Privacy binnen Ziekenhuis Rivierenland

Een onderzoek naar de verstrekking van persoonsgegevens aan derden.

Sietske Koot

In opdracht van: Ziekenhuis Rivierenland Tiel

Valkenswaard, 25 mei 2014

Privacy binnen Ziekenhuis Rivierenland

Een onderzoek naar de verstrekking van persoonsgegevens aan derden.

Naam:	Sietske Koot
Studentnummer:	2036384
Opdrachtgever:	Ziekenhuis Rivierenland Tiel
Afstudeermentor:	Mw. G.J. Bransz
Eerste afstudeerdocent:	Dhr. B.F.M. Kratsborn
Tweede Afstudeerdocent:	Dhr. B.C.M. Hooijdonk
Afstudeerperiode:	Februari 2014 - juni 2014
Plaats:	Valkenswaard
Datum:	25 mei 2014

Voorwoord

Op 3 februari 2014 ben ik gestart met afstuderen in het kader van mijn opleiding HBO-rechten aan de Juridische Hogeschool Avans-Fontys. Ik heb van 3 februari 2014 tot en met 9 mei 2014 stage gelopen bij Ziekenhuis Rivierenland Tiel. Gedurende deze periode heb ik onderzoek gedaan naar welke aanpassingen er nodig zijn in het privacybeleid van Ziekenhuis Rivierenland, zodat Ziekenhuis Rivierenland voldoet aan de nu en in de toekomst geldende privacywetgeving met betrekking tot verstrekking van persoonsgegevens aan derden. Privacy is een interessant onderwerp dat actueel is en veel discussie oproept, in de huidige informatie- en technologie maatschappij, ik heb me dan ook met veel plezier verdiept in het onderwerp.

Via deze weg wil ik iedereen die heeft bijgedragen aan de totstandkoming van mijn scriptie bedanken. In het bijzonder wil ik mijn begeleidster Janneke Bransz bedanken voor haar begeleiding, inhoudelijke feedback en wijze raad gedurende het gehele onderzoeksproces. Verder wil ik ook mijn begeleider van school Bram Kratsborn bedanken voor de begeleiding en de inhoudelijke feedback.

Het resultaat van het onderzoek ligt voor u, ik wens u veel leesplezier toe.

Sietske Koot

Valkenswaard, mei 2014

Inhoudsopgave

Voorwoord .....
Lijst van afkortingen .....
Begrippenlijst .....
Samenvatting .....
1. Inleiding 7
1.1 Probleembeschrijving 7
1.2 Vraagstelling 8
1.3 Doelstelling 8
1.4 Onderzoeksmethodiek 8
1.5 Leeswijzer 9
2. Juridisch kader 10
2.1 Internationale wetgeving 10
2.1.1 Richtlijn 95/46/EG 10
2.1.2 Art. 8 EVRM 10
2.1.3 Art. 12 UVRM en art. 17 IVBPR 10
2.1.4 Art. 8 Handvest van de grondrechten van de Europese Unie 10
2.1.5 Art.16 VWEU 11
2.2 Nationale wetgeving 11
2.2.1 Grondwet 11
2.2.2 Wet bescherming persoonsgegevens 11
2.2.3 WGBO 17
2.2.4 Wet BIG 18
2.3 Toekomstige wetgeving 18
2.3.1 Voorstel privacyverordening 18
3. Verwerken van persoonsgegevens 21
3.1 Persoonsgegevens 21
3.2 Wijze waarop persoonsgegevens worden verwerkt 21
3.3 Doeleinden voor verwerking 22
3.4 Systemen 22
3.5 Beveiliging persoonsgegevens 24
4. Verstrekking van persoonsgegevens aan derden 25
4.1 Persoonsgegevens 25
4.2 Wijze waarop persoonsgegevens worden verstrekt aan derden 25

4.3 Doeleinden voor verstrekking aan derden 26
4.4 Partijen 26
4.5 Systemen 27
4.6 Beveiliging 28
5. De verwerking en verstrekking van persoonsgegevens getoetst aan de wet- en regelgeving 30
5.1 Verwerking van persoonsgegevens 30
5.2 Verstrekking van persoonsgegevens aan derden 30
5.3 Beveiliging 31
5.4 Toetsingsmatrix 32
5.5 Toetsing doorbraakprogramma Cardiovasculair Risicomanagement 32
5.6 Toetsing gegevensverstrekking laboratorium aan Regioapotheek 35
6. Het Landelijk SchakelPunt 39
6.1 Werking van het LSP 39
6.2 Beveiliging van de persoonsgegevens 40
6.3 Aangesloten zorgverleners in de regio 41
6.4 Voor- en nadelen 41
6.4.1 Voordelen 41
6.4.2 Nadelen 41
7. Conclusies 43
8. Aanbevelingen 46
Evaluatie 48
Literatuurlijst 49

Lijst van afkortingen

Art.	Artikel
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek
CBP	College Bescherming Persoonsgegevens
CVRM	Cardiovasculair Risicomanagement
DFT	
ECT	Eerstelijns Centrum Tiel
EPD	Elektronisch Patiënten Dossier
EVRM	Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele vrijheden
GBZ	Goed Beheerd Zorgsysteem
GW	Grondwet
HL7	Health Level Seven
IVBPR	Internationaal Verdrag Inzake Burgerrechten en Politieke Rechten
JGZ	Jeugdgezondheidszorg
LAZR	Landelijke Ambulante Zorg Registratie
LMR	Landelijke Medische Registratie
LSP	Landelijk SchakelPunt
KIS	Keten Informatiesysteem
KNMG	Koninklijke Nederlandse Maatschappij tot bevordering der Geneeskunst
MvT	Memorie van Toelichting
NEN	Nederlandse Norm
NVZ	Nederlandse Vereniging van Ziekenhuizen
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
SEH	Spoedeisende hulp
UVRM	Universele Verklaring van de Rechten van de Mens
UZI	Unieke Zorgverleners Identificatie
VPN	Virtueel Particulier Netwerk
VWEU	Verdrag betreffende de Werking van de Europese Unie
VZVZ	Vereniging voor Zorgaanbieders voor Zorgcommunicatie
Wbp	Wet bescherming persoonsgegevens
Wet BIG	De Wet op de Beroepen in de Individuele Gezondheidszorg
WGBO	Wet op de Geneeskundige Behandelovereenkomst
WPR	Wet persoonsregistraties
ZIS	Ziekenhuis informatiesysteem
ZRT	Ziekenhuis Rivierenland Tiel

Begrippenlijst

Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;

Betrokkene: degene op wie een persoonsgegeven betrekking heeft; de patënt;

Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;

Medische gegevens: gegevens betreffende de gezondheid van een patiënt;

Ontvanger: degene aan wie de persoonsgegevens worden verstrekt;

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; in deze scriptie worden met persoonsgegevens enkel persoonsgegevens betreffende een patiënt bedoeld;

Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, 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;

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

Verstrekken van persoonsgegevens: Het bekend maken of ter beschikking stellen van persoonsgegevens;

Verzamelen van persoonsgegevens: het verkrijgen van persoonsgegevens;

Samenvatting

Ziekenhuis Rivierenland krijgt steeds vaker het verzoek van zorgverleners uit de omgeving om aan hen persoonsgegevens van patiënten te verstrekken of inzage te verschaffen in de dossiers van het ziekenhuis. Ziekenhuis Rivierenland heeft geen geëxpliciteerd beleid vastgelegd omtrent het uitwisselen van persoonsgegevens met derden. Het beleid dat zij voeren met betrekking tot het verstrekken van persoonsgegevens aan derden berust op de wettelijke bepalingen, maar is niet vastgelegd in specifiek beleid. Het huidige privacyreglement is hiervoor niet toereikend, de bepalingen uit dit reglement zijn gebaseerd op de Wet persoonsregistratie (hierna: WPR) en stamt uit 1990.

In dit onderzoeksrapport is onderzoek gedaan naar de aanpassingen die nodig zijn in het privacybeleid van Ziekenhuis Rivierenland, zodat Ziekenhuis Rivierenland voldoet aan de nu en in de toekomst geldende privacywetgeving met betrekking tot verstrekking van persoonsgegevens aan derden. Aan de hand van een analyse van rechtsbronnen en literatuur is het juridisch kader uiteengezet. De huidige wijze van verwerking en verstrekking van persoonsgegevens door Ziekenhuis Rivierenland is in kaart gebracht door middel van interviews. Verder is er nog gebruik gemaakt van twee casestudy's om het huidige beleid te toetsen aan de wet- en regelgeving. Ook is er gekeken wat voor gevolgen aansluiting bij het Landelijk SchakelPunt met zich mee brengt voor Ziekenhuis Rivierenland en of het LSP een middel is om de verstrekking van persoonsgegevens mee te bewerkstelligen.

In het onderzoek is naar voren gekomen dat de persoonsgegevens van patiënten binnen Ziekenhuis Rivierenland rechtmatig verwerkt worden op grond van art. 8 lid 1 sub b jo. art. 21 lid 1 Wbp. Op grond van de zorgovereenkomst en als basis voor een goede behandeling voor de patiënt is het noodzakelijk om persoonsgegevens te verzamelen en te verwerken. De verwerking dient echter wel op basis van een privacyreglement te berusten, om de privacy van patiënten te kunnen garanderen en om te voldoen aan de nu- en in de toekomst geldende privacywetgeving.

Uit het onderzoek is verder naar voren gekomen dat de verstrekking van persoonsgegevens door Ziekenhuis Rivierenland aan derden in de meeste gevallen berust op een rechtvaardigingsgrond uit de wet. Omdat je bij verstrekking steeds te maken hebt met verschillende gegevens en verschillende ontvangers is het van belang om per verstrekking of tenminste per categorie van verstrekkingen te kijken of de verstrekking van persoonsgegevens door Ziekenhuis Rivierenland aan derden voldoet aan de wettelijke vereisten en gerechtvaardigd is.

Patiënten van Ziekenhuis Rivierenland worden onvoldoende ingelicht over de doeleinden waarvoor hun persoonsgegevens worden verwerkt en verstrekt. Verder worden zij onvoldoende ingelicht over de wijze waarop hun persoonsgegevens worden verwerkt binnen het ziekenhuis en worden verstrekt aan derden. Daarom is het van belang dat het privacyreglement wordt aangepast en de informatiefolders worden aangepast, zodat patiënten beter geïnformeerd kunnen worden. Daarnaast is het van belang dat de medewerkers op de hoogte zijn van het privacybeleid, om een goed privacybeleid te kunnen voeren en te volgen is het immers van belang dat medewerkers zich bewust zijn van de privacy van een patiënt.

Het verstrekken van persoonsgegevens is in beginsel altijd gerechtvaardigd als patiënten daarvoor hun uitdrukkelijke toestemming hebben gegeven. Als patiënten toestemming geven voor het verstrekken van hun persoonsgegevens aan derden kan Ziekenhuis Rivierenland makkelijker en sneller gegevens verstrekken aan derden. Als patiënten hun uitdrukkelijke toestemming geven voor de verstrekking, is de verstrekking van persoonsgegevens gerechtvaardigd. Daarom is het van belang dat er toestemming wordt verkregen van patiënten.

1. Inleiding

In dit hoofdstuk wordt de aanleiding voor het onderzoek uiteengezet. Verder wordt het doel van het onderzoek, de centrale vraag van het onderzoek en de gebruikte onderzoeksmethodiek beschreven. Tenslotte zal kort worden toegelicht hoe het rapport verder is opgebouwd.

1.1 Probleembeschrijving

Meneer Beeks gaat al jaren, één keer in de maand naar het cardiovasculair risicomanagement (CVRM) spreekuur bij zijn huisarts. Meneer Beeks heeft last van hoge bloeddruk, rookt een pakje sigaretten per dag en eet vaak ongezond. Hierdoor heeft hij een verhoogd risico op hart- en vaatziekten. Om dit risico te beperken heeft zijn huisarts samen met de specialist (cardioloog) een individueel zorgplan opgesteld. In dit zorgplan is vastgelegd welke stappen er genomen moeten worden om het risico op hart- en vaatziekten te verkleinen. Dit zorgplan dient opgenomen te worden in een Keten Informatie Systeem, zodat de specialist kan zien wat de huisarts heeft gedaan en andersom, ze werken samen in een gemeenschappelijk dossier. Hierdoor kan de huisarts ook makkelijker de expertise van de specialist inroepen, indien dit noodzakelijk is.[1]

Naar aanleiding van bovenstaande casus kunnen er op het gebied van privacy verschillende vragen worden gesteld. Zoals: mogen zorgverleners wel zomaar alle medische gegevens aan elkaar verstrekken? Onder welke voorwaarden mogen persoonsgegevens worden verstrekt aan derden? Welke zorgvuldigheidseisen moeten in acht worden genomen bij het verstrekken van persoonsgegevens aan derden? Welke randvoorwaarden kunnen gesteld worden aan het gebruik van een Keten Informatie Systeem? Dit zijn vraagstukken waarmee Ziekenhuis Rivierenland steeds vaker te maken krijgt, omdat ze steeds vaker het verzoek van huisartsen en andere zorgverleners uit de regio krijgen, om hen toegang te verschaffen tot de persoonsgegevens die binnen Ziekenhuis Rivierenland beschikbaar zijn.

