

Implementatie van AVG op retrospectief wetenschappelijk onderzoek in het Reinier de Graaf Gasthuis

[Afstudeerscriptie Bachelor - Mens en Techniek | Bewegingstechnologie]

Fransie Schuurman
DE HAAGSE HOGESCHOOL

Implementatie van AVG op retrospectief wetenschappelijk onderzoek in het Reinier de Graaf Gasthuis

Auteur

Pieterella Fransie Schuurman

Student nummer

14097842

Studie & school

Mens en Techniek | Bewegingstechnologie – De Haagse Hogeschool

Beroepsrol

Management | Kwaliteit en risico

Functie

Afstudeer stagiair bij het Reinier de Graaf Gasthuis, orthopedie afdeling

Extern project

Ja

Bedrijf en afdeling

Reinier de Graaf Gasthuis, orthopedie afdeling

Opdrachtgever

Nina Mathijssen | onderzoekcoördinator Reinier de Graaf Gasthuis

Periode

5 maart 2018 – 13 juni 2018

Docent begeleider

1st Begeleider – De Haagse Hogeschool: Karen L. van Stein Callenfels
Email: k.l.vanstein-callenfels@hhs.nl

2^{de} Begeleider – De Haagse Hogeschool: Willem N. Looije
Email: w.n.looije@hhs.nl

Externe Begeleider – RdGG: Nina M.C. Mathijssen
Email: N.Mathijssen@rdgg.nl

Email auteur

fransie_94@hotmail.com

Voorwoord

Afgelopen vier jaar heb ik (Fransie Schuurman) Bewegingstechnologie (BT) gestudeerd aan de Haagse Hogeschool te Den Haag. Dé studie die de brug slaat tussen mens en techniek. Deze scriptie vormt de laatste fase naar mijn Bachelor. Door de jaren heen heb ik ervaren dat management de kant is die mijn interesse wekt. Zo heb ik een minor gedaan (projectmanagement) om mijn managementkennis uit te breiden, wat resulteerde in een PRINCE 2 certificaat. Door projecten binnen BT en de minor heb ik mijn zinnen gezet op een management afstudeeropdracht. Een combinatie die nog niet is voorgekomen binnen Bewegingstechnologie. Ik neem het voortouw in het slaan van de brug tussen Management en Mens & Techniek in plaats van alleen Mens & Techniek. Samen met mijn begeleider Karen van Stein Callenfels, ben ik bezig geweest om een passende opdracht te vinden om deze brug te bewerkstelligen. Zo ben ik terecht gekomen bij de Orthopedische afdeling van het Reinier de Graaf Gasthuis (RdGG).

De orthopedische afdeling van het RdGG is in mei 2017 ISO 9001 gecertificeerd. In het kort: 'NEN-EN-ISO-9001:2015 is een internationaal kwaliteitsmanagementsysteem, waarin de eisen van de klanten, de wet- en regelgeving en het bedrijf centraal staat. De ISO 9001 hanteert procesmatig werken door middel van risico gebaseerd denken en de Plan – Do – check – Act – cyclus. Elk jaar moet het RdGG opnieuw ge-audit worden, om het certificaat te behouden. Zo ook is het RdGG in mei 2018 door KIWA ge-audit. Aan mij is in januari 2018 gevraagd om, in het kader van mijn management afstudeerproject, inzichtelijk te maken of het RdGG voldoet aan de eisen en normen van de ISO 9001.

Enmaal aangekomen in het RdGG werd duidelijk dat de ISO 9001 veel omvat en dat de opdracht afgebakend dient te worden. Zo vallen bijvoorbeeld eisen van de patiënt, eisen van het RdGG en Wet- en Regelgeving binnen de ISO 9001 kaders. Ik heb bewust gekozen voor wet- en regelgeving, juist omdat in deze periode cruciale wijzigingen in de Wetgeving moeten worden ingevoerd en omdat de afbakening van mijn afstuderen daarmee scherp geformuleerd is. Het voldoen aan Wet- en regelgeving is onder andere een van de belangrijkste eisen in de ISO 9001 norm. Met de komst van de nieuwe Europese wet: Algemene Verordening Gegevensbescherming (AVG), is het noodzakelijk om te kijken hoe deze Verordening geïmplementeerd kan worden in het RdGG. Zo kwam mijn doel naar voren: Inzichtelijk maken hoe het RdGG de AVG kan implementeren.

Deze opdracht heeft mij veel nieuwe kennis gegeven over het uitvoeren van een stakeholderanalyse, risicomanagement en wet- en regelgeving. Daarnaast heeft deze opdracht ook veel zelfkennis en persoonlijke ontwikkelingen teweeggebracht. Graag wil ik vier persoonlijke eigenschappen aan het licht brengen in dit voorwoord:

- Mijn doorzettingsvermogen en wilskracht om groenlicht te krijgen voor deze opdracht bij de Haagse Hogeschool en het Reinier de Graaf Gasthuis. Het is spannend om ergens de eerste in te zijn, het kan namelijk twee kanten opgaan. Ondanks dat deze combinatie van Mens & Techniek en management nieuw was voor bewegingstechnologie en hierdoor een groot risico met zich mee brengt, heb ik mijn best gedaan om een management opdracht te krijgen. Dit zie ik als een sterk punt van mij als persoon.
- Daarnaast kwam een valkuil naar boven: onzekerheid. Deze onzekerheid was voornamelijk gericht op mijn kennis en kunnen en dat anderen je hierom zullen veroordelen. Dit zorgde ervoor dat ik iedereens mening en ideeën toe probeerde te passen op mijn project, wat

resulteert in een onsamenhangende methode en resultaat. Maar belangrijker is wat ik hiervan heb geleerd. Karen heeft mij laten inzien dat ik mag vertrouwen op mijn eigen kennis en dat ik me niet moet laten afwijken van mijn oorspronkelijke plan. Desalniettemin is hier een grote slag te slaan, maar door dit project is deze valkuil voor mij inzichtelijk geworden.

- Communicatieve vaardigheden en logisch denken zijn mijn sterke pluspunten. Als ik iets begrijp, dan kan ik dit verbaal goed overbrengen. Ik vertel enthousiast en ook beargumenteer ik waarom ik iets vind. In vergaderingen en presentaties komen mijn vaardigheden goed van pas.
- Als laatste mag ik mijn schriftelijke uitdrukkingsvaardigheden nog flink verder ontwikkelen. Ik heb allerlei ideeën in mijn hoofd en wanneer ik deze moet presenteren komt dit goed over, maar wanneer ik deze moet rapporteren zorgt dit voor kwaliteitsvermindering. Dit is een vaardigheidstekort dat in mijn afstudeerperiode constant naar voren komt en veel stress met zich mee heeft gebracht. Toch ben ik ervan overtuigd dat ik mij met elk project weer een beetje zal verbeteren.

Kortom: het eindresultaat dat hier voor u ligt is bereikt met vele omwegen. Als deze omwegen er niet waren geweest dan was dit project waarschijnlijk meer gestructureerd uitgevoerd. Maar met meer omwegen komen er ook meer overwegingen te pas wat resulteert in weloverwogen beslissingen. Ik ben van mening dat het niet erg is om niet in een rechte lijn naar het eindresultaat te gaan, dat omwegen juist voordelen hebben. Met als kanttekening dat wel grenzen getrokken moeten worden om weer terug op de juiste koers te raken.

Graag dank ik in het speciaal Karen van Stein Callenfels bij het helpen met mijn proces van begin tot eind en bij mijn persoonlijke ontwikkelingen. Ook dank ik graag Nina Mathijssen in het speciaal, voor het mogelijk maken van deze management afstudeeropdracht en het actief betrekken in het Reinier de Graaf Gasthuis. Daarnaast dank ik Willem Looije voor zijn hulp om dit project naar een hoger niveau te brengen.

Ook ben ik Brechtje Hesselink en Dominique van Woensel dankbaar voor hun bijdrage bij het maken van de risico-inventarisatie en natuurlijk alle overige stakeholders.

Ik wens u veel leesplezier

Inhoudsopgave

Verklarende woordenlijst + afkortingen.....	6
Samenvatting.....	7
1. Inleiding	8
2. Hanteren van ISO 9001 norm	10
2.1 Wet en regelgeving.....	10
2.1.1 Is AVG van toepassing op wetenschappelijk onderzoek?.....	10
2.1.2 AVG-informatie	11
Grondslagen	11
AVG privacy rechten	12
2.1.3 Conclusie	15
2.2 Contextanalyse	15
2.2.1 Stakeholderanalyse.....	15
Stap 1 - Analyseren procedures RdGG	16
Stap 2 - Participeren vergaderingen	17
Stap 3 - Contact met elke stakeholder	18
Stakeholder kwalificering	18
2.2.2 Systemenanalyse.....	19
2.3. Risicomanagement	20
3. Risico-inventarisatie met RISMAN methode	21
3.1 Vaststellen doel	21
3.2 In kaart brengen risico's	21
3.3 Vaststellen belangrijke risico's	22
3.4 In kaart brengen beheersmaatregelen	23
3.5 Vaststellen beheersmaatregel + implementatie advies	24
3.5.1 Ongewenste topgebeurtenis 1	24
Risico 1	24
Advies 1	24
Advies 2	24
Advies 3	25
Advies 4	25
Uitien advies 5.....	25
3.5.2 Ongewenste topgebeurtenis 2	25
Risico 2	25
Advies 6	26
Advies 7	26
Risico 3	26
Advies 8	26
Advies 9	26
Risico 4	26
Advies 10	27

Verklarende woordenlijst + afkortingen

AP: autoriteit persoonsgegevens. AP houdt toezicht op de naleving van de AVG. De Autoriteit onderzoekt het gebruik van persoonsgegevens binnen bedrijven en overheidsorganisaties. AP legt boetes op bij overtredingen.

AVG: Algemene verordening gegevensbescherming, de nieuwe privacywet waarover dit advies rapport gaat.

BW: Burgerlijk wetboek. Hier staan de wetten van burgers beschreven.

EPD: Elektronisch patiëntendossier, wat gebruikt wordt in ziekenhuizen. Onder andere in het RdGG.

FG: Functionaris gegevensbescherming, een aangestelde functionaris door het RdGG die gespecialiseerd is in de AVG.

GCP'er: Een persoon die in bezit is van een Good Clinical Practice certificaat, dit is verplicht om hoofdonderzoeker te zijn.

ISO 9001: afkorting van NEN-EN-ISO 9001: 2015, een kwaliteitsmanagementsysteem waar het RdGG voor gecertificeerd is.

METC: Medisch ethisch toetsing commissie, die betrokken moet worden bij elk medisch wetenschappelijk onderzoek.

PDCA –cyclus: Plan Do Check Act – cyclus, Een feedbackcirkel die gebruikt wordt in de ISO 9001 norm.

Persoonsgegevens: Alle informatie over een identificeerbaar persoon. Identificeerbaar wordt gezien als een natuurlijk persoon die direct of indirect kan worden geïdentificeerd.

PIF: Proefpersoon informatie formulier, moet worden ondertekend om toestemming te krijgen van een proefpersoon.

RdGG: Reinier de Graaf Gasthuis, het ziekenhuis waarvoor dit adviesrapport is opgesteld.

STZ: Samenwerkende topklinische opleidingsziekenhuizen, RdGG is een van deze ziekenhuizen. En dient te voldoen aan het beleid wat geschreven is door het STZ.

Advies 11	27
Advies 12	27
Risico 5	27
Advies 13	27

4. Evaluatie	28
5. Discussie.....	28
6. Conclusie	29
Bronnen	30
Bijlage – RISMAN methode.....	31
Bijlage projectvoorstel.....	34
Bijlage – Reflectie Leerdoelen	40

Samenvatting

25 mei 2018 is de Europese Algemene Verordening Gegevensbescherming (AVG) in werking getreden.

