te nemen wanneer daarom wordt gevraagd. Zo heeft een patiënt volgens artikelen 15 t/m 20 recht op inzage, recht op rectificatie, recht op vergetelheid, recht op beperking van verwerking, recht op de kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking en het recht op overdraagbaarheid van gegevens. Daarnaast wordt verplicht dat een persoon vooraf toestemming moet geven wanneer persoonsgegevens worden verwerkt. Deze toestemming zal te allen tijde moeten kunnen worden ingetrokken, de zogenoemde 'opt-out functie' (EUR-Lex, 2016).

Bij het Landelijk Schakelpunt moet ook specifiek toestemming worden gegeven voordat het BSN wordt opgenomen in de verwijsindex van het systeem. Patiënten ervaren dit als volgt:

"*Ik ben niet goed geïnformeerd. Ze hadden mij daar iets meer over kunnen vertellen en over welk beperkt kringetje het is, dat heb ik zelf uitgezocht. Je geeft gewoon toestemming en dan wordt het gelijk in de computer gezet. Ik heb zelf ja gezegd, maar dat komt omdat je dan in een traject zit. Je gezondheid gaat voor alles, dus je geeft toe. Het gaat om je gezondheid en later ga je dan misschien eens denken ja had het allemaal wel nodig geweest?"* – Respondent 1.

Er bestaan informatiefolders waarbij schriftelijk toestemming kan worden gegeven. Echter wordt in de praktijk, zo blijkt uit de interviews, vaak mondeling toestemming gevraagd tijdens een bezoek of moet de toestemming direct op het inschrijfformulier worden aangevinkt. Respondent 2 heeft de verlening van toestemming op een onprettige manier ervaren:

"*Ik ben recentelijk verhuisd, dus ik had een nieuwe dokter nodig. En toen zeiden ze van ja we hebben wel je medische gegevens nodig. Ze stelden wel een keuze, maar*

als ik het er niet mee eens was dat mijn gegevens overgingen dan had ik geen nieuwe dokter. Ik wilde eerst wat onderzoek verrichten, toen heb ik het eigenlijk en beetje links laten liggen, en daarna hebben ze me nog een paar keer gebeld dat ze toch echt die gegevens nodig hadden." - Respondent 2.

Het zorgelijke aan bovengenoemde situatie is dat toestemming niet vrijblijvend is, terwijl dat wel zo zou moeten zijn. Patiënten hebben te allen tijde het recht om te weigeren, dan wel eerder verleende toestemming terug te trekken. Deze ervaringen illustreren de mogelijke consequenties als toestemming wordt geweigerd, namelijk dat geen juiste zorg wordt verleend.

4.5.2 Authenticatie

Authenticatie bij het thema 'Underspecification of structures' omvat verschillende elementen. In de eerste plaats gaat dit thema over de vraag hoe een zorginstelling –bijvoorbeeld een ziekenhuis, een apotheek, of een huisartsenpost – op het digitale systeem kan worden aangesloten. Daarnaast betreft het ook hoe de medewerkers die het systeem raadplegen voor hun werkzaamheden toegang verkrijgen tot het systeem.

Het VZVZ heeft opgetekend op welke manier kan worden aangesloten op het Landelijk Schakelpunt, die bestaat uit drie stappen (VZVZ, 2019a). De eerste stap is dat sprake moet zijn van een Goed Beheerd Zorgsysteem (GBZ). Dit houdt in dat het informatiezorgsysteem moet voldoen aan een programma van technische en organisatorische eisen, waardoor een goede en veilige uitwisseling van medische gegevens kan plaatsvinden. Een organisatie stelt een GBZ-beheerder aan – welke intern of extern kan zijn – die het technisch beheer verzorgt en waarborgt dat het systeem te allen tijde blijft voldoen aan de beveiligingseisen voor gegevensuitwisseling met andere GBZ'en via het LSP. Deze beheerder is daarnaast ook de contactpersoon in situaties van verstoringen. De lijst van geaccepteerde zorginformatiesystemen is opgenomen in Bijlage 2. De tweede stap omvat een Goed Beheerd Zorgnetwerk (GZN). Dit netwerk zal zorgen voor een goede en veilige communicatie tussen het GBZ en het Landelijk Schakelpunt (VZVZ, 2019a). De lijst van geaccepteerde zorgnetwerken is opgenomen in Bijlage 3. Na deze twee stappen

volgt de derde stap: de UZI-middelen. Deze middelen omvatten het UZI-servercertificaat en een UZI-zorgverlenerspas. Het certificaat heeft als functie om de elektronische identiteit van het systeem te bevestigen wanneer de zorgaanbieder inlogt bij het LSP. De pas gaat in op authenticatie van een zorgverlener door, in combinatie met de bijbehorende pincode, de identiteit van de zorgverlener te achterhalen. Autorisatie speelt hierbij ook een rol en omvat de specifieke gebruiksrechten. De pas bevat informatie over welke gegevens kunnen worden geraadpleegd (VZVZ, 2019a). De hierboven genoemde stappen kunnen allemaal online worden ingediend. De aansluit assistent helpt bij het doorlopen van het proces, waarbij ook documentatie wordt opgevraagd. Het risico van een digitaal aansluitbeleid is de mogelijkheid van fraude. Het aansluitbeleid tracht het risico te mitigeren door de mogelijkheid van controle door VZVZ op ieder gewenst moment. Aangesloten zorginstellingen dienen dus te allen tijde te kunnen aantonen dat zij voldoen aan de vereisten en documentatie op orde te hebben.