In beginsel komt de beschikbaarheid en uitwisseling van persoonsgegevens de zorgverlening in het kader van patiëntveiligheid ten goede. Doordat de gegevens bij zowel de specialist, de huisarts en de apotheek bekend zijn kunnen fouten worden voorkomen, hierbij kan gedacht worden aan het uitwisselen van medicatiegegevens. Daarbij hebben alle partijen hetzelfde doel, het garanderen van patiëntveiligheid en het leveren van kwalitatief goede patiëntenzorg.

Ziekenhuis Rivierenland heeft geen geëxpliciteerd beleid vastgelegd omtrent het uitwisselen van persoonsgegevens met derden. Het beleid dat zij voeren met betrekking tot het verstrekken van persoonsgegevens aan derden berust op de wettelijke bepalingen, maar is niet vastgelegd in een beleidsnotitie. Het huidige privacyreglement is hiervoor niet toereikend, de bepalingen uit dit reglement zijn gebaseerd op de Wet persoonsregistratie (hierna: WPR) en stamt uit 1990. Inmiddels is de WPR vervangen door de Wbp daarom dient het reglement onder de loep te worden genomen en te worden aangepast aan de hand van de huidige en toekomstige wet- en regelgeving. In het privacyreglement omtrent persoonsgegevens dienen duidelijke regels te worden opgenomen over de interne verwerking van de persoonsgegevens, hoe gegevens extern kunnen worden uitgewisseld, met wie, in welke situatie en onder welke voorwaarden.

Om te bepalen of de persoonsgegevens van patiënten van Ziekenhuis Rivierenland kunnen worden verstrekt aan derden, is het van belang dat de huidige wijze waarop persoonsgegevens worden verwerkt en verstrekt binnen het ziekenhuis in kaart wordt gebracht.
Het in kaart gebrachte beleid zal vervolgens moeten worden getoetst aan het wettelijk kader. Vervolgens zullen de wettelijke bepalingen worden geïmplementeerd in het privacybeleid

[1] Doorbraakprogramma CVRM

met betrekking tot persoonsgegevens. Zodat aan de hand van het privacybeleid kan worden afgewogen welke persoonsgegevens verstrekt kunnen worden aan derden.

1.2 Vraagstelling

Centrale vraag: welke aanpassingen zijn er nodig in het privacybeleid van Ziekenhuis Rivierenland, zodat Ziekenhuis Rivierenland voldoet aan de nu en in de toekomst geldende privacywetgeving met betrekking tot verstrekking van persoonsgegevens aan derden?

Deelvragen:

1. Wat is het juridisch kader voor het verwerken en uitwisselen van persoonsgegevens?
   - Welke internationale wetgeving is van toepassing?
   - Welke nationale wetgeving is van toepassing?

2. Op welke wijze worden persoonsgegevens binnen het ziekenhuis verwerkt?
   - Welke persoonsgegevens worden verwerkt?
   - Voor welke doeleinden worden persoonsgegevens verwerkt?
   - Door wie worden de persoonsgegevens verwerkt?
   - Welke middelen (systemen) worden gebruikt om de persoonsgegevens te verwerken?
   - Welke maatregelen zijn er getroffen om de verwerkte persoonsgegevens te beveiligen?

3. Op welke wijze worden persoonsgegevens uitgewisseld tussen het ziekenhuis en derden?
   - Welke persoonsgegevens worden uitgewisseld?
   - Met wie worden persoonsgegevens uitgewisseld (organisaties)?
   - Welke afdelingen wisselen persoonsgegevens uit met derden?
   - Welke middelen worden gebruikt om persoonsgegevens uit te wisselen?
   - Welke maatregelen zijn er getroffen om de uitgewisselde persoonsgegevens te beveiligen?

4. Welk beleid wordt gevolgd voor het verwerken en uitwisselen van persoonsgegevens en voldoet dit aan de wet?

5. Wat voor gevolgen brengt aansluiting bij het LSP met zich mee voor Ziekenhuis Rivierenland?
   - Wat is het LSP?
   - Hoe werkt het LSP?
   - Welke zorgverleners uit de regio zijn allemaal aangesloten bij het LSP?
   - Wat zijn de voor-en nadelen van het LSP?
   - Welke mogelijkheden biedt het LSP en heeft het een meerwaarde voor ZRT?

1.3 Doelstelling

Het doel van dit onderzoek is dat er op 26 mei 2014 binnen Ziekenhuis Rivierenland een handleiding beschikbaar is, aan de hand waarvan afgewogen kan worden welke persoonsgegevens van patiënten verstrekt kunnen worden aan derden.

1.4 Onderzoeksmethodiek

Voor dit onderzoek is gebruik gemaakt van verschillende strategieën, methoden en technieken van onderzoek. De gebruikte strategieën zijn een rechtsbronnen- en literatuuronderzoek en een kwalitatief onderzoek, namelijk een casestudy.[2]
Er is een enkelvoudige casestudy uitgevoerd. Aan de hand van twee casestudy's is bekeken of de verstrekking van persoonsgegevens aan derden gerechtvaardigd is. Het recht is

[2] Van Schaaijk 2011, p. 80-81.

onderzocht door middel van een analyse van rechtsbronnen en de literatuur. De praktijk is onderzocht door middel van interviews en analyses van interne documenten.

Het juridisch kader is aan de hand van een inhoudsanalyse van wetgeving, jurisprudentie, kamerstukken, literatuur en artikelen uiteengezet. De verwerking en de verstrekking van persoonsgegevens binnen Ziekenhuis Rivierenland is in kaart gebracht door middel van het afnemen van interviews.[3] Aan de hand van het uiteengezette juridisch kader en het in kaart gebrachte beleid, is getoetst of dit beleid voldoet aan de wet- en regelgeving. Aan de hand van de toetsingsmatrix[4] zijn twee casestudy's uitgevoerd.

Verder heb ik een interview afgenomen in twee andere ziekenhuizen, om te kijken hoe ver andere ziekenhuizen zijn met het ontwikkelen van privacybeleid omtrent het verstrekken van persoonsgegevens aan derden.[5] Aan de hand van deze interviews heb ik meer informatie verkregen over de wijze waarop andere ziekenhuizen omgaan met privacy in het kader van verstrekken van patiëntgegevens.

1.5 Leeswijzer

In het rapport zal eerst de relevante wetgeving uiteengezet worden, zowel de internationale, de nationale wetgeving als de toekomstige wetgeving. Vervolgens wordt het huidige privacybeleid van Ziekenhuis Rivierenland besproken, er wordt in kaart gebracht hoe de verwerking van persoonsgegevens en de verstrekking van persoonsgegevens aan derden is georganiseerd. In hoofdstuk 5 zal vervolgens het huidige beleid worden getoetst aan het juridische kader. In hoofdstuk 6 worden de vragen van Ziekenhuis Rivierenland met betrekking tot het LSP beantwoord. Tot slot worden er in hoofdstuk 7 conclusies getrokken en aanbevelingen gedaan. Naar aanleiding van dit onderzoek is er een concept privacyreglement met betrekking tot persoonsgegevens van patiënten opgesteld en een checklist aan de hand waarvan kan worden afgewogen welke persoonsgegevens mogen worden verstrekt aan derden. Het reglement is opgenomen in bijlage 11 en de checklist is opgenomen in bijlage 10.

[3] Zie bijlage 1 t/m 9
[4] Zie bijlage 10: Toetsingsmatrix
[5] Zie bijlage 14 en 15

2. Juridisch kader

In dit hoofdstuk wordt het juridische kader, met betrekking tot het verwerken van persoonsgegevens en het verstrekken van persoonsgegevens aan derden, uiteengezet. In dit hoofdstuk wordt achtereenvolgens de internationale, de nationale en de toekomstige wetgeving besproken.

2.1 Internationale wetgeving

Op internationaal niveau is het recht op privacy verankerd in het art. 8 EVRM, art. 12 UVRM, art. 17 IVBPR, art. 8 Handvest van de grondrechten van de Europese Unie en art. 16 VWEU. Verder is de privacyrichtlijn 95/46/EG van belang voor het recht op privacy op internationaal niveau. De privacyrichtlijn 95/46/EG vormt namelijk de basis voor de Wbp, deze richtlijn is geïmplementeerd in de Wbp. In de volgende paragrafen zullen de voornoemde bepalingen worden besproken.

2.1.1 Richtlijn 95/46/EG

Op 24 oktober 1995 is 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 in werking getreden. Deze richtlijn wordt de privacyrichtlijn genoemd. Deze richtlijn heeft twee doelstellingen: het fundamentele recht op gegevensbescherming waarborgen en het vrije verkeer van persoonsgegevens tussen de lidstaten van de Europese Unie garanderen. Verder ziet de richtlijn erop toe dat er binnen de Europese Unie dezelfde maatstaven worden gehanteerd voor de bescherming van persoonsgegevens.[6]

De privacyrichtlijn stelt beperkingen aan het verzamelen en gebruiken van persoonsgegevens en verlangt dat er een nationaal onafhankelijk toezichtsorgaan wordt opgericht, dat toeziet op de bescherming van persoonsgegevens. In Nederland hebben we hier het CBP voor, zij zien toe op de bescherming van persoonsgegevens.[7]

2.1.2 Art. 8 EVRM

In dit artikel is de bescherming van persoonsgegevens als grondrecht verankerd. Hierin is opgenomen dat een ieder het recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Bij de uitoefening van dit recht is inmenging van het openbaar gezag niet toegestaan, tenzij dit mag op grond van de wet, dit voor de democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

2.1.3 Art. 12 UVRM en art. 17 IVBPR

In deze twee artikelen is het recht op eerbiediging van de persoonlijke levenssfeer opgenomen. Conform deze artikelen is bepaald dat niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.

2.1.4 Art. 8 Handvest van de grondrechten van de Europese Unie

Dit artikel ziet toe op de bescherming van persoonsgegevens. Een ieder heeft het recht op bescherming van de hem betreffende persoonsgegevens. Deze gegevens moeten op een eerlijke manier worden verwerkt voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.

[6] De Vries & Rutgers 2001, p.13.
[7] Thole, Van der Jagt & Roerdink 2010, p. 16.

Een ieder heeft recht op toegang tot de over hen verzamelde gegevens en op rectificatie daarvan. Verder dient een onafhankelijke autoriteit toe te zien op de naleving van deze regels, in Nederland is dat de CBP.

2.1.5 Art.16 VWEU

In art. 16 VWEU is de grondslag voor de Europese privacyrichtlijn gelegen. In dit artikel is bepaald dat een ieder het recht heeft op bescherming van zijn persoonsgegevens.

2.2 Nationale wetgeving

De nationale wetgeving die van belang is voor het verwerken van persoonsgegevens en het verstrekken van persoonsgegevens aan derden zijn de Grondwet, Wbp, WGBO, Wet BIG. In deze paragraaf ga ik de belangrijkste bepalingen uit bovenstaande wetten nader toelichten.

2.2.1 Grondwet

In de Grondwet zijn verschillende bepalingen opgenomen met betrekking tot privacy. In de grondwet zijn zowel klassieke grondrechten als sociale grondrechten opgenomen. Klassieke grondrechten zijn burgerlijke en politieke rechten en sociale grondrechten zijn economische, sociale en culturele rechten. Beide soorten grondrechten hebben een ander effect op handhaving van de overheid. De klassieke grondrechten beogen onthouding van de overheid, geen inmenging van de overheid. Bij de sociale grondrechten wordt juist overheidsoptreden verwacht. Het recht op privacy is een klassiek grondrecht, burgers hebben het recht op privacy, de overheid mag zich niet mengen in het privéleven van burgers.

In art. 10 GW is bijvoorbeeld het recht op eerbiediging en bescherming van de persoonlijke levenssfeer opgenomen, het recht op privacy. Dit is een klassiek grondrecht, in dit artikel is bepaald dat iedereen, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van de persoonlijke levenssfeer heeft. Hierin is tevens in lid 2 opgenomen dat in de wet nadere regels zijn gesteld ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Verder is in lid 3 bepaald dat de wet regels stelt inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik wat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens. De bepalingen uit lid 2 en 3 worden regelingsverplichtingen genoemd deze bepalingen kunnen niet worden aangemerkt als sociaal grondrecht.[8]

In de Grondwet zijn verder in de artikelen 11, 12 en 13 GW bepalingen opgenomen over de lichamelijke integriteit, het huisrecht en het recht op brief-, telefoon-, telegraafgeheim.[9]

2.2.2 Wet bescherming persoonsgegevens

De Wbp is een kaderwet met een ruime toepassing. De wet is van toepassing op geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens alsmede de niet geautomatiseerde verwerking van persoonsgegevens in verschillende sectoren van het maatschappelijk leven.[10] De Wbp geeft regels voor de verwerking van persoonsgegevens, onder welke voorwaarden persoonsgegevens verwerkt mogen worden en voor welke doeleinden ze verwerkt mogen worden.

Om te beginnen dient uitgelegd te worden wat de begrippen “persoonsgegevens en verwerking van persoonsgegevens” precies inhouden. “Persoonsgegevens” zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

[8] Koekkoek 2000, p. 155-158.
[9] Thole, Van der Jagt & Roerdink 2010, p.15.
[10] De Vries & Rutgers 2001, p.17.