De wetenschapsgroep van de orthopedische afdeling in het Reinier de Graaf wil voorkomen dat de implementatie van de AVG onverwachte (catastrofale) situaties met zich meebrengt. Dit vormt het volgende doel van deze afstudeerscriptie:

De orthopedie afdeling in het Reinier de Graaf Gasthuis (RdGG) wil advies over de interpretatie en implementatie van de AVG om de volgende twee ongewenste topgebeurtenissen te voorkomen:

- Het RdGG ontvangt een boete, door het niet voldoen aan de AVG
- Wetenschappelijk onderzoek kan niet worden uitgevoerd, met de komst van de AVG

Dit doel is bereikt door middel van de richtlijnen van de NEN-EN-ISO 9001:2015 (ISO 9001) te volgen. Bij de ISO 9001 staat risico gebaseerd denken centraal, daarom wordt er gebruik gemaakt van risicomanagement. Echter staat er geen aanbevolen methodiek voor risicomanagement. Voor deze scriptie is er bewust gekozen voor de RISMAN-methode.

De volgende vijf risico's en beheersmaatregelen kwamen voort uit de risicoanalyse, de risico's zijn weergegeven van boven naar beneden in mate van prioritering:

	Kans	Gevolg	Totaal	Beheersmaatregel
Risico 1. Iemand die onbevoegd patiëntgegevens inziet en verwerkt.	5	4	20	Vermijden/reducen
Risico 2. De patiënt geeft geen actief toestemming om zijn persoonsgegevens te verwerken voor wetenschappelijk onderzoek.	3	4	12	reducen
Risico 3. Patiënt doet beroep op zijn recht van bezwaar.	3	4	12	accepteren
Risico 4. Patiënt doet beroep op zijn vergoelheidsrecht	2	2	4	accepteren
Risico 5. De AVG wordt gezien als een te grote barrière, waardoor niemand meer iets durft te doen met persoonsgegevens.	1	4	4	

De orthopedische afdeling is al goed op weg met het implementeren van de AVG. Mede door het kwaliteitsmanagementsysteem, die zorgt voor procesbeschrijvingen, evaluatie en aanpassingen. De contextanalyse fungeerde als goede basis om de risicoanalyse op uit te voeren. Ook gaf dit inzicht in welke processen het RdGG al bezit en welke van deze processen ingezet kan worden om risico's te beheersen.

De orthopedische afdeling heeft veel oplossingen al in huis. Het advies is om op sommige processen wat meer nadruk te leggen, zoals het delegation log, actief toestemming ragen en de SMART formulering van de onevenredige veel inspanning.

1. Inleiding

"HagaZiekenhuis waarschuwt 85 medewerkers na inzien dossier Barbie" Security 26 april 2018 ^[1]
"bedrijven in paniek over Europese Privacy wet" Het financieel dagblad (14 augustus 2017) ^[2],
"wetswijziging in 2018: privacy is hot topic" RTL nieuws (8 feb 2018) ^[3], "duizenden sportclubs niet klaar voor nieuwe privacywet" AD (3 april 2018) ^[4], "Veel bedrijven niet klaar voor nieuwe privacywet" NRC. (3 april 2018) ^[5]

Type de woorden 'AVG' en 'nieuwsartikelen' in op de browser en in 0,38 seconde zijn er 16.400 links te vinden naar artikelen over de AVG die recent zijn geschreven. Een actueel en veel besproken onderwerp, maar wat houdt het precies in en wat gaat er veranderen voor wetenschappelijk onderzoek in ziekenhuizen?

25 mei 2016 is de Algemene verordening gegevensbescherming (AVG) in werking getreden. Dit betekent dat alle decentrale overheden in de Europese Unie tot 25 mei 2018 de tijd hadden om aan de regels uit de AVG te voldoen. Wanneer een bedrijf de wet overtreedt riskeert deze een maximale boete van 20 miljoen euro of 4% van de jaarlijkse omzet. De AVG is de opvolger van de wet bescherming persoonsgegevens, deze is komen te vervallen op 25 mei 2018.

Bedrijven in heel de Europese Unie zijn de afgelopen maanden hard bezig geweest om zich AVG klaar te maken. Onder deze bedrijven valt ook het Reinier de Graaf Gasthuis (RdGG), een ziekenhuis te Delft. Het RdGG heeft een functionaris gegevensbescherming (FG) aangenomen om voor heel het ziekenhuis een beleid te schrijven omtrent de AVG. Een ziekenhuis bestaat echter uit verschillende disciplines, waardoor het beleid specifiek is voor elke discipline afzonderlijk. De wetenschapsgroep voorziet het probleem dat de implementatie van de AVG onverwachte (catastrofale) situaties met zich meebrengt. Dit vormt het volgende doel van deze afstudeerscriptie:

De orthopedie afdeling in het Reinier de Graaf Gasthuis (RdGG) wil advies over de interpretatie en implementatie van de AVG om de volgende twee ongewenste topgebeurtenissen te voorkomen:

- Het Reinier de Graaf ontvangt een boete, door het niet voldoen aan de AVG
- Wetenschappelijk onderzoek kan niet worden uitgevoerd, met de komst van de AVG

Scope:

Omdat de AVG een groot onderwerp is, wordt deze scriptie afgebakend op de grondslagen en de privacy rechten. Daarnaast wordt er gekeken naar alleen retrospectief wetenschappelijk onderzoek, omdat bij deze vorm van wetenschappelijk onderzoek gebruik wordt gemaakt van recht van bezwaar in plaats van actief toestemming vragen. Dit vormt een groot risico voor de AVG, in deze scriptie zal duidelijk worden waarom.

Vormgeving:

Om dit doel te bereiken wordt er allereerst nagegaan wat er verwacht wordt van dit afstudeerproject.

De Haagse Hogeschool heeft afstudeercriteria waaraan een Bachelor scriptie moet voldoen en het RdGG heeft de eis dat er een advies wordt gegeven. Zo is er gekozen om dit project op te splitsen in twee vormen:

1. De afstudeerscriptie, geschreven voor De Haagse Hogeschool en het RdGG waarbij het doorlopen proces duidelijk naar voren komt en alles gedetailleerder wordt beschreven. Hierin komen de eisen van zowel De Haagse Hogeschool als het RdGG tot zijn recht;

2. Een samenvattend filmpje, waarin de context, risico's en adviezen samenvattend naar voorkomen. Dit kan gezien worden als product wat gemaakt is voor het RdGG.

In deze twee producten zullen beheersmaatregelen met bijbehorend implementatie advies benoemd worden, om zo de ongewenste topgebeurtenissen te voorkomen.

Plan van aanpak:

De orthopedische afdeling werkt met de richtlijn van de NEN-EN-ISO 9001 (Hierna te noemen ISO 9001) om de kwaliteit te beheersen, deze wordt dan ook toegepast in dit project. In dit kwaliteitssysteem staat risico gebaseerd denken centraal. Daarom is er gekozen om een risico-inventarisatie en risicoanalyse uit te voeren om tot een passend advies te komen.

De volgende stappen zijn ondernomen:

- Stroomdiagram van de AVG is invullen, om te kijken of de AVG van toepassing is op retrospectief wetenschappelijk onderzoek
- Vervolgens worden de grondslagen en de privacy-rechten van de AVG vermeld
- Daarna wordt er een contextanalyse uitgevoerd op retrospectief wetenschappelijk onderzoek met daarin de volgende onderwerpen:
 - o De stappen die genomen worden bij retrospectief onderzoek
 - o De stakeholder die bij deze stappen komen kijken
 - o De systemen die bij deze stappen gebruikt worden
- Na de contextanalyse wordt de risicomethodenmethode RISMAN toegepast met daarin:
 - o Vaststellen doel
 - o In kaart brengen risico's
 - o Vaststellen belangrijke risico's
 - o In kaart brengen beheersmaatregelen
 - o Vaststellen beheersmaatregel + implementatie advies
- Deze adviezen worden gepresenteerd in het RdGG.

2. Hanteren van ISO 9001 norm

Zoals vermeld in de inleiding hanteert het RdGG de ISO 9001. ISO 9001 is een kwaliteitsmanagementsysteem met als doel om kwaliteit te waarborgen. Dit project zal ook de richtlijnen die betrekking hebben op dit afstudeerproject gebruiken om stapsgewijs tot een advies te komen. De ISO 9001 richtlijnen die betrekking hebben op dit afstudeerproject worden geciteerd en toegepast in dit hoofdstuk. De drie richtlijnen zijn:

1. Wet- en regelgeving
2. Contextanalyse
3. Risicomanagement

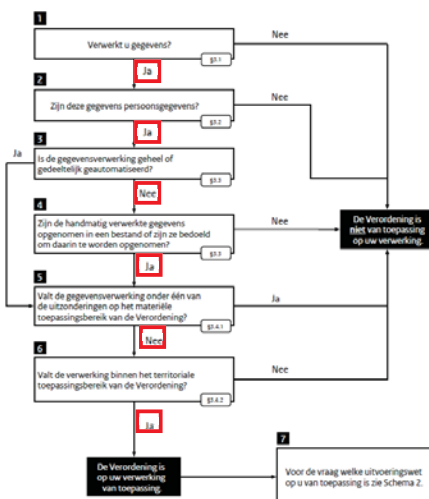
2.1 Wet en regelgeving

Een citaat uit NEN-EN-ISO 9001:2015, blz. 13 ^[11] "Deze internationale norm specificeert eisen voor een kwaliteitsmanagementsysteem van een organisatie die moet aantonen dat zij in staat is om consequent producten en diensten te leveren die voldoen aan de eisen van de klant en aan de van toepassing zijnde wet- en regelgeving."

Of terwijl, het RdGG moet aan kunnen tonen te voldoen aan de van toepassing zijnde wet- en regelgeving. Allereerst wordt gekeken of de Algemene Verordening Gegevensbescherming van toepassing is op wetenschappelijk onderzoek in het RdGG aan de hand van een stroomschema die afkomstig is van Autoriteit Persoonsgegevens (AP) ^[12].

2.1.1 Is AVG van toepassing op wetenschappelijk onderzoek?

Figuur 2 geeft het stroomdiagram weer, toegepast op wetenschappelijk onderzoek binnen het RdGG. In het stroomdiagram staan begrippen die veel gebruikt worden met betrekking tot de AVG en de definities van belangrijke begrippen staan beschreven in de begrippenlijst.



Figuur 1: stroomschema AVG. Bron: Autoriteit persoonsgegevens, oktober 2017 ^[12]

2.1.2 AVG-informatie

25 mei 2018 is de Algemene Verordening Gegevensbescherming rechtstreeks van toepassing in alle lidstaten van de Europese Unie. Het doel van de AVG is om de bescherming van personen te waarborgen in verband met het verwerken van persoonsgegevens en het vrije verkeer van persoonsgegevens te waarborgen binnen de EU. (Autoriteit persoonsgegevens, oktober 2017 ^[13])

Grondslagen

Volgens de AVG is het rechtmatig om persoonsgegevens te verwerken als er voldaan wordt aan één van de volgende AVG-grondslagen:

1. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst
2. De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijk verplichting
3. De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen

- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Alleen grondslag 1 is bij wetenschappelijk onderzoek van toepassing. Dit betekent dat er voor verwerking van wetenschappelijk onderzoek altijd toestemming nodig is van de betrokkenen zelf.

Als er vervolgens een grondslag van toepassing is en persoonsgegevens worden verwerkt. Wat zijn dan de rechten van de betrokkene?

AVG privacy rechten

De komst van de AVG versterkt de positie van de betrokkene. De betrokkene heeft zeven privacy rechten, waarvan twee nieuwe en de overige vijf bestaande rechten zijn sterker worden.

Het recht om gegevens over te dragen - artikel 20 AVG ^[6] (nieuw):

De proefpersoon moet, wanneer hij hier omvraagt, zijn persoonsgegevens ontvangen. (Autoriteit persoonsgegevens, oktober 2017^[7]). Het bedrijf (RdGG) moet dit in de vorm doen dat het voor de betrokkenen makkelijk maakt om hun gegevens te hergebruiken. RdGG is dus wettelijk verplicht (artikel 20) om de gegevens gestructureerd, veelgebruikt en machine leesbaar formaat te verstrekken. Het beste formaat om gegevens te verstrekken, zal per sector verschillen. De Europese toezichthouders doen een oproep aan alle belanghebbenden en brancheorganisaties om samen te werken aan een set van standaarden en formaten om het recht op dataportabiliteit vorm te geven. Het RdGG werkt met een elektronisch patiëntendossier (EPD): HIX, dit is een machine leesbaar formaat.