Naast het gegeven dat het systeem van een zorginstelling toegang moet verkrijgen tot de infrastructuur van het Landelijk Schakelpunt, dienen medewerkers op individueel niveau ook toegang te verkrijgen tot het systeem. De autorisaties die hierbij van kracht zijn – de specifieke rechtensets – kunnen verschillen van persoon tot persoon. Uit de interviews met de respondenten die classificeren als patiënten, blijkt dat men verschillend denkt over authenticatie en autorisaties.

"*Wat ik vervelend vind is dat er in mijn omgeving mensen zijn die als medisch specialist werken en die eventueel in mijn dossier kunnen komen, dat vind ik niet fijn."* – Respondent 1.

"*Er zijn beroepsgeheimen, waar mensen zich aan moeten houden. Maar het is wel een klein iets in mijn gedachten van oké, het kan dat mensen mijn gegevens heel makkelijk kunnen inzien en de risico's zitten er wel."* – Respondent 2.

Voor de medisch specialisten zijn de autorisaties een vanzelfsprekendheid. Wanneer zij in dienst komen, ontvangen zij een contract, een pas en een account

met bijbehorende inloggegevens. Afhankelijk van een bepaalde functie worden bepaalde rechten toegekend aan het account. Maar een overzicht van functies met bijbehorende rechten ontbreekt. Hierdoor worden niet direct vergelijkingen gemaakt tussen verschillende personen, terwijl deze wel degelijk bestaan. Echter heerst bij de medisch specialisten vertrouwen en acceptatie dat de juiste rechten zijn toegekend, waardoor zij hun werk naar behoren kunnen uitvoeren.

4.5.3 Governance

Wanneer het gaat om de governance bij underspecification of structures wordt onder andere gekeken naar het herzien van procedures. Hierbij moet continu worden gemonitord of het systeem daadwerkelijk voldoende veilig en betrouwbaar is voor de uitwisseling van medische gegevens zoals het beoogt te zijn. Dit omvat zowel de aansluitingsprocedure voor nieuwe zorginstellingen, maar ook de wijze van raadpleging binnen het systeem en de technische en organisatorische beveiligingsmaatregelen die worden genomen.

Het LSP maakt gebruik van het BSN als identificatiemethode. Wanneer een patiënt toestemming geeft om zijn medische gegevens inzichtelijk te maken via het LSP, dan wordt feitelijk toestemming gegeven om het BSN op te nemen in de verwijsindex van het systeem (Volg Je Zorg, 2019a). Uit de interviews met zowel de patiënten als de IT-auditors en privacy specialisten komt naar voren dat dit niet het meest betrouwbaar wordt gevoeld of geacht. Alle respondenten classificerend als patiënten gaven aan het niet prettig te vinden dat het BSN wordt gebruikt:

"*Ik wist niet dat medische gegevens worden bekeken aan de hand van BSN, en vind het een slechte zaak. Je denkt redelijk beschermd te zijn en dat blijkt dus niet zo te zijn."* – Respondent 1.

"*Een ander nummer zou misschien wel veiliger zijn, misschien dat je dan ook niet het idee hebt dat iedereen zomaar alles van jouw hele leven kan inzien, of erbij kan komen. Met BSN kan iemand zo mijn identiteit overnemen."* – Respondent 2.

"*Over het BSN-nummer hoor je steeds meer, ook dat er steeds meer mee kan, zoals allerlei gegevens opvragen. Mensen weten bijvoorbeeld waar ik woon, nou dat vind ik toch best wel heftig; dat onbekende mensen die niks met mij te maken hebben of van mij nodig hebben, dingen weten over mij."* – Respondent 3.

De groep patiënten geeft aan risico's te zien in het gebruik van BSN's. Dit kan ook worden verklaard vanuit het gegeven dat het BSN een uniek nummer is dat wordt gekoppeld aan een persoon. Het nummer is niet vervangbaar en blijft van iemand voor de rest van zijn leven. Dit maakt het speciaal en impliceert dat mensen voorzichtig met het nummer moeten omgaan of het zelfs geheim dienen te houden. Alle respondenten staan open voor een andere identificatiemethode, zoals een nummer dat alleen voor medische gegevens wordt gebruikt. Dit wordt niet als extra last ervaren, maar juist als extra bescherming en veiligheid. Vanuit de respondenten die kwalificeren als IT-auditor en privacy specialisten worden ook kritische kanttekeningen bij het BSN geplaatst:

"*Het BSN is bijzonder slecht gekozen. Eigenlijk is het als een primaire sleutel bedacht bij de overheid, om te zorgen dat alle informatie aan 1 burger kan hangen. In de zorg snap ik het ook, want je wilt natuurlijk zorgen dat je de juiste persoon hebt. Ik je zou eigenlijk zeggen maak een tweede nummer eraan, wat wel gekoppeld is aan het BSN, maar dat het een zorgnummer is."* – Respondent 4.

