Elektronische gegevensuitwisseling in beweging

Een onderzoek naar de mogelijke veranderingen op het gebied van elektronische gegevensuitwisseling in de zorg

Yorgos Vidos

Privacy werkorganisatie UMCG
Hanzehogeschool HBO-Rechten

Groningen, mei, 2016

Studentenbureau UMCG

Universitair Medisch Centrum Groningen

© 2015 Studentenbureau UMCG Publicaties Groningen, Nederland.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j° het Besluit van 20 juni 1974, St.b. 351, zoals gewijzigd in Besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht. Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

Trefw elektronische gegevensuitwisseling, wetsvoorstel, cliëntenrechten elektronische verwerking

Elektronische gegevensuitwisseling in beweging

Een onderzoek naar de mogelijke veranderingen op het gebied van elektronische gegevensuitwisseling in de zorg en in hoeverre het Universitair Medisch Centrum Groningen in de huidige situatie aan de reeds geldende en toekomstige wettelijke eisen kan voldoen.

Groningen, mei 2016

Auteur	Yorgos Vidos
Studentnummer	269719
Afstudeerscriptie in het kader van	Instituut voor Rechtenstudies HBO-Rechten Hanzehogeschool Groningen
Opdrachtgever	Mr. R.E. Jager UMC-staf Juridische Zaken, UMCG
Begeleider onderwijsinstelling	Dr. M.J. Riemens Instituut voor Rechtenstudies Hanzehogeschool Groningen
Begeleider UMCG	B.M.Y. Sieperda Privacy werkorganisatie, UMCG

Samenvatting

Dit onderzoek is een gevolg van de wens van het Universitair Medisch Centrum Groningen (hierna UMCG) om meer zicht te krijgen op de mogelijke veranderingen in wetgeving ten gevolge van een aanhangig wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens.* Op het moment dat dit onderzoek wordt geschreven is het zeer waarschijnlijk dat dit wetsvoorstel zal worden aangenomen. De wet brengt veranderingen met zich mee die betrekking hebben op de elektronische uitwisseling van persoonsgegevens. Het UMCG wil inzicht krijgen in deze veranderingen en de manier waarop dit een impact zal hebben op de huidige werkwijze van de uitwisselingssystemen die het UMCG momenteel gebruikt om deze uitwisseling van persoonsgegevens te faciliteren. Als het wetsvoorstel wordt aangenomen is het voor het UMCG van belang om tijdig te weten welke aanpassingen er aan systemen moeten worden gedaan, en in hoeverre deze systemen in staat zijn om aan deze nieuwe eisen te voldoen. Het UMCG kiest ervoor om naar een selectie van drie uitwisselingssystemen te kijken. Deze selectie is volgens de organisatie representatief voor de uitwisselingsystemen binnen het UMCG en onderzoek hierop zal daarom resultaten opleveren die een eerste indruk kunnen geven in hoe het UMCG er met betrekking tot dit wetsvoorstel voorstaat. De uitwisselingssystemen uit deze selectie zijn Palga, XDS en Zorgmail.

Het doel van dit onderzoek is het inventariseren voor de Privacy werkorganisatie en het hoofd UMC-staf Juridische Zaken van toekomstige wettelijke bepalingen uit het nieuwe wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens,* het in kaart brengen van de effecten van de wijzigingen uit het wetsvoorstel op de huidige werking van Palga, XDS en Zorgmail en in hoeverre deze systemen 'compliant' zijn met de eisen uit de bestaande en eventueel nieuwe wettelijke regelgeving. Dit doel is uiteindelijk gerealiseerd door bepalingen uit bestaande regelgeving en nieuwe regelgeving uit het wetsvoorstel systematisch te analyseren. Waarna vervolgens de werking van deze systemen vastgesteld zijn en de werking van deze systemen getoetst zijn aan de bestaande en nieuwe wettelijke bepalingen. Het voorgaande is bewerkstelligd door experts binnen de verschillende afdelingen te interviewen, de verantwoordelijken voor de verschillende gegevensuitwisselingssystemen te interviewen en door de mening van de betrokken medewerkers omtrent de werking en eventuele knelpunten van deze systemen te peilen.

De centrale onderzoeksvraag is:
In hoeverre kunnen de elektronische uitwisselingssystemen Palga, XDS en Zorgmail voldoen aan het wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens* en wat zijn de eventuele knelpunten die geconstateerd worden door verschillende experts en verantwoordelijke medewerkers binnen het UMCG?

De deelvragen zijn:
-Welke eisen worden er gesteld aan een EUS in de wet?
-Welke eisen worden gesteld aan een EUS in de NEN-normen?
-Welke nieuwe eisen kunnen uit het wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens* worden afgeleid?
-Wat zijn volgens de juridische literatuur de gevolgen van het wetsvoorstel *cliëntenrechten bij elektronische -- verwerking van gegevens* voor zorgaanbieders?
-Op welke wijze behoren de gegevensuitwisselingssystemen te functioneren met het oog op het wetsvoorstel?
-Hoe werken de gegevensuitwisselingssystemen van XDS, Palga en Zorgmail op dit moment binnen het UMCG?
-Op welke wijze wordt het toestemmingsvereiste in de huidige systemen vorm gegeven?
-Op welke punten schieten gegevensuitwisselingssystemen met betrekking tot huidige en eventueel toekomstige wetgeving tekort volgens verschillende betrokken medewerkers en experts?
-Welke conclusies kunnen worden getrokken na de vergelijking van de theorie en de praktijk?
-Welke conclusies kunnen worden getrokken door de elektronische uitwisselingssystemen met elkaar te vergelijken?

De conclusie van dit onderzoek luidt:
In dit onderzoek is gebleken dat Palga, XDS en Zorgmail (nog) niet voldoen aan de eisen uit het nieuwe wetsvoorstel. Door de beslissing van de minister van Volksgezondheid, Welzijn en Sport om de inwerkingtreding van verschillende bepalingen uit het wetsvoorstel uit te stellen is er voor het UMCG een kans gecreëerd om in een periode van drie jaar na inwerkingtreding van het wetsvoorstel tot de gewenste eindsituatie te komen. De gewenste eindsituatie is dat alle elektronische uitwisselingen van het UMCG compliant zijn met bestaande en nieuwe wettelijke regelgeving. Deze recente beslissing van de minister sluit naadloos aan bij de knelpunten die niet alleen door belangenorganisaties buiten het UMCG maar ook door de verschillende experts binnen het ziekenhuis worden voorzien.

Op dit moment is er een grote afstand tussen de huidige situatie en de gewenste eindsituatie. In het onderzoek komt naar voren dat de onderzochte systemen soms niet voldoen aan bestaande wetgeving. Een belangrijke rol is hierbij weggelegd voor de informatiebeveiligingsorganisatie, die momenteel niet overal even effectief is. Zij zal in effectiviteit moeten toenemen als ze in de toekomst beter in staat wil zijn om structurele wettelijke strijdigheden in elektronische uitwisselingssystemen te detecteren en te verhelpen. Het UMCG kan niet verwachten dat nieuwe wetgeving succesvol geïmplementeerd zal worden als bestaande wetgeving in veel systemen nog niet goed wordt nageleefd. Het is zeer waarschijnlijk dat vergelijkbare problemen ook in andere uitwisselingssystemen, die niet in dit onderzoek zijn meegenomen, te vinden zullen zijn. Het is zorgelijk dat de informatiebeveiliging op dit moment in de praktijk niet altijd in staat is uitwisselingssystemen compliant te krijgen met huidige wetgeving. Hier zal meer aandacht, geld en tijd in moeten worden geïnvesteerd.

Uit het onderzoek blijkt dat de werking van Palga en Zorgmail niet gemakkelijk kunnen worden aangepast om aan het nieuwe wetsvoorstel te voldoen. Daarnaast is het onwenselijk om bij elk bestaand uitwisselingssysteem aparte functies in te bouwen. XDS zou met verschillende aanpassingen in de toekomst wellicht in staat kunnen zijn andere uitwisselingssystemen compliant te maken met het nieuwe wetsvoorstel. In XDS zitten veel softwarematige aanknopingspunten met het nieuwe wetsvoorstel. Zou XDS zodanig worden aangepast dat het compliant is met het nieuwe wetsvoorstel, dan zou via XDS een groot aantal systemen compliant gemaakt kunnen worden. Nader onderzoek zou eventueel uit moeten wijzen welke aanpassingen XDS precies zal moeten ondergaan.

Op basis van het onderzoek zijn de volgende (samengevatte) aanbevelingen geformuleerd:

1. Om te zorgen dat bestaande uitwisselingsystemen compliant zijn met bestaande wet- en regelgeving is het van belang te inventariseren op welke wijze alle huidige uitwisselingssystemen binnen het UMCG werken en of in die werking aan alle eisen uit de WBP en WGBO wordt voldaan.

2. Het UMCG zou de wettelijke eisen uit de Wbp en de WGBO een meer uitgesproken en centrale plek moeten geven in zijn controleproces op alle uitwisselingssystemen binnen de organisatie.

3. Voor het UMCG is het van belang in direct contact te staan met beroep- en cliëntenorganisaties uit de zorgsector om op die manier de ontwikkelingen rondom het implementatieplan van het nieuwe wetsvoorstel bij te houden en tijdig op te kunnen volgen om zo tot een succesvolle implementatie van het nieuwe wetsvoorstel binnen de organisatie te komen.

4. Het UMCG zou moeten onderzoeken wat de potentie van XDS is met betrekking tot haar capaciteit om in de toekomst een standaard te zijn die verschillende systemen in haar werkwijze opneemt en mogelijk andere uitwisselingssystemen overbodig maakt.

5. Het UMCG zou gelet op zowel bestaande als nieuwe wetgeving moeten kijken naar een centraal moment waarop patiënten geïnformeerde toestemming kunnen geven voor het verwerken van persoonsgegevens via elektronische uitwisselingssystemen.

6. Het UMCG zou binnen de zorgsector moeten kijken welke zorgaanbieders reeds beschikken over een patiëntportaal dat elektronisch inzage verschaft en in hoeverre dit al is afgestemd op de eisen uit het toekomstige wetsvoorstel.

7. Het UMCG zou de ontwikkeling van baselines binnen de organisatie in verdere mate moeten stimuleren. Deze baselines geven afdelingen de mogelijkheid nieuwe systemen succesvol te implementeren of te toetsen, en bieden in het algemeen een zeker handvat op basis waarvan gewerkt kan worden.

8. Veel van de professionals die met de uitwisselingssystemen werken kennen de mankementen in de verschillende systemen maar lijken zich soms niet te realiseren welke wettelijke impact dit heeft. Het UMCG zou meer moeten doen om te bewustwording onder medewerkers hierin te vergroten zodat strijdigheden in systemen eerder worden gemeld, geconstateerd en aangepakt. Apart onderzoek zou uit kunnen wijzen welke aanpak hiervoor het meest effectief is.

Voorwoord

Dit onderzoek is de afsluiting van mijn opleiding HBO-Rechten en daarmee komt voor mij een einde aan een belangrijke periode uit mijn leven. Een periode waarop ik met veel plezier terug kijk, en waarin ik gelukkig ook veel heb mogen leren. De afgelopen maanden heb ik het genoegen gehad om onderzoek te mogen doen bij het UMCG naar een onderwerp dat niet alleen nieuw was voor mij, maar ook zeer boeiend en actueel. U zult in dit onderzoek nog bijzonder veel over dit onderwerp lezen, maar wat u niet zal tegenkomen is bladzijden vol over mijn ervaringen met de medewerkers van het UMCG en de organisatie als geheel. U begrijpt ongetwijfeld waarom. Het is om deze reden dat ik graag dit moment zou willen aangrijpen om alle medewerkers binnen het UMCG van harte te bedanken. Een ziekenhuis is helaas nooit een plek waar mensen alleen maar beter worden. Er is ook altijd veel narigheid binnen de muren van een ziekenhuis, en die narigheid kan de sfeer van een ziekenhuis enorm beïnvloeden. Desalniettemin heeft het UMCG een warmte in zich die ik tot op heden alleen in dit ziekenhuis zo heb ervaren. Ik bewonder dat enorm en mijn dank gaat uit naar alle medewerkers van het UMCG die deze warmte op mij hebben overgebracht. Ik kan alleen maar hopen dat zij dit in de toekomst ook voor anderen kunnen blijven doen.

Dit onderzoek zou niet mogelijk zijn geweest zonder de bijdrage van een aantal personen. Allereest zou ik mijn opdrachtgever Robert Jager willen bedanken. Zonder zijn onderzoeksopdracht had ik dit onderzoek nooit kunnen doen. Ik wil Boudien Sieperda bedanken voor al haar hulp, feedback, steun, advies en vooral ook haar geduld. Ik had mij geen betere praktijkbegeleidster kunnen wensen. Dank ook aan Cathy Zelhorst. Ook dank aan mijn afstudeerdocent Michael Riemens voor al zijn feedback en advies. Ook wil ik alle medewerkers bedanken die de tijd hebben genomen om mee te werken aan de interviews. Zonder hen had het praktijkonderzoek weinig voorgesteld.

Graag bedank ik mijn vrienden en familie. Mirjam Mollema, Ioanko Vidos, Martijn Kolenbrander, Tim Dekens en in het bijzonder mijn ouders Hanneke Vidos-Helder en Ioannis Vidos. Dit onderzoek is net zo veel van jullie als van mij. Bedankt voor alles.

Tot slot wens ik iedereen veel leesplezier.

Inhoud

1 Inleiding

1.1 Onderzoekskader

Dit onderzoek is een gevolg van de wens van het UMCG om meer zicht te krijgen op de mogelijke veranderingen in wetgeving ten gevolge van een aanhangig wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens.*

Het Universitair Medisch Centrum Groningen (UMCG) is één van de grootste ziekenhuizen in Nederland. Er werken ruim 12.000 medewerkers, en daarmee is het de grootste werkgever in Noord-Nederland. De werknemers houden zich voornamelijk bezig met patiëntenzorg, onderwijs en wetenschappelijk onderzoek. Het UMCG onderhoudt een nauwe samenwerking met de Rijksuniversiteit Groningen (RUG). Via de RUG zijn er veel studenten die jaarlijks hun opleiding volgen binnen de muren van het UMCG. Het is de missie van het UMCG om in deze drie kerntaken te 'excelleren én innoveren'.[1]

Goede kwaliteit van zorg wordt in ons huidige tijdperk gekenmerkt door het voorhanden zijn van actuele medische patiëntgegevens bij alle artsen en medische experts die zich direct met de behandeling van de patiënt bezig houden. Het komt dus steeds vaker voor dat niet één maar juist verschillende artsen vanuit verschillende achtergronden en instellingen zich buigen over eenzelfde behandeling. Gezien de technologische mogelijkheden van nu, moet geconcludeerd worden dat het papieren dossier binnen de medische sector, zoals binnen zoveel sectoren, hierdoor steeds meer plaats maakt voor een elektronische wijze van dossiervorming, om zo de samenwerking tussen verschillende medische professionals te kunnen faciliteren. Door deze ontwikkeling hebben patiënten, medici en politici de afgelopen jaren zich in steeds grotere mate afgevraagd in hoeverre zorginstellingen in staat zijn om met succes de veiligheid en vertrouwelijkheid van deze medische gegevens te kunnen waarborgen.[2] Deze bescherming van medische gegevens is voor de burger altijd al essentieel geweest, maar tegenwoordig zeer actueel, gezien het feit dat door diezelfde technologische vooruitgang het onrechtmatig bemachtigen van deze informatie ook eenvoudiger is geworden. Deze bescherming hangt vanzelfsprekend nauw samen met de wettelijke geheimhoudingsplicht van medisch personeel. Het medische beroepsgeheim kent een aantal strenge eisen die met de huidige technologische ontwikkelingen onder druk komen te staan. Doordat artsen minder controle hebben over de wijze van verwerking en uitwisseling van medische gegevens kan er vaker en veelal onbedoeld, sprake zijn van schending van de wettelijke bepalingen van hun geheimhoudingsplicht.
Op 19 februari 2009 werd door de Tweede Kamer een wetsvoorstel aangenomen waarmee het elektronisch patiëntendossier (EPD) werd geïntroduceerd. Deze wetswijziging, dat een onderdeel van de *Wet cliëntenrechten zorg* had moeten worden, was een poging tot vergaande regulering van de wijze waarop in heel Nederland digitale patiëntendossiers in een landelijk systeem zouden worden beheerd en uitgewisseld tussen verschillende zorgverleners. Op 5 april 2011 werd dit wetsvoorstel verworpen door Eerste Kamer. De Eerste Kamer kwam tot haar beslissing omdat men twijfelde aan de proportionaliteit, effectiviteit en de veiligheid van een dergelijk systeem.[3] Hiermee kwam er een eind aan de intentie om het landelijk EPD systeem in te voeren. Na het wetsvoorstel verworpen te hebben, werd de motie-Tan aangenomen waarin de Eerste Kamer haar wens voor een alternatief wetsvoorstel kenbaar maakte.[4]
In de motie werd de regering verzocht een wetsvoorstel op te stellen binnen de kaders van de reeds bestaande *Wet bescherming persoonsgegevens* (Wbp), *Wet op de beroepen in de individuele gezondheidszorg* (BIG) en *Wet op de geneeskundige behandelingsovereenkomst* (WGBO). Met dit wetsvoorstel zou er aanvullende wetgeving moeten komen die moest zorgen dat er aanvullende eisen/randvoorwaarden werden gesteld aan bestaande en/of toekomstige elektronische patiëntendossier-systemen. Het wetsvoorstel moest zich richten tot het reguleren van:

-normen en standaarden voor zowel digitale dossiervorming en –ontsluiting, als de overdracht van gegevens
-eisen met betrekking tot de veiligheid
-toezicht, handhaving en sancties
-inzage door de patiënt, het verstrekken van afschrift aan de patiënt en transport van gegevens op verzoek van de patiënt

Het doel van deze wetgeving moest zijn het mogelijk maken van veilige digitale uitwisseling van gegevens tussen zorgverleners binnen regio's (zowel pull als push verkeer).[5] Dit voornamelijk ook met het oog op het realiseren van extra privacybescherming voor patiënten.[6]

---

[1] 'Het UMCG - Missie en visie', *website UMCG*, 30 september 2015, www.umcg.nl.
[2] Deze stelling is gebaseerd op hetgeen te lezen is in het 'Boze Huisartsen' Arrest, alsmede M.C. Ploem, 'Elektronische gegevensuitwisseling in de zorg: zit de wetgever op het goede spoor?', *Tijdschrift voor Gezondheidsrecht* 2015, p. 1.
[3] *Handelingen I* 2010/11, 20, nr. 2, 7 en 22. Zie ook Ploem, 'Elektronische gegevensuitwisseling', p. 1.
[4] 'Elektronisch patiëntendossier', *website Eerste Kamer*, 30 september 2015, www.eerstekamer.nl (zoek op **31.466).**
[5] 'Gewijzigde motie-Tan', *website Eerste Kamer,* 30 september 2015, www.eerstekamer.nl (zoek op EK 31.466, Y)

Op 21 december 2012 is de uitwerking van bovengenoemde motie, het wetsvoorstel genaamd *cliëntenrechten bij elektronische verwerking van gegevens* aangenomen door de Tweede Kamer. Op 1 juli 2014 is dit wetsvoorstel door de Eerste Kamer in behandeling genomen.[7]
De verwachting is dat de Eerste Kamer dit wetsvoorstel zal aannemen.
De veranderingen die het wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens* met zich meebrengt zijn dus gebaseerd op de bestaande wetgeving. De wetten die op dit moment al regels bevatten omtrent de uitwisseling van patiëntgegevens zijn voornamelijk de Wbp en de WGBO, maar bijvoorbeeld ook *Het Wetboek van Strafrecht* (WvSr) en de BIG etc. Daarnaast zijn er ook beveiligingsnormen voor de zorg opgesteld door het Nederlandse Normalisatie instituut, relevant zijn NEN-normen 7510 tot en met 7513. Art. 16 Wbp verbiedt nadrukkelijk de verwerking van medische patiëntengegevens, hieronder valt ook het uitwisselen van die gegevens (art. 1 Wbp). Op dat algemene verbod bestaat vervolgens een aantal uitzonderingen. De uitzonderingen waaronder gegevensverwerkingen/uitwisseling mogen bestaan, zijn geformuleerd in art. 21 Wbp. Ook moet er een wetmatige grondslag zijn waarop deze gegevensverwerking is gebaseerd (art. 8 Wbp). Artikel 13 Wbp voegt ten slotte een verplichting toe de gegevens waar nodig zowel technisch als organisatorisch zo te beveiligen dat er geen sprake kan zijn van verlies of onrechtmatige verwerking van gegevens. Daarnaast zijn er nog bepalingen die de gegevensverwerking onmogelijk maken zonder nadrukkelijke toestemming van de 'datasubject' (patiënt) en met inachtneming van de geheimhoudingsplicht (zie art. 34 Wbp, art. 272 WvSr, art 88 BIG, art. 7:457 WGBO) Op deze manier heeft de wetgever al op zekere wijze geprobeerd juiste en veilige medische patiëntgegevensuitwisseling te waarborgen.
In het wetsvoorstel worden in grote lijnen de volgende veranderingen gerealiseerd, en door Mr. Dr. M.C. Ploem (2015) kort en bondig in verschillende categorieën opgedeeld:

> *"Hoofddoel van het wetsvoorstel(…) is het bieden van extra privacybescherming aan patiënten (in het wetsvoorstel: cliënten) wanneer zorgaanbieders voor het uitwisselen van hun gegevens gebruik maken van een elektronisch uitwisselingssysteem in de zin van de wet(…) De extra bescherming wordt gerealiseerd door een aantal bijzondere bepalingen voor elektronische verwerking van patiëntgegevens wettelijk te verankeren(…) De bijzondere bepalingen betreffen:*
>
> - *Definities van onder andere 'elektronisch uitwisselingssysteem' en 'behandelrelatie';*
> - *Voorwaarden waaronder gegevens via een EUS* [elektronisch uitwisselingssysteem] *beschikbaar mogen worden gesteld;*
> - *Voorwaarden waaronder gegevens via een EUS mogen worden geraadpleegd;*
> - *Rechten van patiënten bij uitwisseling van gegevens via een EUS;*
> - *Toegangsverboden voor zorgverzekeraars en bepaalde categorieën artsen en een meldplicht voor de verantwoordelijke bij de Nederlandse Zorgautoriteit bij overtreding van dit verbod."*[8]

Men kan hieruit concluderen dat het wetsvoorstel een *lex specialis* zal zijn met artikelen die zich volledig richten op het benoemen van aanvullende regels en randvoorwaarden bij het gebruik van een EUS in de zorg. Een belangrijk gegeven is dat waar men in het wetsvoorstel spreekt van een elektronisch uitwisselingssysteem, er sprake moet zijn van een systeem dat zich ook daadwerkelijk richt op het uitwisselen van gegevens met minstens één andere zorgaanbieder. Systemen die slechts intern worden gebruikt door dezelfde zorgaanbieder vallen niet onder de reikwijdte van het wetsvoorstel. De belangrijkste bepalingen uit het wetsvoorstel schrijven voor dat er toestemming nodig is van de patiënt (in de wet genaamd cliënt) om diens gegevens op te nemen in een EUS. De toestemming moet gespecificeerd zijn, wat betekent dat het mogelijk moet zijn voor de patiënt om een selectie te maken welke gegevens worden opgenomen en welke niet, als ook dat de patiënt moet kunnen kiezen voor welke zorgaanbieders of groepen zorgaanbieders deze informatie inzichtelijk is. Op het moment dat er zorgaanbieders aan het systeem worden toegevoegd moet uiteraard, waar van tevoren geen generieke toestemming is verleend, opnieuw aan de patiënt om toestemming worden gevraagd. Wanneer gegevens door een zorgaanbieder vervolgens worden opgevraagd, moet daar ook weer een aparte toestemming voor worden gevraagd. Voor noodsituaties wordt hierin een uitzondering gemaakt. Zorgverzekeraars, bedrijfsartsen, verzekeringsartsen en keuringsartsen worden uitgesloten van deelname in dit nieuwe voorstel gezien hun rol binnen de medische zorgverlening. Het wetsvoorstel geeft de patiënt verder als aanvulling op art. 7:456 WGBO het recht op elektronische inzage in, welke zorgaanbieder op welke wijze en wanneer, de medische gegevens van de patiënt via het EUS heeft ingezien. Deze inzage moet kosteloos zijn.

---

[6] Ploem, 'Elektronische gegevensuitwisseling', p. 5.
[7] 'Cliëntenrechten bij elektronische verwerking gegevens', *website Eerste Kamer,* 30 september 2015, www.eerstekamer.nl (zoek op 33.509)
[8] Ploem, 'Elektronische gegevensuitwisseling', p. 5.