Het recht op vergeten te worden – artikel 17 AVG ^[6] (Nieuw):

De betrokkene heeft het recht om zijn persoonsgegevens te laten verwijderen wanneer hij dit wil. (Autoriteit persoonsgegevens, oktober 2017^[7])

Als een betrokkene erom vraagt, moeten in sommige gevallen zijn persoonsgegevens verwijderd worden (artikel 17).

Dit is van toepassing wanneer:

- De persoonsgegevens niet meer nodig zijn;
- De persoon eerst toestemming heeft gegeven, maar nu de toestemming terugtrekt;
- De betrokkene bezwaar maakt tegen de verwerking van zijn persoonsgegevens;
- De organisatie onrechtmatig gegevens verwerkt;
- De organisatie wettelijk verplicht is om de gegevens na bepaalde tijd te wissen;
- De betrokkene jonger is dan 16 jaar en de persoonsgegevens zijn verstrekt via een app of een website.

Het recht om in te zien – artikel 15 ^[6]:

Personen hebben het recht om te vragen welke persoonsgegevens RdGG van hen bezit. Ook hebben ze het recht deze in te zien. Bij de inzage moet RdGG ook laten weten: voor wel doeleinde persoonsgegevens opgeslagen zijn, hoe lang de persoonsgegevens bewaard worden en op basis van welke logica een besluit over iemand genomen wordt. (Autoriteit persoonsgegevens, oktober 2017^[7])

Recht om te wijzigen – artikel 16 ^[6]:

Onjuist persoonsgegevens mogen gewijzigd worden en aangevuld. RdGG is verantwoordelijk om persoonsgegevens juist te verwerken en te actualiseren wanneer nodig. (Autoriteit persoonsgegevens, oktober 2017^[7])

Deze wijzigingen moeten ook aan een derde partij doorgegeven worden, wanneer persoonsgegevens foutief zijn doorgegeven.

Recht op beperking van de verwerking – artikel 18 AVG ^[6]

Deze wet zegt dat je gegevens niet mag gebruiken/verwerken in bepaalde gevallen, namelijk (Autoriteit persoonsgegevens, oktober 2017^[7]):

- Gegevens zijn mogelijk onjuist: Dus deze moeten eerst gecontroleerd worden voordat ze gebruikt worden
- De verwerking is onrechtmatig: U mag bepaalde gegevens niet verwerken maar de betrokkene wil niet dat deze verwijderd worden. Omdat hij deze later nog wil opvragen bijvoorbeeld
- Gegevens zijn niet meer nodig: De persoonsgegevens zijn niet meer nodig voor het doel waarvoor het RdGG ze verzameld heeft, maar de betrokkenen heeft de gegevens nog wel nodig dus mogen niet verwijderd worden.
- Betrokkene bezwaar maakt: Wanneer iemand bezwaar maakt, mogen de persoonsgegevens niet verwerkt worden

Recht op informatie – artikel 13 AVG ^[6]

Wanneer er persoonsgegevens van een betrokkene worden verzameld, moet de verwerkingsverantwoordelijke de volgende informatie geven:

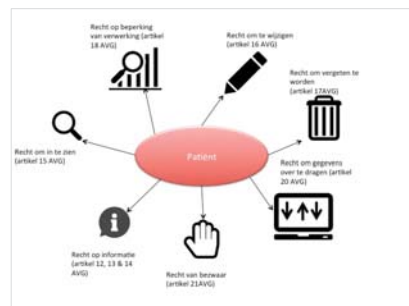
- De identiteit en contactgegevens van de verwerkingsverantwoordelijke.
- De contactgegevens van de functionaris gegevensbescherming
- De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, mede de grondslag voor de verwerking
- De gerechtvaardigde belangen van de verwerkingsverantwoordelijke

Het recht om bezwaar te maken – artikel 21 ^[6]

De AVG geeft mensen het recht om bezwaar maken tegen het verwerken van persoonsgegevens. (Autoriteit persoonsgegevens, oktober 2017^[7]) Maakt iemand bezwaar dan moet er gelijk gestopt worden met verwerken van de persoonsgegevens. Tenzij er dwingende gerechtvaardigde gronden voor de verwerking zijn, die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene.

In figuur 2 zijn alle privacy rechten samen in één figuur geplaatst. De twee omcirkelde rechten, zijn de rechten die voornamelijk invloed zullen hebben op wetenschappelijk onderzoek.

12



Figuur 2: overzicht AVG privacy rechten. Bron: zelfgemaakt

Uitzondering op wetenschap

Bovengenoemde privacy-rechten en grondslagen kunnen in sommige gevallen komen te vervallen.

AVG artikel 14 beschrijft: "Recht op informatie komt te vervallen wanneer het verstrekken van die informatie onmogelijk blijkt te zijn of onevenredig veel inspanning zou vergen, in het bijzonder met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statische doeleinden"

AVG artikel 17 beschrijft: "Artikel 17 is niet van toepassing voor zover de verwerking nodig is: Met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statische doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen, mits de betrokkene geen uitdrukkelijk bezwaar heeft gemaakt"

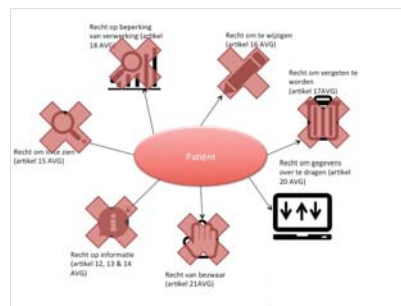
Daarnaast staat er in AVG artikel 89: "Wanneer persoonsgegevens met het oog op wetenschappelijk of historisch onderzoek of statische doeleinden worden verwerkt, kan in het Unierecht of het lidstatelijke recht worden voorzien in afwijkingen van de in de artikelen 15, 16, 18 en 21 genoemde rechten, behoudens de in lid 1 van dit artikel bedoelde voorwaarden en waarborgen, voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken."

In de AVG uitvoeringswet artikel 24 staat: "Persoonsgegevens mogen verwerkt worden zonder toestemming wanneer, het vragen van uitdrukkelijk toestemming onmogelijk blijkt of een onevenredige inspanning kost".

Deze artikelen samengevoegd in figuur 3 levert het volgende op:

14

13



Figuur 3: Overzicht te vervallen privacy-rechten door uitzonderingen. Bron: zelfgemaakt.

Er zou nu gesteld kunnen worden dat de AVG totaal geen risico vormt voor wetenschappelijk onderzoek. Maar dit is niet het geval. Ten eerste omdat er in uiterste gevallen beroep mag gedaan worden op deze "uitzonderingsartikelen". Ten twee zijn deze artikelen niet SMART geformuleerd. De vragen en daarmee mogelijke risico's die naar boven komen zijn: "Wanneer dreigt een onderzoek onmogelijk te zijn?", "Wanneer kost iets onevenredig veel inspanning?" Deze vragen worden in dit stadium van het onderzoek nog niet beantwoord, wel is het duidelijk dat het niet SMART geformuleerde artikelen zorgen voor interpretatie en aangezien niet alle mensen hetzelfde denken brengt dit dus risico's met zich mee.

2.1.3 Conclusie

De AVG is van toepassing op wetenschappelijk onderzoek bij Reinier de Graaf Gasthuis. En de AVG brengt ook risico's met zich mee die effect hebben op de ongewenste topgebeurtenissen. Om deze risico's in kaart te kunnen brengen is de volgende stap een contextanalyse. Deze stap is tevens terug te vinden in de ISO 9001.

2.2 Contextanalyse

Om aan te kunnen tonen dat het RdGG voldoet aan wet- en regelgeving beschrijft de ISO 9001 als eerste stap het volgende: "De organisatie moet het volgende vaststellen:

Welke belanghebbende relevant zijn voor het kwaliteitsmanagementsysteem" (NEN-EN-ISO 9001:2015, blz. 14^[12])

Wanneer dit vertaald wordt naar dit project staat er: Welke stakeholders zijn relevant voor het bewerkstelligen van wetenschappelijk onderzoek? Om deze vraag te beantwoorden wordt er een stakeholderanalyse uitgevoerd.

2.2.1 Stakeholderanalyse

Om de stakeholders in kaart te brengen zijn de volgende drie stappen gezet:

15

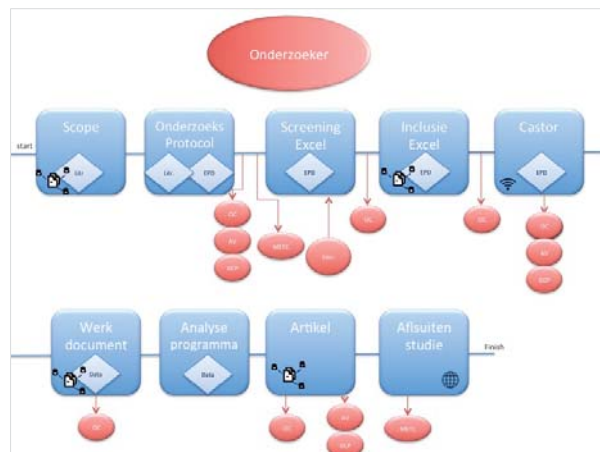
Stap 1: Analyseren procedures RdGG
 Stap 2: Participeren vergaderingen
 Stap 3: Contact met elke stakeholder

Stap 1 - Analyseren procedures RdGG

Er is gebruik gemaakt van de procedures die opgesteld zijn door het RdGG voor het doorlopen van wetenschappelijk onderzoek. In deze procedures staat stap voor stap beschreven wat er moet gebeuren voor, tijdens en na het uitvoeren van wetenschappelijk onderzoek. Hierdoor worden de rollen van de stakeholders duidelijk. De rollen zijn: proefpersoon, onderzoeker, onderzoekscoördinator, afgevaardigde vakgroep, hoofdonderzoeker (ook wel GCP'er genoemd), secretaresse, METC en Castor (leverancier van online database "Castor"). De personen die bij deze rollen horen komen niet naar voren door middel van deze procedures. De mate van invloed is hierdoor moeilijk in te schatten met alleen het gebruik van de procedures. Daarnaast beschrijven de procedures de ideale situatie, de realiteit wijkt hier wel eens van af. Des al niet te min vormen deze procedures een goede basis voor het inzichtelijk maken van de stakeholders. De volgende negen stappen staan beschreven in de procedures:

1. Allereerst wordt er een scope opgesteld door de onderzoeker. Hierin komt de probleemstelling naar voren, en de inclusiecriteria. Hiervoor is informatie uit de literatuur nodig.
2. Vervolgens wordt er een onderzoeksprotocol gemaakt door de onderzoeker. Omdat het op retrospectief onderzoek gaat moet hier al in het EPD gekeken worden. Om de methode te baseren op de informatie die in het EPD beschreven staat. Het onderzoeksprotocol dient door de onderzoekscoördinator (OC), afgevaardigde vakgroep (AV) en de GCP'er gecontroleerd. Vervolgens door het METC, om te controleren of de studie WMO-plichtig is.
3. Wanneer het onderzoeksprotocol is goedgekeurd worden er screeningslijsten gemaakt in Excel. In deze screeningslijsten komen persoonsgegevens te staan van patiënten die voldoen aan de inclusiecriteria voor het onderzoek. Deze lijsten worden zowel door onderzoekers als de secretaresse gemaakt. Deze lijsten worden gecontroleerd door de OC.
4. De patiënten die echt daadwerkelijk geïncludeerd worden in de studie komen in de inclusielijst te staan, ook weer in Excel. Deze wordt gemaakt door de onderzoeker zelf. Deze lijst wordt gecontroleerd door de OC.
5. Vervolgens worden de persoonsgegevens overgeplaatst naar de online database: Castor. De onderzoeker machtigt de OC, AV en de GCP'er om in Castor te kunnen.
6. Vanuit Castor wordt een werkdocument gemaakt, in het werkdocument staan geanonimiseerde gegevens.
7. Vanuit dit werk document worden analyses uitgevoerd, door middel van analyseprogramma's.
8. Vervolgens wordt het artikel geschreven. Dit artikel wordt gecontroleerd door de OC, AV en GCP.
9. De laatste stap is het afsluiten van de studie en het publiceren van het artikel.