Onder “verwerking van persoonsgegevens” wordt verstaan elke handeling of geheel van handelingen met betrekking tot persoonsgegevens,
waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, samenbrengen, afschermen, uitwissen en vernietigen van gegevens wordt verstaan.

Algemene bepalingen verwerking
Persoonsgegevens mogen op grond van art. 6 Wbp alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt, dit is het zogenaamde rechtmatigheidsbeginsel.[11] Persoonsgegevens moeten op een eerlijke en rechtmatige wijze worden verwerkt. De betrokkene moet kennis kunnen hebben van het bestaan van de verwerking. Verder moet de betrokkene volledig worden ingelicht over de omstandigheden waaronder zijn gegevens kunnen worden verkregen.

In art. 7 Wbp is bepaald dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. Voordat er tot gegevensverzameling kan worden overgegaan dient het doel voor de verzameling vast te staan. De doelomschrijving dient duidelijk zijn, zodat getoetst kan worden of het verzamelen van de gegevens noodzakelijk is voor het gestelde doel.[12]

Persoonsgegevens mogen niet verder verwerkt worden op een wijze die onverenigbaar is met de wet, art.9 Wbp. Om te beoordelen of een verwerking onverenigbaar is wordt rekening gehouden met:
- de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
- de aard van de betreffende gegevens;
- de gevolgen van de beoogde verwerking door de betrokkene;
- de wijze waarop de gegevens zijn verkregen;
- de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Art. 7 en 9 Wbp vormen samen het zogenaamde doelbindingsprincipe.[13]

Persoonsgegevens worden op grond van art. 11 Wbp enkel en alleen verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend ter zake dienend en niet bovenmatig zijn. De verantwoordelijke moet de nodige maatregelen treffen om te waarborgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn. Dit is het zogenaamde kwaliteitsbeginsel.[14]

Gronden voor verwerking
De verwerking van persoonsgegevens dient op een grond voor gegevensverwerking te berusten, deze rechtvaardigingsgronden zijn opgenomen in art. 8 Wbp:
- ondubbelzinnige toestemming van de betrokkene;
- de verwerking is noodzakelijk voor het sluiten of uitvoeren van een overeenkomst;
- de verwerking is noodzakelijk voor het nakomen van een wettelijke verplichting;
- de verwerking is noodzakelijk ter vrijwaring van een vitaal belang van betrokkene;
- de verwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijk taak;
- de verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke.[15]

[11] De Vries & Rutgers 2001, p.22.
[12] MvT, p.79.
[13] Huydecoper 2006, p.28.
[14] De Vries & Rutgers 2001, p.28.
[15] De Vries & Rutgers 2001, p.22-28.

Als de verwerking van persoonsgegevens niet op een van voornoemde rechtvaardigingsgronden berust, is de verwerking onrechtmatig.
Verder dient elke verwerking te voldoen aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel ziet er op toe dat de inbreuk op de belangen van de betrokkene niet onevenredig is in verhouding met het te dienen doel. Het subsidiariteitsbeginsel ziet er op toe dat de verwerkte gegevens in redelijkheid niet op een andere, minder nadelige wijze kunnen worden verwerkt, gezien het te dienen doel.[16]

De toestemming van betrokkene als rechtvaardigingsgrond, geeft beschikkingsmacht aan de betrokkene over zijn gegevens. De toestemmingsgrond is echter geen exclusieve grond, ook op basis van andere gronden kunnen gegevens worden verwerkt. Om op grond van toestemming van de betrokkene gegevens te kunnen verwerken dient de verantwoordelijke zeker te weten dat hij toestemming heeft verkregen van de betrokkene, hier mag geen twijfel over bestaan. Indien hier twijfel over bestaat dient de verantwoordelijke dit na te gaan bij de betrokkene. Verder is in de jurisprudentie bepaald dat bij elke gegevensverwerking moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit. Als de betrokkene erop wijst dat met zijn belangen onvoldoende rekening is gehouden, zal de verwerker alsnog een belangenafweging moeten maken. Als de betrokkene toestemming geeft voor de verwerking neemt dat niet weg dat er altijd een belangenafweging op grond van het proportionaliteitsbeginsel en het subsidiariteitsbeginsel gemaakt moet worden alvorens de gegevens te verwerken.[17]

In voornoemde uitspraak van de Hoge Raad zijn gegevens van betrokkene verwerkt over een betalingsachterstand. Inmiddels heeft de betrokken de vordering voldaan en heeft de verantwoordelijke verzocht om de gegevens te verwijderen. Zowel de rechtbank als het Hof hebben de betrokkene in het gelijk gesteld en de verantwoordelijke opgedragen de gegevens te verwijderen. De Hoge Raad verwerpt het beroep in cassatie. Er dient, voordat er wordt overgegaan tot het verwerken van gegevens op grond van art. 8 Wbp, altijd een belangenafweging te worden gemaakt. Het verplicht maken van een belangenafweging op grond van de beginselen van proportionaliteit en subsidiariteit, geldt niet alleen voor gegevens die worden verwerkt op grond van art. 8 onder f Wbp, maar voor alle verwerkingen op grond van art. 8 Wbp. Verder neemt toestemming van de betrokkene voor de verwerking niet weg dat er een belangenafweging gemaakt moet worden.[18]

Als de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst, is het van belang dat de betrokkene partij is, bij de desbetreffende overeenkomst. Hiermee wordt bedoeld dat de betrokkene bewust moet deelnemen aan de overeenkomst.[19] De betrokkene kan hierdoor zelf toezien op de van hem verwerkte persoonsgegevens. Onder deze rechtvaardigingsgrond valt ook het verwerken van gegevens voor het nemen van precontractuele maatregelen die noodzakelijk zijn voor het sluiten van een overeenkomst. De behandelovereenkomst zoals bedoeld in art. 7:466 BW, tussen een zorgverlener en een patiënt kan gekwalificeerd worden als een desbetreffende overeenkomst.

Om gegevens te kunnen verwerken, omdat dit noodzakelijk is voor het nakomen van een wettelijke verplichting, moet de verwerking getoetst worden aan twee criteria. Er moet sprake zijn van een noodzakelijkheidscriteria en wettelijke verplichting van de verantwoordelijke. De wettelijke verplichting dient noodzakelijkerwijs met zich mee te brengen dat de gegevens worden verwerkt. Het nakomen van de wettelijke verplichting moet redelijkerwijs niet goed mogelijk zijn zonder de betreffende gegevens te verwerken. Er moet een duidelijk verband bestaan tussen de gegevensverwerking en de wettelijke verplichting.

[16] MvT, p.80.
[17] HR 9 september 2011, ECLI:NL:HR:2011:BQ8097.
[18] HR 9 september 2011, ECLI:NL:HR:2011:BQ8097.
[19] Hooghiemstra &Nouwt 2013, p. 47

Verder mogen er niet meer gegevens verwerkt worden dan noodzakelijk is voor het nakomen van de wettelijke verplichting.[20] Niet alleen de verwerking maar ook de verstrekking van persoonsgegevens aan derden kan gerechtvaardigd worden op grond van een wettelijke bepaling, dit is opgenomen in de WGBO.[21]

Van gegevensverwerking op grond van het noodzakelijk vrijwaren van een vitaal belang is sprake, als een ernstig gevaar voor de gezondheid van betrokkene moet worden bestreden. Deze rechtvaardigingsgrond is slechts in beperkte gevallen toepasbaar. Voor toepassing van deze rechtvaardigingsgrond moet er sprake zijn van een dringende (medische) noodzaak. Er moet sprake zijn van levensbedreigende situaties, waarin het een zaak van leven of dood is.

Als de verwerking noodzakelijk is voor de uitvoering van een publiekrechtelijke taak, dient de verwerking toegespitst te zijn op een goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel aan het bestuursorgaan waaraan de gegevens worden verstrekt. Een taak is publiekrechtelijk als deze is gebaseerd op een speciaal voor het openbaar bestuur bij of krachtens de wet geschapen grondslag.[22] Grondslagen voor de verwerking van persoonsgegevens op basis van deze rechtvaardigingsgrond zijn bijvoorbeeld te vinden in de Wet Publieke Gezondheidszorg.

Gegevensverwerking is gerechtvaardigd als deze verwerking noodzakelijk is voor de behartiging van het gerechtvaardigd 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. Deze rechtvaardigingsgrond is een soort vangnet voor als een van de voorgaande rechtvaardigingsgronden niet van toepassing zijn. Deze rechtvaardiginggrond is dan ook veel algemener dan de andere rechtvaardigingsgronden. Voordat gegevens verwerkt mogen worden op grond van deze rechtvaardigingsgrond moeten de belangen van de betrokkene tegen de belangen van de verantwoordelijke of de derde worden afgewogen. Hierbij dienen de beginselen van proportionaliteit en subsidiariteit in acht te worden genomen.[23]

In een uitspraak van het CBP is bepaald dat: wanneer gegevens worden verwerkt ter behartiging van een gerechtvaardigd belang van een derde, vergt het belang van de betrokkene in de regel dat hij vooraf in de gelegenheid wordt gesteld bezwaar te maken tegen een dergelijke voorgenomen verstrekking. Indien de betrokkene bezwaar maakt, dient dit bezwaar meegewogen te worden in de afweging die de verantwoordelijke moet maken.[24]

Beveiliging van persoonsgegevens
In de artikelen 12, 13 en 14 Wbp zijn bepalingen opgenomen over de beveiliging en bescherming van persoonsgegevens. De verantwoordelijke moet op grond van art. 13 Wbp passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen verlies of enige onrechtmatige verwerking.

Deze maatregelen zien toe op het voorkomen van onnodig verzamelen van persoonsgegevens en het voorkomen van verdere verwerking van persoonsgegevens. Indien de gegevens worden verwerkt door een bewerker dient de verantwoordelijke ervoor te zorgen dat de bewerker voldoende beveiligingsmaatregelen treft (art.14 Wbp).[25]

[20] MvT, p.82.
[21] Deze rechtvaardigingsgrond voor het verstrekken van persoonsgegevens aan derden wordt nader toegelicht in paragraaf 2.2.3.
[22] MvT, p.84.
[23] Hooghiemstra & Nouwt 2013, p. 48
[24] CBP 21 mei 2003, z2003-00214.
[25] De Vries & Rutgers 2001, p. 30.

Verder is in art. 12 Wbp een geheimhoudingsplicht opgenomen voor een ieder die handelt onder het gezag van de verantwoordelijke of de bewerker en de bewerker zelf. Zij zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens uitzonderingen in de wet.[26]

Verwerking bijzondere persoonsgegevens
In art. 16 Wbp is een verbod opgenomen voor het verwerken van gevoelige persoonsgegevens. Hieronder dient te worden verstaan de verwerking van persoonsgegevens betreffende iemand godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens. Bijzondere persoonsgegevens kunnen worden opgedeeld in direct en indirecte persoonsgegevens. Een direct bijzonder persoonsgegeven is bijvoorbeeld dat iemand katholiek, joods of moslim is. Een indirect bijzonder persoonsgegeven is een gegeven dat als zodanig niet direct betrekking heeft op een gevoelig kenmerk, maar waaruit wel de aanwezigheid van een gevoelig kenmerk kan worden afgeleid. Bijvoorbeeld als je als lid van de katholieke kerk opgenomen bent in de ledenlijst op de website van de kerk, hieruit kan indirect opgemaakt worden dat jij katholiek bent.[27]

Uitzondering verwerking bijzondere persoonsgegevens
In de artikelen 17 t/m 23 Wbp zijn uitzonderingen op het voormelde verbod opgenomen. Ik ga alleen in op art. 21 Wbp waarin uitzonderingen op het verbod op gegevensverwerking betreffende gezondheid zijn opgenomen. Onder gegevens betreffende iemands gezondheid wordt verstaan de gegevens betreffende de aard van de ziekte, enkel het feit dat iemand ziek is, is geen gezondheidsgegeven betreffende de Wbp. In een uitspraak van het CBP is bepaald dat, gelet op het ruime begrip 'gezondheid', onder omstandigheden, gegevens over IQ en sociaal-emotionele problematiek gezondheidsgegevens kunnen zijn.[28]

In dit artikel is bepaald dat het verbod niet geldt indien de gegevens worden verwerkt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat noodzakelijk is voor de goede behandeling of verzorging van de betrokkene, dan wel voor het beheer van de instelling of beroepspraktijk noodzakelijk is. Verder mogen ook zorgverzekeraars, scholen voor speciaal onderwijs, de Minister van Justitie, bestuursorganen, werkgevers en instellingen die voor hen werkzaam zijn deze bijzondere persoonsgegevens verwerken. In art. 21 Wbp zijn alle afzonderlijke noodzakelijkheidscriteria voor deze instanties opgenomen. [29]

Verder is bepaald dat alleen personen die uit hoofde van hun ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst een geheimhoudingsplicht hebben deze persoonsgegevens betreffende de gezondheid mogen verwerken. In lid 3 is opgenomen dat andere bijzondere persoonsgegevens zoals ras of godsdienst mogen worden verwerkt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat noodzakelijk is als aanvulling op de verwerkte persoonsgegevens met het oog op de goede behandeling of verzorging van de betrokkene.

Verder staat in lid 4 dat het verwerken van persoonsgegevens betreffende erfelijke eigenschappen in beginsel is toegestaan, voor zover de verwerking plaatsvindt met betrekking tot de betrokkene bij wie de betreffende gegevens zijn verkregen.