Belangrijk om op te merken is dat er in het wetsvoorstel geen waarde meer wordt gehecht aan de vraag of de zorgaanbieder die de gegevens opvraagt direct betrokken is of als vervanger optreedt bij de behandeling van de patiënt. In plaats hiervan moet de patiënt tegenwoordig bij elke opvraag van informatie door een zorgaanbieder eerst van tevoren toestemming geven.
Het grootste verschil zit in de wijze waarop de gespecificeerde toestemming werkt[9], ten opzichte van de eerdere wijze van toestemmingsverlening. Deze toestemmingsvorm is veel uitgebreider en complexer om te faciliteren. Een andere belangrijke verandering zal zijn dat de patiënt straks in staat moet worden gesteld om via een elektronische weg zijn medische gegevens in te zien, en toegang krijgt tot een uitdraai van een elektronische loggegevens over wie wat wanneer heeft ingezien.
Het introduceren van de zogeheten 'gespecificeerde toestemming' kan momenteel op veel weerstand rekenen onder de verschillende belangenbehartigingsorganisaties uit de zorg. Zo hebben onder andere het KNMG, GGZ Nederland, KNMP, NVZ, Actiz en VGN in een reactie laten weten dat het wettelijk vastleggen van deze toestemmingsvorm tot veel problemen kan gaan leiden. Verwacht wordt dat de zorgaanbieders momenteel niet goed in staat zullen zijn met de huidige systemen deze vorm van uitsluiting van bepaalde zorgaanbieders door patiënten te faciliteren. Daarnaast wordt door verschillende organisaties gewezen op de onwenselijke situaties die kunnen ontstaan wanneer een uitgesloten zorgaanbieder een essentiële rol te vervullen heeft in de optimale behandeling van de patiënt. Men vraagt zich af hoe de wetgever dit zich heeft voorgesteld. De oproep om uitstel van deze specifieke bepaling in het wetsvoorstel is groot, en wordt dus door een aantal praktische argumenten onderbouwd.[10]
Om te zorgen dat het UMCG op tijd kan voldoen aan deze eventuele nieuwe wetgeving moet er gekeken worden naar de werking van drie belangrijke EUS en in hoeverre deze systemen moeten worden aangepast om te voldoen aan de eisen uit het nieuwe wetsvoorstel. Dit is het kader waarin dit onderzoek zal plaats vinden.

1.2 Interventiecyclus

Dit onderzoek is er één in een reeks van onderzoeken die bij het UMCG zijn en worden gedaan, die alle te maken hebben met een groeiende realisatie van de organisatie dat privacy en het beschermen van persoonsgegevens een steeds belangrijker onderwerp is. Met het oog op het in kaart brengen van juridische en praktische risico's met betrekking tot huidige en aankomende privacywetgeving is binnen het UMCG, onder de afdeling Juridische Zaken, de Privacy werkorganisatie opgericht die zich bezig houdt met het inventariseren, voorkomen en oplossen van deze risico's. De doelstelling van de werkorganisatie is onder andere om de praktijksituatie binnen het UMCG te veranderen. Het gaat hierbij om een verandering in de manier waarop de organisatie op dit moment omgaat met relevante privacy wetgeving. Daarbij hoort ook het zorgvuldig uitwisselen van medische gegevens met andere zorgaanbieders. Door de komst van het nieuwe wetsvoorstel *'Cliëntenrechten bij elektronische verwerking gegevens*' zal een aantal zaken rondom de uitwisseling van medische gegevens gaan veranderen. Het uiteindelijke streven is om alle uitwisselingen van medische gegevens te laten plaatsvinden met inachtneming van de veranderingen die voortkomen uit het aanhangige wetsvoorstel. In de aanpak van dit probleem, kan men een aantal fasen onderscheiden. Er kan sprake zijn van een *Probleemsignalerend onderzoek, diagnostisch onderzoek, ontwerpgericht onderzoek, verandergericht onderzoek* of een *evaluatieonderzoek.* Dit onderzoek bevindt zich in de eerste en tweede fase, en is daarmee deels een probleemsignalerend onderzoek en deels een diagnostisch onderzoek.[11] Tijdens deze fase doet men onderzoek naar wat het probleem is. In de praktijk is er sprake van een bepaalde huidige situatie die niet overeenkomt met de gewenste situatie. Deze gewenste situatie kan gebaseerd zijn op een nieuwe norm of (wettelijke) regeling. In dit geval is daar dus ook sprake van. In een diagnostisch onderzoek wordt dieper ingegaan op de achtergrond van het probleem.

Het nieuwe wetsvoorstel brengt met zich mee dat er een nieuwe wenselijke situatie ontstaat. Een situatie waarin het UMCG zijn elektronische gegevensuitwisselingssystemen zo wil inrichten dat deze voldoen aan de nieuwe bepalingen uit het wetsvoorstel. Binnen dat kader is het ook van belang om de huidige wetgeving mee te nemen, en te kijken aan welke voorwaarden de huidige systemen al moeten voldoen. Het doel van dit onderzoek is het analyseren van de huidige situatie, en vervolgens constateren waar eventueel de problemen zitten, en aanbevelingen doen ten opzichte van de in de toekomst te realiseren wenselijke praktijksituatie.

1.3 Doelstelling onderzoek

Het doel van dit onderzoek is:

---

[9] Zie artikel 15a lid 2 wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens,* Zie Ploem, 'Elektronische gegevensuitwisseling', p. 7. Zie ook *Brief reactie wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens,* 13 februari 2015 p. 1.
[10] Zie voor meer informatie omtrent dit onderdeel *Brief reactie wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens,* 13 februari 2015.
[11] P. Verschuren & H. Doorewaard, *Het ontwerpen van een onderzoek*, Den Haag: Boom Lemma Uitgevers 2007.

Het inventariseren voor de Privacy werkorganisatie en het hoofd UMC-staf Juridische Zaken van de toekomstige wettelijke bepalingen uit het nieuwe wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens,* het in kaart brengen van de effecten van de wijzigingen uit het wetsvoorstel op de huidige werking van Palga, XDS en Zorgmail en in hoeverre deze systemen 'compliant' zijn met de eisen uit de bestaande en eventueel nieuwe wettelijke regelgeving.

Door

Het systematisch analyseren van bepalingen uit bestaande regelgeving en nieuwe regelgeving uit het wetsvoorstel, de werking van deze systemen vast te stellen en deze werking te toetsen aan de bestaande en nieuwe wettelijke bepalingen. Het voorgaande door experts binnen de verschillende afdelingen te interviewen, de verantwoordelijken voor de verschillende gegevensuitwisselingssystemen te interviewen en door de mening van de betrokken medewerkers omtrent de werking en eventuele knelpunten van deze systemen te peilen.

1.4 Onderzoeksvragen

1.4.1 De centrale onderzoeksvraag

In hoeverre kunnen Palga, XDS en Zorgmail zo worden ingericht, dat deze elektronische uitwisselingssystemen voldoen aan het wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens* en wat zijn de eventuele knelpunten die geconstateerd worden door verschillende experts en verantwoordelijke medewerkers binnen het UMCG?

1.4.2 Deelvragen

Deelvragen gericht op de theorie:
-Welke eisen worden er gesteld aan een EUS in de wet?
-Welke eisen worden gesteld aan een EUS in de NEN-normen?
-Welke nieuwe eisen kunnen uit het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens worden afgeleid?
-Wat zijn volgens de juridische literatuur de gevolgen van het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens voor zorgaanbieders?
-Op welke wijze behoren de gegevensuitwisselingssystemen te functioneren met het oog op het wetsvoorstel?

Deelvragen gericht op de praktijk:
-Hoe werken de gegevensuitwisselingssystemen van XDS, Palga en Zorgmail op dit moment binnen het UMCG?
-Op welke wijze wordt het toestemmingsvereiste in de huidige systemen vorm gegeven?
-Op welke punten schieten gegevensuitwisselingssystemen met betrekking tot huidige en eventueel toekomstige wetgeving tekort volgens verschillende betrokken medewerkers en experts?

Deelvragen gericht op de analyse:
-Welke conclusies kunnen worden getrokken na de vergelijking van de theorie en de praktijk?
-Welke conclusies kunnen worden getrokken door de elektronische uitwisselingssystemen met elkaar te vergelijken?

1.5 Onderzoeksmethoden

Om een antwoord te krijgen op de geformuleerde theoretische deelvragen, zal er literatuuronderzoek gedaan moeten worden. Op basis van relevante wet- en regelgeving en andere juridische literatuur, moet inzichtelijk worden welke wettelijke eisen er op dit moment aan een elektronisch gegevensuitwisselingssysteem worden gesteld. Na de bestudering van de literatuur kan een juridische analyse volgen met als doel het helder formuleren van alle relevante vereisten en voorwaarden waar een elektronisch gegevensuitwisselingssysteem aan moet voldoen. Literatuuronderzoek moet ook een antwoord gaan geven op de vraag welke veranderingen het wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens* met zich mee brengt, en wat juridisch gezien mag worden verstaan onder een gegevensuitwisselingssysteem.
Om de praktische deelvragen te kunnen beantwoorden, zal er gekeken moeten worden naar de werking van de systemen die door het UMCG geselecteerd zijn. Dit moet door middel van telefonisch onderzoek en diepte-interviews met de verschillende afdelingen inzichtelijk worden. Door met de verantwoordelijke personen te kijken naar de exacte werking van de gegevensuitwisselingssystemen, moet het mogelijk zijn om antwoord te geven op de praktijkdeelvragen die in het onderzoeksvoorstel zijn geformuleerd.

Het aanhouden van de hierboven genoemde volgorde is cruciaal, om te garanderen dat met genoeg achtergrondinformatie naar interne gegevensuitwisselingssystemen kan worden gekeken.

1.6 Leeswijzer

Dit onderzoek bestaat uit twee delen. Het eerste deel bestaat uit literatuuronderzoek en het tweede deel bestaat uit praktijkonderzoek. Hoofdstuk 3 tot en met hoofdstuk 6 vormen samen het literatuuronderzoek. Eerst wordt de wet bescherming persoonsgegevens behandeld (hoofdstuk 3), daarna zal er dieper ingegaan worden op de eisen rondom de beveiliging van persoonsgegevens (hoofdstuk 4). Vervolgens komt de medische behandelrelatie aan bod (hoofdstuk 5). Hierna zal het toekomstige wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens worden behandeld (hoofdstuk 6).

Het praktijkonderzoek bestaat uit hoofdstuk 7 tot en met hoofdstuk 9. Eerst zal er een begin gemaakt worden met het praktijkonderzoek (hoofdstuk 7). Daarna komen de onderzoeksresultaten aan bod (hoofdstuk 8). Vervolgens wordt er een analyse gemaakt (hoofdstuk 9).

Tot slot zijn de conclusie en aanbevelingen opgenomen in hoofdstuk 10.

2 Methodologische verantwoording

2.1 Inleiding
In dit onderzoek zijn verschillende methoden gebruikt om tot het antwoord op de centrale onderzoeksvraag te komen. In dit hoofdstuk zal worden toelicht welke methoden en werkwijzen tijdens het onderzoek zijn gevolgd en inzicht worden gegeven in welke keuzes zijn gemaakt bij de uitwerking en voorbereiding van de verschillende hoofdstukken in dit onderzoek.

2.2 Vooronderzoek
In het vooronderzoek is er bewust gekozen om het onderwerp zeer aandachtig te bestuderen. Hierin is gekeken naar alle relevante wetsbepalingen, kamerstukken en tijdschriftartikelen. Vervolgens is er een onderzoeksvoorstel opgesteld aan de hand van de opgedane kennis rondom het onderwerp. Dit onderzoeksvoorstel is vervolgens aangepast en omgevormd tot een onderzoeksopzet dat vervolgens door de toetsingscommissie van de Hanzehogeschool Groningen is goedgekeurd. Om tot een degelijk onderzoeksopzet te komen was het voor de onderzoeker van belang om een duidelijk onderzoekskader te formuleren. Hiermee kon het onderzoek duidelijk worden afgebakend. Bij aanvang van het onderzoek was het de intentie van de opdrachtgever om het onderzoek een breder geheel aan systemen te laten bestaan. Uiteindelijk is er in overleg gekozen voor een selectie van drie systemen om het onderzoekskader enigszins te verkleinen. Deze aanpassing was nodig gelet op de enorme hoeveelheid elektronische uitwisselingssystemen die het UMCG gebruikt. De onderzoeksopzet bevatte daarnaast de doelstelling van het onderzoek, de deelvragen en centrale onderzoeksvraag, een onderzoeksmodel, een lijst met relevante bronnen en een uiteenzetting van de fase van de interventiecyclus waarin dit onderzoek zou vallen. Al deze componenten hebben bijgedragen aan een fundament waarop het verdere onderzoek kon worden uitgevoerd.

2.3 Literatuuronderzoek
In dit onderzoek is ervoor gekozen om te beginnen met desk research. Hierbij worden de relevante theoretische bronnen[12] die betrekking hebben op dit onderzoek uitgewerkt in verschillende hoofdstukken. In deze fase van het onderzoek is een juridische inhoudsanalyse uitgevoerd door alle relevante literatuur, wet en regelgeving en jurisprudentie te bestuderen. Deze bronnen hadden betrekking op het gezondheidsrecht en wetgeving rondom privacy in het algemeen en specifiek voor de zorgsector.

2.3.1 hoofdstuk 3
In hoofdstuk 3 is er voor gekozen om aan de hand van Kranenborg & Verhey[13] en de relevante wetsbepalingen in de Wbp met de daarbij behorende memorie van toelichting een uiteenzetting te geven van de bepalingen die van belang zijn voor dit onderzoek. Hierin heeft de Kranenborg & Verhey geholpen als steun om tot een juiste afweging te komen van de bepalingen die in dit hoofdstuk zouden worden behandeld. Wat de lezer zal opvallen is dat er echter niet per definitie enorm veel verwezen wordt naar literatuur maar des te maar naar de daadwerkelijke kamerstukken die bij deze wet behoren. Doordat de kamerstukken van deze wet bijzonder duidelijk geformuleerd zijn is er in dit onderzoek voor gekozen om zo dicht mogelijk bij de originele bron te blijven. Verwijzingen naar literatuur die weer naar kamerstukken verwijzen zou in dit geval een onnodige belasting zijn geweest op de grondige lezer van dit onderzoek. Deze afweging hangt echter nauw samen met de leesbaarheid van de kamerstukken die bij deze wet horen.

2.3.2 hoofdstuk 4
Hoofdstuk 4 is geboren uit de overduidelijke diepgang die het beveiligingsaspect uit de Wbp met zich mee brengt. Hoofdstuk 4 kan als zodanig ook gezien worden als de uitgebreide behandeling uit een bepaling die slechts summier behandeld wordt in hoofdstuk 3. De reden om dit te doen is omdat deze bepaling en zijn toelichting van groot belang is voor het verdere vervolg van dit onderzoek. Dit bleek ook uit de juridische inhoudsanalyse die verricht is bij hoofdstuk 3. Om tot een grondige uitwerking van dit hoofdstuk te komen is ervoor gekozen om te kijken op welke manier de beveiligingsbepalingen uit de Wbp worden gehandhaafd en gecontroleerd. Hierbij hebben de richtsnoeren van het voormalig CBP[14] enorm veel inzicht kunnen geven waardoor het mogelijk was om de lezer deze complexe bepalingen uit te leggen. Ook in dit hoofdstuk is ervoor gekozen om zo veel mogelijk naar de originele bronnen te verwijzen zoals ook bij hoofdstuk 3 is gedaan.

---

[12] M.C. Ploem, 'Elektronische gegevensuitwisseling in de zorg: zit de wetgever op het goede spoor?', *Tijdschrift voor Gezondheidsrecht* 2015, afl 5 p. 300-312; H.J.J. Leenen e.a., *Handboek gezondheidsrecht Deel I: Rechten van mensen in de gezondheidszorg,* Hoofddorp: Boom Juridische uitgevers 2011; H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011; Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens.

[13] H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011

[14] *CBP richtsnoeren beveiliging van persoonsgegevens,* Den Haag, 2013.

2.3.3 hoofdstuk 5
In hoofstuk 5 wordt de medische behandelrelatie behandeld, een onderwerp wat zeker nauw verbonden is met de eerdere hoofdstukken, maar zijn grondslag vindt in andere wetgeving. Op basis van een juridische inhoudsanalyse is bij dit hoofdstuk Leenen[15] en de WGBO bestudeerd omdat deze bronnen meer raakvlak hadden met het behandelde onderwerp. Bij de bestudering is nauwkeurig gekeken welke aspecten uit dit deel van het gezondheidsrecht van toepassing waren op dit onderzoek, en in hoeverre dit relevant was voor de lezer van dit onderzoek. Het mag duidelijk zijn dat er in zijn geheel veel geschreven kan worden over het onderwerp uit dit hoofdstuk, maar in dit onderzoek is er nadrukkelijk voor gekozen om hetgeen over dit onderwerp in dit onderzoek is opgenomen te beperken tot dat wat noodzakelijk was voor het vervolgen van het onderzoek en het begrijpelijk houden van de materie voor de lezer.

2.3.4 hoofdstuk 6
Bij dit hoofdstuk heeft de onderzoeker kunnen beschikken over een beperkt aantal bronnen gezien het feit dat dit hoofdstuk voorziet in de uitwerking van een aanhangig wetsvoorstel. Het is inherent aan de aard van een wetsvoorstel dat er in de periode voor aanname (of afwijzing) van het voorstel weinig tot geen literaire bronnen zijn die zich hierin verdiepen. Daarmee is in hoofdstuk 6 duidelijk te zien dat in dit onderzoek heel nauwkeurig gekeken is naar het wetsvoorstel en alle kamerstukken die zich daaromheen begeven om zo een helder beeld te krijgen van de impact en veranderingen die de verschillende bepalingen uit het wetsvoorstel met zich mee brengen. Aan het einde van hoofdstuk 6 waren de laatste onderzoekspunten geformuleerd. Bij het opstellen bij van de onderzoekspunten is veelal de theoretische inhoud van het bijbehorende hoofdstuk bepalend geweest voor de uiteindelijke formulering van deze punten. Alle onderzoekspunten vloeien logischerwijs voort uit de uiteenzetting die daarvoor heeft plaats gevonden. Bij hoofdstuk 3 is er nadrukkelijk voor gekozen om een aspect uit de theorie niet terug te laten komen in de onderzoekspunten omdat deze, zoals ook blijkt uit de daaraan voorafgaande uitwerkingen, niet relevant waren voor de systemen die in dit onderzoek centraal staan. Voorgaande heeft betrekking op paragraaf 3.6. Deze paragraaf gaf aan dat het onderscheid binnen de wet tussen de ‘gewone’ en bijzondere persoonsgegevens erg belangrijk was. De aard van de onderzochte systemen was zodanig dat verondersteld kon worden dat het hier ging om verwerkingen van persoonsgegevens uit de laatste categorie. Zodoende is ervoor gekozen om niet een onderzoekspunt op te nemen die zich zou richten op de vraag in hoeverre er bij de verwerking door de systemen sprake was van bijzondere persoonsgegevens.

2.4 Praktijkonderzoek

2.4.1 Interviews
Bij deze fase van het onderzoek is gekozen voor kwalitatief onderzoek. Omdat dit onderzoek zich richt op een drietal uitwisselingssystemen is ervoor gekozen om het praktijkonderzoek te baseren op gesprekken met experts en andere betrokkenen met gedegen kennis van de verschillende systemen. Door voor deze werkwijze te kiezen is het voor de onderzoeker mogelijk geworden om diepgaande vragen te stellen over de werking van de systemen aan personen die gezien hun functie en kennis in staat zijn om het nodige inzicht te verschaffen in de verschillende vraagstukken die tijdens dit onderzoek aan bod komen. De interviewvragen waren een mix van open en gesloten vragen en zijn terug te vinden in bijlage 1. Bij de uitwerking van de resultaten uit het praktijkonderzoek is er bewust voor gekozen om de respondenten anoniem te houden. Tijdens de verschillende interviews is het van belang geweest dat respondenten vrijuit konden spreken en mede hierom heeft de onderzoeker ervoor gekozen om bij aanvang van elk gesprek de vertrouwelijkheid hiervan te garanderen. Uiteindelijk zijn er acht interviewmomenten geweest. Eén gesprek was met twee respondenten tegelijk. De functies van de in totaal negen respondenten liepen sterk uiteen. Onder de respondenten zitten afdelingshoofden, experts, beheerders en tot slot medewerkers die gebruik maken van het systeem. Door deze keuze van respondenten is het mogelijk om vanuit verschillende lagen van de organisatie antwoorden te krijgen op dezelfde vragen. Op deze manier is er in dit onderzoek geprobeerd om de kwaliteit van het onderzoek zo veel mogelijk te bevorderen. Om alle resultaten uit de interviews zo goed mogelijk te verwerken in het onderzoek zijn alle gesprekken opgenomen, vervolgens zijn de gesprekken uitgeschreven. De verschillende stukken uit deze transcripties zijn daarna per onderwerp gelabeld en gesorteerd. In de interviews zijn vaak zeer uitgebreide antwoorden gegeven, waarin ook veel informatie verweven zat die te maken had met andere systemen en andere vragen. Zodoende was het noodzakelijk om bij de uitwerking bepaalde delen van de transcriptie op te delen en te verplaatsen zodat relevante informatie geordend kon worden bij het onderwerp waar het betrekking op had. Overbodige stukken zijn er vervolgend uitgehaald. Dit geheel is verwerkt in de verschillende onderdelen van het praktijkonderzoek. Het eerste deel van het praktijkonderzoek is een verzameling van informatie die door de verschillende gesprekken tot stand heeft kunnen komen, en dat nadrukkelijk bedoeld is om de lezer een

[15] H.J.J. Leenen e.a., *Handboek gezondheidsrecht Deel I: Rechten van mensen in de gezondheidszorg,* Hoofddorp: Boom Juridische uitgevers 2011

context te verschaffen waarin de verdere praktijkresultaten beter begrepen kunnen worden. Het uitschrijven van de interviews heeft het mogelijk gemaakt om vervolgens tot een heldere uiteenzetting van de onderzoeksresultaten te komen.

In de beginfase van het onderzoek is overwogen om ook andere UMC's te betrekken in het onderzoek. Uiteindelijk heeft is ervoor gekozen om hiervan af te zien. De onderzoeker kwam later in het onderzoek tot het oordeel dat het betrekken van andere UMC's weinig toe zou voegen aan de beantwoording van de onderzoeksvragen. Andere UMC's worstelen immers met dezelfde toekomstige eisen. Daarnaast zou daarmee het onderzoek ook te groot zijn geworden, zonder dat het zijn evenredigheid aan waarde aan onderzoeksresultaten zou opleveren.

2.4.2 Onderzoeksresultaten

In dit hoofdstuk is op basis van het proces beschreven in de vorige paragraaf gekozen om de resultaten niet per systeem te behandelen. In plaats daarvan er gekozen voor een systematiek die beter aansluit bij de uiteindelijke resultaten. In het hoofdstuk met de onderzoeksresultaten zijn specifieke onderwerpen geformuleerd die in grote lijnen gebaseerd is op de volgorde van onderwerpen zoals deze ook in de theoretische hoofdstukken van het onderzoek aan de orde komen. Hoewel een behandeling per systeem wellicht voor de hand ligt, zou dit bij dit onderzoek het leggen van de verbanden tussen de verschillende systemen hebben bemoeilijkt. Uiteindelijk is voor deze opzet gekozen omdat de resultaten hierdoor begrijpelijker op de lezer over konden worden gebracht.

2.4.3 Analyse, conclusie en aanbevelingen

Door de uitkomsten van de theorie naast de praktijkresultaten te leggen kon een analyse worden gemaakt. Hierbij is er voor gekozen om per onderzoekspunt uit de theorie te kijken naar de praktijkresultaten die daarop van toepassing waren. Door deze analyse was het vervolgens mogelijk om een conclusie en tot slot aanbevelingen te formuleren. In de formulering van de conclusie en aanbevelingen is er gekozen voor een strikt juridische benadering. In het slot van dit onderzoek in daarom ook te zien dat de aanbevelingen vrij dwingend geformuleerd worden. Hiermee is het niet de bedoeling geweest om op de stoel van de bestuurders van de organisatie te gaan zitten. De onderzoeker is van mening dat de bewuste keuze om de aanbevelingen zodanig te formuleren de juridische noodzaak van deze aanbevelingen goed naar voren laat komen. De lezer dient zich echter te realiseren dat bij de besluitvorming bij een grote organisatie als het UMCG niet alleen juridische aspecten, maar bijvoorbeeld ook budgettaire of organisatorische factoren een rol kunnen spelen. Dit onderzoek is vanuit een puur juridisch kader opgesteld, en dat levert een minder genuanceerd eindoordeel op.

2.5 Kwaliteit

Door te kiezen voor een werkwijze waarbij een selecte groep respondenten wordt geïnterviewd, ontstaat terecht de vraag in hoeverre een dergelijk onderzoek representatief kan zijn. Hierbij is het van belang om te onthouden dat dit onderzoek uiteindelijk niet alleen een onderzoek is naar de specifiek onderzochte systemen, maar naar de impact van het aanhangige wetsvoorstel als geheel. Door een weloverwogen afweging te maken in de geïnterviewde respondenten is niet alleen getracht om een zo representatief mogelijk resultaat te krijgen, maar ook om vanuit verschillende invalshoeken inzicht te krijgen in wat de organisatie als geheel te wachten staat bij de eventuele inwerkingtreding van dit nieuwe wetsvoorstel. Door zo objectief mogelijk alle gesprekken te voeren, is het voor de onderzoeker mogelijk geworden om de kwaliteit van het onderzoek zo veel mogelijk te garanderen. Eerder gevoerde gesprekken hadden geen invloed op de objectiviteit van de onderzoeker in verdere gesprekken. Door de informatie uit latere gesprekken kon de onderzoeker bij het uitwerken van bandopnames van eerder gevoerde gesprekken soms bepaalde zaken beter begrijpen. Dit bevestigd dat deze werkwijze de kwaliteit ten goede is gekomen. Daar komt nog bij dat tijdens de interviews getracht is om respondenten zo veel mogelijk aan het woord te laten, doch waar nodig wel doorgevraagd is om te zorgen dat de soms zeer technische aspecten duidelijk uitgelegd werden. Mede door de professionaliteit en kunde van de respondenten is het mogelijk geworden voor de onderzoeker om deze technische aspecten te begrijpen, te vereenvoudigen en uiteindelijk te verwerken in het onderzoek. Veel van de figuren in het onderzoek, zijn hier het resultaat van.

2.6 Het proces

In het verloop van het onderzoek is niet altijd alles volgens de oorspronkelijke planning verlopen. In deze paragraaf wordt er kort aandacht besteed aan het onderzoeksproces.