"*Het is heel vreemd dat BSN wordt gebruikt voor identificatie, omdat je daarmee het risico introduceert dat je al deze data op basis van BSN ook met andere gegevensverwerkingen kan combineren die niets met de zorg te maken hebben. Naar mijn idee, als je zoiets doet als dit dan zou je eigenlijk een sectoraal identificatienummer moeten hebben."* – Respondent 6.

Respondent 5 heeft een andere mening: "*Als ik je BSN weet dan kan ik daar wat mee. Aan de ene kant kan het heel veilig zijn, maar wat ik wel bij een hele boel dingen merk is dat we het heel erg moeilijk maken. Het moet eigenlijk leuk zijn om in te loggen in een applicatie. Bij een hele boel dingen werpen we een hele boel*

barrières op waardoor iedereen denkt van laat maar. En dat maakt het soms ook wel weer risicovol. "

Door een digitaal systeem zo effectief en efficiënt mogelijk in te richten – en met name te focussen op de inrichting vanuit een juridisch perspectief – kan zijn voorgekomen dat minder aandacht is besteed aan de risico's van het gebruiken van het BSN en het gevoel dat dit geeft aan de patiënten die het nummer ('verplicht') moeten laten opnemen, doordat zij niet zonder medische zorg kunnen.

4.5.4 Subconclusie

Door middel van het concentreren op underspecification of structures kan flexibel worden omgegaan met de processen in een organisatie. Door niet altijd te reageren vanuit protocollen en procedures kan meer worden gereageerd vanuit deskundigheid, ongeacht de laag waarin de medewerker in een hiërarchie zou worden geplaatst. Door het creëren van erkenning kunnen medewerkers zich meer betrokken en verantwoordelijk voelen om een bijdrage te leveren. De medewerkers worden op deze manier gestimuleerd om oplossingsgericht te werk te gaan. Dit verhoogt echter ook het risico op het ontstaan van verschillende behandelingen van gelijke situaties.

Een ordelijke procedure is een breed concept en kan worden ingesteld vanuit verschillende lagen, zoals de landelijke politiek, een koepelorganisatie of een organisatie zelf. Bij het LSP wordt ook onderscheid gemaakt tussen het beleid vanuit de overheid, VZVZ en de zorginstellingen zelf. Eerder heeft de overheid zich teruggetrokken van het ontwerp van het EPD en voorwaarden gesteld voor het verder ontwikkelen van een soortgelijk systeem. Het VZVZ heeft een beleid opgesteld voor het reguleren van aansluitingen. Een organisatie zelf gaat vooral in op procedures en protocollen om werkzaamheden te stroomlijnen en gezamenlijke overeenstemming voor de behandeling van situaties te bereiken. Hierbij is weinig ruimte voor het nemen van eigen beslissingsbevoegdheden. Flexibiliteit komt tot uiting door het verwelkomen van feedback. Met een dergelijk systeem als het LSP is maar de vraag of flexibiliteit wenselijk is. Te veel ruimte kan ertoe leiden dat

medewerkers met eigen oplossingen komen, waardoor onoverzichtelijke situaties ontstaan en de meest passende manier van werken in het gedrang komt.

Een focus op het thema underspecification of structures van het High Reliability Organization perspectief van Weick, Sutcliffe & Obstfeld (2008) kan zowel een bevorderende als een belemmerende impact hebben op de bedrijfsvoering van het LSP en het garanderen van privacy. Dit komt door een spagaat in de werking van procedures en protocollen. Op het eerste gezicht lijkt het hanteren van een protocol of procedure bevorderlijk voor het op de juiste manier laten uitvoeren van werkzaamheden. Echter, er kunnen ook structurele fouten in de vooraf beschreven en vaststaande procedure zitten. Wanneer procedures niet regelmatig worden herzien en fouten in de procedure zijn opgetreden, zullen de fouten zich blijven herhalen. Privacy binnen het LSP kan vanuit dit thema worden bevorderd door regelmatige controle of het beleid nog steeds voldoet. Dit betreft het voldoen aan wet- en regelgeving maar ook de interne structuren die van kracht zijn binnen een zorginstelling.

4.6 Eindconclusie

In de voorgaande paragrafen zijn het ontwerp en de bedrijfsvoering van het Landelijk Schakelpunt geanalyseerd. Deze analyse is uitgevoerd aan de hand van het eerder opgestelde conceptueel kader waarin de kenmerken van het HRO-perspectief van Weick, Sutcliffe en Obstfeld (2008), namelijk (1) preoccupation with failure, (2) reluctance to simplify interpretations, (3) sensitivity to operations, (4) commitment to resilience, en (5) underspecification of structures, zijn gekoppeld aan de kenmerken die zijn geïdentificeerd vanuit de privacywetgeving, bestaande uit (1) beleid, (2) authenticatie, (3) kennis, (4) governance, en (5) systeemveiligheid. De analyses focussen zich op de beantwoording van de onderzoeksvraag: *In hoeverre kan de bedrijfsvoering van het Landelijk Schakelpunt (LSP) ten aanzien van privacy worden versterkt door toepassing van de High Reliability Organization (HRO) theorie van Weick, Sutcliffe & Obstfeld (2008)?*