[26] Hooghiemstra & Nouwt 2013, p. 66
[27] Thole, Van der Jagt & Roerdink 2010, p.75.
[28] CBP 22 april 2003, z2003-00284.
[29] Berkvens & Prins 2007, p.169.

Hier kan van worden afgeweken als er een zwaarwegend geneeskundig belang prevaleert of de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek of statistiek.[30]

In art. 23 Wbp zijn algemene uitzonderingen op het verbod opgenomen. Van het verbod op verwerking van bijzondere persoonsgegevens kan worden afgeweken, bijvoorbeeld met uitdrukkelijke toestemming van de betrokkene of als de betrokkene de gegevens zelf kenbaar heeft gemaakt.

Informatie verstrekking betrokkene
Op grond van art. 33 en 34 Wbp, dient de betrokkene voorafgaand aan de verkrijging van de persoonsgegevens te worden geïnformeerd door de verantwoordelijke. De verantwoordelijke deelt de betrokkene zijn identiteit, en de doeleinden voor de verwerking mede. Indien nodig verstrekt de verantwoordelijke nadere informatie aan de betrokkene. Indien de gegevens niet bij de betrokkene zelf worden verkregen dient de verantwoordelijke informatie te verstrekken aan de betrokkene, zoals in art. 34 lid 2 en 3 Wbp is bepaalt. Deze informatie hoeft niet te worden verstrekt indien de betrokkene reeds op de hoogte is op het moment van vastlegging of wanneer de gegevens bestemd zijn om te worden verstrekt aan derden, en de betrokkene van die verstrekking reeds op de hoogte is op het moment van eerste verstrekking.

Rechten van de betrokkene
In de artikelen 35 t/m 42 zijn de rechten van de betrokkene opgenomen. De betrokkene heeft recht op inzage, correctierecht, recht van verzet en recht op bescherming tegen geautomatiseerde beslissingen.[31]

De betrokkene heeft het recht om zich tot de verantwoordelijke te wenden met het verzoek hem mede te delen of over hem gegevens worden verwerkt en welke gegevens over hem worden verwerkt. De verantwoordelijke is verplicht binnen vier weken schriftelijk mede te delen of er gegevens over de betrokkene worden verwerkt. Hierin dient opgenomen te zijn welke gegevens verwerkt zijn, voor welke doeleinden deze verwerkt zijn, de categorie van gegevens waarop de verwerking betrekking heeft, de ontvangers van de gegevens en de eventuele beschikbare informatie over de herkomst van de gegevens. [32]

Het correctierecht is opgenomen in art. 36 Wbp, de betrokkene kan de verantwoordelijke verzoeken de verwerkte gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. De betrokkene kan de correctieverzoek indienen als de gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins worden verwerkt in strijd met wettelijke voorschriften.[33]

Het recht van verzet is opgenomen in art. 40 en art. 41 Wbp. Het recht van verzet kan worden opgedeeld in twee categorieën, namelijk relatief verzet en absoluut verzet. Als de gegevens van betrokkene rechtmatig worden verwerkt op grond van art. 8 sub e of f Wbp kan de betrokken verzet aantekenen vanwege bijzondere persoonlijke omstandigheden. Dit is het geval wanneer de verwerking noodzakelijk is voor de vervulling van een publiekrechtelijke taak of noodzakelijk is voor de behartiging van het gerechtvaardigd belang. Dit wordt relatief verzet genoemd. [34] In art. 41 Wbp is het recht op absoluut verzet opgenomen. Tegen verwerking van persoonsgegevens voor directe marketingdoeleinden kan ten alle tijden verzet worden aangetekend.

[30] Hooghiemstra & Nouwt 2013, p. 89.
[31] Huydecoper 2006, p.38.
[32] Thole, Van der Jagt & Roerdink 2010, p.49.
[33] Hooghiemstra & Nouwt 2013, p. 152-153
[34] Thole, Van der Jagt & Roerdink 2010, p.52.

De hoofdregel is dat er voorafgaande toestemming van betrokkene nodig is om voor het gebruik van persoonsgegevens voor commerciële, charitatieve en ideële doeleinden, tegen dergelijke verwerkingen staat absoluut verzet open.

2.2.3 WGBO

De WGBO is opgenomen in boek 7 van het Burgerlijk Wetboek (hierna: BW), de WGBO is met name gericht op de privaatrechtelijke verhouding tussen hulpverleners en patiënten.[35] In de WGBO zijn verschillende rechten van de patiënt opgenomen zoals het recht op informatie, het toestemmingsvereiste, het recht op inzage en het recht op privacy en geheimhouding van medische gegevens.

Het recht op informatie is opgenomen in art. 7:448 BW, de hulpverlener is verplicht de patiënt in te lichten over het voorgenomen onderzoek, de behandeling en de gezondheidstoestand van de patiënt. Voor de uitvoering van de behandelovereenkomst is toestemming van de patiënt vereist, dit is bepaald in art. 7:450 BW.[36]

In art. 7:454 BW is een dossierplicht voor hulpverleners opgenomen. Hulpverleners zijn verplicht een dossier bij te houden met betrekking tot de behandeling van de patiënt. In het dossier worden aantekeningen van de gegevens omtrent de gezondheid van de patiënt, ten diens aanzien uitgevoerde verrichtingen en andere stukken opgenomen die voor de goede hulpverlening noodzakelijk zijn.[37] De patiënt heeft op zijn beurt weer het recht om een verzoek in te dienen ter vernietiging van het dossier of tot inzage van het dossier, art. 7:455 en 7:456 BW.

Medisch beroepsgeheim

In de WGBO is een geheimhoudingsplicht opgenomen in art. 7:457 BW. De hulpverlener draagt er zorg voor dat er geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden worden verstrekt aan een ander dan de patiënt, tenzij de patiënt daar toestemming voor heeft gegeven. Dit artikel ziet toe op het recht op privacy en geheimhouding van medische gegevens van de patiënt.

Op het verbod om geen medische gegevens betreffende een patiënt te verstrekken aan derden zijn enkele uitzonderingen. In de volgende gevallen mogen inlichtingen en inzage worden verstrekt aan derden:

- Als diegene rechtstreeks betrokken is bij de uitvoering van de behandelingsovereenkomst (7:457 lid 1);
- Als diegene optreedt als vervanger van de hulpverlener (7:457 lid 1);
- Als diegene de wettelijk vertegenwoordiger van de patiënt is (7:457 lid 2);

De verstrekking van medische gegevens aan de rechtstreeks betrokkene en de vervanger van de hulpverlener moet noodzakelijk zijn voor de door hen in dat kader te verrichten werkzaamheden. Indien de hulpverlener door inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, verstrekt hij deze gegevens niet.[38]

Het beroepsgeheim is niet absoluut en kan worden doorbroken. De redenen voor doorbreking zijn een wettelijke plicht, toestemming van de patiënt of een conflict van plichten. Bij een conflict van plichten wordt een hulpverlener geconfronteerd met een andere plicht die in strijd is met het bewaren van het beroepsgeheim.

[35] Berkvens & Prins 2007, p. 171.
[36] Leenen & Gevers 2011, p.203-206.
[37] *Richtlijnen inzake het omgaan met medische gegevens*, KNMG, 2010, p.2.
[38] Bannier e.a. 2008, p. 91-94.

Om te spreken van een conflict van plichten moet aan verschillende voorwaarden voldaan zijn:

- De hulpverlener moet geprobeerd hebben toestemming te krijgen van de patiënt;
- Als het geheim niet wordt doorbroken lijdt een ander ernstige schade;
- De arts is in gewetensnood;
- Het doorbreken van het beroepsgeheim voorkomt of beperkt de schade voor de ander;
- Er moet voldaan worden aan de eisen van proportionaliteit, het geheim moet zo min mogelijk worden geschonden.[39]

We kunnen dus concluderen dat er zes redenen zijn om af te wijken van het beroepsgeheim en het verbod om medische gegevens te verstrekken aan derden. Deze reden zijn:

- Met toestemming van de patiënt;[40]
- Als diegene rechtstreeks betrokken is bij de uitvoering van de behandelingsovereenkomst;
- Als diegene optreedt als vervanger van de hulpverlener
- Als diegene de wettelijk vertegenwoordiger is van de patiënt;
- Een wettelijke plicht;
- Een conflict van plichten.[41]

2.2.4 Wet BIG

In art. 88 Wet BIG is de geheimhoudingsplicht voor medische hulpverleners vastgelegd. Conform art. 88 Wet BIG is een ieder verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd. Onder “het geheim” wordt verstaan, het toevertrouwen van een geheim, het ter kennis komen van een geheim of het ter kennis komen van informatie waarvan het vertrouwelijk karakter begrepen moet worden.[42]

2.3 Toekomstige wetgeving

De huidige privacyregelgeving zal binnenkort gewijzigd worden. Zowel de richtlijn 95/46/EG als de Wbp zullen worden vervangen door de op 25 januari 2012 gepubliceerde voorstel privacyverordening. De wijzigingen die deze verordening met zich mee zal brengen worden in de volgende paragraaf besproken.

2.3.1 Voorstel privacyverordening

Door de Europese commissie is er een voorstel privacyverordening opgesteld in 2012. Wanneer de verordening zal worden aangenomen en inwerking zal treden is nog onduidelijk. Deze privacyverordening zal er uiteindelijk toe leiden dat privacyrichtlijn 95/46/EG vervalt en dat de tekst van de privacyverordening wordt opgenomen in de Wbp. De privacyverordening zal leiden tot een aanscherping van de regels met betrekking tot de verwerking van persoonsgegevens. Met name door alle technische ontwikkelingen zal de voorgestelde verordening heel wat wijzigingen met zich meebrengen.[43]

De belangrijkste en meest ingrijpende wijzigingen die zullen worden doorgevoerd, als de voorstel privacyverordening van kracht gaat, zijn:

- Ruimere informatieplicht;
- Het recht van betrokkene om “vergeten te worden”;
- De betrokkene kan makkelijker gegevens overdragen aan een andere verantwoordelijke (het recht op gegevensoverdraagbaarheid);

[39] Bannier e.a. 2008, p. 15-16 en 94.
[40] CBP 26 februari 2004, z2003-01597.
[41] Centraal Tuchtcollege voor de Gezondheidszorg 10 februari 2005, 2004/161.
[42] *Informatieblad geheimhouding van medische gegevens*, CBP, 2011.
[43] Lassche 2014, p. 4-6.

- Het verplicht voeren van een privacybeleid;
    - Het verplichten van documentatie over de verwerking van persoonsgegevens;
    - Het verplicht uitvoeren van privacyeffectbeoordelingen (PIA);
    - Het verplicht aanstellen van een functionaris voor gegevensbescherming;
- Het verplicht melden van datalekken aan toezichthoudende autoriteit en betrokkene;
- Het opleggen van boetes bij niet-naleving van de privacyverordening.

Ruimere informatieplicht
In de verordening zijn verschillende aanvullingen op de informatieplicht opgenomen. Zo moeten inlichtingen aan de betrokkene worden verstrekt over zijn rechten, zoals het recht op rectificatie, het recht om persoonsgegevens te laten wissen en het klachtrecht. Verder moet informatie worden verstrekt over de bewaartermijn, waaruit de gegevens afkomstig zijn en of de intentie bestaat om de persoonsgegevens te verstrekken aan derde landen.[44]

Het recht om "vergeten" te worden
Een nieuw recht van de betrokkene is opgenomen in art. 17 dit is het recht om vergeten te worden. Dit recht is een uitwerking van het recht om niet relevante of onjuiste persoonsgegevens te laten wissen.[45] De betrokkene kan bij de verantwoordelijke een verzoek indienen om "vergeten te worden". De gegevens moeten gewist worden als het voor de doeleinden waarvoor ze zijn verkregen niet langer noodzakelijk is om de gegevens te bewaren, als de betrokkene zijn toestemming intrekt, als de betrokkene bezwaar maakt of de verwerking onrechtmatig is. De verantwoordelijke is verplicht de gegevens te wissen als er geen sprake is van een uitzonderingsgrond zoals opgenomen in lid 3.

Indien de gegevens openbaar zijn gemaakt, dient de verantwoordelijke derden op de hoogte te stellen van het verzoek van betrokkene. De verantwoordelijke dient derden te verzoeken om iedere koppeling naar een kopie of reproductie van de persoonsgegevens uit te wissen. In dit artikel is ook het recht om in bepaalde gevallen de verwerking te laten beperken opgenomen.

Het recht op gegevensoverdraagbaarheid
In art. 18 van de verordening is bepaald dat de betrokkene het recht heeft om zijn gegevens van het ene elektronische verwerkingssysteem naar het andere over te dragen. De verantwoordelijke mag dit niet weigeren. De betrokkene heeft het recht om deze gegevens te ontvangen in een gestructureerd en algemeen gebruikt formaat. Dit recht ziet erop toe dat de toegang van betrokkenen tot hun persoonsgegevens wordt verbeterd.

Verplicht voeren privacybeleid
Art. 22 van de privacyverordening legt aan de verantwoordelijke de verplichting op om privacybeleid te voeren. De verantwoordelijke dient passende maatregelen te nemen, om ervoor te zorgen dat de verwerking van persoonsgegevens in overeenstemming met de verordening wordt uitgevoerd.