Bij het formuleren van de onderzoeksopzet is het nodig geweest om het kader van het onderzoek aan te passen. In eerste instantie zou dit onderzoek zich richten op het hele geheel aan uitwisselingssystemen van het UMCG. Na overleg is besloten om het onderzoekskader te beperken tot een drietal systemen die wel verschillend van aard, maar door de organisatie als representatief worden gezien voor het totaal aan elektronische uitwisselingssystemen binnen het UMCG. Hierdoor heeft het onderzoek in het begin enige vertraging opgelopen. Daarnaast bleek al snel

dat de tijd die van te voren was ingeraamd voor de uitwerking van de theoretische hoofdstukken niet voldoende zou zijn dit gedeelte van het onderzoek in af te ronden. Door deze vertraging schoof de planning van het onderzoek iets vooruit, waardoor het moment waarop de interviews gepland zouden worden samen viel met verschillende vakantieperioden. De interviews waren, ondanks de vertraging, uiteindelijk een enorme bron aan informatie, en zijn door de onderzoeker met veel plezier afgenomen. Met dank aan de openheid en benaderbaarheid van de respondenten. Zonder hen was dit onderzoek veel minder leuk geweest om uit te voeren.

Tot slot is het goed om te vermelden dat in de aanbevelingen wordt aangespoord om onderzoek te doen naar de capaciteiten van XDS om zodanig te functioneren dat het de organisatie kan helpen bij het compliant maken van de organisatie aan bestaande en toekomstige wettelijke eisen. Ook raad ik het UMCG aan onderzoek te doen naar de wijze waarop medewerkers en personeel van het UMCG bewust kunnen worden gemaakt van de wettelijke impact van de eventuele mankementen in de systemen waar zij mee werken, zodat misstanden eerder aan het licht komen en worden aangepakt.

3 Wet bescherming persoonsgegevens

3.1 Inleiding
Dit hoofdstuk behandelt de theorie. In dit hoofdstuk wordt een deel van het antwoord geformuleerd op de deelvraag:
- *Welke eisen worden er in de wet gesteld aan een elektronisch uitwisselingssysteem?*

Achtereenvolgens worden de volgende onderwerpen besproken: geschiedenis (§3.2), reikwijdte (§ 3.3), belangrijke begrippen (§3.4), algemene voorwaarden verwerken persoonsgegevens (§3.5), bijzondere gegevens (§3.6), de conclusie (§3.7) en tot slot de onderzoekspunten (§3.8). Dit hoofdstuk heeft als doel om de lezer kennis te laten maken met deze wet om zo de komende hoofstukken beter te kunnen begrijpen.

3.2 Geschiedenis
De achtergrond van het ontstaan van de Wet Bescherming Persoonsgegevens hangt heel nauw samen met wat er dagelijks om ons heen gebeurt. Burgers leven in een informatiemaatschappij, wier ontwikkeling haast geen einde lijkt te kennen. Ondanks de vele voordelen die dit informatietijdperk met zich mee brengt, zijn er natuurlijk ook gevaren. Eén gevaar is bijvoorbeeld de wijze waarop informatietechnologie een inbreuk kan maken op onze persoonlijke leefsfeer.[16] Informatievergaring kan op zichzelf erg nuttig zijn, maar daarbij moet het recht op privacy niet vergeten worden. In de Europese Unie houden verschillende bestuurlijke organen zich al jaren bezig met de vraag hoe wij verantwoordelijk met deze nieuwe ontwikkelingen om moeten gaan, en in hoeverre de Europese burger beschermt moet worden tegen de gevaren die deze technologische vooruitgang met zich mee brengt. Dat de huidige ontwikkelingen op het gebied van informatievergaring veel voordelen hebben staat hierbij niet ter discussie. In 1995 kwam de Richtlijn 95/46/EG *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens* tot stand.[17] Deze richtlijn bood een kader waarbinnen lidstaten zelf een nieuwe privacywet moesten opstellen of eventueel een oudere wet moesten aanpassen. Het doel van de richtlijn was privacywetgeving tussen de verschillende lidstaten enigszins te harmoniseren. De Wet Bescherming Persoonsgegevens (hierna Wbp) is de Nederlandse uitwerking van deze richtlijn en is sinds 1 september 2001 van kracht. [18] De Wbp verving de Wet persoonsregistratie (Wpr).

3.3 Reikwijdte

3.3.1 Inleiding
Dat er wetten zijn die voorwaarden stellen aan het verwerken van persoonsgegevens mag duidelijk zijn, maar wanneer zijn deze eigenlijk van toepassing? Onder welke voorwaarden is er sprake van verwerking van persoonsgegevens en wanneer niet? Om een antwoord op deze vraag te krijgen moet eerst de reikwijdte van de Wbp bepaald worden.

3.3.2 Wettelijk kader
De Wbp geeft zelf een duidelijk kader, waarbinnen zij van toepassing is.[19] Artikel 2 lid 1 Wbp zegt dat de wet van toepassing is op alle geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. De wet is echter ook van toepassing op de verwerking van persoonsgegevens die handmatig worden verwerkt en in een bestand worden of zullen worden opgenomen. Deze omschrijving vormt de basis voor de reikwijdte van de Wbp. Het is belangrijk om te benadrukken dat alle persoonsgegevens die onderdeel van een bestand zijn of gaan zijn dus onder deze wet vallen. Hierbij maakt het dus niet uit of deze gegevens handmatig, geautomatiseerd of deels handmatig en deels geautomatiseerd verwerkt zijn.

Het begrip ‘bestand’ vraagt om verdere toelichting. Een bestand kan handmatig of geautomatiseerd worden bijgehouden. Is er sprake van geautomatiseerde verwerking, dan doet het er niet toe of er sprake is van een bestand of niet. Waar het een handmatig gevoerd bestand betreft doet dit er wel toe.

---

[16] Een grondrecht zoals vastgelegd in artikel 10 lid 1 Grondwet, artikel 8 Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 17 Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR).
[17] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 3.
[18] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 4-5.
[19] Artikel 1, 2, 3 en 4 Wbp.

Handmatig gevoerde bestanden vallen alleen onder de Wbp als er sprake is van bestanden waarbij 'bijzondere maatregelen met het oog op raadpleging' getroffen zijn.[20] Met andere woorden, als er maatregelen genomen zijn om het makkelijker te maken om een bestand te ordenen of inzichtelijk te maken en er iets in terug te zoeken, valt deze onder het bereik van de Wbp. Bestanden bestaande uit persoonsgegevens in de vorm van beeld en geluid zijn hierop geen uitzondering.[21]

De rest van artikel 2 en artikel 3 Wbp benoemen vervolgens een aantal uitzonderingen op het bereik van de Wbp. Zo zijn er bijvoorbeeld uitzonderingen voor verwerking van persoonsgegevens door de krijgsmacht maar ook voor verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden.[22] De 'verantwoordelijke' voor de verwerking van de persoonsgegevens heeft zich aan de Wbp te houden wanneer deze gevestigd is in Nederland of ergens anders in de EU.[23] De Wbp stelt ook dat wanneer iemand buiten de EU persoonsgegevens verwerkt over personen in Nederland, zij dan verplicht zijn in Nederland een persoon of instantie als vertegenwoordiger aan te wijzen die namens de gegevensverwerker handelt volgens de regels uit de Wbp. Hiermee worden persoonsgegevens beschermd, ook als zij door buitenlandse personen of instanties worden verwerkt. Hierop bestaat eventueel een uitzondering als er slechts sprake is van doorvoer van persoonsgegevens. Zodra deze gegevens echter ergens worden opgeslagen vervalt deze uitzondering.[24]

3.4 Belangrijke begrippen

3.4.1 Inleiding

Om de wettekst van de Wbp te kunnen begrijpen, is het noodzakelijk om aandacht te besteden aan de verschillende begrippen die de Wbp hanteert. De wet formuleert al deze begrippen in artikel 1. Hier volgt een uiteenzetting van de belangrijkste hiervan.

3.4.2 Persoonsgegeven

Als de wet spreekt over een persoonsgegeven, dan bedoelt zij elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon. Alle gegevens die wijzen naar een natuurlijk persoon die daardoor identificeerbaar wordt, zijn persoonsgegevens.[25] Gegevens over rechtspersonen of overleden personen vallen hier niet onder. Men kan zich afvragen wanneer een natuurlijk persoon 'identificeerbaar' of 'redelijkerwijs identificeerbaar' is aan de hand van een bepaald gegeven, en wanneer bijvoorbeeld juist niet. Er zal altijd een afweging gemaakt moeten worden tussen enerzijds de hoeveelheid middelen die moeten worden ingezet om het gegeven tot de bijbehorende persoon te herleiden, en de aannemelijkheid dat deze middelen daadwerkelijk daarvoor worden gebruikt. Een andere belangrijke factor in het vaststellen of een natuurlijk persoon te identificeren valt, is de stand van de techniek op dat moment. Men moet er rekening mee houden dat de voortgang van de techniek ook de eenvoud in het herleiden van personen kan vergroten of verkleinen.[26] In de Memorie van toelichting op de Wbp is te lezen dat de wetgever ervan uit gaat dat er sprake is van een persoonsgegeven als de persoon op basis van het gegeven redelijkerwijs geïdentificeerd kan worden, zonder dat daar onevenredige inspanning voor nodig is.[27]
Niet elk verband tussen gegeven en persoon maakt dus van een gegeven een persoonsgegeven. Als de mogelijkheid theoretisch bestaat dat iemand op basis van een gegeven te identificeren is, maar in de praktijk eigenlijk niet voor kan komen, dan is er ook geen sprake van een persoonsgegeven.
In veel gevallen zullen persoonsgegevens gegevens zijn over eigenschappen, gedragingen of opvattingen van een persoon. In andere gevallen kan de context waarin een bepaald gegeven gebruikt of verwerkt wordt ook meespelen. Het maatschappelijk gebruik van een bepaald gegeven kan het tot een persoonsgegeven maken.[28] Een eenvoudig voorbeeld hiervan is een telefoonnummer.

3.4.3 Verwerking

Ook het begrip 'verwerking' biedt meer ruimte dat in eerste instantie wellicht kan worden aangenomen. Het Wbp bepaalt namelijk dat onder verwerking ook mag worden begrepen: 'Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren,

---

[20] *Kamerstukken II* 1997/1998, 25982, nr. 11, p. 3.
[21] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 70-71.
[22] Artikel 2 en 3 Wbp.
[23] Artikel 4 Wbp.
[24] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 76-77.
[25] *Kamerstukken II* 1997/1998, 25982, nr. 11, p. 46.
[26] *Kamerstukken II* 1997/1998, 25982, nr. 9, p 1-2.
[27] *Kamerstukken II* 1997/1998, 25982, nr. 3, p. 47-48.
[28] *Kamerstukken II* 1997/1998, 25982, nr. 3, p. 46-47.

bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens'. [29] Hiermee wordt het begrip 'verwerking' juridisch breed getrokken.

3.4.5 Verantwoordelijke

Met dit begrip heeft de wetgever bewust gekozen om het begrip 'houder' te vervangen. Hiermee kan ook inzichtelijk gemaakt worden wat het doel is van dit begrip.[30] Men wil te allen tijde een verantwoordelijke aanwijzen in de Wbp om zo ook in het geval van geautomatiseerde gegevensverwerking altijd iemand aan te kunnen wijzen die verantwoordelijkheid draagt voor de verwerking. De wetgever legt de nadruk op het feit dat de persoon of instantie die vaststelt welk doel de gegevensverwerking heeft en welke middelen daarvoor gebruikt mogen worden, ook als verantwoordelijke gezien moet worden. Deze partij is immers de bepalende factor achter het feit dat er überhaupt persoonsgegevens verwerkt worden.

3.4.6 Betrokkene, bewerker & derde

De betrokkene is de persoon over wie het persoonsgegeven informatie bevat. De bewerker is de rechtspersoon of natuurlijke persoon die de persoonsgegevens verwerkt op grond van een contractuele relatie, maar niet onder het directe gezag valt van de verantwoordelijke. Een voorbeeld hiervan is als de persoonsverwerking uitbesteed wordt aan een ander bedrijf. Een derde is iemand die gemachtigd is persoonsgegevens te verwerken maar die geen betrokkene, bewerker of verantwoordelijke is in de zin van de Wbp. In de praktijk kan het bijvoorbeeld voorkomen dat een persoonsgegeven betrekking heeft op meer dan één persoon. In een dergelijk geval zijn deze personen betrokkene voor zichzelf en derde ten opzichte van elkaar.[31]

3.5 Algemene voorwaarden verwerken persoonsgegevens

3.5.1 Inleiding

Nu het kader van de wet is afgebakend en de begrippen ons duidelijk zijn, richt deze paragraaf zich op de voorwaarden die worden gesteld bij het verwerken van persoonsgegevens. Iemand mag namelijk niet zomaar persoonsgegevens verwerken.

3.5.2 Voorwaarden

Persoonsgegevens dienen altijd verzameld te worden op basis van vooraf vastgestelde doeleinden. Deze doeleinden moeten van tevoren duidelijk en schriftelijk worden opgesteld.[32] Persoonsgegevens mogen alleen op gerechtvaardigde gronden worden verwerkt, en die gronden worden in artikel 8 Wbp gegeven. Dit artikel bevat een zogeheten 'limitatieve opsomming' van gronden.[33] Biedt het artikel geen grond voor verwerking, dan is het dus ook niet toegestaan.[34] Op deze regel bestaan geen uitzonderingen.[35] De gronden van artikel 8 luiden als volgt:

Persoonsgegevens mogen slechts worden verwerkt indien:

- ***a.****de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;*
- ***b.****de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;*
- ***c.****de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;*
- ***d.****de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;*
- ***e.****de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of*
- ***f.****de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.*(Artikel 8 Wbp)

---

[29] Artikel 1 sub b Wbp.
[30] *Kamerstukken II*1997/1998, 25982, nr. 3, p. 39.
[31] Voorbeeld gegeven door voormalig CBP, Wbp naslag, hoofdstuk 1, omschrijving betrokkene.
[32] Artikel 7 Wbp,
[33] *Kamerstukken II*1997/1998, 25982, nr. 3, p. 80.
[34] Artikel 9 Wbp.
[35] *Kamerstukken II*1997/1998, 25982, nr. 13, p. 5-6.

Hierbij is sub b voor dit onderzoek van groot belang. Hierin ligt namelijk de grondslag voor persoonsgegevensverwerking op basis van een geneeskundige behandelingsovereenkomst. Hierover meer in hoofdstuk 5.

Nadat de doeleinden zijn vastgesteld, mag de verwerking van persoonsgegevens plaatsvinden. Echter moet die verwerking toereikend, niet overmatig en ter zake dienend zijn. Dit wordt beoordeeld op basis van het doeleinde. Men mag dus niet meer en niet minder aan gegevens verzamelen dan voor het doel noodzakelijk.[36] Op de 'verantwoordelijke' ligt ook een verplichting om de nodige maatregelen te treffen om de juistheid en nauwkeurigheid van de gegevens te waarborgen. Hierbij legt de wetgever de 'verantwoordelijke' de verplichting op om alle maatregelen te nemen die redelijkerwijs nodig zijn om de juistheid en nauwkeurigheid van de gegevens zo veel mogelijk te garanderen.[37]

Persoonsgegevens die verwerkt worden, moeten uiteraard beveiligd worden. Artikel 13 Wbp zegt hierover dat:
"passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking."(artikel 13 Wbp)
Dit artikel geeft een eerste aanzet voor de technische eisen die worden gesteld aan de beveiliging van persoonsgegevens en systemen die die gegevens uitwisselen. Hierover meer in hoofdstuk 4.

Een laatste voorwaarde bij het verwerken van persoonsgegevens is dat de 'verantwoordelijke' de 'betrokkene' informeert over het feit dat zijn persoonsgegevens verwerkt zullen gaan worden. Dit is alleen noodzakelijk als de 'betrokkene' hier nog niet van op de hoogte is. Deze informatieplicht is vooral belangrijk bij vergaring van persoonsgegevens die niet via de 'betrokkene' zelf worden aangeleverd, en bij gegevensverwerking die niet is gebaseerd op de grondslag genoemd in artikel 8 sub a Wbp.[38]

3.6 Bijzondere gegevens

3.6.1 Inleiding

Binnen het begrip persoonsgegevens wordt onderscheid gemaakt tussen gewone persoonsgegevens en bijzondere persoonsgegevens. De wet heeft een speciale positie en aanvullende eisen geformuleerd waar het specifieke gegevens betreft. Maar om welke gegevens gaat dat dan?

3.6.2 Gezondheidsgegevens

Bijzondere persoonsgegevens zijn gegevens over *"(…) iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging"* (artikel 16 Wbp).
Persoonsgegevens met betrekking tot iemands gezondheid zijn dus bijzonder in de ogen van de Wbp en daar dient men dus ook anders mee om te gaan. Volgens artikel 16 Wbp bestaat er een algeheel verbod op het verwerken van dergelijke gegevens. Dit verbod is in sommige gevallen echter niet van toepassing. In artikel 21 van de Wbp worden deze gevallen benoemd. De wet zegt dat er een uitzondering bestaat voor:
"hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover (de verwerking persoonsgegevens betreffende iemands gezondheid) *met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is"* (artikel 21 lid 1 sub a Wbp)
In bovenstaande gevallen: *"worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht."* (artikel 21 lid 2 Wbp)

Voor zorgverleners is deze uitzonderingsbepaling dus van groot belang, anders zou het verwerken van persoonsgegevens in de zorg bijna onmogelijk zijn geweest. Artikel 23 Wbp geeft een andere weg waarmee een basis voor verwerking van gezondheidsgegevens kan ontstaan. Het artikel noemt verschillende gronden waarop verwerking mogelijk wordt, maar lid 1 sub a is voor dit onderzoek het meest relevant. Geeft de 'betrokkene' nadrukkelijke toestemming voor gegevensverwerking, dan is op basis daarvan ook een legitieme basis gecreëerd waarmee gegevensverwerking wetmatig kan plaatsvinden.

---

[36] Artikel 11 Wbp, *Kamerstukken II* 1997/1998, 25982, nr. 3, p. 96-97.
[37] *Kamerstukken II* 1997/1998, 25982, nr. 3, p. 97.
[38] Artikel 33 en 34 Wbp.

3.7 Conclusie

Een groot deel van de theorie achter de eerste deelvraag is hier behandeld. Duidelijk is dat de Wbp veel voorwaarden en eisen stelt aan de wijze waarop persoonsgegevens mogen worden verwerkt. Voor medische gegevens bestaat er zelfs een algeheel verbod. In sommige gevallen is het verwerken van medische persoonsgegevens toch toegestaan, mits aan alle aanvullende eisen wordt voldaan. De Wbp biedt een duidelijk kader waaruit men kan werken. Nu de belangrijkste bepalingen uit deze wet aan bod zijn gekomen, zal er in de volgende hoofdstukken aandacht besteed worden aan de beveiligingseisen, de geneeskundige behandelingsovereenkomst en de rol van het medisch beroepsgeheim.

3.8 Onderzoekspunten

De onderzoekspunten uit dit hoofdstuk zijn:

- Is bij de verwerking van persoonsgegevens voldaan aan de voorwaarden uit de Wbp?

- Wat is het doel van de verwerking?

- Zijn die doeleinden gebaseerd op een rechtmatige grond?

- Is de verwerking toereikend, niet overmatig en ter zake dienend?

- Weet de patiënt dat zijn gegevens verwerkt worden, is hij/zij hier over juist geïnformeerd en heeft hij/zij toestemming gegeven?

4. Beveiliging persoonsgegevens

4.1 Inleiding

Uit het vorige hoofdstuk is duidelijk geworden dat aan het verwerken van persoonsgegevens verschillende eisen worden gesteld. Een van die eisen is dat de persoonsgegevens goed beveiligd zijn. In de wet heeft de wetgever het over passende maatregelen en een passend beveiligingsniveau. Maar wat is dan 'passend'?
Dat is de vraag waar dit hoofdstuk zich over buigt. Dit hoofdstuk behandelt de theorie, en formuleert gedeeltelijk het antwoord op de vraag:
- Welke eisen worden er in de wet gesteld aan een elektronisch uitwisselingssysteem?

Achtereenvolgens worden de volgende onderwerpen behandeld: beveiliging (§4.2), beveiliging door een bewerker (§4.3), beveiliging in de praktijk (§4.4), betrouwbaarheidseisen (§4.5), de maatregelen (§4.6), de conclusie (§4.7) en tot slot de onderzoekspunten (§4.8). Dit hoofdstuk heeft als doel om de lezer inzicht te geven in de wijze en mate waarin persoonsgegevens beveiligd moeten te worden.

4.2 Beveiliging

De Wbp eist in artikel 13 dat alle persoonsgegevens die worden verwerkt, beveiligd moeten worden. De letterlijke tekst van het artikel luidt als volgt:
"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."(artikel 13 Wbp)
De wetgever spreekt over passende maatregelen om persoonsgegevens te beveiligen. Uit het artikel kan echter niet heel concreet op worden gemaakt om welke maatregelen het dan precies gaat. Bij het formuleren van die maatregelen is een taak weggelegd voor de Autoriteit Persoonsgegevens (hierna AP) dat voor 2016 bekend stond als het College Bescherming Persoonsgegevens (Hierna CBP).[39] De AP is belast met het toezicht op de privacywetgeving die voortvloeit uit de Privacyrichtlijn 95/46/EG. Artikel 28 van die richtlijn verplicht het instellen van een dergelijke toezichthoudende autoriteit. Uit die wet is ook af te leiden dat het aan de AP is om duidelijkheid te verschaffen over de praktische uitwerking van verschillende wetsbepalingen.[40] Met het oog op deze verplichting heeft het voormalige CBP dan ook zogeheten 'richtsnoeren' opgesteld aan de hand waarvan men kan nagaan welke 'passende' maatregelen in de ogen van de wet verwacht worden.
Deze richtsnoeren zijn voor dit onderzoek van groot belang, omdat hiermee invulling wordt gegeven aan hoe men volgens de wet de huidige elektronische uitwisselingsystemen bij het UMCG zou moeten hebben ingericht. Verderop in het onderzoek zal bij de behandeling van het nieuwe wetsvoorstel besproken worden welke eventuele veranderingen het UMCG op dit gebied kan verwachten. Dit neemt niet weg dat de interpretatie van het voormalige CBP de basis is waarop een EUS ingericht moet zijn.

In de richtsnoeren wordt duidelijk een begin gemaakt om de juridische vereisten uit de wet vast te knopen aan het domein van de informatiebeveiliging. Deze verweving van werelden is bij dit onderzoek onvermijdelijk en zal vanaf dit hoofdstuk waar nodig voorzien worden van toelichting waar het termen betreft uit de informatiewereld die niet voor zich spreken. In de richtsnoeren wordt een tweedeling gemaakt tussen beveiligingseisen in het algemeen en de eisen die gesteld worden op het moment dat een bewerker, in opdracht van een verantwoordelijke, de persoonsgegevens verwerkt. De Wbp maakt hier namelijk ook een onderscheid in. Artikel 13 stelt de algemene beveiligingseis maar artikel 12 en 14 Wbp gaan dieper in op de eisen die aan een bewerker worden gesteld.

Artikel 13 begint als volgt: *"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking."* (artikel 13 Wbp). Onder onrechtmatige verwerking wordt verstaan de aantasting van de persoonsgegevens of de onbevoegde kennisneming, wijziging of verstrekking van deze gegevens.[41]

Het artikel geeft vervolgens zeer duidelijk aan dat deze eerder genoemde maatregelen een garantie moeten bieden voor een passend beveiligingsniveau: "*Deze maatregelen garanderen, rekening houdend met de stand van de*

[39] Afkortingen AP en CBP worden door elkaar gebruikt maar kunnen voor dit onderzoek in principe als dezelfde instantie gezien worden.
[40] Artikel 28 Privacyrichtlijn 95/46/EG.
[41] *Kamerstukken II,* 1997/98, 25 892, nr. 3, p.98.

techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen."(Artikel 13 Wbp)

Het is goed om op te merken dat het artikel rekening houdt met de ontwikkelingen van de huidige technieken van beveiliging. Door de zin als zodanig te formuleren geeft het artikel de verplichting om waakzaam te zijn op deze veranderingen, waarbij telkens de verplichting voor adequate beveiliging blijft bestaan. Wat meteen zichtbaar wordt is dat de wetgever door het woord 'passend' te gebruiken, ruimte laat voor interpretatie. In de Memorie van Toelichting heeft de wetgever aangegeven dat er sprake moet zijn van een zekere proportionaliteit tussen de beveiligingsmaatregelen en de te beschermen gegevens. Er moet een evenwichtige verhouding bestaat tussen de maatregelen en de gegevens.[42] Hiermee wordt duidelijk wat de wetgever wil bereiken. Niet elk persoonsgegeven moet op dezelfde manier bewaakt worden. Er moet sprake zijn van proportionaliteit tussen de persoonsgegevens en de te nemen beveiligingsmaatregelen. Er zijn verschillende beveiligingsniveaus, voor verschillende soorten persoonsgegevens. Het ene persoonsgegeven kan namelijk gevoeliger, of meer inbreuk maken op iemands levenssfeer, dan het andere persoonsgegeven. Hierbij heeft de wetgever in de Wbp bijvoorbeeld al een onderscheid gemaakt tussen gewone persoonsgegevens en bijzondere persoonsgegevens.[43] Er zal dus altijd een afweging plaats moeten vinden, die in de praktijk wel een garantie moet bieden voor adequate beveiliging. Dit betekent echter niet dat de beveiliging in een bepaald geval dus altijd onverslaanbaar moet zijn.[44] Uit de toelichting van de wetgever kan afgeleid worden dat eenzelfde beveiligingsmaatregel soms passend en soms ook niet passend kan zijn. Bepalend hierbij is de verhouding tussen de geringe extra kosten van de te nemen maatregel ten opzichte van toename in veiligheid van de gegevens. Zijn de te maken kosten 'disproportioneel' aan de extra beveiliging die daardoor wordt gerealiseerd dan is de maatregel niet passend.[45]
De afwegingen zoals boven omschreven zullen na een bepaalde tijd opnieuw gemaakt moeten worden, omdat eventuele kosten van beveiligingsmaatregelen of het ontstaan van nieuwe beveiligingsmogelijkheden tot een andere afweging kunnen leiden.[46]

De laatste zin van artikel 13 Wbp geeft aan dat de maatregelen die getroffen worden, ook nog een ander doel hebben: *"De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."* (Artikel 13 Wbp)

Hiermee legt de wetgever een laatste verplichting in de wet die samen met alle eerdere eisen, erg veel invloed heeft op de inrichting van het gehele proces van persoonsgegevensverwerking. De wetgever geeft namelijk aan dat de wijze waarop artikel 13 Wbp is opgezet, de nadruk legt op de structuur van de gebruikte informatiesystemen. Daarmee moet worden voorkomen dat men vervalt in 'voortdurende controle op individuele gevallen van onrechtmatig gegevensgebruik'.[47] Met andere woorden, een verantwoordelijke is verplicht om veel beveiligingsrisico's op voorhand te inventariseren en te beveiligen door het proces van verwerking bij oprichting al zodanig vorm te geven dat alle beveiligingsrisico's die onaanvaardbaar zijn vanuit de wet, zich niet voor kunnen doen. Wat onaanvaardbaar is hangt in dit geval samen met de eerder beschreven afwegingen die, natuurlijk niet alleen herhaaldelijk maar ook aan het begin van dit proces, gemaakt moeten worden. In de praktijk ziet men dat er toch wel degelijk een vorm van voortdurende controle is, omdat het vaak lastig blijkt te zijn om alle (toekomstige) beveiligingsrisico's op voorhand te voorzien.