De deelconclusies weergeven zowel thema's die kunnen worden herleid in de bedrijfsvoering van het LSP, als thema's waar nog veel van kan worden geleerd. Het thema preoccupation with failure komt niet scherp terug in het LSP-systeem. Dit is te wijten aan de focus op het voorkomen van fouten, in plaats van het gevoelig worden voor tekenen van mogelijke mislukkingen waardoor lerend vermogen kan worden uitgebreid. Uit de eerdere afwijzing van het EPD zijn wel degelijk lessen getrokken. Hierdoor herhalen fouten zich niet in het LSP en kan veiligheid en privacy worden gewaarborgd. Het thema reluctance to simplify interpretations kan het privacy element in de bedrijfsvoering van het LSP versterken. Het creëren van een technisch stabiel systeem is een noodzaak, maar daarnaast zal het systeem te allen tijde afhankelijk zijn van de menselijke besturing ervan. Het creëren van bewustzijn van medewerkers en het bewerkstelligen van coördinatie en overeenstemming over het belang van de geldende protocollen en procedures levert hieraan een positieve bijdrage. Het thema sensitivity to operations versterkt ook het privacy element in de bedrijfsvoering van het LSP. Wanneer inzichtelijk is gemaakt hoe het systeem in elkaar zit, kunnen strategische keuzes worden gemaakt en kan de beste omgang met het systeem worden bepaald. Vervolgens kan een beleid worden ingesteld en kunnen medewerkers worden gemotiveerd om kennis uit te breiden. De zorginstellingen zorgen voor het aanscherpen van het belang van het systeem en de mogelijke consequenties die handelingen hebben voor patiënten. Hierdoor weten medewerkers het systeem in de juiste context te plaatsen en zijn taken en verantwoordelijkheden duidelijk. Het thema commitment to resilience komt tot op heden gematigd naar voren in de bedrijfsvoering van het LSP, zodat bij toepassing van dit thema nog veel te winnen valt ten aanzien van privacy. Bij de bedrijfsvoering gaat de focus naar een perfecte inrichting van het systeem, waardoor ervan uit wordt gegaan dat ruimte voor het optreden van fouten nagenoeg ontbreekt. Vanuit privacy is het wenselijk dat zo veel mogelijk fouten worden voorkomen; tegelijkertijd lijkt dit een illusie. Het lijkt een kwestie van tijd voordat incidenten zich voordoen. Ook de gesplitste verantwoordelijkheden en de gelaagdheid die aanwezig is bij zorginstellingen vermoeilijken het oplossen van incidenten. Door dergelijk beleid wordt commitment to resilience zelfs belangrijker, zodat het vermogen om met onverwachte gevaren te kunnen omgaan wordt vergroot. Uit de analyse is gebleken

dat het thema underspecification of structures zowel een bevorderende als een belemmerende impact kan hebben op de bedrijfsvoering van het LSP en het garanderen van privacy. In eerste instantie lijkt het hanteren van een protocol of procedure bevorderlijk voor het op de juiste manier laten uitvoeren van werkzaamheden en het garanderen van privacy. Echter, er kunnen ook structurele fouten in de vooraf beschreven en vaststaande procedure zitten waardoor een protocol of procedure juist een belemmerende uitwerking heeft. Om privacy toch te blijven waarborgen, is het van belang dat het beleid en de procedures regelmatig worden herzien om te bepalen of het nog steeds voldoet. Het aansluitbeleid van VZVZ is een vaststaand protocol. De herziening van de procedures zal voornamelijk voorkomen bij de zorginstellingen zelf, doordat zij het lerende vermogen toepassen op (ongewenste) situaties die hebben plaatsgevonden. Concluderend komen de thema's preoccupation with failure en commitment to resilience nauwelijks naar voren in de bedrijfsvoering van het LSP. Daarentegen versterken de thema's reluctance to simplify interpretations en sensitivity to operations het privacy element. Het thema underspecification of structures heeft een tweeledige uitwerking met zowel een bevorderende als een belemmerende functie. Bij een gevoelig systeem, zoals het LSP, is essentieel dat niet alleen wordt gecommuniceerd *wat* er gebeurt, maar ook *waarom* het gebeurt.

5. Discussie en reflectie

In het voorgaande hoofdstuk is de analyse aan bod gekomen en is afgesloten met een conclusie zijnde de beantwoording van de centrale onderzoeksvraag van dit onderzoek. Dit hoofdstuk vormt de discussie en reflectie op de bevindingen. Allereerst wordt gereflecteerd op het conceptueel model. Vervolgens worden de effecten van de toepassing van het HRO-perspectief en beleidsaanpassingen behandeld. Tot slot wordt afgesloten met aanbevelingen voor toekomstig onderzoek.

5.1 Conceptueel model

Het conceptueel model dat centraal staat in dit onderzoek bestaat uit een koppeling tussen de concepten die zijn afgeleid van het HRO-perspectief van Weick, Sutcliffe & Obstfeld (2008) en concepten die zijn herleid uit privacywetgeving. Na een afweging tussen de verschillende invalshoeken is besloten dat dit onderzoek zal worden uitgevoerd aan de hand van het HRO-concept. De keuze voor dit perspectief is gemaakt omdat het ruimte biedt voor het ingaan op de technische middelen van een systeem. Daarnaast wordt ingegaan op de meer menselijke kant, wat wordt gerepresenteerd door het lerend vermogen en bewustzijn. Het LSP-systeem focust op het tot stand brengen van een beveiligde verbinding waarop verschillende aangesloten zorginstellingen medische data kunnen raadplegen in elkaars systemen.