De procedures zijn schematisch weergegeven in figuur 4. De lijn representeert een tijdslijn, vervolgens zijn de negen stappen te onderscheiden.



Figuur 4: Tijdslijn wetenschappelijk onderzoek. OC: onderzoekscoördinator, AV: afgevaardigde vakgroep, GCP: Good clinical practice (Hoofdonderzoeker), METC: medisch ethisch toetsing commissie, Secr: secretaresse, Lit: literatuur, EPD = Elektronisch patiëntendossier. Bron: zelfgemaakt.

Omdat de rollen alleen bekend zijn door deze stap, maar niet de personen die deze rollen vervullen worden stappen 2 en 3 ook gezet. Dit is nodig om de stakeholders te kunnen kwalificeren.

Stap 2 - Participeren vergaderingen

Participeren bij wetenschapsvergaderingen: Hierin wordt de voortgang van de lopende wetenschappelijk onderzoeken besproken, met de onderzoekscoördinator en twee onderzoekers. Door te participeren in deze vergadering wordt duidelijk welke rollen en personen aan elkaar gekoppeld zijn. Tijdens deze vergaderingen is te signaleren dat subjectieve overtuigingen van de personen mede bepalend zijn voor besluiten binnen het proces. Dat empathisch gedrag (denk aan vermeende werklust) binnen de vergadering ertoe leidt dat sommige verzoeken niet worden gesteld aan stakeholders. Aan de andere kant is er een risico dat wel om acties wordt gevraagd, maar dat de betrokkenheid niet genoeg is om antwoord te geven. Met andere woorden er ontstaat hierdoor inzicht in de betrokkenheid van rolhouders en het functioneren van het proces. Als een persoon geen antwoord geeft op verzoeken die in het kader van de procedure nodig zijn, functioneert de procedure niet en daarmee het bovenliggende

16

kwaliiteitssysteem. Het kwaliteitssysteem komt lost van de organisatie en de stakeholders zien de toegevoegde waarde niet van alle stappen in het systeem. Op basis van deze informatie is geconcludeerd dat betrokkenheid van de stakeholders essentieel is. Dit heeft ertoe geleid dat met iedere stakeholder individueel contact is gezocht en is meegelopen met hun werkzaamheden.

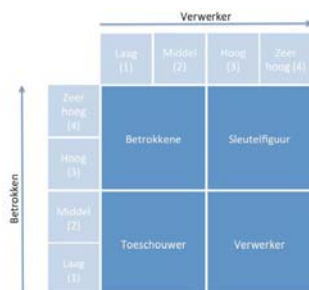
Stap 3 - Contact met elke stakeholder

Er is meegelopen met kwaliteitsvergaderingen, operaties, de polikliniek en de onderzoekscoördinator. Door verschillende dialogen met de stakeholders, tijdens deze werkzaamheden is er een beeld gekregen van de mate van de betrokkenheid per stakeholder en de obstakels die deze stakeholder hierbij ondervinden.

Concluderend uit deze drie stappen komt de definitie van een stakeholder die in dit project wordt gehanteerd naar voren: Een persoon die enerzijds betrokken is bij wetenschappelijk onderzoek en anderzijds omgaat met persoonsgegevens van de patiënten.

Stakeholder kwalificering

De stakeholders zijn gekwalificeerd, om in dit rapport inzichtelijk te maken wat het effect is van de stakeholder op de AVG bij het doen van wetenschappelijk onderzoek. Er wordt gebruik gemaakt van een kwalificeringsschema (figuur 4), waarin enerzijds de betrokkenheid in verwerkt staat en anderzijds de mate van verwerking. Met in acht neming van dat deze analyse specifiek gaat over het verwerken voor wetenschappelijk onderzoek en de betrokkenheid bij wetenschappelijk onderzoek. Bijvoorbeeld een GCP'er is arts en verwerkt dus dagelijks persoonsgegevens, maar kan alsnog laag scoren in dit schema omdat de arts geen persoonsgegevens verwerkt voor wetenschappelijk onderzoek.



Figuur 5: kwalificering stakeholders. Bron: Zelfgemaakt.

Wanneer een stakeholder hoog (3) of zeer hoog (4) scoort in beide categorieën dan betekent dit dat deze persoon veel invloed heeft op de AVG en wetenschappelijk onderzoek. Wanneer een stakeholder

hoog (3) of zeer hoog (4) scoort als verwerker, maar middel of laag in betrokken dan vormt de persoon een groot risico voor de AVG. Een betrokkene of een toeschouwer vormen een minder groot risico voor de AVG zelf, wel kunnen deze stakeholders invloed uitoefenen op wetenschappelijk onderzoek. De resultaten van de stakeholderanalyse staan verwerkt in tabel 1.

Tabel 1: resultaten stakeholderanalyse

Stakeholder	Betrokken	Verwerker	Totaal	Kwalificering
Patiënt	4	4	8	Sleutelfiguur
Onderzoeker	4	4	8	Sleutelfiguur
Onderzoekscoördinator	4	3	7	Sleutelfiguur
Afgevaardigde vakgroep	2	2	4	Toeschouwer
GCP'er	2	3	5	Verwerker
Secretaresse	1	3	4	Verwerker
METC	1	1	2	Toeschouwer
Castor	1	2	3	Toeschouwer

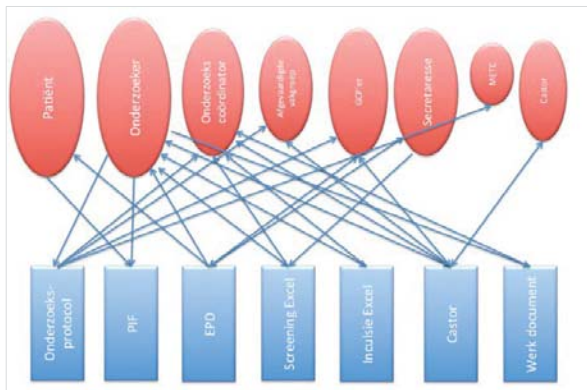
2.2.2 Systemenanalyse

Naast de stakeholderanalyse is ervoor gekozen om ook een systemenanalyse uit te voeren. In het ziekenhuis worden voornamelijk persoonsgegevens verwerkt in het EPD, maar met wetenschappelijk onderzoek worden persoonsgegevens verwerkt in meerdere systemen. Het rechtmatig verwerken van persoonsgegevens en de wijze waarop deze persoonsgegevens verwerkt worden, is het meest belangrijk voor de AVG. De systemen in kaart brengen is hierdoor een belangrijk onderdeel in de gehele contextanalyse. Om te kunnen controleren waar persoonsgegevens opgeslagen worden, of deze beveiligd zijn en welke stakeholder bij deze gegevens kunnen.

De systemen zijn verkregen uit figuur 4, die gebaseerd is op de procedures. De systemen zijn gekoppeld aan de stakeholders, om inzichtelijk te maken welke stakeholder informatie uit een systeem kan halen of bewerken. In figuur 6 is een overzicht te zien, waarin zowel de stakeholderanalyse als de systemenanalyse samengevoegd zijn. De rode ovals representeren de stakeholders, waarin de grootte van de ovals de mate van invloed weergeven. Hoe groter het ovaal, hoe risicovoller de stakeholder is. De blauwe vierkanten zijn de systemen. Een pijl naar een systeem toe gericht staat, betekent dat de betreffende stakeholder gegevens verwerkt in dit systeem. Een pijl van het systeem af, betekent dat de stakeholder informatie haalt uit dit systeem.

18

19



Figuur 6: overzicht stakeholders wetenschap momenteel. Bron: Zelfgemaakt.

Nu de context duidelijk is van de stakeholders en de systemen die gebruikt worden in het RdGG bij het uitvoeren van wetenschappelijk onderzoek kan er gestart worden met de risico's in kaart brengen en dus door naar onderdeel drie van de ISO norm: risico management.

2.3. Risicomanagement

Risico gebaseerd denken stelt een bedrijf in staat om de factoren te bepalen die ertoe zouden kunnen leiden dat processen afwijken van het geplande resultaat en hierop preventief te anticiperen door beheersmaatregelen in te zetten. Deze beheersmaatregelen kunnen negatieve effecten minimaliseren en ervoor zorgen dat kansen maximaal benut worden.

De ISO 9001 zegt dit over risicomanagement: "Hoewel in 6.1 is voorgeschreven dat de organisatie acties moet plannen om risico's op te pakken, is er geen eis voor formele methoden voor risicomanagement of een gedocumenteerd risicomanagementproces. Organisaties kunnen zelf beslissen om al dan niet een uitgebreidere methodiek voor risicomanagement te ontwikkelen dan volgens deze internationale norm vereist is, bijvoorbeeld door de toepassing van andere richtlijnen of normen." (NEN-EN-ISO 9001:2015, blz. 35^[13]).

De ISO 9001 geeft aan dat het RdGG een risicomanagement moet hebben, maar zelf een methode mag toepassen. Voor dit project is er gekozen voor de RISMAN methode. Volgens hoofdstuk wordt geweid aan de toepassing van de RISMAN methode en dus de risicoanalyse.

Figuur 7: Risicovol gebied in procedures. Bron: Zelfgemaakt.

Stap 2: Vervolgens zijn deze stappen besproken met de meest risicovolle stakeholder in combinatie met een inhoudelijk deskundige. De meest risicovolle stakeholder is de onderzoeker, omdat deze stakeholder verbonden staat met alle systemen (zie figuur 6). De FG wordt beschouwd als inhoudelijk deskundige. Uit deze vergadering bleek dat de FG zich het meest zorgen maakt over een data lek: onbevoegde mensen zien persoonsgegevens in. Dit met name door mailverkeer of het niet vergrendelde systemen.

Daarnaast gaf de onderzoeker aan de definitie van "bevoegde personen" onduidelijk. Met name of alleen personeel in loondienst (PIL'ers) bevoegd is of ook personeel niet in loondienst bevoegd (PNIL'ers) is.

Daarnaast gaf de FG aan dat de privacy-rechten: recht van bezwaar en recht om vergeten te worden het meest van toepassing zijn op wetenschappelijk onderzoek.

Stap 3: Vervolgens zijn er open gesprekken gevoerd met alle stakeholders. Waar in onduidelijkheden, frustraties en angsten naar voren kwamen omtrent de AVG. Deze zijn vertaald naar de risico's en gecombineerd met de informatie over de AVG en het gesprek met de FG en onderzoeker.

De combinatie van deze drie stappen vormen concluderend deze risico's:

Risico 1. Iemand die onbevoegd patiëntgegevens inziet en verwerkt.

Risico 2. De patiënt geeft geen actief toestemming om zijn persoonsgegevens te verwerken voor wetenschappelijk onderzoek.

Risico 3. Patiënt doet beroep op zijn recht van bezwaar.

Risico 4. Patiënt doet beroep op zijn recht om vergeten te worden.

Risico 5. De AVG wordt gezien als een te grote barrière, waardoor niemand meer iets durft te doen met persoonsgegevens.

3.3 Vaststellen belangrijke risico's

Doormiddel van een puntensysteem zijn de prioriteeringsniveaus van de risico's bepaald, tabel 2. De keuze kan gemaakt worden op een schaal van één tot en met vijf, waarbij de het 'gevolg' respectievelijk zeer gering, laag, middel, hoog, catastrofaal is en 'kans' respectievelijk zeer gering, laag, middel, hoog, vrijwel zeker gaat. Het totaal wordt berekend door de vermenigvuldiging van kans maal gevolg.

De kwalificering van risico 1 is gebaseerd op de statistieken afkomstig van AP en de secretaresses die veel te maken hebben met datalekken. Daarnaast is in figuur 6 te zien dat er 20 pijlen staan, elke pijl brengt een risico met zich mee als het gaan om het rechtvaardig persoonsgegevens inziden. Ook is in figuur 7 te zien dat er persoonsgegevens opgeslagen worden in vier verschillende systemen. Hoe meer opslaglocaties hoe groter het risico op een data lek.

De kwalificering van risico 2 t/m 4 is gebaseerd op de gesprekken met de onderzoeker en onderzoekscoördinator. Deze stakeholders hebben veel ervaring met het gedrag van patiënten met betrekking tot wetenschappelijk onderzoek. Tot slot is de kwalificering van risico 5 gebaseerd op het meedraaien in het RdGG, waarbij de angsten van veel stakeholders herhaaldelijk naar voren kwamen.