Bij de vormgeving van dit proces van gegevensverwerking ziet de wetgever een belangrijke rol weggelegd voor software.[48] Hierbij noemt de wetgever ook de zogeheten *privacy enhancing technologies* (PET). PET is een verzamelterm die allerlei informatietechnieken omvat. Deze technieken hebben als doel om de risico's van het verwerken van persoonsgegevens zo veel mogelijk te beperken.[49] Een belangrijk principe achter deze technologieën is het verminderen van herleidbaarheid van het persoonsgegeven tot de betrokkene. Sommige technieken zijn zelfs in staat om persoonsgegevens volledig te anonimiseren.[50]

---

[42] *Kamerstukken II,* 1997/98, 25 892, nr. 3, p.99.
[43] Artikel 16 Wbp.
[44] *Kamerstukken II,* 1997/98, 25 892, nr. 3, p.99.
[45] *Kamerstukken II,* 1997/98, 25 892, nr. 92c, p.15.
[46] *Kamerstukken II,* 1999-2000, 25 892, nr. 92c, p.15.
[47] *Kamerstukken II,* 1999-2000, 25 892, nr. 22.
[48] *Kamerstukken II,* 1997/98, 25 892, nr. 3, p. 99.
[49] *Privacy enhancing technologies, Witboek voor beslissers,* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag, december 2004, p. 5.
[50] *CBP Richtsnoeren Beveiliging van persoonsgegevens,* Den Haag, 2013, p. 10.

4.3 Beveiliging door een bewerker

Omdat de wet nadere bepalingen heeft opgesteld met betrekking tot het gebruiken van een bewerker is het van belang om kort in te gaan op het verschil dat ontstaat ten opzichte van de eerder uiteengezette wettelijke vereisten. Een bewerker, iemand die in zekere zin altijd van 'buiten' de organisatie komt, heeft in de wet een vrij autonome positie. Een bewerker valt desondanks toch onder de verantwoordelijkheid van een opdrachtgever. De gedachte achter de extra bepalingen van artikel 12 en 14 Wbp, is dat het niet mogelijk moet zijn dat bewerker en verantwoordelijke zich kunnen verschuilen achter de verantwoordelijkheden die beide partijen hebben.[51] Maakt één van de betrokken partijen een fout, dan moet helder zijn wie de verantwoordelijkheid draagt en wie aanspreekbaar is.

Om te beginnen geeft artikel 12 Wbp aan dat de bewerker die in opdracht werkt van de verantwoordelijke, onder het gezag valt van de verantwoordelijke. Deze draagt dan ook de verantwoordelijkheid. Aan de opdracht die de bewerker uitvoert voor de verantwoordelijke ligt een overeenkomst ten grondslag. Hier wordt goed zichtbaar waar de verantwoordelijkheid van de verantwoordelijke ophoudt. Als de bewerker ervoor kiest directe aanwijzingen te negeren of de letter van de overeenkomst niet te volgen dan kan de verantwoordelijke daar niets aan doen.[52]
In artikel 12 Wbp wordt ook vastgesteld dat voor iedereen die met persoonsgegevens werkt, een geheimhoudingsplicht rust. Dit geldt voor zowel ondergeschikten als bewerkers.[53]

Artikel 14 Wbp legt een grote verantwoordelijkheid bij de verantwoordelijke neer. De verantwoordelijke heeft de verplichting te zorgen dat de bewerker voldoende waarborg biedt dat de nodige technische en organisatorische beveiligingsmaatregelen worden getroffen om de persoonsgegevens te beschermen. De verantwoordelijke heeft daarnaast een verplichting toe te zien op de naleving hiervan. Ook moeten de te nemen beveiligingsmaatregelen worden vastgelegd in de 'bewerkersovereenkomst'. Mocht een bewerker een sub-bewerker in willen schakelen om de persoonsgegevens te verwerken dan is daar de nadrukkelijke toestemming van de verantwoordelijke voor nodig. De verantwoordelijke blijft verantwoordelijk voor het deel van de werkzaamheden die door een sub-bewerker worden uitgevoerd.

Doorslaggevend bij de afbakening van het begrip 'verantwoordelijke' en 'bewerker' is wie er uiteindelijk zeggenschap heeft over welke doeleinden de verwerking van persoonsgegevens heeft en welke middelen hiervoor mogen worden gebruikt. In de praktijk komt het voor dat een bewerker veel invulling geeft aan de details rondom de beveiliging omdat de bewerker ook een zekere expertise heeft op dat gebied. Dat maakt een bewerker nog geen verantwoordelijke. Door het bestaan van een overeenkomst tussen verantwoordelijke en bewerker kan altijd worden vastgesteld wie er zeggenschap heeft gehad. Als de bewerker zeggenschap heeft over de doeleinden van verwerking of de te gebruiken middelen, dan is de bewerker geen bewerker meer maar een verantwoordelijke. [54]

4.4 Beveiliging in de praktijk

Nu de wetsbepalingen duidelijk zijn, is het van belang om deze eisen te vertalen naar de praktijk. De AP heeft bij de toepassing van de Wbp drie elementen benoemd die nodig zijn om passende maatregelen te kunnen treffen met betrekking tot de beveiliging van persoonsgegevens. De beveiligingsstandaarden, de risicoanalyse en een 'plan-do-check-act-cyclus'.

4.4.1 Beveiligingsstandaarden

Beveiligingsstandaarden geven een belangrijk houvast bij het implementeren van beveiligingsmaatregelen. In Nederland zijn er de Nederlandse Normen (NEN) die worden beheerd door het Nederlands Normalisatie-instituut. De Code voor Informatiebeveiliging is één van die normen.[55] Daarnaast bestaat ook nog ook nog een andere norm, de NEN ISO / IEC 27001:2013 nl. Samen vormen deze twee normen de standaard voor informatiebeveiliging. Deze algemene normen zijn vervolgens speciaal voor de zorgsector verder uitgewerkt in op zichzelf staande NEN-normen.[56] In de uitwerking van deze normen wordt, net als in de richtsnoeren van het voormalige CBP, aangegeven wat van een organisatie kan worden verwacht bij het beveiligen van informatie. De richtsnoeren van het voormalige CBP zijn gebaseerd op deze normen. Ondanks dat de normen aangeven wat een organisatie moet doen om informatie te beveiligen, worden er geen expliciete aanwijzingen gegeven over welke specifieke technische maatregelen getroffen moeten worden in bepaalde specifieke gevallen.[57] De reden die hiervoor gegeven wordt is

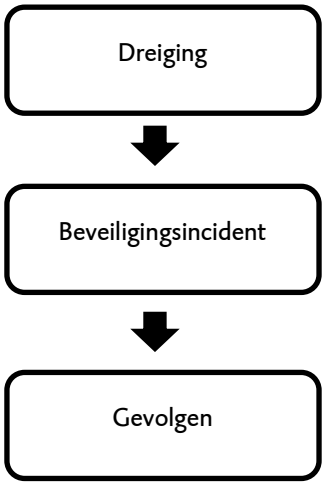
---

[51] *Kamerstukken II,* 1997/98, 25 892, nr. 3, p. 99.
[52] *Kamerstukken II,* 1997/98, 25 892, nr. 3, p 97.
[53] Artikel 12 lid 2 Wbp.
[54] Zie toelichting in *Brief CBP relatie verantwoordelijke en bewerker*, 14 mei 2002, p.2.
[55] NEN-ISO / IEC 27002:2013 nl.
[56] NEN 7510:2011 nl, NEN 7512:2015 nl, NEN 7513:2010 nl.
[57] NEN 7510:2011 nl, Inleiding, par. 0.3,

natuurlijk dat elke organisatie anders is, en dus een afweging over welke beveiligingsmaatregel getroffen dient te worden in zekere zin altijd sterk afhankelijk is van de organisatie in kwestie. Om organisaties duidelijkheid te geven over wat er van ze verwacht wordt, beschrijft het voormalige CBP een aantal belangrijke processen dat in een organisatie geïmplementeerd moet worden, op het moment dat er sprake is van verwerking van persoonsgegevens.

4.4.2 De Risicoanalyse

Een uitvoeren van een risicoanalyse richt zich op het identificeren van mogelijke risico's. Deze risico's kunnen, zodra deze in kaart gebracht zijn, afgedicht worden met beveiligingsnormen uit de beveiligingsstandaarden. Een risicoanalyse ziet er volgens het voormalige CBP als volgt uit:



Zie CBP Richtsnoeren Beveiliging van persoonsgegevens, Den Haag, 2013, p. 15.

Er zijn 3 verschillende fases waarin een risico aan het licht kan komen. Als er sprake is van dreiging maar het risico heeft zich nog niet gerealiseerd, dan zijn *preventieve maatregelen* op zijn plaats. Heeft een risico zich al gemanifesteerd (beveiligingsincident) dan kunnen er *detectieve en repressieve maatregelen* genomen worden met als doel het probleem het risico in het vervolg tijdig te detecteren en de huidige nadelen van het risico te beperken. Hebben de gevolgen van het risico zich al aangedaan dan kan men *herstelmaatregelen* treffen om de negatieve gevolgen terug te draaien. In al deze fase kan men *correctieve maatregelen* treffen om gebleken tekortkomingen in de beveiliging te repareren. De risicoanalyse heeft een eigen plek binnen het 'plan-do-check-act-cyclus'.

4.4.3 Plan-do-check-act-cyclus

Voorgaande elementen komen samen in de plan-do-check-act-cyclus. De reden dat het AP een dergelijke cyclus voorschrijft, vind zijn oorsprong in het continuele karakter van de wetstekst die in feite vraagt van een organisatie om telkens alert te zijn op de mogelijke gevaren van de verwerking van persoonsgegevens en de veranderingen op het gebied van informatiebeveiliging.

Om de cyclus te begrijpen zal er eerst dieper in moeten worden gegaan op een aantal begrippen die veel gebruikt worden in de wereld van de informatiebeveiliging. Een begrip wat binnen de informatiebeveiliging centraal staat is 'betrouwbaarheid'. Dit begrip reflecteert, zoals men wellicht kan vermoeden, de mate aan waarin een bepaalde organisatie op een informatiesysteem kan rekenen. De mate van betrouwbaarheid zegt dus iets over hoe goed een bepaald systeem in staat is om de nodige informatiebeveiliging te bieden. De betrouwbaarheid moet om te zetten zijn in zekere betrouwbaarheidseisen, en die worden vastgesteld op basis van 'vertrouwelijkheid', 'beschikbaarheid', 'integriteit' en 'controleerbaarheid'.[58] Deze begrippen moeten als volgt geïnterpreteerd worden:

'Vertrouwelijkheid' zegt iets over de exclusiviteit van de toegang tot het informatiesysteem voor geautoriseerde personen. Hoe meer ongeautoriseerde gebruikers aan de informatie kunnen komen, hoe minder vertrouwelijk de informatie is.

'Beschikbaarheid' spitst zich op het waarborgen van de toegang die gebruikers hebben tot een bepaald informatiesysteem. Essentieel bij de beoordeling van de beschikbaarheid is dat de geautoriseerde personen op de juiste momenten bij de benodigde informatie kunnen.

[58] *CBP Richtsnoeren Beveiliging van persoonsgegevens,* Den Haag, 2013, par. 2.2.

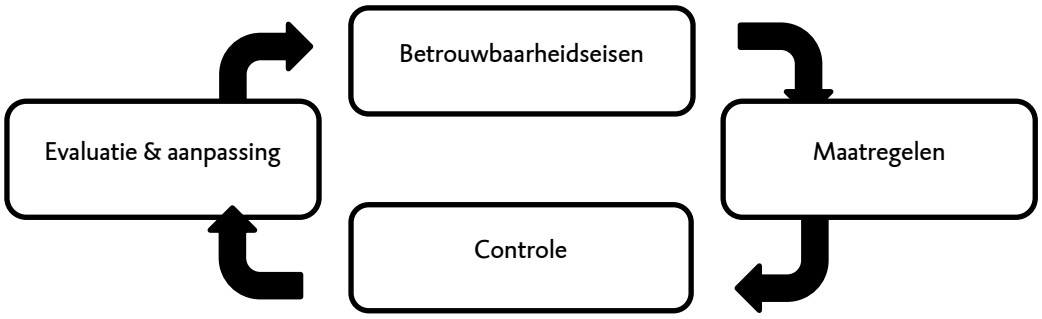
‘Integriteit’ is het criterium dat aangeeft hoe juist, tijdig en volledig de informatie en de verwerking van die informatie is.

‘Controleerbaarheid’ geeft aan in hoeverre het mogelijk is na te gaan of aan de vorige drie elementen is voldaan.

Wat opvalt, is dat in al deze elementen veel van de eerder behandelde wettelijke bepalingen terug te vinden zijn. Het voormalige CBP geeft ook aan dat de term ‘betrouwbaarheid’ sterk overeenkomt met het begrip ‘beveiligingsniveau’ wat in de Memorie van Toelichting bij het Wbp wordt gebruikt.[59]

[59] Ibidem, p. 13.

De plan-do-check-act-cyclus ziet er als volgt uit:



Zie CBP Richtsnoeren Beveiliging van persoonsgegevens, Den Haag, 2013, p. 14

De geformuleerde betrouwbaarheidseisen leiden tot maatregelen die geïmplementeerd kunnen worden. Vervolgens kan er een controle plaats vinden om na te gaan op daarmee aan de vastgestelde betrouwbaarheidseisen is voldaan. Vervolgens vind er 'regelmatig' een evaluatie plaats waarna ook aanpassingen kunnen worden gedaan. Het voormalige CBP schrijft geen termijn voor bij deze cyclus. Het is dus aan de organisatie om te bepalen hoe vaak deze cyclus wordt afgewerkt. Wel spreekt het CBP over de plek van deze cyclus in de dagelijkse praktijk. Omdat er een blijvend en passend beveiligingsniveau moet worden bereikt zal deze cyclus in de ogen van het CBP een continue proces moeten vormen.[60]

Deze cyclus levert dus maatregelen op, net zoals een risicoanalyse maatregelen oplevert. Deze twee processen worden in de praktijk gecombineerd.

4.5 Betrouwbaarheidseisen

Bij het formuleren van de betrouwbaarheidseisen is een grote rol weggelegd voor de verantwoordelijke organisatie. De formulering van deze eisen bepaalt simpel gezegd hoe goed het hele proces van verwerking van persoonsgegevens beveiligd moet zijn. Om tot een goed eisenpakket te komen verwacht de AP dat er een 'Privacy Impact Assessment' (PIA) wordt verricht om te inventariseren wat de risico's zijn voor de betrokkene wiens gegevens verwerkt worden. Bij een PIA wordt gelet op de aard van de gegevens en het gevaar van het verwerken van die gegevens.[61] Zodra dat helder is, kan aan de hand van de drie elementen van betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) de betrouwbaarheidseisen worden geformuleerd. Hoe de risico's zich vertalen naar betrouwbaarheidseisen, wordt door de AP aan de verantwoordelijke overgelaten. Het is dus belangrijk om te constateren dat ondanks alle wetten en richtlijnen, er uiteindelijk een grote ruimte overblijft waarin de verantwoordelijke naar eigen inzicht moet bepalen hoe goed of slecht een bepaald informatieverwerkingsproces beveiligd moet worden. Uiteraard geldt dat hoe groter het risico voor de betrokkene, hoe zwaarder de betrouwbaarheidseis moet zijn. Men wordt verder nog geholpen door de begrippen en bepalingen die hierboven zijn genoemd, maar de uiteindelijke afweging is aan de verantwoordelijke zelf.[62] Dit laatste geeft niet de zekerheid die een organisatie wellicht bij het opzetten van de verwerking van persoonsgegevens zou willen hebben. Om te voorkomen dat men dus tekortschiet, is het bij twijfel altijd raadzaam meer maatregelen te nemen in plaats van minder.

4.6 De maatregelen

In dit hoofdstuk is al meerdere malen gesproken over beveiligingsmaatregelen, maar tot op heden is nog niet duidelijk gemaakt wat die maatregelen precies inhouden. Wil een organisatie in staat zijn om bovengenoemde processen succesvol te implementeren, moet duidelijk zijn welke beveiligingsmaatregelen genomen kunnen worden. De AP, als controlerende instantie, geeft een lijst met maatregelen die als gebruikelijk en soms zelfs als noodzakelijk worden gezien. Het zijn ook deze maatregelen waarop wordt gelet bij onderzoeken en beoordelingen die de AP verricht. Ondanks het feit dat er eventueel ook andere maatregelen denkbaar zijn, is het bij de inrichting van de processen rondom de verwerking van persoonsgegevens dus niet onverstandig om uit te gaan van de maatregelen gegeven door de AP.

De lijst van maatregelen wordt door het voormalige CBP in de richtsnoeren als volgt opgesomd:

---

[60] Ibidem, p. 14.
[61] Ibidem, p. 18.
[62] Ibidem.

• Beleidsdocument voor informatiebeveiliging
Het beleidsdocument gaat expliciet in op de maatregelen die de verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.
• Toewijzen van verantwoordelijkheden voor informatiebeveiliging
Alle verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, zijn duidelijk gedefinieerd en belegd.
• Beveiligingsbewustzijn
Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met (bijzondere of anderszins gevoelige) persoonsgegevens.
• Fysieke beveiliging en beveiliging van apparatuur
IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.
• Toegangsbeveiliging
Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen. De procedures omvatten alle fasen in de levenscyclus van de gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben. Waar van toepassing wordt bijzondere aandacht besteed aan het beheren van toegangsrechten van gebruikers met extra ruime bevoegdheden, zoals systeembeheerders.
• Logging en controle
Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.
De verantwoordelijke moet er rekening mee houden dat er, als de gegevens in de logbestanden tot personen herleidbaar zijn, sprake is van een verwerking van persoonsgegevens in de zin van de Wbp waarop de verplichtingen uit deze wet van toepassing zijn. In dat geval kan er ook sprake zijn van een personeelsvolgsysteem in de zin van artikel 27 lid 1 van de Wet op de ondernemingsraden (WOR), waarvoor instemming van de ondernemingsraad is vereist.
• Correcte verwerking in toepassingssystemen
In alle toepassingssystemen, inclusief toepassingen die door gebruikers zelf zijn ontwikkeld, zijn beveiligingsmaatregelen ingebouwd. Tot deze beveiligingsmaatregelen behoort de controle dat de invoer, de interne verwerking en de uitvoer aan vooraf gestelde eisen voldoen (validatie). Voor systemen waarin gevoelige persoonsgegevens worden verwerkt of die invloed hebben op de verwerking van gevoelige persoonsgegevens, kunnen aanvullende beveiligingsmaatregelen nodig zijn.
• Beheer van technische kwetsbaarheden
Software, zoals browsers, virusscanners en operating systems, wordt up-to-date gehouden. Ook installeert de verantwoordelijke tijdig oplossingen die de leverancier uitbrengt voor beveiligingslekken in deze software. Meer in het algemeen verkrijgt de verantwoordelijke tijdig informatie over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden wordt geëvalueerd en de verantwoordelijke treft geschikte maatregelen voor de behandeling van de risico's die daarmee samenhangen.
• Incidentenbeheer
Er zijn procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd. Het beoordelen van de risico's voor de betrokkenen en het effectief informeren van de betrokkenen en, waar van toepassing, de toezichthouder is in deze procedures opgenomen. De lessen getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging waar mogelijk structureel te verbeteren. Als een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel- of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
• Afhandeling van datalekken en beveiligingsincidenten

De verantwoordelijke meldt datalekken die onder een wettelijke meldplicht vallen bij de betreffende toezichthouder. Als hij daartoe wettelijk verplicht is, of als er anderszins aanleiding voor is, informeert hij ook de betrokkenen over het beveiligingsincident of het datalek.

• Continuïteitsbeheer

Door natuurrampen, ongevallen, uitval van apparatuur of opzettelijk handelen kunnen persoonsgegevens verloren gaan. Door in de organisatie continuïteitsbeheer in te richten worden de gevolgen tot een aanvaardbaar niveau beperkt, waarbij gebruik wordt gemaakt van een combinatie van preventieve maatregelen en herstelmaatregelen.

• Gegevensbescherming en geheimhouding van persoonsgegevens

De organisatie heeft beleid ontwikkeld voor de bescherming en voor de geheimhouding van persoonsgegevens. Dit beleid is vastgelegd en geïmplementeerd en de organisatie communiceert dit naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens. In het beleid is opgenomen dat persoonsgegevens uitsluitend worden verwerkt in opdracht van de verantwoordelijke.

• Geheimhoudingsovereenkomsten

De verplichting tot geheimhouding van persoonsgegevens is vastgelegd in geheimhoudingsovereenkomsten.

• Encryptie (versleuteling) en hashing

De verantwoordelijke maakt gebruik van cryptografische bewerkingen om de persoonsgegevens die hij verwerkt te beveiligen. Hij past encryptie (versleuteling) toe bij verzending van persoonsgegevens via het internet, bij de opslag van persoonsgegevens op draagbare apparatuur en op verwijderbare media zoals usb-sticks en in andere situaties waar persoonsgegevens kwetsbaar zijn voor toegang door onbevoegden (bijvoorbeeld persoonsgegevens die via het world wide web kunnen worden benaderd). Bij de opslag en verwerking van wachtwoorden maakt hij gebruik van hashing. Bij het toepassen van cryptografische technieken past hij alle gangbare voorzorgsmaatregelen toe, zoals goed ingericht sleutelbeheer en het gebruik van sleutellengten en versleutelingstechnieken die in overeenstemming zijn met de actuele stand van de techniek.

• Omgang met e-waste (afgedankte apparatuur en opslagmedia)

Alle apparatuur die opslagmedia bevat, zoals laptops of smartphones, wordt ontdaan van de nog eventueel aanwezige persoonsgegevens alvorens het apparaat te verwijderen of hergebruiken. Opslagmedia met gevoelige persoonsgegevens worden fysiek vernietigd of de persoonsgegevens worden vernietigd, verwijderd of overschreven met technieken die het onmogelijk maken om de oorspronkelijke persoonsgegevens terug te halen. Hetzelfde geldt voor verwijderbare media zoals usb-sticks.[63]

Al deze maatregelen zijn gebaseerd op de vaak uitgebreidere uitwerking in de verschillende NEN-normen.[64] Met de toelichting van het CBP behoeven deze maatregelen geen verdere toelichting.
Om een situatie te bereiken waarin 'passende maatregelen' zijn getroffen om de verwerking van persoonsgegevens voldoende te beveiligen, kan de verantwoordelijke naar eigen inzicht putten uit bovengenoemde maatregelen.

4.7 Conclusie

De verwerking van persoonsgegevens adequaat beveiligen is nog niet zo eenvoudig. Het beveiligingsproces vraagt om een structurele aanpak, die door middel van een controlerende cyclus constant op de achtergrond plaats vindt. Passende maatregelen zijn passend als ze proportioneel zijn aan het risico dat een betrokkene loopt bij de verwerking van zijn persoonsgegevens. De afweging, ondanks dat deze wel enigszins wordt gestuurd door bestaande wetten en regels, blijft toch voor een groot deel een kwestie van interpretatie door de verantwoordelijke die telkens weer zal moeten beslissen welke beveiligingsmaatregelen gepast zijn. Hierbij zijn de uitwerkingen van de verschillende normen en de richtsnoeren van het CBP leidend. Nu dat de wijze van beveiliging van persoonsgegevens duidelijk is geworden, zal de geneeskundige behandelingsovereenkomst als grond voor gegevensverwerking en de rol van het medisch beroepsgeheim worden uitgewerkt in hoofdstuk 5.

4.8 Onderzoekspunten

De onderzoekspunten uit dit hoofdstuk zijn:
- Is bij de beveiliging van een EUS sprake een plan-do-check-act cyclus?
- In hoeverre maakt een risicoanalyse onderdeel uit van deze cyclus?
- In hoeverre worden richtlijnen van de AP en de NEN-normen aangehouden in deze cyclus?

---

[63] Ibidem, par. 3.2.
[64] NEN-ISO / IEC 27001:2013, nl NEN-ISO / IEC 27002:2013, als ook nl NEN 7510:2011 nl, NEN 7512:2015 nl, NEN 7513:2010 nl.