Zoals eerder is aangehaald in het theoretisch kader, is er naast HRO een tweede stroming die zich richt op systeemveiligheid onder complexe omstandigheden; de Normal Accident Theory (NAT). HRO onderscheidt zich van NAT door te focussen op mogelijke fouten en mislukkingen. Deze fouten worden beschouwd als lessen voor toekomstige scenario's, waardoor betrouwbaarheid en procesverbetering kunnen worden gerealiseerd. Het NAT-perspectief beschouwt de ongelukken bij systemen als normaal en onvermijdelijk omdat ze niet kunnen worden voorkomen, ongeacht de effectiviteit van het beheer of het functioneren. Overeenkomsten tussen beide stromingen bestaan uit onder andere de focus op de sociale en organisatorische fundamenten van systeemveiligheid en de oorzaken, gevolgen en preventie van ongevallen. Desondanks kan HRO worden geïnterpreteerd vanuit optimisme en NAT vanuit pessimisme. Leveson et al. (2009)

concluderen dat waarschijnlijk sprake is van hogere ongevalspercentages bij complexe systemen, doordat de potentiële interacties in dergelijke systemen niet grondig kunnen worden gepland, begrepen, verwacht en bewaakt. Dit komt doordat een systeem theoretisch wordt opgetekend, terwijl interacties in de praktijk op een andere manier tot uiting komen. Complexe systemen worden vaak niet grondig getest en geanalyseerd voordat ze in gebruik worden genomen. Hierdoor is er meer kans op ongemerkte ontwerpfouten. Met het vormgeven van het LSP-systeem is geanticipeerd op de redenen voor afwijzing van het eerder voorgestelde EPD systeem. Omdat dit onderzoek is gefocust op het versterken van het privacy concept in de bedrijfsvoering van het LSP, is het HRO-perspectief meer bruikbaar bevonden dan het NAT-perspectief. Dit kan worden verklaard vanuit het gegeven dat HRO streeft naar een verbetering van het systeem door middel van het actief anticiperen op fouten. Daarentegen accepteert NAT dat fouten voorkomen, zonder een drang om hier lessen uit te trekken. Om deze reden is geconcludeerd dat het karakter van dit onderzoek beter aansluit bij het HRO-perspectief.

Niet alles van de onderzochte stroming komt even duidelijk naar voren in de bedrijfsvoering van het LSP. Dit is niet negatief ervaren, maar biedt juist kansen om hiervan te leren en de bedrijfsvoering aan te passen. De toepassing van de kenmerken van het HRO-perspectief en de concepten die zijn ontleend aan privacywetgeving, is bruikbaar bevonden. De combinatie biedt een weergave van onderwerpen waaraan veel aandacht is besteed bij de optekening van het LSP-systeem. Een voorbeeld hiervan is het actief toestemming verkrijgen van patiënten voordat medische gegevens beschikbaar worden gesteld voor het systeem. Een patiënt wordt geacht een vrije keuze te hebben zonder dat hier negatieve consequenties aan zijn verbonden. Daarnaast heeft het conceptueel model ook ruimte gegeven voor verbetering van het onderzochte object. Een voorbeeld hiervan is het verduidelijken van taken en verantwoordelijkheden. De individuele medewerkers hebben aangegeven nauwelijks op de hoogte te worden gebracht van de afbakening van systemen, waardoor uitgevoerde werkzaamheden in twijfel worden getrokken. Door het verbeteren van dit inzicht kan meer wederzijds begrip ontstaan. Het conceptueel model heeft een bijdrage geleverd aan het verduidelijken

van de verhoudingen in de bedrijfsvoering van het Landelijk Schakelpunt en benadrukt welke concepten van privacy kunnen worden versterkt.

5.2 Effecten en aanbevelingen

In de voorgaande paragraaf is geconcludeerd dat het conceptueel model van dit onderzoek een bijdrage heeft geleverd aan het verduidelijken van het privacy concept binnen de bedrijfsvoering van het Landelijk Schakelpunt. Naast het inzichtelijk maken van de huidige situatie kan het HRO-perspectief een positieve werking hebben op het verder versterken van privacy binnen de bedrijfsvoering. De toepassing van de elementen kan worden beschouwd als een SWOT-analyse. Een SWOT-analyse bestaat uit een opsomming van kansen en bedreigingen in de markt, waardoor sterktes en zwaktes van een organisatie kunnen worden geïdentificeerd. Door de jaren heen is de focus komen te liggen op privacy, zowel in de zorgsector als in andere sectoren. Het is voor patiënten belangrijker geworden om controle te hebben over hun eigen medische gegevens. Daarnaast is ook meer wet- en regelgeving ontwikkeld, waaraan organisaties moeten voldoen. Omdat het LSP-systeem gevoelige informatie betreft, is het noodzakelijk om de context van het systeem te verhelderen. Dit betreft zowel de technische kenmerken, de plaats die het systeem inneemt in de maatschappij en de besturing van het systeem dat afhankelijk is van menselijke factoren.