Hieronder valt de verplichting om documentatie te voeren over de verwerking van persoonsgegevens uit artikel 28. In deze documentatie dient in ieder geval de naam en de contactgegevens van de verantwoordelijke, de verkregen toestemming van de betrokkene, doeleinden voor verwerking, een beschrijving van de categorieën betrokkenen, een beschrijving van hen betreffende persoonsgegevens en de ontvangers van persoonsgegevens te worden opgenomen.[46]

[44] Voorstel verordening 2012/0011, p.32.
[45] Engelfriet 2014, p.4.
[46] Art. 28 Voorstel verordening 2012/0011, p. 66-67.

Verder valt ook de verplichting om een privacyeffectbeoordeling uit te voeren onder het te voeren privacybeleid. Als de verwerkingen van persoonsgegevens gezien hun aard, reikwijdte of doeleinden bijzondere risico's inhouden voor de rechten en vrijheden van de betrokkenen, dient er eerst een privacyeffectbeoordeling plaats te vinden voordat de verwerking plaatsvindt.[47]

In art. 35 is de verplichting opgenomen om een functionaris voor gegevensbescherming aan te stellen. Iedere organisatie die van meer dan 250 werknemers heeft, dient een functionaris voor gegevensbescherming aan te stellen. De functionaris ziet toe op de uitvoering en toepassing van het verplicht uit te voeren beleid en de uitvoering en toepassing van de verordening met betrekking tot de bescherming van persoonsgegevens.

Meldplicht datalekken
In art. 31 en 32 van de verordening is een meldplicht voor datalekken opgenomen. Als er een inbreuk wordt gemaakt in verband met persoonsgegevens dient zowel de toezichthoudende autoriteit als de betrokkene op de hoogte te worden gesteld van deze inbreuk. Dit dient niet later dan 24 uur nadat de inbreuk is opgemerkt te geschieden. Indien de melding toch later dan 24 uur nadat de inbreuk is opgemerkt geschiedt, dient er verantwoording te worden afgelegd over de verlate melding.

Boetes
In art. 53 jo. art. 79 van de verordening is bepaald dat de toezichthoudende autoriteit administratieve sancties op kan leggen bij niet-naleving van de verordening. De administratieve sanctie dient in elke zaak doeltreffend, evenredig en afschrikkend te zijn. De administratieve geldboete wordt vastgesteld aan de hand van de aard, de ernst en de duur van de inbreuk. Verder wordt ook gekeken of de inbreuk opzettelijk of uit nalatigheid is gepleegd, de mate waarin de natuurlijke of rechtspersoon aansprakelijk is en of er al eerder inbreuken zijn gepleegd, de technische en organisatorische maatregelen die ten uitvoer zijn gelegd en de mate waarin met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen. De hoogste boete die kan worden opgelegd is 1.000.000 euro of 2% van de gehele wereldwijde jaaromzet.[48]

[47] Art. 33 Voorstel verordening 2012/0011, p. 71.
[48] Art. 79 Voorstel verordening 2012/0011, p. 103-104.

3. Verwerken van persoonsgegevens

In dit hoofdstuk wordt besproken hoe de persoonsgegevens van patiënten binnen Ziekenhuis Rivierenland worden verwerkt.

3.1 Persoonsgegevens

Binnen Ziekenhuis Rivierenland worden dagelijks honderden persoonsgegevens verwerkt. Niet alleen naam, geboortedatum, BSN maar ook de medische gegevens en de medicatie gegevens worden verwerkt. Zoals we al in het vorige hoofdstuk zagen bestaat er een verschil tussen “algemene” persoonsgegevens en bijzondere persoonsgegevens. Binnen het ziekenhuis worden beide type persoonsgegevens verwerkt.

Als een patiënt voor de eerste keer in het ziekenhuis komt, moet hij zich registeren als patiënt. Dit gebeurt door middel van het aanmaken van een patiëntenpas. De volgende persoonsgegevens van een patiënt worden opgenomen op de pas: foto, naam, geboortedatum, BSN en patiëntennummer. De aangemaakte patiëntenpas geldt als identiteitsbewijs binnen het ziekenhuis. Op grond van art. 6 van de Wet gebruik burgerservicenummer in de zorg jo. art. 1 van de Wet op de identificatieplicht is het ziekenhuis verplicht om de identiteit van de patiënt vast te stellen en het BSN op te nemen in het dossier.[49]

Vervolgens wordt bij een consult of opname van de patiënt de anamnese afgenomen. Hierbij worden de persoonsgegevens van de patiënt gecheckt en worden persoonsgegevens met betrekking tot de gezondheidstoestand van de patiënt verwerkt, in het dossier en het informatiesysteem van de betreffende afdeling. Het doel van de anamnese is om zo veel mogelijk informatie te verkrijgen over de gezondheidstoestand van de patiënt. De medische gegevens die worden verwerkt zijn bijzondere persoonsgegevens die geplaatst kunnen worden in de categorie: gegevens betreffende iemands gezondheid op grond van art. 16 jo. art. 21 Wbp.

3.2 Wijze waarop persoonsgegevens worden verwerkt

Binnen Ziekenhuis Rivierenland kan een onderscheid gemaakt worden tussen geheel of gedeeltelijk geautomatiseerde gegevensverwerking en niet-geautomatiseerde gegevensverwerking. De eerste categorie ziet toe op de verwerking van persoonsgegevens in het elektronisch patiëntendossier. De laatste categorie ziet toe op handmatig verzamelde gegevens. Deze handmatig verzamelde gegevens zijn bestemd om opgenomen te worden in een bestand. Dit kan bijvoorbeeld een dossierverzameling zijn, die logisch is gerangschikt door middel van elektronisch bestand met een verwijssysteem.[50] De papieren dossiers die zijn opgeslagen in het medisch archief van Ziekenhuis Rivierenland vallen onder deze categorie van niet-geautomatiseerde gegevens. Ongestructureerde handmatige dossiers, die niet bestemd zijn om opgenomen te worden in het medisch archief, vallen niet onder de Wbp.[51]

Persoonsgegevens van de patiënt worden in Ziekenhuis Rivierenland door verschillende mensen verwerkt. Er worden persoonsgegevens verwerkt door onder meer medisch specialisten, verpleegkundigen, fysiotherapeuten, polikliniek assistentes, secretaresses en stagiaires. De medische gegevens van de patiënt worden verzameld bij het eerste consult van de patiënt bij een medisch specialist. Deze gegevens worden vastgelegd en geordend in het dossier van de patiënt, dit kan zowel digitaal als op papier. De dossiers worden vervolgens bewaard in het systeem of in het medisch archief. Op het moment dat er ontwikkelingen zijn in het zorgproces van de patiënt worden de gegevens, waar nodig, bijgewerkt en gewijzigd, zodat het dossier altijd up-to-date is.

---

[49] Patiëntenpas en identificatieplicht, www.zrt.nl (zoek bij patiënten → patiëntenpas en identificatie)
[50] Thole, Van der Jagt & Roerdink 2010, p.20.
[51] L.B. Sauerwein en J.J. Linnemann 2002, p.15.

De persoonsgegevens die zijn vastgelegd in het dossier kunnen worden opgevraagd, geraadpleegd of gebruikt door het medisch personeel van het ziekenhuis als zij hiervoor geautoriseerd zijn. Verder kunnen de persoonsgegevens van een patiënt ook worden verstrekt aan derden als deze direct betrokken zijn bij de behandeling van de patiënt of als de patiënt hiervoor zijn toestemming geeft. Een patiënt kan ook inzage krijgen in zijn eigen dossier, gegevens laten wijzigen, laten uitwissen of vernietigen. Als de bewaartermijn van het dossier verstreken is worden de gegevens vernietigd, de standaard bewaartermijn is 15 jaar.

Welke gegevens digitaal of op papier worden verwerkt, verschilt per afdeling en per behandeling. Iedere afdeling heeft zijn eigen protocollen en richtlijnen met betrekking tot de behandeling van patiënten. Er zijn wel verschillende standaard formulieren, die gebruikt worden in heel het ziekenhuis voor de verwerking van persoonsgegevens, bijvoorbeeld het opname formulier en het anamnese formulier. Doordat afdelingen niet allemaal met dezelfde systemen werken is het lastig om de precieze wijze van verwerking in kaart te brengen.

3.3 Doeleinden voor verwerking

Alle persoonsgegevens dienen met een uitdrukkelijk omschreven, welbepaald en gerechtvaardigd doel te worden verwerkt. De “algemene” persoonsgegevens mogen alleen worden verwerkt als de verwerking berust op een van de rechtvaardigingsgronden uit art. 8 Wbp. De bijzondere persoonsgegevens (medische gegevens) mogen alleen verwerkt worden als dit noodzakelijk is met het oog op een goede behandeling of verzorging van de patiënt, dan wel noodzakelijk is voor het beheer van ziekenhuis. Ziekenhuis Rivierenland verwerkt persoonsgegevens voor verschillende doeleinden. Het hoofddoel om medische gegevens te verwerken binnen Ziekenhuis Rivierenland is het bieden een goede behandeling, verantwoorde en veilige zorg. Er zijn daarnaast nog een paar nevendoelstellingen waarvoor medische gegevens worden verwerkt. De verwerking van medische gegevens vindt namelijk plaats voor doeleinden zoals, het ondersteunen van onderwijs, het ondersteunen van intercollegiale toetsing, ondersteunen van wetenschappelijk onderzoek en ten behoeve van een doelmatig beleid en beheer van het ziekenhuis.

De verwerking van “algemene” persoonsgegevens heeft als doel het nakomen van de zorgovereenkomst tussen het ziekenhuis en de patiënt. Verwerking van medische persoonsgegevens binnen het ziekenhuis is noodzakelijk om een goede behandeling en verzorging van de patiënt te garanderen. Als alle gegevens, zowel “algemene” persoonsgegevens als medische gegevens, van een patiënt worden verwerkt, komt dit ten goede aan de patiëntveiligheid. Bijvoorbeeld op het gebied van medicatieveiligheid, als een arts alle medische gegevens van een patiënt kan inzien, kan er ook bepaald worden welke medicatie kan worden voorgeschreven. Soms komt het voor dat een patiënt allergisch is voor een bepaald medicijn, doordat dit bekend is, kan een ander medicijn voorgeschreven worden. Daarom is het van belang dat, de bij een behandeling betrokken zorgverleners over alle relevante persoonsgegevens van de patiënt kunnen beschikken.

3.4 Systemen

In het ziekenhuis wordt gebruik gemaakt van verschillende systemen voor het verwerken van persoonsgegevens. Er kan zoals eerder besproken een onderscheid gemaakt worden tussen geheel of gedeeltelijk geautomatiseerde verwerking en niet-geautomatiseerde verwerking. Allereerst worden gegevens niet-geautomatiseerd, maar handmatig verwerkt in papieren dossiers. Alvorens de geautomatiseerde verwerking door middel van de verschillende elektronische informatiesystemen toe te lichten, ga ik eerst het een en ander toelichten over de papieren dossiers.

Op de afdeling zorgadministratie worden alle papieren dossiers beheerd. Ieder specialisme heeft zijn eigen dossier, zij zijn de enige die gegevens in dat dossier verwerken.

Doordat ieder specialisme één dossier heeft kan een patiënt wel tien verschillende dossiers hebben. Bij de zorgadministratie kunnen de dossier worden opgevraagd middels een digitale aanvraag waarin het unitnummer en een specifieke code dient te worden vermeld.
Als degene die het dossier opvraagt geautoriseerd is om het dossier op te vragen en in te zien wordt het dossier aan diegene verstrekt. De zorgadministratie registreert alle inkomende en uitgaande dossiers. Ieder specialisme heeft in principe recht op zijn eigen dossiers, sommige specialisme mogen meerdere dossiers inzien indien dit noodzakelijk is voor een goede behandeling. De zorgadministratie hanteert hiervoor een autorisatiematrix.

Het dossier is ingedeeld in drie delen, in het eerste deel zit de correspondentie, in het tweede deel zit de anamnese, het zorgplan, alles wat tijdens de consulten wordt besproken en de notities van de arts. In het laatste deel zitten alle uitslagen van onderzoeken. Van bijna alle patiënten in het ziekenhuis zijn nog papieren dossiers. Alleen van nieuwe patiënten van de afdelingen neurologie, plastische chirurgie, urologie en kindergeneeskunde zijn geen papieren dossiers beschikbaar. De dossiers van deze patiënten zijn volledig geautomatiseerd, in het EPD van het ziekenhuis.[52]

De geautomatiseerde verwerking geschiedt door middel van verschillende elektronische informatiesystemen. Binnen ziekenhuis Rivierenland wordt gebruik gemaakt van systemen zoals Soarian, X/Care, Glims, Syngo en nog vele andere systemen.[53] De belangrijkste systemen zullen achtereenvolgens worden besproken.

Soarian is het elektronisch patiëntendossier (Hierna: EPD) van het Ziekenhuis, waarin alle persoonsgegevens worden verzameld en verwerkt. Soarian zorgt ervoor dat alle persoonsgegevens uit verschillende systemen samen worden gevoegd in een volledig elektronisch patiëntendossier. Verder stemt Soarian trajecten op elkaar af waarbij verschillende afdelingen betrokken zijn en stelt juiste behandelmethoden voor.