- In hoeverre is er sprake van een bewerker en een bewerkersovereenkomst?

5 De medische behandelrelatie

5.1 Inleiding
In hoofdstuk 3 is gebleken dat het gezondheidsrecht een belangrijke rol heeft in het geheel van regels rondom de verwerking van persoonsgegevens in de zorg. Dit hoofdstuk gaat dieper in op hoe de regels over geneeskundige behandelingsovereenkomst en het medisch beroepsgeheim zich verhouden tot de verwerking van persoonsgegevens in de zorg. Dit hoofdstuk geeft deels antwoord op de deelvraag:
- Welke eisen worden er in de wet gesteld aan een elektronisch uitwisselingssysteem?

Achtereenvolgens worden de volgende onderwerpen behandeld: de geneeskundige behandelingsovereenkomst (§5.2), geheimhoudingsplicht (§5.3), de conclusie (§5.4) en tot slot de onderzoekspunten (§5.5). Dit hoofdstuk heeft als doel om de lezer duidelijk te maken wat de rol is van de medische behandelrelatie bij het verwerken van persoonsgegevens.

5.2 De geneeskundige behandelingsovereenkomst
In hoofdstuk 3 is aan bod gekomen welke eisen worden gesteld aan het verwerken van persoonsgegevens die betrekking hebben op de gezondheid van een persoon. Deze 'bijzondere' gegevens moeten op basis van een gerechtvaardigde grond verwerkt worden, anders is de verwerking onrechtmatig.[65] Een van deze legitieme gronden, en in de medische praktijk de meest voorkomende, is de geneeskundige behandelingsovereenkomst.[66] De geneeskundige behandelingsovereenkomst is vastgelegd in titel 5 van boek 7 van het Burgerlijk wetboek. Men noemt dat deel van het Burgerlijk wetboek de Wet op de geneeskundige behandelingsovereenkomst (WGBO), ondanks het feit dat de WGBO dus geen op zichzelf staande wet is.

De WGBO is de grondslag voor wat men zou omschrijven als de behandelrelatie tussen een patiënt en een arts. Artikel 7:446 lid 1 BW omschrijft de behandelingsovereenkomst als volgt: '*De overeenkomst inzake geneeskundige behandeling is de overeenkomst waarbij een natuurlijke persoon of een rechtspersoon, de hulpverlener, zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde.'*

In de WGBO zijn alle algemene rechten van patiënten opgenomen.[67] Er is een nauw verband tussen de rechten van patiënten omschreven in de WGBO en de wettelijke eisen aan de verwerking van persoonsgegevens. Belangrijke voorbeelden van patiëntenrechten zijn bijvoorbeeld het recht op informatie en de toestemmingsvereiste.[68] Deze rechten zien we ook weer verankerd in de Wbp.

5.2.1. Informatierecht
Het recht op informatie is vastgelegd in artikel 7:448 BW. De hulpverlener is verplicht om op duidelijke wijze de patiënt te informeren over de voorgestelde behandeling of voorgenomen onderzoek. Het goed informeren van patiënten is volgens de Hoge Raad essentieel als de patiënt op een juiste wijze invulling wil geven aan zijn zelfbeschikkingsrecht.[69] Het is van belang dat een hulpverlener duidelijk inzicht geeft in alle risico's die een behandeling met zich meebrengt. In alle gevallen moet de hulpverlener rekening houden met het kennisverschil tussen beide partijen. Dit betekent dat de hulpverlener in sommige gevallen de wijze van informeren moet aanpassen aan het bevattingsvermogen van een patiënt.[70] Informeren stopt niet nadat de behandeling voltrokken is of de toestemming gegeven is. Hulpverleners zijn verplicht om ook naderhand de patiënt volledig te blijven informeren. Denk hierbij aan het mededelen van onderzoeksresultaten of het uitvoeren van een follow-up.[71]

5.2.2. Toestemmingsvereiste
Een recht van patiënten dat nauw verbonden is met het informatierecht is met het toestemmingsvereiste. Artikel 7:450 BW is de grondslag voor dit vereiste. In de Verenigde Staten gebruikt men de term 'informed consent' om een helder verband aan te geven tussen enerzijds duidelijke en volledige informatie over een behandeling en anderzijds

---

[65] Zie artikel 8 Wbp.
[66] Valt onder artikel 8 sub b Wbp.
[67] H.J.J. Leenen e.a., *Handboek gezondheidsrecht Deel I: Rechten van mensen in de gezondheidszorg,* Hoofddorp: Boom Juridische uitgevers 2011, p. 182.
[68] Zie artikel 7:448 BW en artikel 7:450 BW, in de uitspraak Hoge Raad 23 november 2001, TvGR 2002/20 en 2002/21 wordt het belang van goede informatievoorziening richting patiënt nogmaals onderstreept.
[69] Hoge Raad 23 november 2001, *TvGR* 2002/20 en 2002/21
[70] Een voorbeeld hiervan zijn kinderen jonger dan 12, artikel 7:448 lid 1 BW.
[71] Leenen 2011, p. 191.

de toestemming voor een behandeling. Toestemming zonder informatie is over het algemeen dus ook niet geldig.[72] Een uitzondering op deze regel is de acute noodsituatie. In een dergelijke situatie mag toestemming worden verondersteld.[73]

5.3 Geheimhoudingsplicht

Het medisch beroepsgeheim, ook wel bekend als de geheimhoudingsplicht is niet alleen een plicht voor zorgverleners maar meer nog een recht van de patiënt. Het is daarom ook terug te vinden in de WGBO.[74] Artikel 7:457 BW stelt dat een hulpverlener geen inlichtingen over de patiënt of inzage in diens medisch dossier mag geven tenzij de patiënt daarvoor toestemming heeft gegeven. Op die hoofdregel is een aantal uitzonderingen van toepassing. De geheimhouding geldt niet richting degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst of een vervanger van de hulpverlener in kwestie en alleen voor zover dat noodzakelijk voor de uitvoering van hun werkzaamheden. Het kan zo zijn dat de patiënt jonger dan twaalf jaar oud is, in dergelijke gevallen geldt de geheimhoudingsplicht ook niet ten opzichte van een ouder, voogd of curator.[75] Deze geheimhoudingsplicht is niet alleen ter bescherming van de patiënt, maar beschermt ook het algemeen belang. In onze maatschappij is een belemmering van de vrije toegang tot de gezondheidszorg van groot belang, en het ontbreken van de geheimhoudingsplicht zou voor veel mensen een belemmering vormen.[76] Op de geheimhoudingsplicht is uiteraard ook een aantal uitzonderingen. Denk bijvoorbeeld aan het gebruik van gegevens voor wetenschappelijk onderzoek of ten behoeve van de statistiek. [77] Soms kan de zwijgplicht ook opgeheven worden door andere wettelijke voorschriften. Artikel 42 Wetboek van Strafvordering vrijwaart zorgverleners van het verbreken van hun zwijgplicht als ze een wettelijk voorschrift uitvoeren. Een voorbeeld hiervan is de verplichting uit de Wet Publieke Gezondheid die voorschrijft dat van bepaalde infectieziekten melding moet worden gemaakt bij de GGD.[78]

Deze uitzonderingen komen in de praktijk wel eens voor maar in alle andere gevallen wordt een zorgverlener geacht zich aan zijn zwijgplicht te houden.

De vraag die in deze paragraaf centraal staat is of het opnemen van medische persoonsgegevens in een elektronisch uitwisselingssysteem in strijd is met de geheimhoudingsplicht. Deze vraag kwam aan de orde in het 'Boze Huisartsen' arrest.[79] In dit arrest sprak de rechter zich onder andere hierover uit. Een groep huisartsen weigerde deel te nemen aan het landelijke EPD omdat ze zich over bepaalde aspecten van het systeem ernstige zorgen maakte. Het EPD was een systeem dat onderdeel uitmaakte van een wet die uiteindelijk niet is aangenomen. De wetgever had het voornemen om een landelijk elektronisch systeem van patiëntendossiers op te zetten. Dit plan sneuvelde en maakte plaats voor het in dit onderzoek behandelde wetsvoorstel. Ondanks het feit dat het EPD-systeem niet werd ingevoerd, is een aantal punten uit dit arrest nog wel degelijk relevant. In de behandeling van dit arrest ging de rechter in op verschillende door de huisartsen aangevoerde bezwaren. Eén daarvan had te maken met de geheimhoudingsplicht. De huisartsen beargumenteerden dat ze bij deelname aan dit elektronisch uitwisselingssysteem, de controle over de medische gegevens van patiënten kwijt zouden raken. In hun ogen konden ze daardoor niet een juiste invulling geven aan hun beroepsgeheim. Hier stelde de rechter de huisartsen in het ongelijk. De rechter bepaalde dat de geheimhoudingsplicht zoals vastgelegd in de wet, geen belemmering hoeft te zijn bij de verwerking en uitwisseling van persoonsgegevens. Hiermee is er vanuit de rechtspraak duidelijkheid gekomen over hoe de geheimhoudingsplicht zich verhoudt tot het gebruik van een elektronisch uitwisselingssysteem.

5.4 Conclusie

De geneeskundige behandelingsovereenkomst is een grondslag op basis waarvan veel persoonsgegevens worden verwerkt. De patiëntenrechten geformuleerd in de WGBO zijn in harmonie met bepalingen uit de Wbp en vullen elkaar op verschillende vlakken aan. De geheimhoudingsplicht van artsen is een belangrijk aspect in de relatie tussen patiënt en zorgverlener, maar vormt geen belemmering voor het elektronisch uitwisselen van gegevens. Dat neemt niet weg dat het elektronisch verwerken van persoonsgegevens al aan verregaande eisen onderworpen is. Nu

---

[72] Leenen 2011, p. 190.
[73] Leenen 2011, p. 191.
[74] Geheimhoudingsplicht in de gezondheidszorg heeft verschillende aspecten en dus ook verschillende verankeringen in de wet. Artikel 272 Wetboek van Strafrecht, artikel 218 Wetboek van Strafvordering, artikel 88 Wet op de Beroep in de Individuele Gezondheidszorg.
[75] Artikel 7:457 lid 2 j.o. lid 3
[76] Leenen 2011, p. 225.
[77] Artikel 7:458 BW.
[78] Artikel 21 Wet Publieke Gezondheid.
[79] Rb. Midden-Nederland 23 juli 2014 *LJN*C/16/340505 / HA ZA 13-205.

duidelijk in kaart is gebracht welke factoren een rol spelen bij het verwerken van persoonsgegevens zal er in het volgende hoofdstuk gekeken worden naar wat er zou veranderen als het nieuwe wetsvoorstel wordt aangenomen.

5.5 Onderzoekspunten

Het onderzoekspunt uit dit hoofdstuk is:

- In hoeverre wordt de behandelrelatie binnen een EUS geborgd?

6. Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens

6.1 Inleiding
Dit hoofdstuk behandelt de theorie, en richt zich op het ontleden van de nieuwe vereisten uit het bij de Eerste Kamer aanhangige wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens. Hiermee wordt antwoord gegeven op de deelvraag:
- Welke nieuwe eisen kunnen uit het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens worden afgeleid?

Achtereenvolgens worden de volgende onderwerpen behandeld: wetsvoorstel (§6.2), realisering (§6.3), de AMvB (§6.4), actuele ontwikkelingen (§6.5), de conclusie (§6.6) en tot slot de onderzoekspunten (§6.7).

6.2 Wetsvoorstel
Om te begrijpen wat het wetsvoorstel precies aan de bestaande situatie verandert, moet een duidelijk onderscheid gemaakt worden in de verschillende gebieden waar dit wetsvoorstel actief is. Het wetsvoorstel dient namelijk als aanvulling op bestaande wetgeving, en dat geeft het voordeel dat de eerder behandelde wettelijke vereisten gewoon van kracht blijven.[80] De achterliggende reden bij dit wetsvoorstel is het bieden van extra bescherming voor de privacy van patiënten.[81] Het kan geen kwaad om dit bij de behandeling van de wetswijziging in het achterhoofd te houden.

Binnen het geheel aan bestaande regels omtrent de verwerking van persoonsgegevens dient het wetsvoorstel een uitbreidende functie. Het geeft nadere bepalingen die in acht moeten worden genomen op het moment dat een zorgaanbieder kiest om persoonsgegevens op te nemen in een elektronisch uitwisselingssysteem. Wat er precies mag worden verstaan onder een elektronisch uitwisselingssysteem wordt ook gedefinieerd in het wetsvoorstel.[82] Hiermee wordt het bereik van het wetsvoorstel netjes afgebakend.

Het wetsvoorstel bestaat enerzijds uit aanvullende bepalingen voor verschillende reeds bestaande wetten en anderzijds uit een Algemene Maatregel van Bestuur (AMvB). Deze AMvB heeft als doel om op basis van artikel 26 Wbp specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling te stellen.[83] Hierin wordt veelvuldig verwezen naar de eerder benoemde NEN-normen.

In het wetsvoorstel worden onder andere de *Wet gebruik burgerservicenummer in de zorg* (WGBZ), de *Wet bescherming persoonsgegevens* (Wbp), de *zorgverzekeringswet*, de *Wet marktordening gezondheidszorg*, *Wet op de beroepen in de individuele gezondheidszorg* (BIG), de *algemene Wet bijzondere ziektekosten* en de *Wet toelating zorginstellingen* aangehaald. De WGBZ zal van naam veranderen zodra het wetsvoorstel van kracht is, waardoor het vanaf dat moment de *Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg* (Wabvpz) zal heten. Veel van deze wijzigingen zijn van formele aard en richten zich op het wijzigen en aanvullen van definities en bepalingen. Daarnaast is er een aantal bepalingen dat ingrijpende veranderingen met zich mee nemen ten opzichte van de huidige situatie. De belangrijkste veranderingen worden nu per onderwerp behandeld.

6.2.1 Toestemming
Het belangrijkste element in dit wetsvoorstel is de wijze waarop het de toestemming reguleert die vanuit de patiënt nodig is om diens gegevens op te nemen in een elektronisch uitwisselingssysteem (EUS). Artikel 15a lid 1 wetsvoorstel zegt dat er nadrukkelijke toestemming vereist is alvorens iemands persoonsgegevens op een dergelijke wijze beschikbaar mogen worden gesteld. Deze verplichting bestond al vanuit artikel 23 Wbp maar wordt hier nogmaals herhaald. Artikel 15a lid 2 gaat hier vervolgens op door en introduceert de zogeheten *'gespecificeerde toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt* (patiënt) *aan te duiden zorgaanbieders of categorieën van zorgaanbieders'* of simpelweg gespecifieerde toestemming. In deze formulering is een aantal belangrijke zaken te onderscheiden. Allereerst heeft de patiënt de keuze om alle of slechts een gedeelte van zijn gegevens op te laten nemen. Vervolgens moet het voor een patiënt mogelijk zijn om een zorgaanbieder of een categorie zorgaanbieders uit te sluiten van inzage in diens gegevens. Er zijn dus twee facetten aan deze toestemming, namelijk de keuze welke gegevens kunnen worden opgenomen in het EUS, en welke zorgaanbieders vervolgens daar inzage in kunnen hebben. Er is sprake van generieke toestemming als een patiënt

[80] *Kamerstukken II* 2012/13, 33 509, nr. 3, p. 1.
[81] Ploem, 'Elektronische gegevensuitwisseling', p. 5.
[82] Wetsvoorstel wijziging WGBZ artikel 1 sub j. *Elektronisch uitwisselingssysteem:* een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier.
[83] *Kamerstukken II* 2012/13, 33 509, nr. 3, p. 5.

ervoor kiest om alle gegevens voor alle zorgaanbieders vrij te geven. Bij deze vorm van toestemming hoeft een patiënt ook niet telkens opnieuw om toestemming te worden gevraagd als een zorgaanbieder de gegevens in wil zien. Kiest men voor een vorm van gespecifieerde (en niet een generieke) toestemming dan moet ook telkens opnieuw toestemming worden gevraagd op het moment dat een zorgaanbieder persoonsgegevens wil inzien.[84] Er ontstaat hierdoor in veel gevallen als het ware een systeem van dubbele toestemming. Toestemming voor opname in het EUS, en toestemming op het moment dat een zorgaanbieder de gegevens in wil zien. Hierin is de laatste toestemming dus slechts vereist waar in eerste instantie geen generieke toestemming is verleent.[85]
Mocht een nieuwe categorie zorgaanbieders zich aansluiten bij het EUS of mocht het EUS op andere wijze substantieel gewijzigd worden dan dient de patiënt daarover te worden ingelicht zodat de patiënt zijn toestemming eventueel kan wijzigen of terug kan trekken.[86] Het wetsvoorstel ziet niet toe op de wijze waarop toestemming moet worden verleent, dus deze kan zowel mondeling als schriftelijk geschieden, maar er rust wel een plicht op de zorgaanbieder om het nodige te registreren zodra er toestemming wordt gegeven. Een zorgaanbieder zal bij moeten houden of er toestemming is gegeven en welke toestemming op welk moment (tijdstip) gegeven is. Daarbij hoort dus ook het registreren van zorgaanbieders die uitgesloten zijn van toegang tot de gegevens zodat daar gevolg aan kan worden gegeven.[87] Geeft de patiënt in zijn geheel geen toestemming voor opname in een EUS dan hoeft dat ook niet te worden geregistreerd.[88] Van essentieel belang bij dit stelsel van toestemming is dat deze niet vereist is in acute noodsituaties.[89] Niet alleen de betreffende zorgverlener maar ook diegenen die rechtstreeks betrokken zijn bij de behandeling of eventueel de vervanger van de zorgverlener mogen de persoonsgegevens via een EUS inzien, hier is geen derde toestemmingsronde voor nodig. De tweede toestemming die af wordt gegeven dient echter wel slechts voor het inzien van de voor de behandeling noodzakelijke gegevens.[90] Daarnaast is een EUS uitsluitend bedoeld voor het uitwisselen van gegevens tussen zorgverleners. Hierdoor zijn zorgverzekeraars, bedrijfsartsen, verzekeringsartsen en keuringsartsen uitgesloten van deelname aan een EUS.[91]

6.2.2 Informatieplicht

De informatieplicht die rust op de zorgaanbieder is er om te voorkomen dat een patiënt op basis van gebrekkige informatie een beslissing neemt in de keuze om opgenomen te worden in een EUS. Artikel 15c lid 1 van het Wetsvoorstel ziet erop toe dat de patiënt alvorens toestemming kan worden gegeven geïnformeerd moet zijn over: *'zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen en over de werking van het elektronisch uitwisselingssysteem dat voor de gegevensuitwisseling wordt gebruikt.'*.[92] De informatieplicht stopt daar niet. Zo is bij de toevoeging van een categorie zorgaanbieders of een andere grote wijziging in de werking van het EUS, de zorgaanbieder verplicht om de patiënt (opnieuw) uit te leggen wat de mogelijkheden zijn om de gegeven toestemming te wijzigen of in te trekken.[93]

6.2.3 Recht op inzage en afschrift

Het recht op inzage in het medisch dossier bestaat al, maar in dit wetsvoorstel wordt daar nog iets aan toegevoegd. Voor een patiënt moet het mogelijk zijn om op elektronische wijze inzage te krijgen in zijn medisch dossier. Hiervan moet ook een uitdraai of afschrift te maken zijn door de patiënt.[94] Het moet op een dergelijk afschrift ook mogelijk zijn om loggegevens in te zien.[95] Deze loggegevens dienen aan te geven wie, wanneer, welke informatie beschikbaar heeft gesteld dan wel heeft ingezien of opgevraagd.

6.3 Realisering

Op welke wijze een zorgverlener deze nieuwe wet faciliteert wordt door de wetgever aan de zorgverlener over gelaten. De wetgever verwacht ook niet dat alle EUS op dezelfde wijze vorm zullen worden gegeven. Er is ook geen verplichting om een bepaalde werkwijze te volgen. Wel wordt in de Memorie van Toelichting gewezen op de mogelijkheid een patiëntportaal op te richten waar patiënten op afstand op elektronische wijze gegevens kunnen inzien en opvragen. Hierbij wordt nadrukkelijk vermeld dat het inzien van gegevens gratis moet zijn (terwijl voor afschriften en loggegevens een redelijke vergoeding mag worden gevraagd) en dat de elektronische toegang niet per

---

[84] Artikel 15b lid 1 wetsvoorstel.
[85] *Kamerstukken II* 2012/13, 33 509, nr. 3, p. 17.
[86] Artikel 15c lid 1 wetsvoorstel.
[87] Artikel 15c lid 2 wetsvoorstel.
[88] *Kamerstukken II* 2012/13, 33 509, nr. 3, p. 18.
[89] Artikel 15b lid 3 wetsvoorstel.
[90] *Kamerstukken II* 2012/13, 33 509, nr. 3, p. 7.
[91] Artikel 15f wetsvoorstel.
[92] Artikel 15c lid 1 wetsvoorstel.
[93] Artikel 15c lid 1 wetsvoorstel.
[94] Artikel 15d wetsvoorstel.
[95] Artikel 15e wetsvoorstel.

definitie over het internet gefaciliteerd hoeft te worden. [96] Dat de identiteit van de persoon die toegang tot de gegevens verzoekt geverifieerd moet worden door middel van een Burgerservicenummer-controle zal ook hier gelden.[97]

6.4 De AMvB

Zoals gezegd is het doel van de AMvB om als aanvulling te dienen op de wetswijziging. Hierbij wordt invulling gegeven aan artikel 26 Wbp dat voorschrijft dat voor bepaalde sectoren (zoals de zorg) nadere regels kunnen worden opgesteld d.m.v. een AMvB.[98] Hiertoe is geen verplichting maar een mogelijkheid, en van die mogelijkheid wordt in dit geval gebruik gemaakt. Waarom de wetgever kiest voor een AMvB om specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling te stellen is omdat de techniek snel veranderd en hierdoor de wet ook snel zou kunnen verouderen. Een AMvB is makkelijker te vervangen op het moment dat de vastgestelde eisen niet meer zouden voldoen, en daarom is er gekozen om speciaal voor dit punt een AMvB op te stellen.[99]

De inhoud van de AMvB heeft een aantal interessante veranderingen ten opzichte van de bestaande wettelijke vereisten. Zo wordt duidelijk dat de wetgever het volgen van de NEN-normen 7510, 7512 en 7513 verplicht stelt. Zelfs het volgen van de terminologie uit deze NEN-normen wordt verplicht.[100] Waar NEN-normen in essentie richtlijnen zijn die men kan volgen, maakt de AMvB duidelijk dat het volgen van deze normen in de zorgsector verplicht is.

Daarnaast wordt ook het instellen van een functionaris voor de gegevensbescherming verplicht gesteld als een zorgaanbieder meer dan 250 werknemers heeft en gebruik maakt of wil gaan maken van een EUS.[101]

De AMvB verbreedt ook de beveiligingsverplichting van de verantwoordelijke door ook de beveiliging van de netwerkverbindingen die door een EUS gebruikt worden hieronder te scharen. In de praktijk worden die verbindingen vaak door zorgserviceproviders beheert. Op grond van de criteria uit de NEN-normen moet een verantwoordelijke samen met de zorgserviceprovider vervolgens vaststellen aan welke eisen deze verbindingen moeten voldoen.[102] De zorgaanbieder blijft echter verantwoordelijk dat de verbindingen aan de norm voldoen. Verder moet er een overeenkomst worden gesloten tussen de verantwoordelijke en eventuele derden zoals bijvoorbeeld een zorgserviceprovider. Hierin moet worden vastgelegd welke maatregelen getroffen moeten worden om gegevens te beschermen.

Deze AMvB zal in werking treden zodra de wetswijziging wordt aangenomen. Op dat moment zullen vertegenwoordigende organisaties van zorgaanbieders en patiënten vast moeten gaan stellen hoe lang loggegevens bewaard dienen te worden en dus inzichtelijk blijven voor patiënten. Welke loggegevens bewaard horen te worden staat in zowel de AMvB als in de Wbp en het nieuwe wetsvoorstel nogmaals benoemd.[103]

6.5 Actuele ontwikkelingen

Op 22 december 2015 heeft de minister van Volksgezondheid, Welzijn en Sport een nadere Memorie van Toelichting gepubliceerd. In deze toelichting adresseert zij een aantal verschillende punten die van belang zijn voor de uiteindelijke uitvoer van het wetsvoorstel, mocht dat uiteindelijk worden aangenomen. Tijdens een bijeenkomst van deskundigen in de Eerste Kamer op 26 mei 2015 hebben verschillende belangenbehartigende organisaties uit de zorgsector zorgen geuit over de uitvoerbaarheid van het wetsvoorstel in zijn huidige vorm. Veel van die zorgen hebben betrekking de wetsbepaling die de gespecificeerde toestemming regelt.[104] De minister is na verder overleg met de verschillende organisaties tot de conclusie gekomen dat het wetsvoorstel een aantal veranderingen zal moeten ondergaan om te zorgen dat het wetsvoorstel uitvoerbaar blijft en om te voorkomen dat de zorgsector wordt belast met aanzienlijke administratieve lasten. Ook het overzicht voor de patiënt speelt bij deze aanpassingen een rol.[105] De grootste aanpassing ten opzichte van het voorgenomen wetsvoorstel is dat de minister de inwerkingtreding van de bepaling rondom de gespecificeerde toestemming uitstelt met drie jaar nadat het wetsvoorstel zelf in werking treed. Hiermee wil de Minister de zorgsector de ruimte geven om naar het punt toe te

[96] *Kamerstukken II* 2012/13, 33 509, nr. 3, p. 6.
[97] Zie artikel 7:456 BW, Artikel 39 Wbp.
[98] Nadere regels met betrekking tot artikel 6 t/m 11 en 13 Wbp.
[99] *Kamerstukken II* 2012/13, 33 509, nr. 3, p. 5.
[100] Artikel 4 AMvB.
[101] Artikel 2 AMvB.
[102] Artikel 5 AMvB.
[103] Artikel 7 AMvB, Artikel 35 Wbp, Artikel 15e wetsvoorstel.
[104] Artikel 15a lid 2 wetsvoorstel.
[105] *Kamerstukken I*, 2015/16, 33509, nr. J, p. 3.

werken waarop zorgaanbieders in Nederland in staat zijn om aan dit wettelijke vereiste te voldoen. Een belangrijke taak is weggelegd voor beroep- en cliëntenorganisaties, die gezamenlijk een plan zullen moeten opstellen waarmee naar de gewenste eindsituatie toegewerkt kan worden.[106] Ook de inwerkingtreding van de bepalingen rondom de elektronische inzage, de elektronische logging en het elektronische afschrift zijn met drie jaar uitgesteld. Tot slot heeft de minister besloten dat de verplichting tot het vragen van toestemming (art. 15b) bij raadpleging zal worden geschrapt.[107]

6.6 Conclusie

Mocht het wetsvoorstel doorgang vinden dan zal er het nodige veranderen in de wijze waarop toestemming van patiënten zal moeten worden gevraagd. Voor het faciliteren van een systeem van gespecificeerde toestemming zal organisatorisch een aantal aanpassingen nodig zijn. Ook het zogeheten loggen van gegevens zal belangrijker worden wanneer er een systeem moet komen voor patiënten om medische gegevens in te zien. Om aan beveiligingseisen te voldoen zal men de NEN-normen moeten volgen en die normen niet alleen betrekken op de beveiliging van een EUS maar ook op de netwerkverbindingen die een EUS gebruikt.