Deze combinatie kan ook worden teruggevonden in het HRO-perspectief van Weick, Sutcliffe en Obstfeld (2008). De toepassing van deze inzichten is bruikbaar voor het maken van een inschatting over de mate waarin het systeem voldoet aan privacy concepten. De uitkomst van de analyse van de kenmerken stelt dat nog veel kan worden geleerd van de HRO-principes om situationeel bewustzijn te creëren en uit te breiden. Dit situationele bewustzijn zou volgens de theorie leiden tot procesverbetering, waardoor een veilig en betrouwbaar systeem kan worden gerealiseerd. Het is echter vanuit het privacy perspectief niet wenselijk om ieder kenmerk van de HRO-theorie binnen de bedrijfsvoering te incorporeren. Dit is te verklaren vanuit het gegeven dat het systeem vertrouwelijke informatie betreft. De effecten van het realiseren van de HRO-principes in de bedrijfsvoering van het LSP kunnen groot zijn; soms zelfs te groot. De prioriteit moet worden gegeven aan het

vinden van een balans tussen het lerend vermogen van fouten zonder dat privacy daarbij in het gedrang komt.

Om te sturen naar het vinden van deze balans is een aantal aanbevelingen opgesteld. Door de gevoeligheid van de data is het belangrijk dat zo min mogelijk fouten worden gemaakt. De meest aannemelijke fouten die zullen worden gemaakt in het LSP-systeem, raken altijd de medische gegevens van patiënten. De huidige periode wordt gekenmerkt door een focus op privacy en controle op eigen medische gegevens. Het gevoelig worden voor fouten is hierdoor in de praktijk onwenselijk. Echter door de IT-auditors en privacy specialisten is aangegeven dat het een kwestie van tijd is voordat een incident zich voordoet. Daarom is aandacht voor mogelijke scenario's betreffende ongewenste situaties en beveiligingsincidenten van belang. Door het uitvoerig testen en analyseren van mogelijkheden kan tijdens een incident zo adequaat mogelijk worden geacteerd, waardoor gevolgen hopelijk kunnen worden ingeperkt. Het is opvallend dat door medisch specialisten wordt aangegeven dat bij het systeem sprake is van voornamelijk routinematig werk. Vanuit het privacy perspectief is dit wenselijk omdat hiermee duidelijkheid wordt verschaft over de te volgen procedures en protocollen. Echter is het van belang dat procedures en protocollen regelmatig worden herzien, zodat ingebedde ontwerpfouten tijdig kunnen worden gecorrigeerd. Er is een sleutelrol weggelegd voor communicatie. Dit betreft het aanscherpen van het belang van een juiste omgang met het systeem; het verduidelijken van taken en verantwoordelijkheden van verschillende organisaties maar ook binnen individuele zorginstellingen; en handelingen die moeten worden gevolgd tijdens een incident. Communicatie dient niet alleen te worden gericht op medewerkers maar ook op patiënten. De respondenten hebben aangegeven onvoldoende op de hoogte te zijn van de werking en mogelijke gevolgen van het LSP. Dit kan worden verholpen door meer informatie beschikbaar te stellen – bijvoorbeeld een informatiepakket voordat een keuze voor het wel of niet geven van toestemming moet worden gemaakt – en alleen schriftelijke toestemming te hanteren. Op deze manier wordt een patiënt meer begeleid en kunnen onzekerheden over de reikwijdte van het systeem worden weggenomen. Tot slot wordt aanbevolen om een andere identificatiemethode te hanteren dan het BSN. Het BSN is oorspronkelijk ingevoerd als identificatienummer voor de overheid.

Aangezien het LSP een private doorstart betreft, lijkt dit een onlogisch gekozen methode. Daarnaast is het BSN onvervangbaar, i.e. het nummer wordt aan een persoon gekoppeld voor de rest van zijn leven en bij incidenten wordt nooit een nieuw nummer verstrekt. Verschillende respondenten, afkomstig uit de diverse categorieën, hebben aangegeven open te staan voor een nieuwe identificatie-methode waarin alleen medische gegevens worden geregistreerd. In het geval van fouten is een dergelijk nummer niet herleidbaar naar het BSN, waardoor er een afbakening van gegevens is. De hiervoor benoemde aanbevelingen versterken het privacy concept binnen de bedrijfsvoering van het LSP, door zowel te focussen op het inhoudelijke systeem, op de menselijke factoren die met het systeem moeten omgaan en de visie van patiënten waarbij het belang van controle over data hoog is.

5.3 Toekomstig onderzoek

Om de geschetste problematiek nog beter in kaart te brengen zal meer onderzoek moeten worden verricht. Zoals eerder is aangegeven in paragraaf 3.4 (betrouwbaarheid en validiteit), kent dit onderzoek enkele beperkingen. Het uitvoeren van toekomstig onderzoek kan bijdragen aan het wegnemen van deze beperkingen Een limitatie die werd geïdentificeerd, is dat sommige respondenten mogelijk de vragen beter of meer wenselijk beantwoorden dan de feitelijke situatie. Verder is gesteld dat respondenten voorzichtig konden worden in het vrijuit spreken over hun opvattingen, omdat ze een groter belang vertegenwoordigen. Dit is betracht weg te zijn genomen door het anonimiseren van herleidbare gegevens naar de respondenten en het benadrukken dat geen oordeelsvorming over de gedane uitspraken zal plaatsvinden.