X/Care is het Ziekenhuis informatiesysteem (ZIS), X/Care biedt geautomatiseerde ondersteuning van zorgtaken, taken op administratief gebied en organisatorisch gebied. Xcare is het bronsysteem dat gekoppeld is aan verschillende deelsystemen voor wat betreft persoonsgegevens, gegevens voor onderzoeksaanvragen en -uitslagen en factureringsgegevens. Op de meeste afdelingen wordt gewerkt met X/Care, de volgende taken worden verricht in X/Care:

- Afspraken- en onderzoeksplanning
- Opnameregistratie
- Registreren en afhandelen van SEH bezoeken
- Dossierbeheer (papieren dossiers)
- Het aanvragen van laboratorium- en radiologie-onderzoeken
- Het raadplegen van laboratoriumuitslagen en radiologie-verslagen
- Verslaglegging
- Het registreren van DBC's en verrichtingen t.b.v. facturering
- Het aanleveren van gegevens aan externe instanties als Landelijke Medische Registratie (LMR) en Landelijke Ambulante Zorg Registratie (LAZR).[54]

Bij het laboratorium wordt gewerkt met Glims, Glims is het laboratorium Informatie Management Systeem. In Glims worden alle onderzoeksresultaten van patiënten verwerkt. De Röntgen afdeling werkt met Syngo, Syngo is het Röngen Informatie Systeem. In dit systeem worden alle persoonsgegevens en röntgen foto's van de patiënt verwerkt.

[52] Zie bijlage 5: Interview Layla Mulay.
[53] Zie bijlage 12: Overzicht systemen.
[54] Zie bijlage 13: Basis Handleiding X/Care, ZRT.

Bijna ieder specialisme werkt naast X/Care en Soarian nog met andere systemen om specifieke specialistische gegevens te verwerken. Deze systemen worden verder niet besproken.[55]

3.5 Beveiliging persoonsgegevens

Het eerste beveiligingsinstrument, voor de beveiliging van medische gegevens, is natuurlijk het medisch beroepsgeheim. Op zorgverleners zoals artsen, verpleegkundigen, verzorgende en andere medische hulpverleners rust een medisch beroepsgeheim.[56]

In art. 13 Wbp is bepaald dat de verantwoordelijke technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Aan de beveiliging van persoonsgegevens worden verschillende eisen gesteld, deze eisen zijn opgenomen in de NEN 7510 norm.[57] Deze norm ziet toe op de informatiebeveiliging in de gezondheidszorg en ziet toe op alle mogelijke manieren waarop informatie wordt weergegeven, vastgelegd en overgedragen. Onder de informatiebeveiliging in de zorg wordt verstaan: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die nodig is om patiënten verantwoorde zorg te kunnen bieden.[58] Binnen Ziekenhuis Rivierenland is de NEN 7510 dan ook geïmplementeerd als de maatstaf voor beveiliging van persoonsgegevens.[59]

Naast de NEN 7510 norm zijn er nog drie normen die als aanvulling dienen op de NEN 7510 norm. Dit zijn de NEN 7511, NEN 7512 en de NEN 7513. NEN 7511 bevat toetsbare voorschriften voor solopraktijken en complexe organisaties. De NEN 7512 ziet toe op de verstrekking van persoonsgegevens tussen zorgverleners onderling en aan patiënten. De NEN 7512 speelt een grote rol in de beveiliging van persoonsgegevens die verstrekt worden aan derden.[60] NEN-7513 ziet volledig toe op de logging, het vastleggen van acties in elektronische patiëntendossiers, zodat het mogelijk is de rechtmatigheid van de toegang tot dossiers te controleren.

In beginsel worden alle verwerkingshandelingen binnen Ziekenhuis Rivierenland gelogd, dit betekent dat alle acties die plaats hebben gevonden met betrekking tot persoonsgegevens worden geregistreerd. Zoals het vastleggen, bijwerken, bewaren en inzien van de persoonsgegevens. Verder wordt er precies geregistreerd wanneer de actie heeft plaatsgevonden en wie de actie heeft uitgevoerd. Hierdoor kan gecontroleerd worden of persoonsgegevens zijn ingezien door onbevoegden.[61] Dit is gebeurt echter niet in alle systemen, in het informatiesysteem van het laboratorium Glims vindt bijvoorbeeld geen logging plaats. Verder wordt ook niet gelogd wie papieren dossiers heeft ingezien, dit kan dan ook niet worden gecontroleerd. Er wordt enkel bijgehouden aan wie het dossier wordt uitgeleend, wat er vervolgens mee gebeurd wordt niet gelogd.

Verder worden de persoonsgegevens beveiligd door inlogcodes. Door middel van inlogcodes worden de gegevens afgeschermd voor onbevoegden. Aan de hand van een autorisatiematrix is bepaald wie welke persoonsgegevens mag inzien. Op dit moment wordt er binnen ziekenhuis Rivierenland gewerkt aan een nieuwe autorisatiematrix. Deze nieuwe autorisatiematrix is van belang om de gegevens nog meer te kunnen afschermen voor onbevoegden en de privacy van patiënten te kunnen waarborgen.[62]

---

[55] Zie bijlage 12: Overzicht systemen.
[56] Berkvens & Prins 2007, p.161.
[57] Norm ontwikkeld door het Nederlands Normalisatie-instituut.
[58] Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm, CBP, 2008, p.31.
[59] *Norm NEN 7510*, Nederlands Normalisatie-instituut, 2011.
[60] Zie paragraaf 4.6
[61] *Gedragscode Elektronische gegevens uitwisseling in de Zorg*, KNMG & Nictiz, 2013.
[62] *Toegang tot digitale patiëntendossiers binnen zorginstellingen,* CBP, 2013, p. 6-10.

4. Verstrekking van persoonsgegevens aan derden

In dit hoofdstuk wordt in kaart gebracht hoe de verstrekking van persoonsgegevens van Ziekenhuis Rivierenland aan derden geschiedt. Eerst wordt toegelicht welke persoonsgegevens worden verstrekt, op welke wijze zij worden verstrekt en voor welke doeleinden zij worden verstrekt aan derden. Verder zullen de systemen waarmee gegevens worden verstrekt en de beveiliging van de verstrekte persoonsgegevens worden toegelicht.

4.1 Persoonsgegevens

Naast de honderden gegevens die per dag binnen Ziekenhuis Rivierenland worden verwerkt, zoals besproken in hoofdstuk 3, worden er dagelijks honderden persoonsgegevens verstrekt aan derden. Gegevens die verstrekt worden aan derden verschillen van “algemene” persoonsgegevens zoals naam, adres, geboortedatum en BSN tot bijzondere persoonsgegevens zoals medicatiegegevens en onderzoekuitslagen. Het laboratorium stuurt bijvoorbeeld elke dag een lijst met labuitslagen door naar de Regioapotheek die gevestigd is in het ziekenhuis.

Op iedere afdeling worden gegevens verstrekt aan derden. Op verpleegafdelingen worden bijvoorbeeld gegevens verstrekt aan de contactpersoon van de patiënt of aan de huisarts van de patiënt. Als een patiënt in een verzorgingstehuis woont, moet bijvoorbeeld de verzorgingshuisarts worden ingelicht over hoe het met de patiënt gaat. In principe mogen alleen medewerkers die direct betrokken zijn bij de behandeling van de patiënt gegevens verstrekken aan derden. In de praktijk is het echter zo dat secretaresses, of afdelingsassistenten met toestemming van een medisch specialist of verpleegkundige enz. gegevens verstrekken aan derden.

4.2 Wijze waarop persoonsgegevens worden verstrekt aan derden

Persoonsgegevens worden zowel digitaal, per post, fax en telefonisch verstrekt aan derden. Gegevens die digitaal worden verstrekt, worden via een van de informatiesystemen van Ziekenhuis Rivierenland verstrekt aan de derden. Welke gegevens precies via welk systeem worden verstrekt wordt in paragraaf 4.5 besproken. Verder worden er veel persoonsgegevens via beveiligde verbindingen, de post, onbeveiligde e-mail, fax en in enkele gevallen telefonisch verstrekt aan derden.

Sommige gegevens worden “automatisch” aan derden verstrekt, zoals lab uitslagen of röntgen foto’s die rechtstreeks door de huisarts zijn aangevraagd. De uitslagen van deze onderzoeken worden rechtstreeks, via een beveiligde verbinding verzonden aan de betreffende huisarts. [63] Als een huisarts een patiënt doorverwijst naar het ziekenhuis, gaat dit middels een verwijsbrief die wordt verstuurd over een beveiligde lijn.[64] Als de patiënt na behandeling in het ziekenhuis weer naar huis mag, gaat er via die beveiligde lijn een ontslagbrief naar de huisarts.

Verder worden er vaak persoonsgegevens verstrekt via de post, e-mail of fax, als er geen beveiligde verbinding is tussen het ziekenhuis en de zorgverlener. In enkele gevallen worden telefonisch persoonsgegevens versterkt. Bij onderzoeken die Ziekenhuis Rivierenland niet kan uitvoeren, zoals pathologisch onderzoek of microbiologisch onderzoek, worden de kweekjes via de post en de “algemene” persoonsgegevens via de beveiligde verbinding verzonden naar een ander ziekenhuis. Verder komt het voor dat een patiënt graag zelf een kopie van zijn dossier, of een onderzoeksuitslag wil hebben, deze kunnen patiënten aanvragen en vervolgens zelf komen ophalen. Zij moeten zich bij ontvangst legitimeren, zodat zeker is dat de gegevens aan de juiste persoon worden verstrekt.

[63] Beveiligde verbindingen zijn: Zorgmail en Portavita
[64] Beveiligde verbinding is: Zorgdomein

Er kan dus een onderscheid gemaakt worden tussen geheel of gedeeltelijk geautomatiseerde verstrekking of niet-geautomatiseerde verstrekking. Een groot deel van de gegevens wordt al geautomatiseerd verstrekt via een beveiligde verbinding. Ziekenhuis Rivierenland heeft echter niet met elke zorgverlener in de omgeving een beveiligde verbinding, dus zullen er nog altijd gegevens niet-geautomatiseerd worden verstrekt. Daarnaast is het zo dat nog niet alle persoonsgegevens binnen Ziekenhuis Rivierenland gedigitaliseerd zijn. Verder is het nog niet mogelijk om gegevens zoals röntgenbeelden of hartfilmpjes te versturen via de beveiligde verbinding. Dit komt omdat de verbindingen van Ziekenhuis Rivierenland nog niet geschikt zijn voor de verstrekking van beelden, deze beelden worden dus altijd via de post verstrekt, of ze moeten worden opgehaald in het ziekenhuis.[65]

4.3 Doeleinden voor verstrekking aan derden

De verstrekking van persoonsgegevens dient op een uitdrukkelijk omschreven, welbepaald en gerechtvaardigd doel te berusten. Het is belangrijk dat persoonsgegevens alleen verstrekt worden als dit op een wettelijke grondslag berust. De persoonsgegevens van Ziekenhuis Rivierenland worden in zijn algemeenheid verstrekt aan derden met als doel om de patiëntveiligheid te verbeteren en een goede behandeling en verzorging van de patiënt te kunnen garanderen.

Verder wordt er altijd naar gestreefd om de persoonsgegevens enkel te verstrekken als er zekerheid bestaat dat de derde een directe behandelrelatie heeft met de patiënt of dat de patiënt toestemming heeft gegeven voor de verstrekking. Dat er sprake is van een directe behandelrelatie, wordt vaak al snel geconcludeerd. Aanvragen van huisartsen en andere ziekenhuizen worden vaak gehonoreerd, zonder na te trekken of de aanvraag ook daadwerkelijk van die zorgverlener afkomstig is. Niet alle afdelingen houden zich even strikt aan de vereiste behandelrelatie of toestemming. Bij de afdeling radiologie worden de persoonsgegevens in de meeste gevallen direct verstrekt als ze een aanvraag binnenkrijgen van bijvoorbeeld een ziekenhuis. Zij vragen niet naar toestemming van de patiënt, ze gaan er direct van uit dat er een behandelrelatie bestaat met de patiënt.[66] De SEH verstrekt echter alleen persoonsgegevens aan een ander ziekenhuis als zij een toestemmingsformulier van de patiënt doorsturen, zonder toestemming van de patiënt worden er in principe geen gegevens verstrekt.[67]

4.4 Partijen

Zoals eerder vermeld worden er aan verschillende partijen gegevens verstrekt. Niet alleen aan huisartsen, apothekers, verzorgingshuisartsen en andere ziekenhuizen. Maar ook aan huisartsposten en samenwerkingsverbanden zoals ECT. Verder worden er gegevens verstrekt aan zorgverleners zoals fysiotherapeuten, diëtisten en andere zelfstandige zorgverleners. De laatste categorie zorgverleners hebben vaak geen groot computersysteem, waardoor er geen beveiligde verbinding gemaakt kan worden met deze zorgverleners. Verstrekking van persoonsgegevens aan deze zorgverleners gebeurd dan ook bijna altijd via niet-geautomatiseerde methodes.