Hiermee komt er een einde aan de uitwerking van de theorie. In het volgende hoofdstuk zal er begonnen worden met het uitwerken van de resultaten uit het praktijkonderzoek.

6.7 Onderzoekspunten

De onderzoekspunten uit dit hoofdstuk zijn:
- *Is in een EUS al sprake van gespecificeerde toestemming?*
- *In hoeverre kan een patiënt bepalen welke gegevens inzichtelijk zijn per (categorie) zorgaanbieders?*
- *In hoeverre kan een patiënt elektronisch gegevens uit een EUS inzien?*
- *In hoeverre kan een patiënt elektronisch loggegevens van een EUS inzien?*

[106] *Kamerstukken I*, 2015/16, 33509, nr. J, p. 3-4.
[107] *Kamerstukken I*, 2015/16, 33509, nr. J, p. 4.

7 Praktijkonderzoek

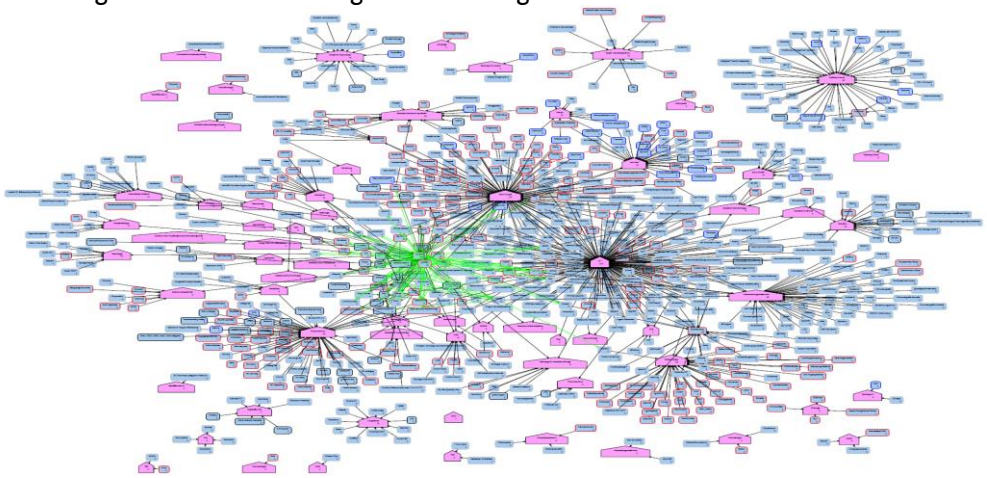
7.1 Inleiding

Om antwoord te krijgen op de vragen die uit de theorie naar voren zijn gekomen, is het uitvoeren van praktijkonderzoek van essentieel belang. Dit praktijkonderzoek is uitgevoerd door middel van het uitvoeren van diepte-interviews met verschillende experts binnen het UMCG. In dit praktijkonderzoek is de aandacht gericht op drie EUS: XDS, Zorgmail en Palga. Aan de hand van deze systemen is na te gaan of het UMCG compliant is met het wetsvoorstel. Hierbij is het goed om te vermelden dat deze systemen geen complete lijst zijn van de EUS die door het UMCG worden gebruikt. Deze systemen vormen een selectie die representatief is voor uitwisselingssystemen die binnen het UMCG in gebruik zijn. Conclusies die daarom op basis van deze systemen getrokken kunnen worden, zijn toepasbaar op alle EUS die het UMCG gebruikt.

In dit hoofdstuk zal eerst de digitale infrastructuur van het UMCG kort worden toegelicht om zo een helder beeld te geven van de digitale omgeving waarin deze EUS opereren. Daarna zal er ingegaan worden op de werking van de drie uitwisselingsystemen. Tot slot zal er gekeken worden naar de wijze waarop het UMCG toeziet op de informatie beveiliging. Hierna zal in opeenvolgende hoofdstukken de onderzoeksresultaten, de analyse, de conclusie en de aanbevelingen aan bod komen. Achtereenvolgens zijn in dit hoofdstuk de volgende paragrafen te vinden: digitale infrastructuur (§7.2), werking XDS (§7.3), werking Zorgmail (§7.4), werking Palga (§7.5), informatiebeveiliging(§7.6) en tot slot de conclusie (§7.7).

7.2 Digitale infrastructuur

Om het UMCG te kunnen laten functioneren zijn er over de jaren heen ontzettend veel systemen en applicaties ontstaan die verschillende werkzaamheden binnen de organisatie mogelijk maken. Het belangrijkste systeem is het ziekenhuis informatie systeem (hierna ZIS). Dit systeem is de basis van het 'digitale ziekenhuis' en bevatte oorspronkelijk alle systemen in het ziekenhuis. Deze systemen waren zo ontworpen dat ze elkaar konden 'verstaan'. Om duidelijk te krijgen hoe de digitale structuur van het UMCG eruit ziet is het belangrijk om te weten dat systemen voor hun functionaliteit vaak in verbinding staan met andere systemen. Een recent overzicht van de verschillende verbindingen is te vinden in de volgende afbeelding.

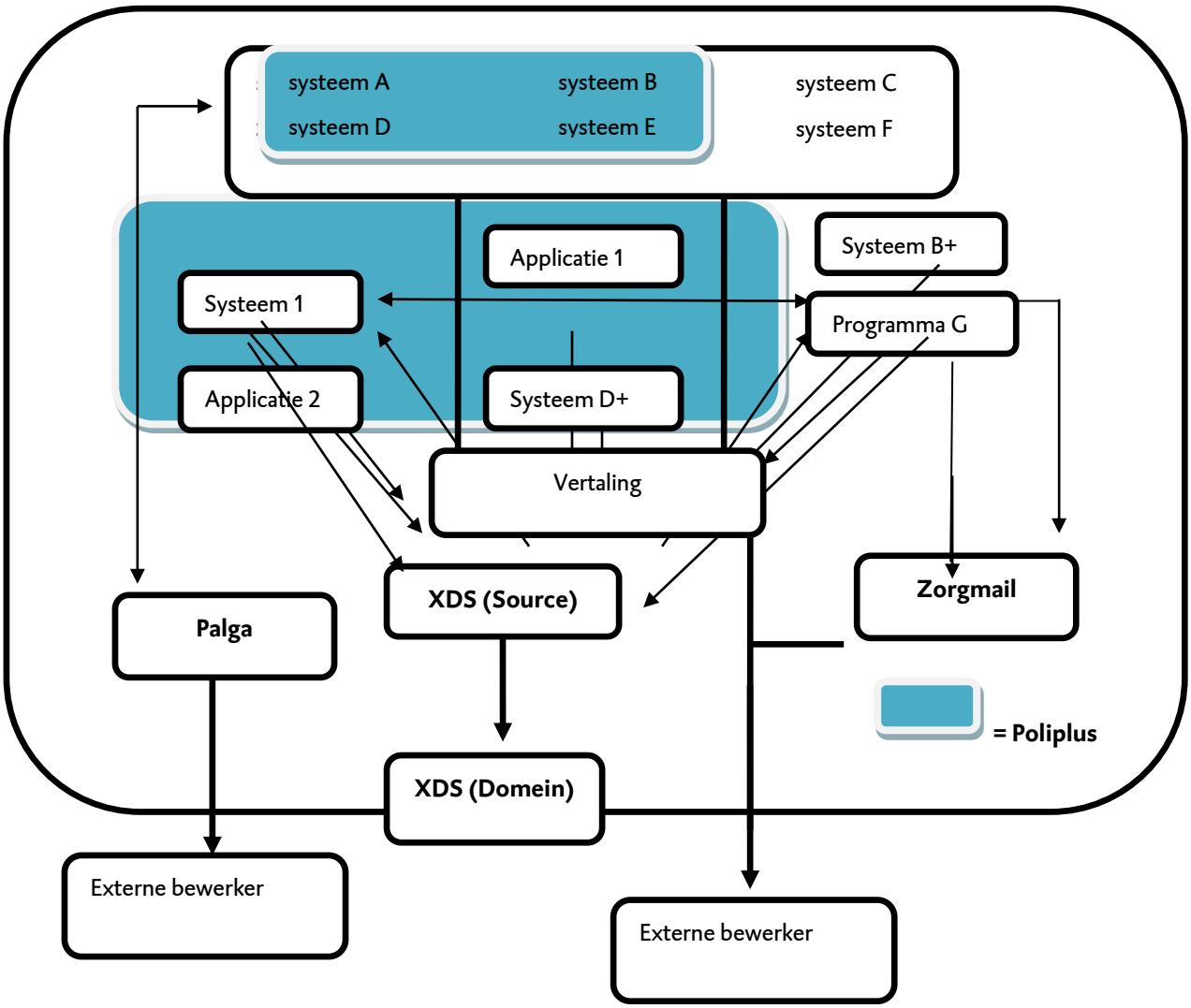


- Het netwerk van systemen van het UMCG kent meer dan 1000 systemen heeft meer dan 1500 onderlinge verbanden.
(afbeelding is afkomstig uit een diapresentatie van een medewerker binnen het UMCG)

Om systemen met elkaar te laten samenwerken, moeten ze met elkaar kunnen communiceren. Een systeem kan echter alleen met een ander systeem 'praten' als ze gebaseerd zijn op dezelfde 'taal'. Dit is echter lang niet altijd het geval. Er bestaat een internationale standaardtaal voor systemen binnen de zorg en dat is Health Level 7 (hierna HL7). Ook binnen het UMCG wordt er geprobeerd om zoveel mogelijk systemen met deze standaardtaal te laten spreken. HL7 kent echter verschillende 'dialecten' en sommige systemen 'spreken' zelfs een hele andere taal. Daardoor bestaat er binnen het digitale ziekenhuis een programma dat 'Cloverleaf' heet. Dit programma fungeert als een 'vertaler' om systemen die niet dezelfde taal spreken toch met elkaar te laten communiceren. De oorspronkelijke systemen in het ZIS konden elkaar uiteraard verstaan zonder de hulp van Cloverleaf. Sinds de aanschaf van het ZIS en diens bijbehorende programma's en systemen zijn er, zoals ook te zien in bovenstaande afbeelding, veel nieuwe programma's en applicaties bij gekomen. Hierdoor is een vertaler als Cloverleaf noodzakelijk geworden. Zowel Palga als Zorgmail zijn voorbeelden van nieuwe systemen die zich buiten het oorspronkelijke ZIS bevinden. Echter is het goed om te benadrukken dat niet elk nieuw(er) systeem per definitie Cloverleaf nodig heeft om te kunnen functioneren.

In dit geheel van systemen bestaat er een systeem dat Poliplus heet. Dit programma verzamelt informatie uit verschillende systemen zodat de informatie eenvoudig in te zien is. Poliplus functioneert daardoor als een intern elektronisch patiëntendossier, en wordt gebruikt om op eenvoudige wijze informatie uit verschillende systemen te bundelen. Veel systemen worden echter buiten Poliplus om geraadpleegd of zijn zelfs helemaal niet in Poliplus opgenomen. Hier volgt een schema om de structuur verder te verduidelijken.

UMCG digitale infrastructuur



Het bovenstaande schema is een versimpelde weergave. In dit schema is duidelijk te zien dat veel systemen slechts intern opereren. In tegenstelling tot gewone systemen hebben EUS ook een functie naar buiten toe. Dit onderscheid is van belang omdat het huidige wetsvoorstel slechts betrekking heeft op systemen met een dergelijke werking. De uitwisselingssystemen moeten, waar het dit wetsvoorstel betreft, dus als een aparte categorie worden beschouwd. De voorgaande illustraties dienen alleen om een overzicht te geven van de digitale infrastructuur waarin de EUS bestaan. Nu duidelijk is hoe de digitale omgeving van het UMCG eruit ziet, kan er gekeken worden naar de werking van de verschillende uitwisselingssystemen.

7.3 Werking XDS

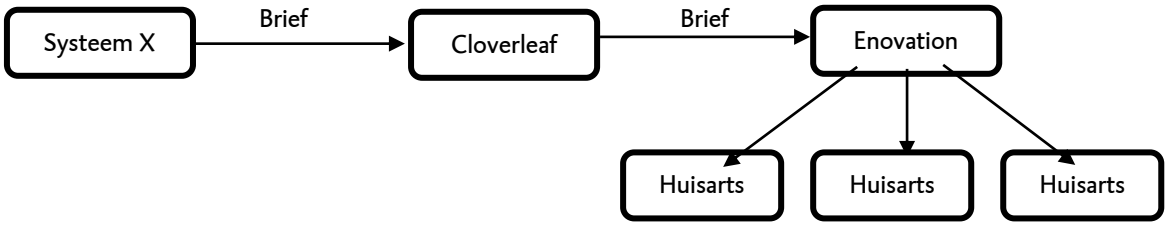
XDS is een wereldstandaard die wordt gebruikt om documenten tussen zorginstellingen uit te wisselen. Hierbij houd XDS rekening met andere standaarden die binnen het werkveld van informatiebeveiliging en informatie-uitwisseling bestaan. XDS staat voor Cross-Enterprise Document Sharing en wordt steeds vaker gebruikt, waardoor het UMCG in 2009 dit systeem is gaan gebruiken. Het doel was in eerste instantie om alleen radiologiebeelden digitaal uit te gaan wisselen met andere zorginstellingen. Om de werking van XDS te kunnen begrijpen is van belang om terug te keren naar de toelichting uit de voorgaande paragraaf. Zoals gezegd worden systemen vaak geschreven in verschillende talen. Dat maakt het uitwisselen van informatie met een andere zorginstelling erg lastig, omdat systemen vaak zodanig van elkaar verschillen dat als een systeem in ziekenhuis A informatie zou sturen naar een

systeem van ziekenhuis B, dat laatstgenoemde die informatie totaal niet zou begrijpen. De functie van XDS is om die miscommunicatie te verhelpen.

XDS heeft een zogenaamde XDS index. Alle aangesloten zorginstellingen kunnen in deze index informatie aanbieden in een digitale inhoudsopgave. De daadwerkelijke documenten die bij deze inhoudsopgave horen komen in de XDS repository[108]. Om vanuit een systeem informatie in de XDS index en repository te kunnen plaatsen moet dat systeem in staat zijn om met XDS te kunnen communiceren. Kan een systeem dat, dan spreken we over een XDS source. Door een systeem aan te passen kan van een gewoon systeem dus een XDS source gemaakt worden. In de praktijk wordt daar vaak koppelsoftware voor gebruikt. In XDS zit ook een 'logging' functie ingebouwd. Daarnaast maakt XDS het mogelijk om binnen de XDS omgeving aan te geven welke toestemmingen een patiënt heeft gegeven met betrekking tot diens gegevens. Dit wordt binnen XDS het Basic Patient Privacy Concept genoemd. Als een ander ziekenhuis de juiste rechten en toestemmingen heeft kan deze via XDS consumer de mogelijk krijgen om in de XDS index en repository te kijken of zelfs de digitale bestanden naar dat ziekenhuis over te halen. De XDS index en de XDS repository bevinden zich in het XDS domein dat op zichzelf staat, en dat bevindt zich buiten de digitale omgeving van ieder ziekenhuis.[109] Dit XDS domein wordt door een onafhankelijke stichting beheerd. Men kan zelf bepalen hoeveel ziekenhuizen toegang hebben tot het domein, en vervolgens is het ook mogelijk om domeinen aan elkaar te koppelen.[110] Hiermee zou uiteindelijk een situatie ontstaan waarin XDS landelijke dekking heeft. Momenteel wordt XDS vaak op regionale schaal toegepast. Zo is het UMCG verbonden met een XDS domein dat zich beperkt tot het noorden van Nederland en in beheer is van stichting GERRIT.

7.4 Werking Zorgmail

Het zorgmail systeem heeft als doel om de digitale verspreiding van patiëntenbrieven richting huisartsen te faciliteren. Vanuit verschillende zorginstellingen gaan er dagelijks brieven naar huisartsen met informatie over patiënten. Omdat veel van deze brieven tegenwoordig uitsluitend digitaal verstuurd worden, is een systeem als zorgmail dus onmisbaar. Zorgmail is software die ontworpen is en onderhouden wordt door VANAD Enovation (hierna Enovation). Zij zorgen met hun systeem dat brieven vanuit het UMCG veilig terecht komen bij de verschillende huisartsen. Zorgmail heeft een ontlastende werking, en is erop gericht om te voorkomen dat een zorginstelling als het UMCG zijn eigen netwerk met huisartsen moet opzetten en veranderingen in dat netwerk bij zou moeten houden. Om een brief vanuit het UMCG correct aan te kunnen leveren bij Enovation moet deze eerst door Cloverleaf worden vertaalt. Zodra dit gebeurt is, wordt de verdere verwerking door Enovation gefaciliteerd. Enovation zet vervolgens de brieven door naar de individuele huisartsen. Onderstaande figuur laat zien hoe dit proces eruit ziet.



Het dagelijkse beheer van Zorgmail bestaat uit het doorsturen van brieven naar Enovation. Daarnaast kan het voorkomen dat brieven worden teruggezonden omdat deze niet bezorgd kunnen worden. Kan een brief niet verzonden worden dan is er vaak een probleem met het elektronisch postbusnummer. Elke huisarts heeft een elektronisch postbusnummer, en dit nummer kan om verschillende redenen veranderen. Voorbeelden hiervan zijn een verhuizing van een huisarts, de vervanging van een uit dienst tredende huisarts, beëindiging van een contract tussen een zorgverzekeraar en een huisarts etc. Als een dergelijk nummer veranderd is, kan het zo zijn dat de brief vanuit het UMCG een elektronisch postbusnummer gebruikt wat op dat moment niet meer bestaat. Zodra Enovation deze brief dan terug stuurt, moet het juiste postbusnummer worden achterhaald, en daarna wordt de brief alsnog verzonden en uiteindelijk afgeleverd.

---

[108] Bij de uitwisseling van beelden schrijft de standaard een net iets andere werkwijze voor. In de XDS repository dient slechts een verwijzing opgenomen te worden die linkt met de daadwerkelijke afbeelding. De achterliggende reden is dat men de belasting op het XDS systeem wil beperken. Omdat de afbeeldingen vaak van hoge kwaliteit zijn hebben deze vaak een aanzienlijke omvang.
[109] Het is ook mogelijk om de XDS repository binnen een ziekenhuis te houden, en niet in het domein te plaatsen.
[110] Deze ontwikkeling is momenteel al gaande, het koppelen van XDS domeinen noemt men XCA.

7.5 Werking Palga

Palga is een systeem dat fungeert als een databank van pathologie gegevens. De term Palga staat voor Pathologisch-Anatomisch Landelijk Geautomatiseerd Archief. Palga wordt beheerd door stichting Palga. Het systeem wordt landelijk door alle pathologieafdelingen gebruikt en dient als een opslag voor al het pathologieonderzoek wat in Nederland wordt verricht. Palga wordt onder andere gebruikt als een landelijke basis voor kankerregistratie en voor de evaluatie en monitoring van bevolkingsonderzoeken en ander wetenschappelijk onderzoek.[111] Palga heeft twee verschillende functies. Binnen Palga wordt namelijk gebruik gemaakt van lokale verslagen en landelijk beschikbare verslagen. Dit verschil wordt bijgehouden door het gebruik van dossiernummers. Het systeem maakt het mogelijk om eerdere pathologieverslagen te koppelen aan de patiënt die op dat moment wordt onderzocht. Via een huisarts of specialist kan er een verzoek gedaan worden tot weefselonderzoek. Dit verzoek wordt verwerkt in een order, en deze order wordt vervolgens door de afdeling pathologie verwerkt. Van de verwerking wordt een verslag opgesteld, en dit verslag komt vervolgens in Palga te staan. Palga heeft dus buiten het UMCG verschillende functies, maar binnen het UMCG wordt het gebruikt om te zien of een patiënt eerder pathologisch onderzoek heeft laten verrichten, en de conclusies die uit dat onderzoek naar voren zijn gekomen. Op deze wijze kan een patholoog geholpen worden bij het maken van de juiste diagnose. Wederom is er sprake van een systeem dat wordt beheerd door een externe partij, die het netwerk tussen de verschillende pathologische afdelingen in Nederland onderhoudt. De gegevens worden via het Palga systeem naar de externe partij gecommuniceerd.

7.6 Informatiebeveiliging

7.6.1 Inleiding

In deze paragraaf zal er dieper ingegaan worden op de wijze waarop de informatiebeveiliging binnen het UMCG is vormgegeven. Hiermee wordt iets vooruitgelopen op de onderzoeksresultaten uit het volgende hoofdstuk. Omdat de informatiebeveiliging nauw samenhangt met de werking van de systemen is het van belang om hier dieper op in te gaan alvorens de onderzoeksresultaten te behandelen. Dit komt de begrijpelijkheid van de resultaten ten goede. Onvermijdelijk is daarmee dat al een deel van de onderzoeksvragen, namelijk die uit hoofdstuk 4, al in dit hoofdstuk beantwoord worden.

7.6.2 Structuur

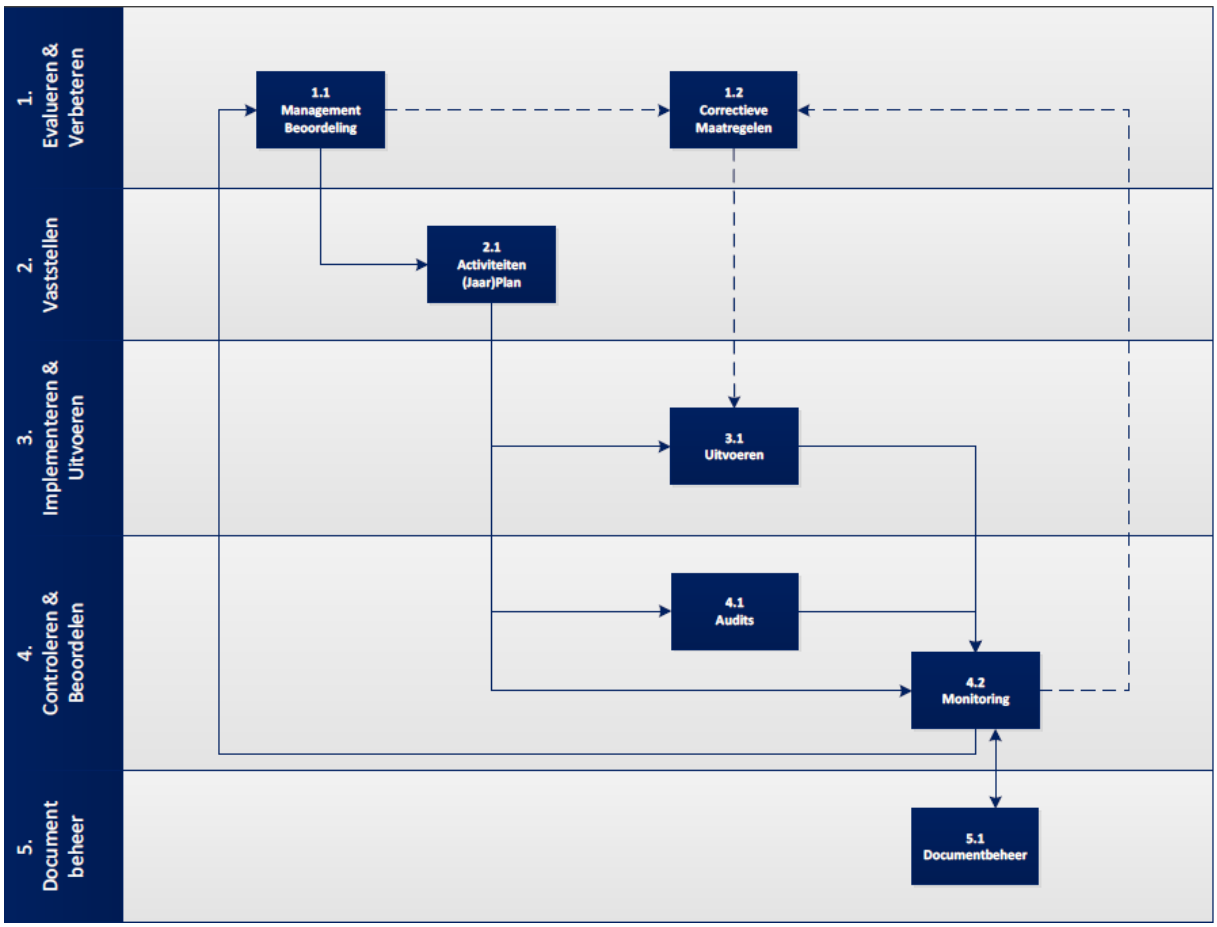
Omdat het UMCG een enorm geheel aan informatie moet verwerken en beheren is het van groot belang dat er binnen het ziekenhuis de nodige aandacht wordt besteed aan informatiebeveiliging. Binnen het UMCG zijn de verschillende directeuren, onder verantwoordelijkheid van de Raad van Bestuur, ieder zelf verantwoordelijk voor de implementatie van het informatiebeveiligingsbeleid. De directeur Medische Zaken is verantwoordelijk voor de vorming van het beleid en voor het sturing geven aan de manier waarop informatiebeveiliging wordt uitgevoerd binnen de organisatie. Dit beleid is gebaseerd op alle standaarden en normen die in hoofdstuk 4 aan bod zijn gekomen. Hiermee is dus een duidelijke takenverdeling geschapen om te zorgen dat de informatiebeveiligingstaken uitvoerbaar blijven.