3. Risico-inventarisatie met RISMAN methode

Voor het komen tot een passend advies wordt er gebruikt gemaakt van de RISMAN methode, dit is besproken met het RdGG. Daarnaast komt deze methode sterk overeen met de ISO 9001 norm en met de PDCA-cyclus, omdat het gaat om het doel en de context eerst duidelijk te hebben om vervolgens een risicoanalyse uit te voeren. Daar het RdGG al volgens het ISO 9001 werkt sluit de RISMAN methode goed aan en is RISMAN een goede methode om te gebruiken voor de risicoanalyse inzake de AVG privacy rechten. De RISMAN methode staat uitgebreid beschreven in de bijlage. De stappen van de RISMAN methode worden gebruikt als hoofdstukoppen, om de toepasbaarheid van de RISMAN methode op dit project inzichtelijk/duidelijk te maken.

3.1 Vaststellen doel

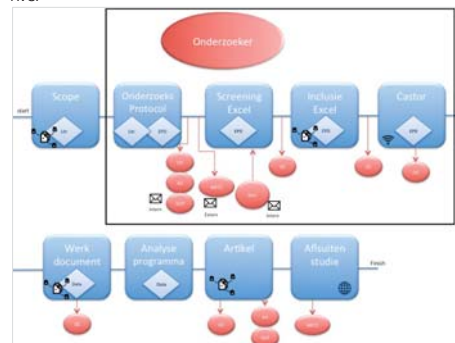
In de inleiding is al vermeld dat het doel van dit onderzoek is het voorkomen van de twee ongewenste topgebeurtenissen (OTG). Dit doel is vastgesteld door het RdGG. Hieronder staan ze nog een keer vermeld.

- OTG1: Het RdGG ontvangt een boete, door het niet voldoen aan de AVG
- OTG2: Wetenschappelijk onderzoek kan niet worden uitgevoerd, met de komst van de AVG.

3.2 In kaart brengen risico's

De RISMAN methode beschrijft als 2e stap van de integrale risicoanalyse, het in kaart brengen van risico's. Een risico is een factor die ervoor kan zorgen dat een OTG tot uiting komt. Het in kaart brengen van de risico's is in 3 stappen gedaan.

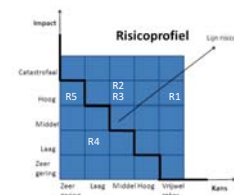
Stap 1: Allereerst is er gekeken in welke stappen van wetenschappelijk onderzoek gewerkt wordt met persoonsgegevens. Deze stappen zijn omcirkeld in figuur 7 en worden als risicovol gezien, met oog op de AVG.



Tabel 2: Risico kwalificeringen.

	Kans	Gevolg	Totaal
Risico 1. Iemand die onbevoegd patiëntgegevens inziet en verwerkt.	5	4	20
Risico 2. De patiënt geeft geen actief toestemming om zijn persoonsgegevens te verwerken voor wetenschappelijk onderzoek.	3	4	12
Risico 3. Patiënt doet beroep op zijn recht van bezwaar.	3	4	12
Risico 4. Patiënt doet beroep op zijn vergetelheidsrecht	2	2	4
Risico 5. De AVG wordt gezien als een te grote barrière, waardoor niemand meer iets durft te doen met persoonsgegevens.	1	4	4

Om een overzicht te krijgen bij welke risico's echt acties ondernomen moet worden zijn de risico's geplaatst in het risicoprofiel (figuur 8). De dikke zwarte lijn die loopt als een trap, vormt de risicotolerantie lijn. Voor alle risico's boven deze lijn (R1, R2 & R3) dienen acties opgesteld te worden.



Figuur 8: Risicoprofiel ingevuld van met R1 t/m R5

Nu de prioritering in kaart is gebracht, moet er bij elk risico een beheersmaatregel vastgesteld worden.

3.4 In kaart brengen beheersmaatregelen

De beheersmaatregelen die staan beschreven in de RISMAN methode en die gebruikt worden bij het RdGG staan weergegeven in tabel 3. Waarbij het effect van hoog naar laag respectievelijk staat voor de beheersmaatregelen vermijden, reduceren, overdragen en accepteren.

Tabel 3: overzicht beheersmaatregelen.

Effect	Risicomaatregelen
Hoog ↑ Laag	Bedreiging
	Vermijden
	Reduceren
	Overdragen
	Accepteren

3.5 Vaststellen beheersmaatregel + implementatie advies

In dit hoofdstuk worden de beheersmaatregelen per risico vastgesteld. Tegelijk wordt hier een advies bij gegeven om deze beheersmaatregelen te implementeren. Deze risico's zijn gekoppeld aan de ongewenste topgebeurtenissen. In totaal worden er dertien adviezen gegeven. Een advies is opgesteld met wat achtergrondinformatie als onderbouwing en aan het einde een concreet actiepunt.

3.5.1 Ongewenste topgebeurtenis 1

"Het Reinier de Graaf ontvangt een boete, door het niet voldoen van de AVG."

Risico 1

Iemand die onbevoegd patiëntgegevens inziet en verwerkt.

De beheersmaatregel bij risico 1 is reduceren of vermijden. Adviezen 1 t/m 4 zijn adviezen om het risico te reduceren. Advies 5 is om het risico te vermijden.

Advies 1

Binnen de AVG draait alles om de verantwoording van het doel en grondslag van het verwerken van persoonsgegevens. Wanneer een patiënt binnen komt wordt er een elektronisch patiëntendossier (EPD) aangemaakt. In het EPD kunnen de patiënt, artsen, verpleegkundige en secretaressen. Deze functionarissen zijn bevoegd omdat deze personen nodig zijn voor de zorg (grondslag: vitale zorg).

Wanneer het gaat om wetenschappelijk onderzoek komen er meer mensen bij te pas dan alleen het medisch team, zie figuur 6. Nu rest de vraag: wanneer is iemand bevoegd om persoonsgegevens in te zien en te verwerken?

Ten behoeve van wetenschappelijk onderzoek op het gebied van volksgezondheid en met uitdrukkelijk toestemming van de betrokkene is een persoon bevoegd om persoonsgegevens in te zien en te verwerken. Mits dit goed gedocumenteerd en aantoonbaar is. Dit gaat om zowel personeel in loondienst als een personeel niet in loondienst (PNIL).

Het Reinier de Graaf werkt met een "delegation log", dit is een document waarin beschreven wordt welke personen in het onderzoeksteam zitten en wat hun rollen zijn.

Actie: Met de komst van de AVG moet er meer nadruk gelegd worden op dit document. Momenteel staat er in de checklist van de procedures nog de term "NVT" achter het delegation log. Haal deze term weg en zorg ervoor dat er bij elk onderzoek een delegation log gebruikt wordt. Zorg ervoor dat er specifiek vermeld wordt welke personen patiëntgegevens in mogen zien, verwerken en wat de doelstelling en de grondslag hiervoor is. Laat dit delegation log controleren door de FG.

Advies 2

Ideaaliter moet de patiënt toestemming geven om de persoonsgegevens in te zien en te verwerken, zoals hierboven benoemd. Deze toestemming kan gezien worden als grondslag. Deze toestemming moet in opt-in vorm in plaats van de opt-out vorm, de betrokkene moet dus actief toestemming geven in plaats van bezwaar kunnen maken.

Het RdGG vraagt bij retrospectief onderzoek vaak geen toestemming. Dit omdat de betrokkene niet belast wordt met vragen of klinisch onderzoek, alleen de gegevens in het EPD worden gebruikt. De patiënt wordt dus niet actief betrokken bij het onderzoek. Deze methode moet worden veranderd.

24

De beheersmaatregel is dit risico reduceren. Hieronder 2 adviezen om dit risico te reduceren.

Advies 6

Om deze oorzaak zo veel mogelijk te reduceren, zal de proefpersoon informatie formulier (PIF) niet te zwaar beladen moeten zijn. Maak een PIF in leken taal met daarin de al eerdergenoemde onderwerpen. Houdt ook een overzicht bij van welke informatie aan wie is gezonden, zodat later aangetoond kan worden welke inspanning er zijn geleverd om toestemming te krijgen. Hiermee kan (op termijn) de onevenredige inspanning aangetoond worden.

Advies 7

Als tweede advies, maar wel uiterlijk advies kan er beroep gedaan worden op het AVG uitvoeringswet artikel 24. Deze beschrijft dat wanneer toestemming vragen onmogelijk blijkt te zijn of onevenredig veel inspanning kost, persoonsgegevens gebruikt mogen worden zonder toestemming. Deze wettekst is voordelig voor de wetenschap. Onevenredig veel inspanning is niet SMART geformuleerd, zorg ervoor dat dit wel gebeurd door het RdGG. Maak een protocol waarin in staat dat bij het includeren van een x aantal personen, dit wordt gezien als onevenredig veel tijd. Laat dit protocol controleren of zelfs opstellen door de FG. Gebruik ook de data die verzameld kan worden uit advies 6 als bewijslast.

Risico 3

Patiënt doet beroep op zijn recht van bezwaar.

Dit risico heeft veel overeenkomsten met het toestemming vragen aan de betrokkenen. Gezien het RdGG momenteel gebruikt maakt van opt-out toestemming vragen, wordt dit risico apart behandeld. De beheersmaatregel is dit risico reduceren. Hieronder 2 adviezen om dit risico te reduceren.

Advies 8

Wanneer de patiënt bezwaar maakt tegen het verwerken van de persoonsgegevens moet hier gehoor aan worden gegeven. De persoonsgegevens mogen niet meer verwerkt worden. Om dit risico te reduceren, is het sterk aan te raden om actief toestemming te vragen aan de patiënten (opt-in), zie ook eerdere onderbouwing bij Risico 1: advies 2.

Wanneer dit toch tijdens het onderzoek gebeurt, dan moeten de persoonsgegevens verwijderd worden uit de inclusielijst. Alle tot dan toe verzamelde data, mag wel gebruikt worden in het artikel. Tenzij er beroep wordt gedaan op de vergetelheid recht.

Advies 9

In een uitzonderlijk geval hoeft er geen gehoor aan gegeven te worden, volgens artikel 89 AVG. Dit is wanneer er actief gekeken is naar de mogelijkheden om de persoonsgegevens niet verder te verwerken, maar dit het wetenschappelijk onderzoek onmogelijk dreigt te maken. Dit moet dan wel volledig onderbouwd worden. Deze onderbouwing kan weer met de data die verzameld wordt uit advies 6. Als blijkt dat x aantal procent geen actief toestemming vraag, waardoor het onderzoek niet uitgevoerd kan worden kan die dienen als bewijs. Vermeld er ook bij dat de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet geschaad wordt.

Risico 4

Patiënt doet beroep op zijn vergetelheidsrecht.

26

Actief toestemming vragen kan als positief worden geïnterpreteerd: Op het proefpersoon informatie formulier (PIF) moet een beknopte versie van het delegation log beschreven worden.

- Wat gaat er gebeuren met de persoonsgegevens van de betrokkene?
- Wie mogen allemaal de persoonsgegevens inzien en verwerken?
- Wat zal dit betekenen voor de betrokkene?

Advies 3

Een andere oorzaak dat onbevoegde mensen persoonsgegevens inzien is dat bestanden niet goed beveiligd zijn of op de verkeerde plaats zijn opgeslagen. Alle bestanden waarin persoonsgegevens staan, dienen vergrendeld te zijn. Recent is hier al aandacht aan besteed in het RdGG, en zijn alle Excel bestanden vergrendeld. Ook is deze stap beschreven in de procedures, weer een stap om het risico te reduceren. Blijf hier aandacht aan besteden, en elkaar controleren tijdens het monitoren wat periodiek gebeurt door het hanteren van de ISO 9001 richtlijnen.

Advies 4

Mail geen persoonsgegevens meer naar mensen, zowel intern als extern. De FG zegt dat intern mailen nog als veilig beschouwd mag worden. Maar om de kans op een data lek zo klein mogelijk te maken wordt nadrukkelijk geadviseerd geen bestanden met daarin persoonsgegevens rond te mailen. Maak gebruik van het EPD zelf, Castor, of de gedeelde schijf. Als hier bestanden al staan opgeslagen is het overbodig om deze rond te mailen. Zorg er dan wel weer voor dat advies 3 dan ook toegepast wordt.