Verder worden er gegevens verstrekt aan de patiënten zelf. Er worden persoonsgegevens vertrekt aan het RIVM voor bevolkingsonderzoek. Gegevens over de bloedvoorziening aan Sanquin, dit is een bloedbank. Ook zijn er ziekenhuizen die onderzoeken voor Ziekenhuis Rivierenland uitvoeren, omdat zij daar zelf de middelen niet voor heeft. Dit zijn de St. Maartenskliniek in Nijmegen, Ziekenhuis Gelderse Vallei in Ede, het Diakonessenhuis in Utrecht en het Antonius Ziekenhuis Nieuwegein.[68]

---

[65] Zie bijlage 7: Interview Peter Schelling.
[66] Zie bijlage 7: Interview Peter Schelling.
[67] Zie bijlage 9: Interview Louise en Arda.
[68] Zie bijlage 6: Interview Bart de Ruiter.

4.5 Systemen
Zoals we al eerder zagen zijn er verschillende systemen om gegevens te verwerken binnen Ziekenhuis Rivierenland. Maar er zijn ook verschillende systemen die zorgen dat gegevens verstrekt kunnen worden aan derden. Allereerst worden er nog gegevens verstrekt via post, e-mail, fax en telefoon. Verder heb je elektronische systemen zoals Portavita, Zorgmail, Zorgdomein en Clausserver. Verder verstrekt Ziekenhuis Rivierenland ook via beveiligde VPN-verbindingen persoonsgegevens aan ziekenhuizen waarmee zij samenwerken.

Via post en fax worden vaak persoonsgegevens verstrekt als deze met een schriftelijke of telefonische aanvraag wordt opgevraagd door een zorgverlener. Voor verstrekking van deze persoonsgegevens is in principe toestemming van de patiënt vereist. Dit is de hoofdregel echter wordt er vaak vanuit gegaan dat er toestemming is van de patiënt omdat de derde een behandelrelatie heeft met de patiënt. Maar dat er überhaupt een directe behandelrelatie bestaat met de patiënt is niet altijd 100% zeker.

Portavita
Door middel van Portavita worden bijvoorbeeld CVRM-dossiers geleverd aan huisartsen. Portavita wordt gebruikt voor het doorbraakprogramma van Ziekenhuis Rivierenland. Het doorbraakprogramma van Ziekenhuis Rivierenland in samenwerking met ECT is een programma om de 1^{e} en 2^{e} lijns CVRM-zorg en diabeteszorg te integreren. Zowel bij het CVRM-programma als bij het diabetes-programma van het doorbraakprogramma wordt gebruik gemaakt van Portavita. Op dit moment wordt Portavita voor CVRM-zorg alleen gebruikt om gegevens over en weer te verstrekken. Bij diabetespatiënten wordt Portavita gebruikt als Keten Informatie Systeem (KIS) waarin het gezamenlijke zorgplan is opgenomen en de huisarts en de medisch specialist van elkaar kunnen zien wat ze hebben gedaan, ze werken als het ware in één gezamenlijk dossier. Het is de bedoeling dat de CVRM-zorg ook gaat werken met het KIS van Portavita.[69]

Zorgmail
Zorgmail is een beveiligde verbinding waarover persoonsgegevens via een edifactbericht worden verstrekt aan derden. [70] Zorgmail is een systeem waarbij persoonsgegevens verstrekt kunnen worden aan derden, maar derden krijgen hierdoor geen toegang tot het systeem van het ziekenhuis. Zorgmail is als het ware een beveiligde e-mail verbinding.

Zorgdomein
Zorgdomein is een verwijssysteem, via zorgdomein ontvangt het ziekenhuis verwijsbrieven en aanvraagformulieren van huisartsen. Het ziekenhuis verstuurd ontslagbrieven via Zorgdomein aan de huisartsen. Zorgdomein kan gezien worden als een beveiligde e-mailverbinding waarmee zorgverleners onderling op een veilige manier communiceren.

Overige systemen
Via Clausserver wordt informatie van het lab over de bloedvoorziening aan Sanquin verstrekt, Sanquin is een bloedbank. Ziekenhuis Rivierenland kan, zoals eerder besproken, sommige onderzoeken niet zelf uitvoeren, zoals pathologisch onderzoek, daarom sturen zij de kweek via de post en de aanvraag via een beveiligde VPN verbinding naar Het Diakonessenhuis in Utrecht. Als de kweek daar onderzocht is wordt de uitslag aan het ziekenhuis toegestuurd via de VPN verbinding. Verder hebben ze voor microbiologisch onderzoek een vergelijkbare samenwerking alleen dan met Ziekenhuis Gelderse Vallei in Ede. Hier sturen zij alleen de aanvraag via de VPN verbinding, de persoonsgegevens en de kweek worden verstuurd via de post.

[69] Zie bijlage 3: Interview Patricia Jansen en Aryanti Mega Ugahary
[70] Edifact bericht is een gestructureerd bericht waarmee vertrouwelijke informatie kan worden verstrekt aan derden, het is een bepaald type bericht dat direct kan worden verwerkt in een informatiesysteem.

Verder worden er via VPN verbinding nog DFT's naar de Sint Maartens kliniek in Ubbergen gestuurd en uitslagen naar het RIVM verstuurd in het belang van bevolkingsonderzoek, dit laatste gebeurd op grond van een wettelijk voorschrift.

4.6 Beveiliging

Alle berichten met persoonsgegevens die vanuit Ziekenhuis Rivierenland worden verstrekt aan derden voldoen aan de technische normen van Health Level Seven (hierna: HL7). HL7 is de wereldwijde standaard voor veilige, elektronische informatie-uitwisseling in de zorg. De gegevensuitwisseling tussen de informatiesystemen van het ziekenhuis en derden vindt plaats door middel van het uitwisselen van elektronische berichten. De structuur van die berichten wordt gedefinieerd door standaarden zoals HL7. Edifact is ook een berichtenstandaard, aan edifactberichten zijn verschillende eisen gesteld. De berichten die verstuurd worden via Zorgmail voldoen aan de eisen van een gestructureerd edifactbericht.[71]

Verder voldoet de beveiliging van persoonsgegevens aan de NEN-7510 norm, deze norm ziet toe op de informatiebeveiliging in de gezondheidszorg en ziet toe op alle mogelijke manieren waarop informatie wordt weergegeven, vastgelegd en overgedragen. Voor de verstrekking van persoonsgegevens aan derden is de NEN-7512 norm van belang, omdat deze toeziet op de verstrekking van gegevens aan derden.

De NEN 7512 norm ziet toe op de elektronische communicatie tussen zorgverleners. Deze Nen-norm vormt de vertrouwensbasis voor gegevensuitwisseling in de zorg, wanneer is een zorgverlener betrouwbaar en wanneer kunnen persoonsgegevens aan deze zorgverlener worden verstrekt. Aan de hand van risicoklassen, een vertrouwensmodel en zekerheidsfactoren, die zijn opgenomen in de norm, kan worden getoetst of de zorgverlener betrouwbaar is. Alleen met een betrouwbare partij kan worden gecommuniceerd.[72]

Inmiddels is er naast de NEN 7512 uit 2005 ook een ontwerp norm 7512 uit 2013. In dit ontwerp is naast de zekerheden die partijen elkaar moeten bieden als voorwaarde voor vertrouwde gegevensuitwisseling ook nadere invulling gegeven aan een aantal richtlijnen van de NEN 7510. In de ontwerp norm wordt beschreven hoe gegevensuitwisseling kan worden geclassificeerd en welke risico's de gegevensuitwisseling met zich meebrengt voor de gezondheidszorg.[73] Bij deze risicobeoordeling wordt aan de hand van de classificatie van beschikbaarheid, integriteit en vertrouwelijkheid, bedreigingen en kwetsbaarheden getoetst welke risico's behandeld moeten worden en welke beheersmaatregelen daarvoor nodig zijn. Deze risicobeoordeling is noodzakelijk om ervoor te zorgen dat de risico's worden beperkt en de gegevens op een betrouwbare manier kunnen worden uitgewisseld.

In beginsel worden alle verwerkingshandelingen van patiëntengegevens, zoals in hoofdstuk 3 besproken gelogd. Dit betekent dat alle geautomatiseerde acties die plaats hebben gevonden met betrekking tot persoonsgegevens zijn geregistreerd. Hieronder valt het vastleggen, bijwerken, bewaren en inzien van gegevens, maar daarnaast ook het verstrekken van gegevens aan derden. Tenminste als dit geautomatiseerd gebeurd, als dit niet geautomatiseerd gebeurd, wordt het als het goed is genoteerd in het dossier van de patiënt, maar dit kan dan niet gelogd worden in het systeem. Hierdoor is er geen toezicht op gegevens die niet geautomatiseerd worden verstrekt. Verder is het nog niet in alle systemen mogelijk om de acties te loggen.

Verder zijn de persoonsgegevens beveiligd door inlogcodes. Door middel van inlogcodes worden de gegevens afgeschermd voor onbevoegden. Aan de hand van een autorisatiebeleid is bepaald wie welke persoonsgegevens mag inzien.

---

[71] Zie bijlage 6: Interview Bart de Ruiter.
[72] *Norm NEN 7512*, Nederlandse Normalisatie-instituut, 2005.
[73] *Ontwerp Norm NEN 7512*, Nederlands Normalisatie-instituut, 2013, p.3.

Een cardiologisch verpleegkundige heeft in principe alleen direct toegang tot persoonsgegevens van patiënten die een relatie hebben met het specialisme of afdeling waar de verpleegkundige werkt. De cardiologisch verpleegkundige mag dus alleen persoonsgegevens inzien van cardiologische patiënten. Er kan echter wel indirect toegang verschaft worden tot het dossier van patiënten waarmee geen directe behandelrelatie bestaat, hiervoor dient een reden en wachtwoord opgegeven te worden. Deze toegangsverschaffing wordt gelogd, mocht de toegangsverschaffing onrechtmatig zijn dan staan daar sancties tegenover.

5. De verwerking en verstrekking van persoonsgegevens getoetst aan de wet- en regelgeving

In dit hoofdstuk wordt de in kaart gebrachte verwerking van persoonsgegevens binnen Ziekenhuis Rivierenland en de verstrekking van persoonsgegevens door Ziekenhuis Rivierenland aan derden uit hoofdstuk 3 en hoofdstuk 4 getoetst aan de wettelijke bepalingen en aan de geldende richtlijnen en normen. Aan de hand van twee casussen wordt getoetst of de verwerking van persoonsgegevens binnen Ziekenhuis Rivierenland en de verstrekking van persoonsgegevens aan derden voldoet aan de wet- en regelgeving.

5.1 Verwerking van persoonsgegevens

Om te kijken of de verwerking van persoonsgegevens binnen Ziekenhuis Rivierenland rechtmatig is en voldoet aan de geldende wet- en regelgeving moet eerst gekeken worden naar het doel van de verwerking. Persoonsgegevens mogen alleen voor een uitdrukkelijk, welbepaald en gerechtvaardigd doel worden verwerkt. Verder moet per verwerking of categorie van verwerking gekeken worden of deze verwerking proportioneel en subsidiair is.[74] Binnen Ziekenhuis Rivierenland worden persoonsgegevens verwerkt met als doel het verbeteren van de patiëntveiligheid en het bieden van verantwoorde en veilige zorg aan patiënten. Het uitvoeren van de behandelovereenkomst is een onderdeel van het bieden van verantwoorde en veilige zorg.

Vervolgens moet worden bepaald of dit doel gerechtvaardigd is, het doel is gerechtvaardigd als de verwerking van “algemene” persoonsgegevens berust op een van de rechtvaardigingsgronden van art. 8 Wbp. In dit geval is de verwerking noodzakelijk voor het uitvoeren van een overeenkomt, namelijk voor het uitvoeren van de behandelovereenkomst tussen het ziekenhuis en de patiënt. Omdat voldaan wordt aan art. 8 Wbp kan dus gesproken worden van een gerechtvaardigd doeleinde voor de verwerking van “algemene” persoonsgegevens de zin van art. 7 Wbp.

Op de verwerking van bijzondere persoonsgegevens rust het verbod van art. 16 Wbp, gegevens betreffende iemands gezondheid vallen onder de categorie bijzondere persoonsgegevens. Op dit verbod kan echter een uitzondering worden gemaakt, op grond van art. 21 Wbp. De verwerking van medische gegevens is gerechtvaardigd als de gegevens worden verwerkt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg voor zover dat noodzakelijk is voor de goede behandeling of verzorging van de betrokkene. De medische gegevens van de patiënt kunnen gerechtvaardigd worden verwerkt binnen Ziekenhuis Rivierenland omdat het doel: het verbeteren van de patiëntveiligheid en het bieden van verantwoorde en veilige zorg aan patiënten, overeenkomt met de rechtvaardigingsgrond van art. 21 Wbp.

5.2 Verstrekking van persoonsgegevens aan derden

Om te kijken of de verstrekking van persoonsgegevens van Ziekenhuis Rivierenland aan derden rechtmatig is en voldoet aan de wet- en regelgeving moet allereerst het doel van de verstrekking duidelijk zijn. De verstrekking van gegevens dient te berusten op een welbepaald en uitdrukkelijk omschreven en gerechtvaardigd doel. De persoonsgegevens van patiënten van Ziekenhuis Rivierenland worden verstrekt met als doel het verbeteren van de patiëntveiligheid en het bieden van verantwoorde en veilige zorg.