7.6.3 Werkwijze

Binnen het UMCG wordt er gebruikt gemaakt van een plan-do-check-act cyclus. In de cyclus wordt een activiteitenplan opgesteld dat vervolgens wordt uitgevoerd. Het activiteitenplan, ook wel bekend als het actieplan, is gebaseerd op risicoanalyses en bevat actiepunten en verbeterpunten. Deze punten moeten vervolgens door de betreffende afdelingen worden uitgevoerd, en op die uitvoering wordt toezicht gehouden. Dat gebeurt in de vorm van audits. Audits zijn controlemomenten waarin door een auditor gekeken wordt in hoeverre het actieplan is geïmplementeerd. Deze resultaten worden meegenomen in een uiteindelijke beoordeling die vervolgens correctieve en/of preventieve maatregelen tot gevolg kunnen hebben. Audits worden gedurende het hele jaar uitgevoerd en vinden over het algemeen plaats op basis van een vooraf opgestelde planning. De planning die momenteel binnen het UMCG wordt gehanteerd streeft ernaar om alle informatiebeveiligingsnormen in een cyclus van drie jaar te toetsen. Door de enorme omvang van informatiesystemen en gegevens is het onmogelijk om alle systemen in deze cyclus mee te nemen. In plaats daarvan wordt naar een doorsnede van alle informatiesystemen gekeken om op die manier een goed beeld te krijgen van de stand van zaken binnen de gehele organisatie. Momenteel wordt er gekeken naar mogelijkheden om de plan-do-check-act cyclus te verbeteren. Hierin wordt onder meer aandacht besteed aan hoe groepen van gelijksoortige informatiesystemen tegelijkertijd geëvalueerd kunnen worden. Hierop worden vervolgens ‘baselines’ opgesteld die de basiseisen voor informatiebeveiliging aangeven. Deze baselines geven een houvast om mee te werken en op basis waarvan afdelingen ook zelf in staat zijn om de veiligheid te controleren. Onderstaand figuur geeft duidelijk weer hoe de cyclus eruit ziet.

---

[111] ‘Website stichting Palga, over ons’, 30 april 2016, http://www.palga.nl/over-ons/stichting-palga/



(2 = plan | 3 = do | 4 = check | 1 = act)
(afbeelding is afkomstig uit een diapresentatie van een medewerker binnen het UMCG)

Een belangrijk element is de rol van externe bewerkers in dit geheel.[112] In de risicoanalyse wordt ook gekeken naar de contracten die met de bewerkers zijn gesloten en de risico's die daarin een rol spelen. Uit de analyse zou bijvoorbeeld naar voren kunnen komen dat een overeenkomst moet worden aangepast.[113] Voor toekomstige contracten is er een standaard bewerkersovereenkomst opgesteld waarin allerlei bepalingen zijn opgenomen die dergelijke risico's voorkomen. De bewerker heeft binnen zijn organisatie vaak een eigen plan-do-check-act cyclus die wordt gevolgd, waaromtrent in een overeenkomst ook nadere afspraken kunnen worden vastgelegd. Een bewerker brengt daarnaast vaak een 'control statement' uit waarin staat vastgelegd dat binnen de organisatie is voldaan aan verschillende veiligheidseisen. Mocht het UMCG dat nodig vinden dan zou het zelfs een derde partij in kunnen huren om een onafhankelijke audit bij de bewerker uit te laten voeren.

7.7 Conclusie

De digitale omgeving van het UMCG is een enorm geheel, waarin veel verschillende systemen bestaan die met elkaar samenwerken. Binnen dat netwerk moet er voor dit onderzoek een duidelijk onderscheid gemaakt worden tussen systemen die slechts intern gebruikt worden en systemen die informatie uitwisselen met andere organisaties. XDS, Palga en Zorgmail vormen een afspiegeling van dat geheel aan uitwisselingssystemen en hebben ieder een afzonderlijke functie. Er zijn duidelijke verschillen maar ook gelijkenissen tussen de systemen te vinden. Wat alle drie de systemen gemeen hebben is hoe ze worden beoordeeld in de informatiebeveiligingscyclus. Deze cyclus ziet door middel van risicoanalyses en audits toe op de borging van de veiligheid van informatie. Voor de beveiliging is een belangrijke taak weggelegd voor de bewerker, en voor het UMCG in het controleren van die bewerker. Door te kijken naar deze werkwijze is het straks mogelijk om een deel van de onderzoeksvragen te beantwoorden. Om uiteindelijk alle onderzoeksvragen te kunnen beantwoorden zal het volgende hoofdstuk de onderzoeksresultaten behandelen.

[112] Alle drie de EUS waar in dit onderzoek naar gekeken wordt hebben te maken met externe bewerkers.
[113] Deze aanpassingen kunnen worden gedaan op het moment dat het contract met de bewerker moet worden verlengd.

8 Onderzoeksresultaten

8.1 Inleiding
De informatie die voortgekomen is uit de gesprekken met acht verschillende experts binnen het UMCG zullen in dit hoofdstuk worden uitgewerkt. Bij de uitwerking zal dezelfde volgorde aangehouden worden als bij de theorie.

8.2 Eisen Wet bescherming persoonsgegevens
In dit onderzoek is hoofdzakelijk onderzocht of het UMCG compliant is met toekomstige wetgeving. Hiervoor is het van belang eerst te bepalen in hoeverre bestaande regelgeving wordt nageleefd. Alle verwerkingen in Palga, Zorgmail en XDS betreffen medische persoonsgegevens, en worden door de Wbp dus aangemerkt als verwerkingen van bijzondere persoonsgegevens. Uit het onderzoek komt naar voren dat de doeleinden voor de gegevensverwerking gebaseerd zijn op een rechtmatige grond.[114] Het gaat bij alle drie de systemen om een uitwisseling die noodzakelijk is voor het uitvoeren van een overeenkomst waar de patiënt partij is.[115] De overeenkomst waarop wordt gedoeld is de geneeskundige behandelingsovereenkomst die een patiënt heeft met een arts.[116] Dat de verwerking gebaseerd is op deze wettelijke grondslag betekent echter niet dat de patiënt geen toestemming dient te verlenen voor opname in een elektronisch uitwisselingssysteem. Die toestemmingsverplichting bestaat reeds, en wordt slechts uitgebreid met de komst van gespecificeerde toestemming in het nieuwe wetsvoorstel. Hier zien we dat alle uitwisselingssystemen tekort schieten. Uit het onderzoek is geen moment naar voren gekomen waarop patiënten worden gevraagd om toestemming.[117] Daarnaast geven verschillende experts aan dat XDS, Palga en Zorgmail ook op andere punten soms moeite hebben om volledig volgens bestaande wetgeving te opereren. De problemen zijn bij elk systeem verschillend. Een voorbeeld van een mogelijke strijdigheid met de wet is de mate waarin informatie via Palga wordt uitgewisseld. De wet geeft aan dat de uitwisseling van persoonsgegevens toereikend, niet overmatig en ter zake dienend moet zijn. Binnen de organisatie wordt er verschillend gedacht over deze wettelijke eis. In de praktijk vraagt een arts of onderzoeker namelijk vaak alle mogelijke informatie op om zo te bepalen of iets relevant is, en systemen als Palga en XDS maken dat ook zeer eenvoudig. Het is begrijpelijk dat artsen en onderzoekers zo veel mogelijk van een patiënt willen weten om te voorkomen dat er een verkeerde conclusie of diagnose wordt vastgesteld. De uiteindelijke afweging of bepaalde gegevens relevant zijn of niet kan in veel gevallen echter pas gemaakt worden nadat de gegevens al zijn ingezien. Het is niet ondenkbaar dat daarmee de uitwisseling van gegevens in veel gevallen ook overmatig kan zijn. De vraag hoe deze wettelijke eis moet worden geïnterpreteerd is ook voor XDS, maar op dit moment vooral voor een systeem als Palga relevant, omdat in dat systeem nu al ontzettend veel informatie over een patiënt te vinden is.

Uit het onderzoek blijkt ook dat men vaak op de hoogte is van het feit dat de uitwisselingssystemen wettelijke strijdigheden bevatten. Toch wordt daar in de praktijk niet altijd actie op ondernomen. Bij XDS wordt bijvoorbeeld een bewuste afweging gemaakt om soms te kiezen voor praktische uitvoerbaarheid ten koste van wettelijke naleving. Bij alle uitwisselingssystemen speelt de financiële factor hierin een grote rol. Op basis van dit onderzoek kan niet een complete lijst met strijdigheden worden opgesteld.

8.3 Beveiliging persoonsgegevens
Om tot een juiste beveiliging van persoonsgegevens te komen wordt er binnen de organisatie van het UMCG ruim aandacht besteed aan het implementeren van beleid rondom informatiebeveiliging. In paragraaf 6.6 is te lezen hoe de plan-do-check-act cyclus, de risicoanalyse en de audit daar een rol in spelen. In deze aanpak vindt men eigenlijk alle eisen terug die wettelijk gesteld zijn aan de wijze waarop er constant moet worden toegezien op dreigende beveiligingsrisico's. Tijdens de interviews is vast komen te staan dat het proces rondom informatiebeveiliging effectiever zou moeten zijn. Tijdens het onderzoek zijn verschillende factoren geconstateerd die in meer of mindere mate bijdragen aan het feit dat de informatiebeveiliging op dit moment niet effectiever is:

- **Omvang aantal systemen**

Door de immense hoeveelheid systemen die het UMCG kent, is het noodzakelijk om op basis van steekproeven de beveiligingskwaliteit te controleren om de werkdruk behapbaar te houden. Hierdoor is het denkbaar dat systemen die al langer in gebruik zijn, toch aan de aandacht ontsnappen.

- **Onderdeel groter geheel**

De beveiliging van persoonsgegevens is een slechts onderdeel van een groter geheel aan beveiligingsnormen waarop moet worden toegezien.

- **Autonomie afdelingen**

---

[114] Artikel 8 Wbp.
[115] Artikel 8 sub b Wbp.
[116] Artikel 7:446 BW.
[117] Zie ook de toelichting van de Minister in *kamerbrief wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens,* 8 maart 2016.

Doordat afdelingen zelf verantwoordelijk zijn voor het daadwerkelijk uitvoeren van de correctieve en/of preventieve maatregelen, zullen er verschillen bestaan tussen afdelingen die hier strenger en minder streng mee omgaan.

- **Financiële kosten**

De financiële kosten die nodig zijn om de problemen bij een bepaald systeem op te lossen kunnen een belemmering vormen om dat ook daadwerkelijk te doen.

- **Wildgroei systemen**

Het ontbreekt aan een totaaloverzicht van systemen. Men is recentelijk begonnen om alle systemen in kaart te brengen, maar dat is nog niet volledig. Door de autonomie van afdelingen in de aanschaf van systemen is dit ook moeilijk te achterhalen.

- **Oud en nieuw werkwijze**

Nieuwe systemen (zoals XDS) worden tegenwoordig onderworpen aan een eerste risicoanalyse voordat deze geïmplementeerd worden, bij oude systemen gebeurde dat niet altijd. Dit draagt bij aan de omvang van niet-geïnventariseerde risico's.

- **Onderbezetting**

Het aantal medewerkers dat is opgeleid om op dit vlak audits uit te voeren is laag. Momenteel worden er acht nieuwe auditors opgeleid om in de toekomst audits uit te kunnen voeren. Dit werd tot op heden slechts door twee medewerkers gedaan.

- **Bewerkersovereenkomsten**

Veel systemen hebben te maken met bewerkers die op grond van de bewerkersovereenkomst beweren niet verplicht te zijn om bepaalde zaken aan te passen. In sommige gevallen ontstaat er discussie of de bewerker of het UMCG verantwoordelijk is om iets uit te voeren of op te lossen.

Uit de verschillende interviews blijkt wel dat er momenteel een inhaalslag wordt gemaakt op het gebied van informatiebeveiliging en de plek daarbinnen voor de beveiliging van (medische) persoonsgegevens. Deze verbeteringen zijn van toepassing op alle bovengenoemde factoren.

8.4 De behandelrelatie

Uit het praktijkonderzoek blijkt dat in alle uitwisselingssystemen maatregelen te vinden zijn die dienen ter waarborging van de behandelrelatie. Hierbij ligt de nadruk op het bewaken van het medisch beroepsgeheim. In de praktijk betekent dit dat binnen de uitwisselingssystemen maatregelen worden getroffen om ervoor te zorgen dat alleen personen die bevoegd zijn om van de persoonsgegevens kennis te nemen, ook daadwerkelijk toegang tot deze gegevens hebben. Ondanks dat in alle drie de EUS voorbeelden van bovengenoemde maatregelen te vinden zijn, betekent dat echter niet dat het borgen van de behandelrelatie altijd succesvol verloopt. Een voorbeeld hiervan is te vinden in Palga. In dit systeem worden pathologische verslagen van een patiënt aan een actueel onderzoekverzoek gekoppeld op basis van verschillende zoekcriteria in de Palga databank. De zoekcriteria bestaan uit voorletters, eerste vier letters van de achternaam en een geboortedatum. Hierdoor komt het heel af en toe voor dat meer dan een patiëntendossier aan hetzelfde onderzoekverzoek gekoppeld wordt. Ondanks dat een dergelijke situatie zelden voorkomt, is de impact van een dergelijk voorval vrij ernstig, mede door de omvang en de aard van de gegevens die daarmee voor een patholoog inzichtelijk worden. Het is uiteindelijk de professionaliteit van de patholoog in kwestie die bepaalt hoeveel van deze informatie op dat moment daadwerkelijk bekeken wordt. Een toezichthoudende instantie zal echter geen onderscheid maken in welke mate een onderzoeker of arts de persoonsgegevens in een dergelijke situatie tot zich neemt. Het bestaan van een inzagemogelijkheid in de historie van pathologische onderzoeksresultaten van een patiënt waar geen behandelrelatie mee is, zou simpelweg niet mogelijk moeten zijn.

Een ander voorbeeld van de schending van de behandelrelatie is te vinden in Zorgmail. Het Zorgmail systeem werkt normaal gesproken op dusdanige wijze dat de inhoud van een medische brief slechts door de huisarts ingezien wordt. Dit gaat echter mis op het moment dat het elektronisch postbusnummer dat gebruikt wordt om de brief naar de juiste huisarts te sturen, niet (meer) klopt. Enovation stuurt op dat moment de brief terug naar het UMCG met de mededeling dat het de brief niet succesvol kan bezorgen. Hierdoor moet het UMCG op zijn beurt gaan achterhalen welke wijziging in het elektronisch postbusnummer heeft plaatsgevonden. Om dit echter te achterhalen moet dit postbusnummer uit de brief worden gehaald. Dat betekent dat een beheerder de brief moet openen om daar de benodigde informatie uit te halen die nodig is om de wijziging in het postbusnummer te kunnen nagaan. Ook hier geldt dat de professionaliteit van de beheerder de enige barrière is die voorkomt dat men zichzelf inzage verschaft in persoonsgegevens van een patiënt zonder dat er een behandelrelatie is tussen die persoon en de patiënt. Dit zijn voorbeelden die tijdens het onderzoek naar voren zijn gekomen maar vormen echter geen totaalbeeld van mogelijke schendingen die in de systemen plaats vinden. Apart onderzoek zou kunnen uitwijzen of er meer van dit soort problemen zijn.

Tekenend bij beide voorbeelden is dat beide in theorie eenvoudig verholpen zouden kunnen worden. Denk hierbij aan het simpelweg aanpassen van de zoekcriteria dat Palga gebruikt om gegevens te koppelen, of het verwerken van het elektronisch postbusnummer in de bestandsnaam van een brief die verstuurd wordt met Zorgmail. Ook is het opmerkelijk dat men zich vaak in de praktijk in zekere mate wel bewust is van de problemen in een systeem. Dit is vooral het geval bij de systemen die al langer in gebruik zijn zoals Palga en Zorgmail. Daarmee is niet gezegd dat medewerkers zich altijd realiseren wat de juridische impact van deze problemen kan zijn. Hoe het mogelijk is dat dergelijke problemen toch bestaan heeft verschillende oorzaken. De exacte oorzaken zijn voor elk probleem verschillend. Een aantal factoren komen in dit onderzoek herhaaldelijk naar voren. Verantwoordelijken hebben bijvoorbeeld vaak rekening te houden met het financiële aspect. Ook de rol van de bewerker staat vaak centraal. Een bewerker kan van mening zijn dat een bepaald probleem voor de verantwoordelijkheid van het UMCG komt, terwijl het UMCG vaak van mening is dat de bewerker een probleem moet oplossen. Gewenning en onwetendheid zijn ook factoren die een rol spelen. Bij het benoemen van deze factoren is het belangrijk om een zeker onderscheid te maken tussen systemen die al langer bestaan (Palga & Zorgmail) en systemen die vrij recent in gebruik zijn genomen (XDS). Het onderzoek naar XDS heeft niet directe voorbeelden opgeleverd van wettelijke strijdigheden. Toch kan uit de interviews worden afgeleid dat beslissingen betreffende de organisatie en inrichting van XDS soms botsen met wettelijke bepalingen. Als deze strijdigheid tijdens de besluitvoering wordt geconstateerd kan het voorkomen dat een meerderheid van beslissingsbevoegde verantwoordelijken er toch voor kiest om deze strijdigheid te negeren. De redenen die die hiervoor worden gegeven zijn het werkbaar, functioneel en/of financieel draagbaar houden van XDS als systeem.

8.5 Het wetsvoorstel

8.5.1 Inleiding

Uiteindelijk heeft het onderzoek de bedoeling gehad om te kijken in hoeverre het UMCG compliant is met het toekomstige wetsvoorstel. [118] Hiermee is gekeken naar de veranderingen die het wetsvoorstel voor ogen heeft, en in hoeverre de uitwisselingssystemen hieraan voldoen. Uit het onderzoek blijkt dat Palga, Zorgmail en XDS op dit moment op geen enkel punt voldoen aan het nieuwe wetsvoorstel. Aangezien het wetsvoorstel nog niet is aangenomen, kan dit ook eigenlijk niet van een organisatie verwacht worden. De onderzoeksvragen uit de theorie met betrekking tot het toekomstige wetsvoorstel zullen hier achtereenvolgens behandeld worden.

8.5.2 Gespecificeerde toestemming

Het in het wetsvoorstel geïntroduceerde gespecifieerde toestemming is een complexe vorm van toestemming, waar uiteraard niet elke patiënt per definitie gebruik van zal maken, maar waar wel de mogelijkheid toe moet zijn. Op dit moment is geen enkel van de drie EUS in staat om een dergelijke registratie van toestemming te registreren. Uit de gesprekken met verschillende experts is niet alleen duidelijk geworden dat de systemen deze toestemmingsvorm momenteel niet kunnen ondersteunen, maar ook dat het ontzettend ingewikkeld zou zijn om de systemen zodanig aan te passen dat dit wel mogelijk zou zijn. De complexiteit van de toestemmingsvorm vervult hierbij een sleutelrol. In theorie geeft deze toestemmingsvorm de patiënt enorm veel controle over zijn persoonsgegevens. Dat betekent dat de software die in de praktijk wordt gebruikt om gegevens uit te wisselen, in staat moeten zijn om een zeer specifiek onderscheid te maken tussen welke gegevens wel of niet beschikbaar zijn en welke zorgverleners wel of geen toegang hebben tot verschillende delen van die persoonsgegevens. Dat is op dit moment voor veel systemen onmogelijk.

8.5.3 Elektronische inzage & logging

Uit het onderzoek blijkt dat er op dit moment geen elektronische vorm van inzage is voor patiënten. Voor alle drie de uitwisselingssystemen geldt dat er op dit punt nog niet voldaan wordt aan het wetsvoorstel. Palga en Zorgmail zijn niet ontworpen met de bedoeling om patiënten inzicht te geven in de persoonsgegevens die hierin worden verwerkt en uitgewisseld. De opzet van het XDS systeem werkt fundamenteel anders dan Palga en Zorgmail, maar is ook niet ontworpen voor gebruik door patiënten. XDS bevat alleen een inzagefunctie voor de medici die ermee moeten werken en niet voor patiënten. Een andere eis van het wetsvoorstel is dat de loggegevens inzichtelijk moeten zijn voor patiënten. XDS heeft als enige systeem een onderdeel ingebouwd dat momenteel al loggegevens opslaat. Deze opslag van loggegevens bestaat echter slechts uit ruwe data waar nog geen software laag overheen zit waarmee deze data ook op een overzichtelijke wijze in kan worden gezien.

[118] Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens

8.6 Conclusie

Nu de resultaten van het praktijkonderzoek behandeld zijn, kan er op basis van deze informatie in het volgende hoofdstuk een analyse gedaan worden om te zien hoe de praktijkresultaten zich verhouden tot de onderzoekpunten uit de theorie.

9 Analyse

9.1 Inleiding
In dit hoofdstuk leggen we de onderzoekspunten die uit de theorie naar voren zijn gekomen, naast de uitkomsten van het praktijkonderzoek. Op grond van deze analyse zal in het volgende hoofdstuk de eindconclusie worden geformuleerd.

9.2 Compliance Wbp
Uit de theorie is gebleken dat het UMCG compliant hoort te zijn met bestaande wetgeving op het gebied van bescherming van persoonsgegevens. Omdat het aanhangige wetsvoorstel voortborduurt op bestaande wetgeving is het van groot belang dat aan deze wetgeving wordt voldaan. Uit de praktijkresultaten blijkt echter dat dit niet altijd het geval is. Verschillende overtredingen zijn tijdens dit onderzoek naar boven gekomen die eigenlijk niet zouden mogen bestaan. Uit het onderzoek is geen sluitend totaal aan overtredingen voortgekomen. Het is daarom niet ondenkbaar dat meer overtredingen gevonden zouden worden als hier gericht onderzoek naar zou worden gedaan. Ondanks voorgaande lijkt het om incidenten te gaan en niet om structurele of zelfs intentionele problemen.

Aan de eisen die in de wet worden gesteld omtrent het doel van verwerking van persoonsgegevens en de basering hiervan op rechtmatige gronden, geldt voor alle onderzochte systemen dat hieraan wordt voldaan. Of elk systeem de verwerking ook zorgvuldig genoeg uitvoert is een kwestie van interpretatie. Juridisch gezien zou men kunnen beargumenteren dat gegevensverwerking en uitwisseling bij sommige systemen wellicht als overmatig kunnen worden beschouwd. Vanuit het medisch werkveld gezien is het echter zeer begrijpelijk dat men het zekere voor het onzekere wil nemen, om zo medische fouten te voorkomen. Voor alle drie de systemen geldt dat er een constante afweging plaats zou moeten vinden om te beoordelen hoe er in een specifiek geval met deze wettelijke eis wordt omgegaan.

Een ander belangrijk aspect uit bestaande wetgeving is het toestemmingsvereiste. Uit het onderzoek blijkt dat aan dit toestemmingsvereiste lang niet altijd voldaan. Veel systemen opereren zonder de nadrukkelijke toestemming van de patiënt. Dit aspect van bestaande wetgeving is met name van belang gelet op de eventuele uitbreiding van het toestemmingsvereiste in het nieuwe wetsvoorstel. Men zal daarom goed moeten gaan kijken waar het verkrijgen van toestemming plaats vindt of plaats zou moeten vinden. Hierbij is het van belang dat het gaat om toestemming van patiënten die hierover op een juiste en volledige wijze zijn geïnformeerd.

9.3 Effectiviteit beveiliging persoonsgegevens
Bij het bestuderen van de theorie rondom de beveiliging van persoonsgegevens is duidelijk geworden dat de nadruk moet liggen op het proces rondom de beveiliging van persoonsgegevens. Het komt namelijk zelden voor dat alle persoonsgegevens altijd 100% beveiligd zijn. Echter als iets niet adequaat beveiligd is moet dat wel snel kunnen worden gedetecteerd en verholpen. Uit de theorie is naar voren gekomen dat een succesvol beveiligingsproces moet bestaan uit verschillende aspecten. Zo moet er sprake zijn van een plan-do-check-act cyclus en ruimte zijn voor risicoanalyses. Door informatiebeveiliging organisatiebreed vorm te geven voorkomt het UMCG dat elk systeem zijn eigen beveiligingsproces moet opzetten. Tijdens het praktijkonderzoek is duidelijk geworden dat het beveiligingsproces in theorie alle belangrijke componenten bevat om tot een goed beveiligingsniveau te komen. Zo kent het proces van het UMCG een plan-do-check-act cyclus, worden er in deze cyclus risicoanalyses uitgevoerd en is er oog voor de rol van de bewerker en de overeenkomst die met een dergelijke bewerker bestaat. Dit gehele proces wordt daarnaast gebaseerd op geldende ISO en NEN-normen. Ondanks dat het informatiebeveiligingsproces voldoet aan alle theoretische eisen is uit de praktijkresultaten duidelijk op te maken dat het proces tot nu toe niet altijd succesvol is, en op bepaalde punten effectiever zou moeten kunnen functioneren. In het voorgaande hoofdstuk is te lezen hoe verschillende factoren hieraan bijdragen. Er zal goed gekeken moeten worden hoe de negatieve effecten op het informatiebeveiligingsproces zich precies tot elkaar verhouden en hoe deze kunnen worden tegen gegaan. Uit het onderzoek blijkt dat de organisatie zelf al de eerste stappen heeft ondernomen om het informatiebeveiligingsapparaat te versterken en uit te breiden. Dit is een noodzakelijke ontwikkeling die verder doorgezet zal moeten worden als het UMCG in de toekomst effectief wil toezien op de beveiliging van alle informatie die binnen haar organisatie wordt verwerkt. Het opleiden van nieuw personeel wat zich bezig houd met het controleren en toezien op deze beveiliging is niet genoeg. Ook de plan-do-check-act cyclus zal moeten intensiveren om te voorkomen dat cruciale gaten in de informatiebeveiliging te laat worden ontdekt. Bewustwording onder personeel wat dagelijks met de verschillende systemen moet werken is daarbij ook erg van belang.