Uitliem advies 5

De beste oplossing voor dit grote risico lijkt: "CTCue". Reinier de Graaf heeft recent CTCue aangeschaft. CTCue is een zoekmachine die ontworpen is voor data-analyse. CTCue kan door alle medische gegevens zoeken, en deze filteren naar de criteria die de onderzoeker heeft. CTCue is ontworpen met gebruik van een "privacy by design" doel. Dit betekent dat CTCue alle data waar mogelijk anonimiseert voordat deze in de database terecht komt. Dit zou betekenen, dat niemand meer bezig is met persoonsgegevens, want wanneer deze geanonimiseerd zijn vallen deze niet onder persoonsgegevens meer.

Het lijkt echter alsof de waarde van deze optie nog niet echt ingezien wordt. Deze oplossing is namelijk pas in het laatste gesprek naar voren gekomen en niet direct door gecommuniceerd wanneer deze was aangeschaft. Daarnaast is er een blijvende discussie gaan over bevoegdheden voor het inzien van het EPD. In plaats van discussies, waar tot nog toe geen antwoord op te vinden is kan er ook gericht worden op CTCue. Die ervoor zorgt dat niemand meer persoonsgegevens in hoeft te zien, als het gaat om wetenschappelijk onderzoek.

3.5.2 Ongewenste topgebeurtenis 2

"Wetenschappelijk onderzoek kan niet worden uitgevoerd, met de komst van de AVG"

Risico 2

De patiënt geeft geen actief toestemming om zijn persoonsgegevens te verwerken voor wetenschappelijk onderzoek.

Het kan zijn dat betrokkenen eerder geneigd zijn om geen toestemming te geven, omdat ze bijvoorbeeld geen zin hebben om de brief te lezen, het niet begrijpen of gewoon simpele weg geen zin hebben om erover na te denken en dus voor het gemak nee zeggen. De kans is middel en de impact is hoog.

25

De beheersmaatregel is dit risico aanvaarden. Hieronder 3 adviezen om dit risico te aanvaarden en toch te beheersen.

Advies 10

Hier moet gehoor aan worden gegeven. Wanneer een patiënt zijn toestemming dus intrekt om de gegevens te verwerken en daarnaast nog vraagt om alle persoonsgegevens te verwijderen moet dit ook daadwerkelijk gebeuren. Ook is de verwerkingsverantwoordelijke, verantwoordelijk voor alle persoonsgegevens die verstuurd zijn naar derde partijen.

Echter wanneer persoonsgegevens volledig geanonimiseerd zijn, dan worden deze gegevens niet meer gezien als persoonsgegevens. Dus wanneer het artikel al geschreven is, dan hoeven de resultaten er niet uitgehaald worden.

Advies 11

Er moet een verwerkingsovereenkomst zijn tussen de onderzoeker (verantwoordelijke) en de zorginstelling (verwerker) die de gegevens aanlevert. Het ziekenhuis moet duidelijk hebben waar persoonsgegevens worden opgeslagen. Wanneer een betrokkene vraagt aan het ziekenhuis om alle persoonsgegevens te verwijderen, zal RdGG een overzicht moeten hebben van de betreffende persoon, waar alle gegevens staan. En zullen de gegevens in de inclusie lijsten en screeningslijsten verwijderd moeten worden.

Advies 12

In een uitzonderlijk geval hoeft er geen gehoor aan gegeven te worden, volgens artikel 17 AVG. Dit is wanneer er actief gekeken is naar de mogelijkheden om de persoonsgegevens niet verder te verwerken, maar dit het wetenschappelijk onderzoek onmogelijk dreigt te maken. Dit moet dan wel volledig onderbouwd worden.

Risico 5

De AVG wordt gezien als een te grote barrière, waardoor niemand meer iets durft te doen met persoonsgegevens.

Met de komst van de wet is er veel onrust in het ziekenhuis over wat wel mag en wat niet mag. De beheersmaatregel is dit risico aanvaarden. Hieronder 1 advies om dit risico te aanvaarden en toch te beheersen.

Advies 13

De verordening is gemaakt om de privacy van betrokkene te beschermen. Dit is omdat (zonder dat betrokkene het weten), er onnodig veel persoonsgegevens opgeslagen zijn op verschillende plaatsen. Er is meer informatie bekend van de betrokkene, dan dat ze daadwerkelijk willen.

De wet is niet om wetenschappelijk onderzoek of überhaupt de gezondheidszorg tegen te gaan. Dit advies kan gebruikt worden, totdat het beleidsplan van het STZ komt. Al zal het beleid dit advies eerder aanvullen dan tegenspreken.

Bovendien staat in de AVG verantwoording, doormiddel van doel en grondslag centraal. Omdat de orthopedie in het RdGG ISO 9001 gecertificeerd is, wordt er met veel procedures/protocollen gewerkt. Deze protocollen zijn opgesteld door risico-inventarisaties en dus goed doordacht. Wat weer ten goede komt in het implementeren van de AVG.

27

4. Evaluatie

De functionaliteit van het product wordt goed bevonden door het RdGG. In de AVG staat verantwoording centraal. Verantwoording kan gegeven worden middels onderzoek. Dit afstudeerproject kan aantonen dat het RdGG actief bezig is geweest met het in kaart brengen van de risico's rondom de AVG.

Dinsdag 12 juni 2018 is er een presentatie gegeven in het RdGG, hierbij waren de onderzoekers en onderzoekcoördinator aanwezig. Daarnaast was er een kwaliteitsmanager van het RdGG en de eerste begeleider van HHS aanwezig.

In deze presentatie zijn de volgende producten gepresenteerd:

- De AVG is kort maar krachtig toegelicht;
- De contextanalyse van de processen, stakeholders en systemen zijn getoond;
- Het risicovolle gebied is gepresenteerd en de hierbij behorende risico's; en
- De adviezen zijn gepresenteerd.

Vooralsnog lijken de aanwezigen erg tevreden met deze producten. Alle aanwezigen konden zich vinden in de redeneringen en adviezen. Daarbij werd gemeld dat het als fijn werd ervaren dat alle onduidelijkheden, frustraties en angsten van iedereen betrokken was in de risico's. Wel werd er nog één aanbeveling gegeven, en dat was een pijl van de stakeholder onderzoeker. Deze moest een twee richting verkeer hebben met het EPD. Deze is dan ook aangepast in het product. Dit veranderde verder niets aan de adviezen, het maakte alleen maar nog meer duidelijk dat de onderzoeker een sleutelstakeholder is.

5. Discussie

In de inleiding is aangegeven dat de wetenschapsgroep van de orthopedische afdeling wil voorkomen dat de implementatie van de AVG onverwachte (catastrofale) situaties met zich meebrengt. Dit vormt het volgende doel van deze afstudeerscriptie:

De orthopedie afdeling in het Reinier de Graaf Gasthuis (RdGG) wil advies over de interpretatie en implementatie van de AVG om de volgende twee ongewenste togebeurtenissen te voorkomen:

- Het Reinier de Graaf ontvangt een boete, door het niet voldoen aan de AVG
- Wetenschappelijk onderzoek kan niet worden uitgevoerd, met de komst van de AVG

De adviezen zijn opgesteld, middels een contextanalyse en risicomanagement. De volgende stap is het toewijzen van risico eigenaren en vervolgens het implementeren van deze adviezen. Verwacht wordt dat dit daadwerkelijk gebeurd om dat het ten eerste een zeer actueel onderwerp is met grote gevolgen. Daarnaast zijn alle stakeholders nauw betrokken geweest bij dit project, dit kan dienen als draagvlak voor het implementeren.

Het is een voordeel dat het RdGG werkt volgens de richtlijnen van de ISO 9001 norm, omdat het RdGG nu gewend is aan het implementeren van beheersmaatregelen. Eén keer in de drie weken wordt er een kwaliteitsvergadering gepland, hierin worden systematisch de lopende PDCA-cyclussen geëvalueerd.

28

Bronnen

[1] Certified secure. Redactie Security (2018, 26 April). HagaZiekenhuis waarschuwt 85 medewerkers na inzien dossier Barbie. Geraadpleegd van: <https://www.security.nl/posting/559996/HagaZiekenhuis+waarschuwt+85+medewerkers+na+inzien+dossier+Barbie>

[2] Het financieel Dagblad. (2017, 14 augustus). Bedrijven in Paniek over Europese privacywet. Geraadpleegd van: <https://fd.nl/economie-politiek/1213263/bedrijven-in-paniek-over-europese-privacywet>

[3] RTL nieuws (2018, 8 februari). Wetswijziging in 2018: privacy is hot topic. Geraadpleegd van: <https://www.rtlnieuws.nl/sponsored-special/wetswijzigingen-in-2018-privacy-is-hot-topic>

[4] Algemeen Dagblad (2018, 3 april) Duizenden sportclubs niet klaar voor nieuwe privacywet. Geraadpleegd van: <https://www.ad.nl/binnenland/duizenden-sportclubs-niet-klaar-voor-nieuwe-privacywet~af07644d/>

[5] NRC (2018, 3 april). Veel bedrijven niet klaar voor nieuwe privacywet. Geraadpleegd van: <https://www.nrc.nl/nieuws/2018/04/19/veel-bedrijven-niet-klaar-voor-nieuwe-privacywet-a1600042>

[6] EU Algemene verordening gegevensbescherming (EU-AVG) (2016, 27 april) Geraadpleegd op: <http://www.privacy-regulation.eu/nl/>

[7] Autoriteit persoonsgegevens (2017, 30 oktober). AVG – Europese privacywetgeving. Geraadpleegd op: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

[8] Burgerlijk wetboek 7. (2018, 2 januari) Geraadpleegd op: <http://wetten.overheid.nl/BWBR0005290/2018-02-01>

[9] Hedeman, B., Heemst G.V. van, Fredriksz H. (2014). *Projectmanagement op basis van PRINCE (2^{de} herziende druk)*. Amersfoort: Van Haren publishing.

[10] Hedeman, B., Riepman, R. (2016). *Projectmanagement op basis van ICB versie 4(3^{de} geheel herziende druk)*. Amersfoort: Van Haren Publishing.

[11] NEN-EN-ISO 9001 (nl). (Oktober 2015). *Kwaliteitsmanagementsystemen – Eisen*. ICS 03.120.10

[12] Kennisbank Twynstra Guddé (N.D.) PDCA/Deming cirkel. Geraadpleegd van: <https://www.twynstraguddekennisbank.nl/pdca/deming-circle>

[13] Kennisbak Twynstra Guddé (N.D.) De stappen binnen risicomanagement. Geraadpleegd van: <https://www.twynstraguddekennisbank.nl/risicomanagement/de-stappen-binnen-risicomanagement>

Dit project bevindt zich nu in de Plan fase, en zal wanneer de risico eigenaren toegekend zijn richting de Do fase gaan en zo terecht komen in de kwaliteitsvergaderingen.

Naast het RdGG blijken (gelukkig) meerdere ziekenhuizen bezig te zijn met de implementatie van het AVG. Ook ziekenhuizen die nauw betrokken zijn met het RdGG, ziekenhuizen waarmee de wetenschap van het RdGG gaat fuseren. Wie weet kan deze scriptie dienen als goede basis, voor de contextanalyse en een start voor het implementeren. Vervolgens kan een analyse uitgevoerd worden op de geïmplementeerde beheersmaatregelen, om de beheersmaatregelen aan te passen.

Duidelijk moet wezen dat kwaliteitsmanagement en risicomanagement nooit klaar is. Dit moet een continu proces blijven, om actueel te zijn.

6. Conclusie

De orthopedische afdeling is al goed op weg met het implementeren van de AVG. Mede door het kwaliteitsmanagementsysteem, die zorgt voor procesbeschrijvingen, evaluatie en aanpassingen.

Het probleem dat het RdGG had, heeft ervoor gezorgd dat in deze afstudeerscriptie de context van AVG en context van wetenschappelijk onderzoek duidelijk is geworden.