Het is wenselijk om zowel vergelijkbaar en vergelijkend onderzoek uit te voeren naar de rol van privacy in gevoelige systemen. De zorgsector representeert een groot belang omdat het kwetsbare personen in de samenleving raakt. Patiënten bevinden zich in een afhankelijke positie, doordat ze niet zonder goede zorg kunnen. Door het uitvoeren van meer onderzoek en het ondervragen van meer respondenten kan worden bepaald of de bevindingen een breed draagvlak hebben. Ook kan dit bijdragen aan het creëren van inzicht over de toepasselijkheid op andere gedigitaliseerde systemen onder complexe omstandigheden. Het is wenselijk om

meer onderzoek te doen naar de vraag of de optekening van een (soortgelijk) systeem als het LSP volledig sluitend kan zijn vanuit een privacy perspectief. De toenemende drang naar controle over eigen medische gegevens en de groeiende aandacht voor privacy worden erkend. Echter moet dit wel haalbaar blijven. Wellicht is de individualisering van personen doorgeslagen in een illusie over controle op ieder aspect in de persoonlijke levenssfeer.

Daarnaast is in samenhang met het LSP een trend te herkennen waarbij inzicht wordt geboden in de medische gegevens via webapplicaties op onder andere mobiele telefoons. Via zogenoemde eHealth toepassingen krijgen patiënten via een persoonlijke digitale gezondheidsomgeving inzicht in hun gezondheid (Rijksoverheid, 2020). Tijdsbesparing vormt een voordeel, doordat mensen eenvoudig online een consult kunnen inplannen met hun zorgverlener. Daarnaast zou een zorgverlener sneller en gerichter met de juiste behandeling kunnen starten, doordat het medisch verleden staat opgeslagen. Evenals bij het LSP spelen bij eHealth dezelfde vragen over het garanderen van privacy. eHealth vormt ook een gedigitaliseerd systeem dat onder complexe omstandigheden inzicht wilt bieden in gevoelige data, namelijk medische gegevens van patiënten. Hierbij is belangrijk dat de mogelijke voordelen niet worden geprioriteerd boven risico's in termen van veiligheid en privacy.

6. Literatuur

AP. (2019). Burgerservicenummer (BSN). Geraadpleegd via: https://autoriteitpersoonsgegevens.nl

CBS. (2018). Jongvolwassenen vaker verslaafd aan sociale media. Geraadpleegd via https://www.cbs.nl

Cohen, M.D., March, J.G., & Olsen, J.P. (1972). A garbage can model of organizational choice. Administrative Science Quarterly, 17, 1–25.

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

De Winter, B. (2010). Toezicht op toegang EPD schiet ernstig tekort. Opgevraagd via https://webwereld.nl

Endsley, M.R. (1997). The role of situation awareness in naturalistic decision making. In C. Zsambok and G. Klein (Eds.), Naturalistic decision making (pp. 269–284). Mahwah, NJ: Erlbaum.

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

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

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.

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

ICT&Health. (2018). LSP lanceert publiekscampagne. Geraadpleegd via: https://www.icthealth.nl

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.

Leveson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems. *Organization studies*, *30*(2-3), 227-249.

March, J.G., & Olsen, J.P. (1986). Garbage can models of decision making in organizations. Marshfield, MA: Pitman.

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. Geraadpleegd via: https://www.volkskrant.nl/

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

Nu.nl (2017). Patiënt zonder elektronisch patiëntendossier krijgt medicatie moeilijk mee. Geraadpleegd via: https://www.nu.nl/

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

OECD. (2013). Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines. OECD Digital Economy Papers, No. 229, OECD Publishing: Paris.

Officiële Bekendmakingen. (2011). Kamerstuk: 31466 nr AB. Geraadpleegd via https://officielebekendmakingen.nl/

Privacyzone. (2018). Identiteitsfraude door selfie op Instagram met pas behaald rijbewijs. Geraadpleegd via https://www.privacyzone.nl

Rijksoverheid. (2019). Inspectie Gezondheidszorg en Jeugd. Geraadpleegd via: https://www.igj.nl/

Rijksoverheid. (2020). E-Health – digitale zorg. Geraadpleegd via: https://www.rijksoverheid.nl

Rutten, P. (2007). *Digitalisering en dynamiek : Over de consequenties van de digitale revolutie voor de media-industrie*. Amsterdam: Leiden University Press

RvIG. (2019). Centraal Meldpunt Identiteitsfraude en –fouten. Opgevraagd via https://www.rvig.nl

Schulman, P.R. (2004). General attributes of safe organizations.

Sutcliffe, K.M. (2012). De kenmerken van high reliability organizations (HRO's). In: Justitiële verkenningen 2012/04. Den Haag: Boom Lemma.

Volg Je Zorg. (2019a). Hoe werkt het Landelijk Schakelpunt? Opgevraagd via: https://www.volgjezorg.nl

Volg Je Zorg. (2019b). Veiligheid en Privacy van het Landelijk Schakelpunt. Opgevraagd via: https://www.volgjezorg.nl

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 Gebruik landelijke zorginfrastructuur 2016 – 2020.