9.4 Borging medische behandelrelatie

Uit de theorie is duidelijk naar voren gekomen dat de medische behandelrelatie ook bij het gebruik van elektronische uitwisselingssystemen een belangrijke rol speelt. Een systeem moet in staat zijn om de vertrouwelijkheid van de behandelrelatie te garanderen. Ondanks dat de verschillende systemen maatregelen nemen om te voorkomen dat de medische behandelrelatie wordt geschonden gebeurt dat echter in sommige gevallen wel degelijk. Het is daarom van belang dat er gekeken wordt waar, en op welke schaal dit voorkomt zodat men dit kan verhelpen. Het informatiebeveiligingsproces zou in staat moeten zijn deze schendingen te constateren zodat de verantwoordelijke afdelingen vervolgens actie kunnen ondernemen om de nodige aanpassingen door te voeren.

Het is een feit dat alle systemen op dit moment nog moeite hebben om de behandelrelatie 100% succesvol te borgen. In het voorgaande hoofdstuk zijn verschillende voorbeelden gegeven waaruit dit ook blijkt. Met betrekking tot XDS bleek uit de onderzoeksresultaten dat de werkwijze die door de verantwoordelijken wordt aangehouden bij de implementatie van het systeem wettelijke strijdigheden oplevert. Deze strijdigheden zijn een gevolg van praktische afwegingen die worden gemaakt die het systeem werkbaar, functioneel en/of financieel draagbaar moeten houden. Ondanks dat het doel van deze werkwijze duidelijk en wellicht zelfs begrijpelijk is, kan het echter enorme gevolgen hebben voor het UMCG om op deze wijze wettelijke strijdigheden te laten bestaan. De omvang van de juridische gevolgen van voorgenoemde is uiteraard afhankelijk van de ernst, omvang en duur van deze wettelijke strijdigheden. Doordat uit de interviews geen concrete strijdigheden zijn af te leiden is het voor dit onderzoek onmogelijk om hierin een juiste risicoafweging te maken. Desalniettemin is het vanuit een juridisch perspectief zeer onverstandig om op deze manier te werk te gaan.

Hoewel uit het onderzoek niet duidelijk is geworden in hoeverre de praktische werkbaarheid van XDS ten koste gaat van wettelijke verplichtingen, is dit systeem van alle drie de EUS in theorie wel verreweg het best in staat om de behandelrelatie te borgen. De werkwijze van XDS ziet er namelijk op toe dat gegevens slechts inzichtelijk of opvraagbaar zijn op het moment dat deze partij over de benodigde toestemming beschikt.[119] Omdat XDS een standaard is die in theorie breed toepasbaar is op een oneindig aantal systemen binnen het UMCG, en daarmee dus deze waarborging naar andere systemen zou kunnen brengen, is het goed om dit te benoemen. Ook Palga en Zorgmail zijn in theorie in staat de behandelrelatie te borgen. In de praktijk gebeurt dat echter nog niet altijd.

9.5 Compliance nieuwe wetsvoorstel

Uit de theorie is er sprake van een inventarisatie van veranderingen die het aanhangige wetsvoorstel met zich mee brengt. Hoofdzakelijk kunnen we drie zaken onderscheiden. De gespecificeerde toestemming als uitbreiding van het bestaande toestemmingsvereiste, de elektronische inzagemogelijkheid voor de patiënt in diens medisch dossier en de verwerking en het inzichtelijk maken van loggegevens in dat elektronisch dossier. Uit de praktijkresultaten komt duidelijk naar voren dat op dit moment nog geen enkel systeem aan deze nieuwe eisen voldoet. Wel kan er een onderscheid gemaakt worden als het gaat om de mate van adaptiviteit van de verschillende uitwisselingssystemen. Zo zou XDS beter in staat zijn om in de toekomst te voldoen aan de nieuwe wettelijke eisen van oudere systemen als Palga en Zorgmail.

[119] Toestemmingen die gebaseerd zijn op het bestaan van een behandelrelatie.

10 Conclusie en aanbevelingen

10.1 Inleiding

Tot slot kunnen er aan de hand van de theorie, de praktijkresultaten en de analyse een conclusie en aanbevelingen worden opgesteld. Deze conclusie en aanbevelingen vormen het antwoord op de centrale onderzoeksvraag:
- In hoeverre kunnen Palga, XDS en Zorgmail zo worden ingericht, dat deze elektronische uitwisselingssystemen voldoen aan het wetsvoorstel *cliëntenrechten bij elektronische verwerking van gegevens* en wat zijn de eventuele knelpunten die geconstateerd worden door verschillende experts en verantwoordelijke medewerkers binnen het UMCG?

10.2 Conclusie

In dit onderzoek is duidelijk gebleken dat Palga, XDS en Zorgmail nog niet voldoen aan de eisen uit het nieuwe wetsvoorstel. Omdat het wetsvoorstel nog volop in ontwikkeling is, is het begrijpelijk dat het UMCG in de huidige situatie nog niet aan de wettelijke eisen voldoet. Door de beslissing van de minister van Volksgezondheid, Welzijn en Sport om de inwerkingtreding van verschillende bepalingen uit het wetsvoorstel uit te stellen is er voor het UMCG, en de zorgsector als geheel, een kans gecreëerd om in een periode van drie jaar na inwerkingtreding van het wetsvoorstel tot de gewenste eindsituatie te komen. Het is daarom van belang dat het UMCG nauw samen gaat werken met beroep- en cliëntenorganisaties om zo de actuele ontwikkelingen in dit dossier te volgen en tijdig kennis te kunnen nemen van het plan dat wordt opgesteld dat moet zorgen voor een succesvolle voorbereiding op de inwerkingtreding van de overgebleven wetsbepalingen. Deze recente beslissing van de Minister sluit naadloos aan bij de knelpunten die niet alleen door belangenorganisaties buiten het UMCG maar ook door de verschillende experts binnen het ziekenhuis werden voorzien. Door dit uitstel kan er uitvoerig gekeken worden naar de problemen rondom het faciliteren en implementeren van de veranderingen die dit wetsvoorstel met zich mee zullen brengen.

Op dit moment is er een grote afstand tussen de huidige situatie en de gewenste eindsituatie. In het onderzoek komt duidelijk naar voren dat de onderzochte systemen soms niet voldoen aan bestaande wetgeving. Een belangrijke rol is hierbij weggelegd voor de informatiebeveiligingsorganisatie, die momenteel nog niet effectief genoeg is. Zij zal in effectiviteit moeten toenemen als het in de toekomst beter in staat wil zijn om structurele wettelijke strijdigheden in elektronische uitwisselingssystemen te detecteren en te verhelpen. Omdat het wetsvoorstel een uitbreiding is op een bestaand fundament van wetgeving, is het belangrijk om het belang van de bestaande regelgeving rondom dit onderwerp niet te onderschatten. Het UMCG moet niet verwachten dat nieuwe wetgeving succesvol geïmplementeerd zal worden als bestaande wetgeving in veel systemen nog niet goed wordt nageleefd. Ondanks dat dit onderzoek zich slechts heeft gebogen over drie van de vele elektronische uitwisselingssystemen die het UMCG in gebruik heeft, is het zeer waarschijnlijk dat vergelijkbare problemen ook in andere uitwisselingssystemen te vinden zullen zijn. Op de algemene werkwijze van de informatiebeveiligingsorganisatie valt in theorie weinig tot niets aan te merken. Toch blijft het zorgelijk dat de informatiebeveiliging in de praktijk niet altijd in staat is om uitwisselingssystemen compliant te krijgen met huidige wetgeving. Hier zal meer aandacht, geld en tijd in moeten worden geïnvesteerd wil het in de toekomst mogelijk zijn om het nieuwe wetsvoorstel, of elk andere wettelijke bepaling op dit gebied, succesvol te implementeren.

Uit het onderzoek blijkt dat de werking van Palga en Zorgmail niet met kleine aanpassingen zo kunnen worden veranderd dat deze systemen in staat zijn om aan het nieuwe wetsvoorstel te voldoen. Daarnaast is het onwenselijk om bij elk bestaand uitwisselingssysteem aparte functies in te bouwen. Op dit onderdeel is er een duidelijk verschil tussen enerzijds XDS en anderzijds Palga en Zorgmail. XDS zou met verschillende aanpassingen in de toekomst wellicht in staat kunnen zijn andere uitwisselingssystemen compliant te maken met het nieuwe wetsvoorstel. XDS is immers een standaard die verschillende informatiebronnen met elkaar verbindt. In XDS zitten veel softwarematige aanknopingspunten met het nieuwe wetsvoorstel. Zou XDS zodanig worden aangepast dat het compliant is met het nieuwe wetsvoorstel, dan zou via XDS een groot aantal systemen compliant kunnen maken door deze systemen simpelweg om te bouwen tot een XDS source. Nader onderzoek zou eventueel uit moeten wijzen welke aanpassingen XDS precies zal moeten ondergaan, hoeveel systemen binnen het UMCG om te zetten zijn naar een XDS source, en hoe omvangrijk dit omzetten zou zijn.

10.3 Aanbevelingen

Het UMCG wordt aanbevolen om met het oog op de uiteindelijke inwerkingtreding van het aanhangige wetsvoorstel een aantal zaken te veranderen. De aanbevelingen luiden als volgt:

1. Om te zorgen dat bestaande uitwisselingsystemen compliant zijn met bestaande wet- en regelgeving is het van belang om te inventariseren op welke wijze de huidige uitwisselingssystemen binnen het UMCG werken en of in die werking aan alle eisen uit de wet wordt voldaan. Dit kan gedaan worden door de informatiebeveiligingsorganisatie,

maar dan zal haar capaciteit in verdere mate moeten toenemen, nu is gebleken dat het in haar huidige vorm niet in staat is alle wettelijke strijdigheden te constateren en te verhelpen.

2. Het UMCG zou de wettelijke eisen uit de Wbp en de WGBO een meer uitgesproken en centrale plek moeten geven in haar controleproces op alle uitwisselingssystemen binnen haar organisatie.

3. Voor het UMCG is het van belang om in direct contact te staan met beroep- en cliëntenorganisaties uit de zorgsector om op die manier de ontwikkelingen rondom het implementatieplan van het nieuwe wetsvoorstel bij te houden en tijdig op te kunnen volgen om zo tot een succesvolle implementatie van het nieuwe wetsvoorstel te komen.

4. Het UMCG zou moeten onderzoeken wat de potentie van XDS is met betrekking tot haar capaciteit om in de toekomst een standaard te zijn die verschillende systemen in haar werkwijze opneemt en mogelijk andere uitwisselingssystemen overbodig maakt. Dit onderzoek zou ook moeten kijken naar de hoeveelheid systemen die voor deze werkwijze in aanmerking zouden komen.

5. Het UMCG zou gelet op zowel bestaande als nieuwe wetgeving moeten kijken naar een centraal moment waarop patiënten geïnformeerde toestemming kunnen geven voor het verwerken van persoonsgegevens via elektronische uitwisselingssystemen. Hiermee voorkomt het UMCG een wildgroei aan eventuele toestemmingsmomenten of het nadrukkelijk ontbreken van een toestemmingsmoment. Het creëren van een centraal moment waarop toestemming wordt gegeven heeft als voordeel dat zodra de wettelijke eis van gespecifieerde toestemming inwerking treed, dit dan eenvoudig in de ontstane werkwijze geïncorporeerd kan worden.

6. Het UMCG zou binnen de zorgsector moeten kijken welke zorgaanbieders reeds beschikken over een patiëntportaal dat elektronisch inzage verschaft en in hoeverre dit al is afgestemd op de eisen uit het toekomstige wetsvoorstel. Hiermee kunnen toekomstige ontwikkelingen worden versnelt en kan er lering getrokken worden uit de reeds opgedane ervaringen van andere zorginstellingen.

7. Het UMCG zou de ontwikkeling van baselines binnen de organisatie in verdere mate moeten stimuleren. Deze baselines geven afdelingen de mogelijkheid om nieuwe systemen succesvol te implementeren of te toetsen, en bieden in het algemeen een zeker handvat op basis waarvan gewerkt kan worden.

8. Veel van de professionals die met de uitwisselingssystemen werken kennen de mankementen in de verschillende systemen maar lijken zich soms niet te realiseren welke wettelijke impact dit heeft, of onderschatten het belang van wettelijke compliance ten opzichte van de praktische werkbaarheid van het systeem. Het UMCG zou meer moeten doen om te bewustwording onder medewerkers hierin te vergroten zodat strijdigheden in systemen eerder worden gemeld, geconstateerd en aangepakt. Apart onderzoek zou uit kunnen wijzen welke aanpak hiervoor het meest effectief is.

Bronnenlijst

Literatuur

Brief CBP relatie verantwoordelijke en bewerker, 14 mei 2002.

Brief reactie wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens, 13 februari 2015.

CBP richtsnoeren beveiliging van persoonsgegevens, Den Haag, 2013.

J.P. de Jong, 'De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp', *Regelmaat* 2015, afl 1 p. 6-18.

Kamerbrief wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens, 8 maart 2016.

H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming per-soonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

H.J.J. Leenen e.a., *Handboek gezondheidsrecht Deel I: Rechten van mensen in de gezondheidszorg,* Hoofddorp: Boom Juridische uitgevers 2011.

M.C. Ploem, 'Elektronische gegevensuitwisseling in de zorg: zit de wetgever op het goede spoor?', *Tijdschrift voor Gezondheidsrecht* 2015, afl 5 p. 300-312.

Privacy enhancing technologies, Witboek voor beslissers, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag, december 2004.

G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom juridische uitgevers, 2011.

P. Verschuren & H. Doorewaard, *Het ontwerpen van een onderzoek*, Den Haag: Boom Lemma Uitgevers 2007.

Wetgeving

Boek 7 Burgerlijk Wetboek
Privacyrichtlijn 95/46/EG
Wet op de Beroep in de Individuele Gezondheidszorg
Wetboek van Strafrecht
Wetboek van Strafvordering
Wet Publieke Gezondheid
Wet bescherming persoonsgegevens

NEN-normen

NEN-ISO / IEC 27002:2013 nl
NEN 7510:2011 nl, NEN 7512:2015 nl, NEN 7513:2010 nl

Kamerstukken

Kamerstukken II 1997/1998, 25892, nr. 3
Kamerstukken II 1997/1998, 25982, nr. 9
Kamerstukken II 1997/1998, 25982, nr. 11
Kamerstukken II 1997/1998, 25982, nr. 13
Kamerstukken II, 1997/98, 25892, nr. 92c
Kamerstukken II, 1999-2000, 25892, nr. 22
Handelingen I 2010/11, 20, nr. 2
Handelingen I 2010/11, 20, nr. 7
Handelingen I 2010/11, 20, nr. 22
Kamerstukken II 2012/13, 33 509, nr. 3
Kamerstukken I, 2015/16, 33509, nr. J

Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens

Jurisprudentie
Hoge Raad 23 november 2001, Nr. C99/259HR
Rechtbank Midden-Nederland 23 juli 2014, *LJN*C/16/340505 / HA ZA 13-205

Literatuur- en jurisprudentielijst

Geraadpleegde literatuur

Brief CBP
Brief CBP relatie verantwoordelijke en bewerker, 14 mei 2002.

Brief reactie wetsvoorstel
Brief reactie wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens, 13 februari 2015.

CBP richtsnoeren
CBP richtsnoeren beveiliging van persoonsgegevens, Den Haag, 2013.

De Jong
J.P. de Jong, 'De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp', *Regelmaat* 2015, afl 1 p. 6-18.

Kamerbrief
kamerbrief wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens, 8 maart 2016.

Kranenborg & Verhey
H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

Leenen
H.J.J. Leenen e.a., *Handboek gezondheidsrecht Deel I: Rechten van mensen in de gezondheidszorg,* Hoofddorp: Boom Juridische uitgevers 2011.

Ploem
M.C. Ploem, 'Elektronische gegevensuitwisseling in de zorg: zit de wetgever op het goede spoor?', *Tijdschrift voor Gezondheidsrecht* 2015, afl 5 p. 300-312.

Privacy enhancing technologies
Privacy enhancing technologies, Witboek voor beslissers, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag, december 2004.

Van Schaaijk
G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom juridische uitgevers, 2011.

Verschuren & Doorewaard
P. Verschuren & H. Doorewaard, *Het ontwerpen van een onderzoek*, Den Haag: Boom Lemma Uitgevers 2007.

Jurisprudentie

23 november 2001
Hoge Raad 23 november 2001, Nr. C99/259HR

23 juli 2014
Rechtbank Midden-Nederland 23 juli 2014, *LJN* C/16/340505 / HA ZA 13-205

Bijlage 1

Interview
(Lijst met belangrijke begrippen in bijlage 1)

Inleiding:
Doel van het gesprek is inventariseren van de huidige situatie, het systeem leren begrijpen.

Begin
- Zou u kunnen toelichten wat de functie is van het systeem en hoe het werkt? (uitgebreid)

Vragen op basis van HS 2 (Wbp)
- Welke (categorieën) persoonsgegevens worden in dit systeem verwerkt?
- Met welke andere zorgverleners worden gegevens opgevraagd of uitgewisseld via dit systeem?
- Wat gebeurt er in het systeem met de persoonsgegevens?

Vragen op basis van HS 3 (Beveiliging)
(Lijst met beveiligingsmaatregelen: bijlage 2)
- Hoe wordt het systeem/de persoonsgegevens beveiligd, en waarom is er voor deze beveiliging gekozen?
- In hoeverre heeft de aanwezigheid van persoonsgegevens invloed op hoe die beveiliging van het systeem er uit ziet? (is er daardoor bijv. sprake van meer of minder beveiliging? Andere soort beveiliging?)
- Hoe wordt er beoordeeld dat de beveilgiging goed genoeg is? Wanneer gebeurt dit?
- Is er sprake van een cyclus waarin de beveiliging geëvalueerd wordt?
- Zo ja, hoe ziet die cyclus eruit?
- Gebruikt men NEN-normen/CBP richtlijnen, spelen deze een rol bij de beveiliging van de persoonsgegevens?

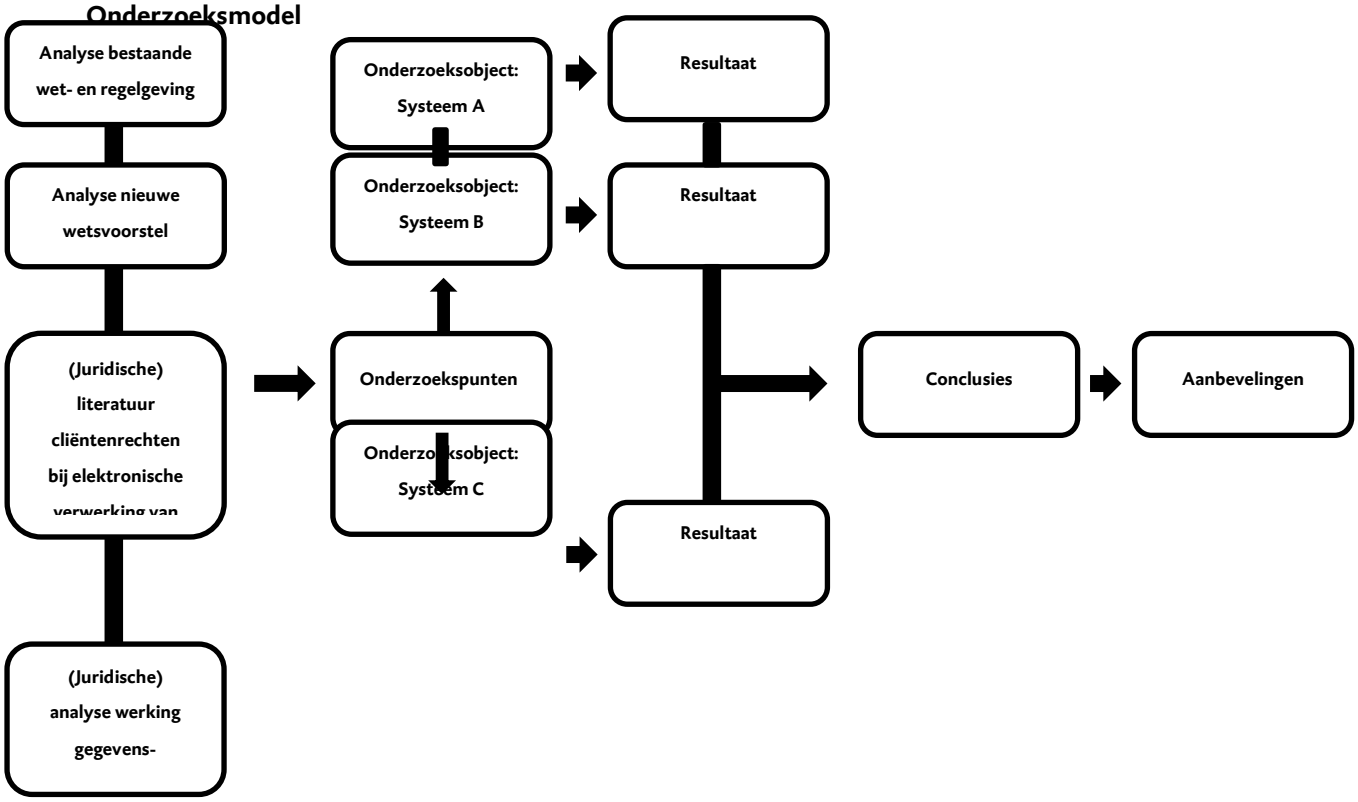
Vragen op basis van HS 4 (Medische behandelrelatie)
- Hoe wordt de behandelrelatie geborgd? (Dus dat men alleen toegang heeft tot die patiënten waarmee een behandelrelatie is.)

Vragen op basis van HS 5 (Nieuwe wetsvoorstel)
- Geeft een persoon/patient op dit moment toestemming voordat zijn gegevens worden opgenomen in/via dit systeem?
- Zo ja, hoe gebeurt dit dan?
- Bestaat er in het systeem de mogelijkheid om iemands persoonsgegevens of een deel van iemands persoonsgegevens af te schermen voor bepaalde zorgverleners (of een hele categorie zorgverleners)?
- Zo niet, is het mogelijk om het systeem zo aan te passen dat dit wel kan?
- Bestaat er in het systeem de mogelijkheid om voor een zorgverlener het inzien van gegevens (het opvragen van gegevens) te blokkeren tot dat de zorgverlener toestemming van de patient heeft gekregen om ze in te zien?
- Zo niet, is het mogelijk om het systeem zo aan te passen dat dit wel kan?
- Is het op dit moment mogelijk voor een patient om in te zien wie zijn persoonsgegevens bekijkt?
- Zou het huidige systeem in staat zijn loggegevens bij te houden als dat nodig zou zijn? (dus welke zorgverlener wat en wanneer op heeft gevraagd/in heeft gezien)

Overige vragen
- Hoe moelijk/makkelijk zou het naar uw mening zijn om een systeem te ontwikkelen waarin een patiënt op elektronische wijze inzage kan krijgen in zijn medisch dossier. In dat systeem zou ook te zien moeten zijn wie die gegevens in heeft gezien en wanneer dat is gebeurt.

Bijlage 2

Onderzoeksmodel



© 2015 Studentenbureau UMCG Publicaties Groningen, Nederland.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande toestemming van de uitgever.
© 2015 Studentenbureau UMCG Publicaties Groningen, Nederland.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j° het Besluit van 20 juni 1974, St.b. 351, zoals gewijzigd in Besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht. Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

Trefw elektronische gegevensuitwisseling, wetsvoorstel, cliëntenrechten elektronische verwerking

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j° het Besluit van 20 juni 1974, St.b. 351, zoals gewijzigd in Besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht. Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

Trefw Zelf bedenken en invullen; zie auteursinstructie

Typ hier de hoofdtitel

Typ hier de ondertitel

Groningen, Klik hier en kies maand en jaar

Auteur	Voornaam en achternaam
Studentnummer	Typ je studentnummer
Afstudeerscriptie in het kader van	Faculteit/instituut Naam studie Naam onderwijsinstelling
Opdrachtgever	Voorletter, titel en naam Naam afdeling, UMCG
Begeleider onderwijsinstelling	Voorletter, titel en naam Faculteit/instituut Opleidingsinstelling
Begeleider UMCG	Voorletter, titel en naam Naam afdeling, UMCG

deze pagina leeg laten

Vanaf deze pagina de eigen A4 scriptie invoegen!!!
De scriptie wordt dubbelzijdig gedrukt!!!

De volgorde van de pagina;s is dan als volg:

1. A4 voorkant met de vlakverdeling
2. Auteursrechtenpagina
3. Titelpagina
4. Lege pagina
5. Start van de van je eigen scriptie (inhoud, dus zonder eigen voorkant en/of titelpagina van de opleiding – die laatste bevat vaak privacygevoelige informatie van de student of begeleider van de opleiding zoals mailadres en soms zelf telefoonnummer)