Om persoonsgegevens te verwerken moet er voldaan worden aan één van de zes AVG grondslagen. Er is in kaart gebracht dat voor wetenschappelijk onderzoek grondslag één (betrokkene geeft actief toestemming) van toepassing is en dat deze grondslag het risico met de grootste prioriteit kan vermijden.

Daarnaast zijn er vier stappen binnen de wetenschapsprocedures die risicovol zijn voor de AVG. In deze vier stappen hebben met name de AVG-privacy rechten: "Recht van bezwaar" en "recht om vergeten te worden" effect op wetenschappelijk onderzoek.

Daarnaast fungeerde de contextanalyse als goede basis om de risicoanalyse op uit te voeren. Ook gaf dit inzicht in welke processen het RdGG al bezit en welke processen het RdGG kan inzetten om de risico's te beheersen.

De orthopedische afdeling heeft veel oplossingen al in huis. Het advies is om op sommige processen wat meer nadruk te leggen, zoals het delegation log, actief toestemming ragen en de SMART formulering van de onevenredige veel inspanning.

29

Bijlage – RISMAN methode

De RISMAN methode is een gebruikelijk methode, ontwikkeld in samenwerking met Rijkswaterstaat, Twynstra Guddé en Gemeentewerken Rotterdam, om een integrale risicoanalyse uit te voeren (Twynstra Guddé, N.D.) [13]. De RISMAN methode doorloopt vijf stappen (zie figuur 9): 1; integrale risicoanalyse, 2; vaststellen beheersmaatregelen, 3; implementeren van beheersmaatregelen, 4; evalueren van beheersmaatregelen, 5; uitvoeren en updaten van risicoanalyse.



Figuur 9: RISMAN methode Twynstra Guddé

RISMA Stap 1: Integrale risicoanalyse:

Tijdens de eerste stap moet in kaart gebracht worden wat de stand van zaken is. Dit gebeurt volgens de RISMAN-methode in vier stappen (zie figuur 10):



Figuur 10: Integrale risicoanalyse RISMAN methode – Twynstra Guddé

30

31

Stap 1: Het vaststellen van het doel, dus duidelijk hebben waarop de risicoanalyse is gebaseerd. Dit is ook terug te vinden in ISO 9001: "Context duidelijk hebben". Het vaststellen van het doel wordt omschreven als ongewenste topgebeurtenis. Dat is de situatie waarvan de projectleider/opdrachtgever absoluut niet wil dat deze plaatsvindt.

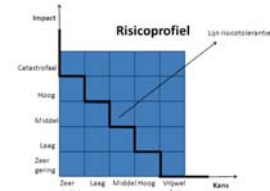
Stap 2: In kaart brengen risico's, De risico's moeten aan de hand van verschillende invalshoeken in kaart gebracht worden. Dit afstudeerproject maakt een risico-inventarisatie door middel van de AVG materie en artikelen. Daarnaast wordt er met alle stakeholders open gesprekken gevoerd. En er wordt een vergadering georganiseerd waarin de sleutelstakeholder samen met een inhoudelijk vak deskundige een risico-inventarisatie maakt.

Stap 3: Vaststellen belangrijkste risico's

Nadat de risico's in kaart zijn gebracht, moet een risicoprofiel gemaakt worden.

Hoe groot de kans is dat de risico's optreden en hoeveel impact de risico's hebben op de doelstelling als ze daadwerkelijk optreden.

Door middel van een risicoprofiel (zie figuur 11) zal een risico beoordeeld worden en vervolgens in een overzicht gezet worden met een puntensysteem. Deze impact gaat dan over de ongewenste topgebeurtenis (imago en geld)



Figuur 11: Risicoprofiel

Stap 4: In kaart brengen beheersmaatregelen, De beheersmaatregelen zijn afhankelijk van de mate van bedreigen op de top ongewenste gebeurtenis.

In tabel 4 is een overzicht te zien van de soorten risicomaatregelen die kunnen ondernomen worden.

Tabel 4: Risicomaatregelen

Effect	Risicomaatregelen
	Bedreiging
Hoog	Vermijden
↕	Reduceren
Laag	Overdragen
	Accepteren

Bijlage projectvoorstel

Implementatie van een risicomanagementprocedure op de orthopedische afdeling in het Renier de Graaf ziekenhuis

P.F. Schuurman – 14097842

Begeleider RDG
N.M.C. Mathijssen

Begeleider HHS
K.L. van Stein Callenfels

1. Inleiding

Om kwaliteit, ook van onderzoeken, te waarborgen is er een internationaal kwaliteitsnorm: NEN-EN-ISO 9001:2015. Om duidelijkheid te krijgen wat een norm precies is, wordt het begrip eerst uitgelegd. Het 'begrip' norm heeft meerdere betekenissen. In het dagelijks leven kan het worden gezien als een manier van doen die volgens algemeen opvatting geldt als normaal. In de kwaliteit is een norm een afspraak die partijen vrijwillig met elkaar maken over de kwaliteit van hun producten, diensten of processen (B. Hedeman & R. Riepma, 2016) Deze kunnen opgesteld worden tussen bedrijven zelf, maar kunnen ook internationaal worden opgesteld. Hiervan is ISO 9001 een voorbeeld.

Deze norm is dus geen vereiste, maar dient als hulpmiddel om een kwaliteitsmanagementsysteem te standaardiseren, bekritisieren en optimaliseren (ISO 9001, 2018). Deze norm zorgt er stapsgewijs voor dat een bedrijf voldoet en blijft voldoen aan de eisen en wensen van de stakeholders, dat het bedrijf voldoet aan de wet- en regelgeving, dat er middels risicomanagement ingespeeld wordt op de kansen en bedreigingen én dat continue verbeteren geborgd is in de organisatie.

Wanneer bedrijven volgens deze normen (willen) werken, kunnen deze ook gecertificeerd worden. In bezit zijn van het certificaat is voor de onderneming goed voor zowel de professionalisering als commerciële waarde.

Het Renier de Graaf Ziekenhuis (RDG) werkt volgens deze norm en is ook in het bezit van het certificaat. Een certificaat is geldig voor drie jaar, begin mei 2018 wordt het RDG opnieuw beoordeeld.

Zoals eerder vermeld is er een ISO norm waarin beschreven staat de een bedrijf zich aan de wet- en regelgeving moet houden. Om het wat duidelijker te maken is het handig het verschil te weten tussen een norm en een de wet- en regelgeving. Zoals eerder beschreven is het werken via een norm niet een vereiste, daarentegen is de wet- en regelgeving een voorschrift: "Een dwingende bepaling met een wettelijke basis afgegeven door een bestuurlijk gezag, in Nederland is dit vaak de Nederlandse overheid." (B. Hedeman & R. Riepma, 2016).

Vermijden – Wanneer de bedreiging erg hoog is moet deze vermeden worden. Dit betekent dat het risico in zijn geheel niet meer kan optreden. Vaak gaat dit samen met een geheel andere aanpak

Reduceren – Een maatregel waarbij de waarschijnlijkheid wordt gereduceerd.

Noodvoorziening treffen- De waarschijnlijkheid neemt hierbij niet af, maar de impact. Er wordt dus een voorziening getroffen die zich voorbereid op als het risico plaatsvindt. Dus het risico wordt niet per se voorkomen, alleen de impact wordt gereduceerd.

Overdragen – Een risico overdragen naar een ander. Denk hierbij aan, als er een financieel risico dreigt kan dit overgedragen worden aan de verzekeringsmaatschappij.

Accepteren – Dit is een bewuste beslissing om geen maatregel te nemen, omdat de impact van het risico zodanig klein is dat het niet de moeite is om een maatregelen te nemen.

RISMAN stap 2: Vaststellen beheersmaatregelen:

Uit de risicoanalyse is voor de belangrijkste risico's een aantal mogelijk beheersmaatregel bedacht. Welke maatregelen er daadwerkelijk uitgevoerd gaan worden, moet door het managementteam vastgesteld worden. Dit gaat door middel van een inschatting te maken hoeveel energie en geld deze maatregel vergt en hoeverre deze wat oplevert voor de te vermijden/reducen risico. Belangrijk is dat bij deze stap de volgende punten beschreven worden:

- Risico
- Beheersmaatregel
- Beheersmaatregel eigenaar.

Dit is weer terug te koppelen aan de ISO 9001 en de Plan van de PDCA-cyclus.

RISMAN stap 3: Implementeren van beheersmaatregelen:

De beheersmaatregel eigenaar gaat ervoor zorgen dat de maatregel ook daadwerkelijk wordt uitgevoerd. Hierbij wordt er aan de planning gehouden en wordt er gerapporteerd. Dit is weer terug te koppelen aan de ISO 9001 en de Do van de PDCA-cyclus.

RISMAN stap 4: Evalueren van beheersmaatregelen

Deze stap moet met regelmaat uitgevoerd worden. Er moet geëvalueerd worden of de beheersmaatregel daadwerkelijk het gewenste effect heeft. Dit is weer terug te koppelen aan de ISO 9001 norm en de Check van de PDCA-cyclus.

RISMAN stap 5: Uitvoeren update van de risicoanalyse:

Door de evaluatie wordt er in kaart gebracht of bepaalde beheersmaatregelen aangepast moeten worden. Zo wordt er gekeken of de risico's weggenomen zijn of gereduceerd. Ook kan het zijn dat de beheersmaatregelen nieuwe risico's met zich mee brengen, hiervoor moeten dan alle stappen opnieuw doorlopen worden. Dit komt overeen met de Act, van de PDCA – cyclus.

Wetten moeten dus geïmplementeerd worden in een bedrijf door het bedrijf zelf, in de ISO norm staat niet letterlijk beschreven op wat voor manier.

In het Renier de Graaf ziekenhuis (RDG) wordt er medisch wetenschappelijk onderzoek verricht. Om te zorgen dat dit onderzoek ethisch verantwoord gebeurt, zijn er wetten opgesteld. De voornaamste wetten zijn de Wet medisch- wetenschappelijk onderzoek met mensen (WMO) en de Embryowet (Centrale Commissie Mens gebonden Onderzoek, 2018). Daarnaast zijn er andere aanvullende wetten die ook van toepassing (kunnen) zijn op onderzoek.

Omdat het gaat om menselijk onderzoek, moeten deze wetten weloverwogen zijn. Hierdoor worden de wetten steeds aangescherpt. Met ingang van 1 maart 2017 is er een aanpassing geweest in de WMO. Dit gaat om de verruiming van mogelijkheden bij medisch wetenschappelijk onderzoek met minderjarige en wilsonbekwame proefpersonen.

Deze wet moet dus geïmplementeerd worden in het RDG op de orthopedische afdeling. Optimaal zou zijn als er een procedure wordt gecreëerd voor wetsverandering, en deze wordt gehandhaafd als standaard.

Hoe wordt ervoor gezorgd dat een wet geïmplementeerd wordt? Dit kan via een risicomanagementprocedure. Volgens de PRINCE2 methode (een projectmanagementmethode), gebeurt dit in vijf stappen, zie figuur 1. Hoe deze stappen gebruikt worden in dit project wordt toegelicht in de methode.



Figuur 12: Stappen risicomanagementprocedure (bron: Projectmanagement op basis van PRINCE 2)

Het doel van dit onderzoek is: ontwerp een risicomanagementprocedure, dat als standaard gebruikt kan worden bij het implementeren van een nieuwe wet.

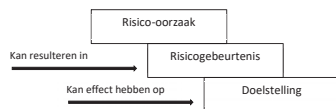
Hierbij dient nieuwe wetsverandering als pilot. Deze kan worden beschreven met de volgende onderzoeksvraag: Is de nieuwe WMO wet, verruiming van mogelijkheden van medisch wetenschappelijk met minderjarige en wilsonbekwamen, geïmplementeerd in het Renier de Graag ziekenhuis?

2. Methode

Stap 1 Identificeren:

Het identificeren wordt opgedeeld in twee onderdelen.