VZVZ. (2019). Over VZVZ. Opgevraagd via: https://www.vzvz.nl

VZVZ. (2019a). Over het LSP – aansluiten. Opgevraagd via: https://www.vzvz.nl

VZVZ. (2019b). VZVZ en het LSP. Opgevraagd via: https://www.vzvz.nl

VZVZ. (2019c). Architectuur AORTA. Opgevraagd via: https://www.vzvz.nl

VZVZ. (2019d). Wie houdt toezicht op het rechtmatig gebruik van het Landelijk Schakelpunt? Opgevraagd via: https://www.vzvz.nl

VZVZ. (2019e). Veelgestelde vragen. Opgevraagd via: https://www.vzvz.nl

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis management*, *3*(1), 81-123.

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

ZorgNu. (2017). Patiënten slecht op de hoogte van ‘het nieuwe EPD’. Opgevraagd via: https://zorgnu.avrotros.nl

Bijlage 1 – Profielschetsen geïnterviewde respondenten

Respondent 1 is een patiënt van middelbare leeftijd en is een aantal jaren geleden na een uitgebreide periode van onderzoeken chronisch ziek verklaard. De medische klachten waren moeilijk te herleiden waardoor de onderzoeken in verschillende ziekenhuizen hebben plaatsgevonden. Daarnaast haalt de respondent medicijnen bij verschillende apotheken. Verder heeft deze persoon mondeling toestemming gegeven voor het Landelijk Schakelpunt en heerst het gevoel van afhankelijkheid van goede zorg, waardoor liever niet wordt stilgestaan bij de mogelijke risico's.

Respondent 2 is een jongvolwassen patiënt en recentelijk verhuisd naar een nieuwe gemeente. Door de relatief lange afstand tussen de oude en nieuwe woonplaats is gekozen om aan te sluiten bij een nieuw gezondheidscentrum. Na het informeren bij dit nieuwe centrum wilde de respondent bedenktijd in plaats van direct toestemming verlenen voor het overhevelen van het medisch dossier. Uiteindelijk heeft de respondent dit op een agressieve manier ervaren doordat degene meerdere keren is benaderd met de mededeling dat geen zorg zou kunnen worden verleend voordat het dossier was overgezet.

Respondent 3 is een jongvolwassen patiënt en heeft verschillende medische klachten. Deze patiënt heeft veel onderzoeken gehad in een relatief korte periode, die achteraf niet allemaal nodig waren geweest. De respondent heeft het gevoel niet goed te zijn geholpen door de huisarts, waardoor een nieuwe huisarts is gezocht. Mede door het werken in de zorg worden wel risico's gezien. Hier wordt echter weinig mee gedaan door de afhankelijkheid van goede zorg.

Respondent 4 is een IT-auditor met ruim 15 jaar ervaring. De respondent heeft uiteenlopende opdrachten gedaan, ook in de medische sector. Daarnaast is sprake van een recente verhuizing waardoor zelf ook een keuze moest worden gemaakt tussen het wel of niet geven van toestemming voor het Landelijk Schakelpunt.

Respondent 5 is zowel IT-auditor en privacy specialist met ongeveer 20 jaar ervaring. Voorheen is de respondent werkzaam geweest bij verschillende zorginstellingen. De rol die hierbij werd vervuld is op het gebied van strategische bedrijfsvoering. Naast de werkzaamheden staat de respondent ook dichtbij een patiënt, waardoor er veel kennis is en de verschillende kanten van de medische sector kunnen worden belicht.

Respondent 6 is zowel IT-auditor als privacy specialist en heeft bijna 40 jaar ervaring. Deze respondent geeft leiding aan 20 personen die zich bezig houden met IT-audits, privacy opdrachten, en cybersecurity opdrachten. Daarnaast heeft de respondent meegewerkt aan verschillende onderzoeken naar systemen met gevoelige informatie, waarvan een aantal adviezen zijn overgenomen en gepubliceerd door de Rijksoverheid.

Respondent 7 wordt geclassificeerd als medisch specialist. Deze respondent is werkzaam in een groot academisch ziekenhuis in de randstad. De rollen die zijn vervuld verschillen van onderzoeker naar arts, allen uitgevoerd bij hetzelfde ziekenhuis.

Respondent 8 is een medisch specialist die werkt als verpleegkundige. Deze respondent heeft zowel ervaring in een kleinschalige thuiszorg instantie, als in een groot academisch ziekenhuis. Eerder is stage gelopen, en daarna was er ruimte om zelfstandig medische handelingen te verrichten. De respondent weergeeft verschillen tussen grotere en kleinere zorginstellingen.

Respondent 9 is een medisch specialist die wisselt tussen verschillende zorginstellingen. De relatief korte arbeidsduur is interessant doordat er steeds opnieuw toegang moet worden verleend tot de systemen van een zorginstelling en het elektronisch patiëntendossier. Daarnaast worden verschillen in de werkwijzen opgemerkt.

Bijlage 2 – Lijst van geaccepteerde zorginformatiesystemen

De volgende XIS-applicaties zijn door VZVZ geaccepteerd:

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 Televiewer (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

Bron: VZVZ, 2019.

Bijlage 3 – Goed Beheerd Zorgnetwerk (GZN)

GZN'en (goed beheerde zorgnetwerken) brengen een beveiligde verbinding tot stand tussen goed beheerde zorgsystemen van zorgaanbieders en het Landelijk Schakelpunt. Onderstaande netwerkleveranciers zijn door VZVZ geaccepteerd als 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

Bron: VZVZ, 2019.