- **Identificeren context:** Het verzamelen van informatie over het project zelf, de context en de doelstellingen. Dit houdt dus dat de WMO wet bestudeerd moet worden via de Centrale Commissie Men gebonden Onderzoek (CCMO). De ISO norm moet helemaal uitgespit worden, deze kan worden verkregen door het RDG. Daarnaast is het essentieel om de stakeholders te identificeren, door middel van een overzicht waarop de contactgegevens komen te staan en functies. Daarbij ook de methodes van het kwaliteitsmanagement van RDG en de communicatie. Door deze kennis te verstrekken in de loop van der tijd, is het van belang dat dit plan van aanpak constant geactualiseerd wordt en aangepast wordt op de methodes van het RDG als deze methodes naar zinnen functioneren. Zo wordt er gekeken of de doelen haalbaar zijn en of deze met het plan behaald kunnen worden.
- **Identificeren risico's:** De techniek die bij dit project van toepassing zal zijn is een brainstormsessie met belanghebbenden en inhoudelijke experts. Er van uitgaande dat een wetsverandering effect zal hebben op meerdere stakeholders, zijn deze stakeholders een essentiële schakel in het identificeren van de risico's rondom hun specialiteit. De risico identificering gebeurt via een risico-oorzaak, zie figuur 2.

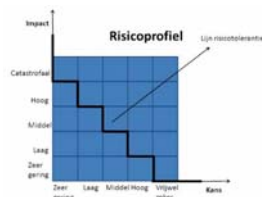


Figuur 13: Risico-oorzaak, -gebeurtenis en -gevolg

Stap 2 Beoordelen

Bij deze stap worden de risico's beoordeeld. Hoe groot de kans is dat de risico's optreden en hoeveel impact de risico's hebben op de doelstelling als ze daadwerkelijk optreden. Hierbij kunnen risico-eigenaren vastgesteld worden.

Een goed overzicht verkrijgen over alle individuele risico's tezamen kan doormiddel van een risicoprofiel, zie figuur 3.



Figuur 14: risicoprofiel

Wanneer de risico's zich bevinden boven de lijn van de risicotolerantie moeten er stappen ondernomen worden. Wanneer ze zich onder de lijn bevinden dan is een maatregel nemen optioneel.

Stap 3 plannen

Na het beoordelen van de risico's, moeten er risicomaatregelen worden bepaald. De risicomaatregelen zijn afhankelijk van de mate van bedreigen op de doelstelling.

In tabel 1 is een overzicht te zien van de soorten risicomaatregelen die kunnen ondernomen worden.

Tabel 5: Risicomaatregelen

Effect	Risicomaatregelen
	Bedreiging
Hoog ↑	Vermijden
	Reduceren
	Noodvoorziening treffen
	Overdragen
Laag ↓	Accepteren

Vermijden – Wanneer de bedreiging erg hoog is moet deze vermeden worden. Dit betekent dat het risico in zijn geheel niet meer kan optreden. Vaak gaat dit samen met een geheel andere aanpak

Reduceren – Een maatregel waarbij de waarschijnlijkheid wordt gereduceerd.

Noodvoorziening treffen – De waarschijnlijkheid neemt hierbij niet af, maar de impact. Er wordt dus een voorziening getroffen die zich voorbereid op als het risico plaatsvindt. Dus het risico wordt niet perse voorkomen, alleen de impact wordt gereduceerd.

Overdragen – Een risico overdragen naar een ander. Denk hierbij aan, als er een financieel risico dreigt kan dit overgedragen worden aan de verzekeringsmaatschappij.

Accepteren – Dit is een bewuste beslissing om geen maatregel te nemen, omdat de impact van het risico zodanig klein is dat het niet de moeite is om een maatregelen te nemen.

Stap 4 Implementeren

Deze stap zorgt ervoor dat de risicomaatregelen geïmplementeerd worden. Hierbij is het noodzaak dat alle risico-eigenaren benoemd zijn. Er moet worden gecontroleerd of de afgesproken maatregelen ook daadwerkelijk worden uitgevoerd. Eveneens moet er gecontroleerd worden of deze maatregelen effect hebben en de risico's kleiner worden.

Zo niet dan moet deze aangepast worden. Het managen van de risico's is een continu proces.

Stap 5 communiceren

Voor het effectief managen van risico's is het van belang dat er regelmatig gecommuniceerd wordt over de status van de risico's en over nieuwe risico's. Zoals in de vorige stap benoemd, is het managen van risico's een continu proces. Zo moet ook het plan steeds geactualiseerd worden.

De ontwikkelingen van risico's moeten opgenomen worden in iedere rapportage en moeten besproken worden bij elk teamoverleg. Vandaar dat het communiceren in het midden van de cirkel staat in figuur 1.

3. Literatuurlijst

Centrale Commissie Men gebonden Onderzoek (2018). *Wet- en regelgeving voor medisch-wetenschappelijk onderzoek*. [Wetten]. Geraadpleegd van: <http://www.ccmo.nl/nl/wet-en-regelgeving-voor-medisch-wetenschappelijk-onderzoek>

Hedeman, B., Heemst G.V. van, Fredriksz, H. (2014). *Projectmanagement op basis van PRINCE2* (2^{de} herziende druk). Amersfoort: Van Haren Publishing.

Hedeman, B., Riepma, R. (2016). *Projectmanagement op basis van ICB versie 4* (3^{de} geheel herziende druk). Amersfoort: Van Haren Publishing.

ISO 9001 register (2018). *Algemeen kwaliteitsmanagementsysteem*. Geraadpleegd van: <https://www.iso-register.nl/Normen/Welke-ISO-normen-zijn-er.html>

4. Persoonlijke leerdoelen

Aan het einde van mijn afstudeerproject kan ik,

- Stakeholders in kaart brengen in een overzicht, waarbij de contactgegevens vermeld + de functie binnen het bedrijf en de functie binnen mijn afstudeerproject. (B3 & B5)
- Volgens de normen van ISO 9001:2015 werken. En deze ook toepassen op een project (B3)
- Risico's identificeren omtrent de implementatie van wet- en regelgeving in het RDG op de orthopedische afdeling, doormiddel van brainstormsessie met experts (B3)
- Risico's beoordelen en zien hoeveel impact deze hebben, doormiddel van een risicoprofiel (B3)
- Risico-eigenaren vaststellen en een structuur bieden in het beoordelen van de risico's (B4 & B5)
- Samen met de stakeholders maatregelen vaststellen, om deze vervolgens toe te passen. (B3)
- Controleren en begeleiding of de maatregelen daadwerkelijk worden toegepast (B4 & B5)
- Analyseren of risico's gereduceerd worden door middel van de vastgestelde maatregelen. (B3)
- Mijzelf goed uitdrukken en aanvoelen hoe de hiërarchie werkt in een vergadering bij het RDG. (B4 & B5)
- Bepalen of de nieuwe WMO geïmplementeerd is in het RDG op de orthopedische afdeling.

5. Planning

Stappen	5-mrt.	12-mrt.	19-mrt.	26-mrt.	2-apr.	9-apr.	12-apr.	23-apr.	30-apr.
Identificeren	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9
Stakeholders identificeren									
ISO 9001 norm bestuderen									
WMO wet bestuderen									
Risico's identificeren									
Beoordelen									
Template risicoprofiel maken									
Risico eigenaren vaststellen									
Risico's beoordelen									
Planen									
Maatregelen vaststellen									
Implementeren									
Maatregelen toepassen									
Checken of maatregelen risico's verminderen									
Communiceren									
Vergadering									
Intermediële									
G-versie scriptie - 1 punt									
Scriptie									
Verdediging									

Stappen	7-mei	14-mei	21-mei	28-mei	4-jun.	11-jun.	18-jun.	25-jun.
Identificeren	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15	Week 16	Week 17
Stakeholders identificeren								
ISO 9001 norm bestuderen								
WMO wet bestuderen								
Risico's identificeren								
Beoordelen								
Template risicoprofiel maken								
Risico eigenaren vaststellen								
Risico's beoordelen								
Planen								
Maatregelen vaststellen								
Implementeren								
Maatregelen toepassen								
Checken of maatregelen risico's verminderen								
Communiceren								
Vergadering								
Intermediële								
G-versie scriptie - 1 punt								
Scriptie								
Verdediging								

Bijlage – Reflectie Leerdoelen

Persoonlijke leerdoelen die opgesteld zijn voor dit afstudeerproject:

- Stakeholders in kaart brengen in een overzicht, waarbij de contactgegevens vermeld + de functie binnen het bedrijf en de functie binnen mijn afstudeerproject. (B3 & B5)
Reflectie: de stakeholderanalyse is naar mijn mening goed gegaan. Er is bewust gekozen om niet automatisch uit te gaan van de stakeholders die worden beschreven in de procedures, maar ook nog verder onderzoek te doen. Er is bewust gekozen om de namen niet te vermelden in deze afstudeerscriptie, dus daarom zijn de rollen alleen vermeld.
- Volgens de normen van ISO 9001:2015 werken. En deze ook toepassen op een project (B3).
Reflectie: De ISO 9001: 2015 is aangehouden. Middels het participeren van kwaliteitsvergaderingen en de richtlijnen lezen heb ik de ISO 9001 mij eigen gemaakt. Dit is ook terug te zien in de benaming van de hoofdstukken.
- Risico's identificeren omtrent de implementatie van wet- en regelgeving in het RdGG op de orthopedische afdeling, doormiddel van brainstormsessie met experts (B3)
Reflectie: Dit is gelukt. Er is contact gelegd met elke stakeholder, en met elke stakeholder is de AVG besproken. De onduidelijkheden, frustraties en angsten kwamen tijdens deze gesprekken goed naar voren, deze zijn vertaald naar risico's.
- Risico's beoordelen en zien hoeveel impact deze hebben, doormiddel van een risicoprofiel (B3)
Reflectie: Dit is gelukt, de risicokwalificering is gebaseerd op gesprekken met alle stakeholders en het meedraaien in het RdGG zelf.
- Risico-eigenaren vast stellen en een structuur bieden in het beoordelen van de risico's (B4 & B5):
Reflectie: Deze stap is niet gelukt. Ik ben gekomen tot het advies. De implementatie, en het toekennen van de risico-eigenaren is aan het RdGG.
- Samen met de stakeholders maatregelen vaststellen, om deze vervolgens toe te passen. (B3)
Reflectie: Er zijn beheersmaatregelen geformuleerd. Deze zijn gekoppeld aan de kwalificering. Er is ook advies gegeven om deze beheersmaatregelen toe te passen, echter zijn deze nog niet daadwerkelijk toegepast.
- Controleren en begeleiding of de maatregelen daadwerkelijk worden toegepast (B4 & B5)
Reflectie: Aan deze stap is nog niet toegekomen. Dit komt omdat het projectplan is opgesteld aan het begin van dit traject. Het plan is steeds geëvalueerd en aangepast, omdat ik begon met abstracte kennis. Tijdens de toepassing van mijn plan, bleken bepaalde processen langer te duren. Processen zoals in contact komen met stakeholders, de AVG goed begrijpen, het verkrijgen van belangrijke documenten. Voornamelijk komt dit doordat een project natuurlijk meerdere stakeholders heeft en niet elke stakeholder heeft dezelfde planning als dat ik heb.
- Analyseren of risico's gereduceerd worden door middel van de vastgestelde maatregelen. (B3)
Reflectie: Aan deze stap ben ik ook niet toegekomen.
- Mijzelf goed uitdrukken en aanvoelen hoe de hiërarchie werkt in een vergadering bij het RdGG. (B4 & B5)
Reflectie: Dit is goed gelukt. Ik heb mijzelf op een goede en professionele manier weten te betrekken in het RdGG. Ik merk dat ik het lastig vind dat er een bepaalde hiërarchie heerst tussen artsen en andere medewerkers. Ik ben een persoon die iedereen gelijk vind. Toch is gelukt om hier goed mee om te gaan, door zelf te analyseren waarom ik iets voel en waardoor dit komt. Ik heb veel zelfreflectie gedaan tijdens dit project.
- Bepalen of de nieuwe WMO geïmplementeerd is in het RdGG op de orthopedische afdeling.
Reflectie: Deze is veranderd naar de AVG. Een mooi voorbeeld dat je plan van aanpak schrijven voordat je in een bedrijf meedraait erg lastig is. Omdat er toch veel over het hoofd wordt

gezien. Maar dit doel gereflecteerd p de AVG i.p.v. WMO, zeg ik dat dit goed behaald is. Middels de contextanalyse is duidelijk geworden dat het RdGG al een heel eind op weg is. En veel risico's kan reduceren, door net wat meer nadruk te leggen op de processen die ze al hebben.