Vervolgens moet worden gekeken of het doel van de verstrekking gerechtvaardigd is, voor de verstrekking van “algemene” persoonsgegevens gelden de rechtvaardigingsgronden van art. 8 Wbp. In dit geval is de verstrekking noodzakelijk voor uitvoering van de behandelovereenkomst, art. 8 lid 1 sub b Wbp.

[74] HR 9 september 2011, ECLI:NL:HR:2011:BQ8097.

Het verbeteren van de patiëntveiligheid en het bieden van verantwoorde en veilige zorg kan worden aangemerkt als een gerechtvaardigd belang van het ziekenhuis, het uitvoeren van de behandelovereenkomst is immers van belang bij het verbeteren van de patiëntveiligheid en het bieden van verantwoorde en veilige zorg. Omdat er sprake is van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel, is de verstrekking van “algemene” persoonsgegevens door Ziekenhuis Rivierenland gerechtvaardigd in de zin van art. 7 Wbp.

De verstrekking van gegevens betreffende de gezondheid van de patiënt (medische gegevens) is in beginsel verboden. Op grond van de art. 7:457 BW kan worden afgeweken van dit verbod. Dit kan met toestemming van de patiënt, als er een directe behandelrelatie bestaat tussen de patiënt en de derde, op grond van een wettelijke bepaling of in een conflict van plichten. Dit alles mag alleen indien het noodzakelijk is voor de behandeling van de patiënt. In principe zijn alle medische gegevens die worden verstrekt aan derden noodzakelijk voor de behandeling van de patiënt en in het belang van de patiënt. Ziekenhuis Rivierenland verstrekt in beginsel alleen persoonsgegevens aan derden als een van de rechtvaardigingsgronden van art. 7:457 BW van toepassing is, binnen Ziekenhuis Rivierenland is geen beleid vastgelegd omtrent het verstrekken van persoonsgegevens. Zij volgen, zowel bij het verwerken als verstrekken de wettelijke bepalingen, maar deze wettelijke bepalingen zijn niet expliciet vastgelegd in een privacyrichtlijn.

5.3 Beveiliging

Om te kijken of de beveiliging van persoonsgegevens binnen Ziekenhuis Rivierenland voldoet aan de wettelijke verplichting van art. 13 Wbp. Moet gekeken worden of de verantwoordelijke voldoende technische en organisatorische maatregelen heeft getroffen om de persoonsgegevens van patiënten te beveiligen. Deze maatregelen garanderen een passend beveiligingsniveau gelet op de risico’s die de verwerking en de aard van de te beschermen gegevens met zich meebrengt.

De beveiliging van persoonsgegevens binnen Ziekenhuis Rivierenland wordt op verschillende manieren gewaarborgd. Allereerst wordt er gebruik gemaakt van beveiligde verwerking en uitwisselingssystemen zoals eerder besproken.[75] De beveiliging is georganiseerd aan de hand van normen zoals de NEN 7510 en de NEN 7512. Verder heeft Ziekenhuis Rivierenland haar digitale gegevens beveiligd met inlogcodes en worden veel acties die verricht worden met betrekking tot persoonsgegevens gelogd. Hierdoor kan gecontroleerd worden of onbevoegden zich toegang hebben verschaft tot persoonsgegevens. Logging is nog niet mogelijk in alle systemen en de acties die worden verricht met betrekking tot persoonsgegevens in de papieren dossiers worden ook niet gelogd. Wie bevoegd is om persoonsgegevens in te zien, is aan de hand van een autorisatiematrix bepaald.

Het beveiligingsniveau kan bepaald worden aan de hand van een plan-do-check-act-cyclus. Allereerst dienen de betrouwbaarheidseisen vastgesteld te worden, vervolgens treft de verantwoordelijke maatregelen waarmee hij de betrouwbaarheidseisen waarborgt. Deze maatregelen kunnen worden bepaald aan de hand van risicoanalyses en het toepassen van beveiligingsafspraken. Vervolgens moeten de getroffen maatregelen worden gecontroleerd, geëvalueerd en waar nodig worden aangepast.[76] Binnen Ziekenhuis Rivierenland is informatiebeveiliging opgenomen als risicogebied in het kwaliteitsplan. De coördinator informatiebeveiliging, de functionaris voor de gegevens bescherming en de security officer houden toezicht op de informatiebeveiliging van het ziekenhuis. Aan de hand van de NEN 7510 norm wordt regelmatig een risicobeoordeling uitgevoerd.

[75] Paragraaf 3.6 en paragraaf 4.6

[76] *CBP Richtsnoeren: Beveiliging van persoonsgegevens, college bescherming persoonsgegevens, 2013.*

Aan de hand van de NEN 7512 zal iedere keer bij verstrekking van gegevens gekeken moeten worden welke risico's de verstrekking met zich meebrengt. Aan de hand van een risicoanalyse zal beoordeeld worden welke risico's aanvaardbaar zijn en welke maatregelen er genomen moeten worden om de risico's te beperken. Door het classificeren van beschikbaarheid, integriteit en vertrouwelijkheid, het in kaart brengen van bedreigingen en kwetsbaarheden kunnen de te behandelen risico's worden bepaald. Aan de hand van deze risicobeoordeling kunnen beheersmaatregelen worden vastgesteld.

5.4 Toetsingsmatrix

Het is moeilijk om de verstrekking van persoonsgegevens in zijn algemeenheid te toetsen aan de wet- en regelgeving. Dit komt doordat het per geval om verschillende persoonsgegevens gaat en deze persoonsgegevens steeds aan verschillende ontvangers worden verstrekt. Verder is het ook lastig omdat er geen vastomlijnd beleid is binnen Ziekenhuis Rivierenland voor het verstrekken van persoonsgegevens aan derden. Daarom is ervoor gekozen om aan de hand van twee casussen te kijken of er wordt voldaan aan de wet- en regelgeving. Zowel de gegevensverstrekking in het Doorbraakprogramma CVRM als de gegevensverstrekking van het laboratorium aan de Regioapotheek is getoetst aan de wet-en regelgeving.

Aan de hand van een toetsingsmatrix[77] kan per geval en per keer bekeken worden of gegevens verstrekt kunnen worden aan derden. De matrix dient als een checklist aan de hand waarvan kan worden afgewogen welke persoonsgegevens wel en welke persoonsgegevens niet kunnen worden verstrekt aan derden. In de checklist zijn de wettelijke vereisten en de vereisten uit de beveiligingsnorm voor gegevensuitwisseling opgenomen.

Aan de hand van de checklist kan beoordeeld worden of de gegevensverstrekking rechtmatig is en kunnen de risico's beoordeeld worden. Uit de risicobeoordeling volgen vervolgens beheersmaatregelen waardoor de risico's kunnen worden ingeperkt. Hieronder zullen achtereenvolgens de getoetste casussen worden besproken.

5.5 Toetsing doorbraakprogramma Cardiovasculair Risicomanagement

Het doorbraakprogramma is een programma om de 1e en 2e lijns behandeling van chronische zorg op het gebied van CVRM te bevorderen. De doelstellingen van het programma zijn: betere zorg, betere zorguitkomsten en terugdringen van de kosten. Deze doelstelling is welbepaald, uitdrukkelijk omschreven en gerechtvaardigd. De doelstelling is uitdrukkelijke omschreven in het projectplan, het doel is ook gerechtvaardigd omdat het verstrekken van gegevens geschiedt op grond van toestemming van de patiënt. Patiënten werken vrijwillig mee aan het programma, zij geven daarmee toestemming aan de medisch specialist en de huisarts om benodigde gegevens uit te wisselen in een keteninformatiesysteem.

Verder is aan de hand van een risicobeoordeling getoetst of de verstrekking niet onnodig veel risico's met zich meebrengt. Aan de hand van een classificatie van de beschikbaarheid, integriteit en vertrouwelijkheid is gekeken en aan de hand van de mogelijke bedreigingen en kwetsbaarheden is gekeken welke risico's de verstrekking met zich meebrengt en welke beheersmaatregelen benodigd zijn om deze risico's te beperken. De verstrekking van gegevens binnen het doorbraakprogramma CVRM is gerechtvaardigd en brengt geen onaanvaardbare risico's met zich mee.

[77] Zie bijlage 10: Toestingsmatrix

Eisen	Project	Voldaan?
Welke gegevens	Individueel zorgplan: Persoonsgegevens zoals naam, adres, BSN, telefoonnummer, geboortedatum enz. Medische gegevens (gegevens betreffende de gezondheid van de patiënt).	Persoonsgegevens zoals naam, adres en geboortedatum vallen onder de “algemene” persoonsgegevens in de zin van de Wbp. De medische gegevens vallen onder bijzondere persoonsgegevens in de zin van art. 16 jo. art. 21 Wbp.
Door middel van welk systeem worden de gegevens verstrekt?	Portavita	Is een beveiligde verbinding, dus voldoet aan de beveiligingsnormen
Informatieverplichting aan patiënt	Aan de patiënten wordt toestemming gevraagd c.q. ze kunnen vrijwillig deelnemen aan het project. Er bestaat geen informatiefolder met betrekking tot het CVRM-project.	Patiënt dienen voorafgaand aan de verzameling van de gegevens op de hoogte te worden gesteld van het doel voor de verstrekking. Dit kan zou middels het verstrekken van een folder kunnen.
Welbepaald en uitdrukkelijk doel	Integratie van de 1e en 2e lijns behandeling van chronische zorg op het gebied van CVRM. Met als doelstellingen: betere zorg, betere zorguitkomsten en terugdringen kosten.	Dit doel is uitdrukkelijk opgenomen in het projectplan en uitdrukkelijk beschreven. Er is dus sprake van een welbepaald en uitdrukkelijk doel in de zin van art. 7 Wbp.
Gerechtvaardigd doel voor verzameling en verwerking Rechtvaardigingsgronden art. 8 Wbp (algemene persoonsgegevens) Rechtvaardigingsgronden art. 21 Wbp (medische persoonsgegevens)	Integratie van de 1e en 2e lijns behandeling van chronische zorg op het gebied van CVRM. Met als doelstellingen: betere zorg, betere zorguitkomsten en terugdringen kosten.	Het doel is gerechtvaardigd, omdat het verenigbaar is met het doel waarvoor de gegevens worden verzameld. De “algememe” gegevens worden namelijk verzameld met als doel het uitvoeren van een overeenkomst (art. 8 lid 1 sub b Wbp). De medische persoonsgegevens worden verzameld met als doel het bieden van verantwoorde en veilige zorg (art. 21 lid 1 sub a Wbp).

Rechtvaardigingsgrond verstrekken bijzondere patiëntgegevens • Toestemming • Directe behandelrelatie • Derde is vervanger van de hulpverlener • Wettelijk vertegenwoordiger van patiënt • Wettelijke bepaling • Conflict van plichten	De patiënt kan zich vrijwillig aansluiten bij het CVRM programma, en dient toestemming te geven voor het verstrekken van zijn medische gegevens.	De verstrekking van bijzondere persoonsgegevens is gerechtvaardigd op grond van toestemming.
Rechtvaardigingsgrond verstrekken “algemene patiëntgegevens” • Toestemming • Uitvoering overeenkomst • Nakomen wettelijke verplichting • Vrijwaring vitaal belang • Vervulling publiekrechtelijke taak • Behartiging gerechtvaardigd belang	De patiënt kan zich vrijwillig aansluiten bij het CVRM programma, de patiënt dient toestemming te geven voor het verstrekken van zijn “algemene” persoonsgegevens.	De verstrekking van “algemene” persoonsgegevens is gerechtvaardigd op grond van toestemming.
Risicobeoordeling NEN 7512 Classificatie : • Beschikbaarheid • Integriteit • Vertrouwelijkheid	 Midden Hoog Hoog	Beschikbaarheid: uitval van de gegevensuitwisseling levert matige gevolgen op voor betrokkenen. Integriteit: onjuistheid of onvolledigheid van de gegevensuitwisseling levert omvangrijke gevolgen op voor de betrokkenen. Vertrouwelijkheid: ongewenste openbaarmaking of verspreiding van de uitgewisselde gegevens levert omvangrijke gevolgen op voor de betrokkene.
Bedreigingen	Vooral uitval netwerkverbinding, fouten in de koppeling en ongeautoriseerde toegang tot persoonsgegevens van de patiënt.	De kans dat deze bedreigingen optreden is middelmatig. De kans dat de bedreigingen optreden is niet onwaarschijnlijk.
Kwetsbaarheden	Geen bijzonderheden , eventueel afhankelijkheid van derde partij bij gebruik van een informatiesysteem.	

Behandeling risico's	Toepassen van beheersmaatregelen.	Wanneer een bedreiging of risiconiveau te hoog is kunnen beheersmaatregelen worden getroffen.
Beheersmaatregelen	Uitwisselingsovereenkomst; Eisen stellen aan derde partij (SLA); Technische maatregelen voor identificatie en authenticatie van de koppeling; Continuïteitsplan.	Deze maatregelen zijn van belang voor het waarborgen van de kwaliteitseisen. Een beheersmaatregel kan specifiek op één kwaliteitseis of generiek voor meer kwaliteitseisen van toepassing zijn.

5.6 Toetsing gegevensverstrekking laboratorium aan Regioapotheek

Het laboratorium van Ziekenhuis Rivierenland verstrekt MDRD-uitslagen aan de Regioapotheek. Op grond van de wet zijn zij verplicht deze gegevens te verstrekken aan apothekers. De gegevens worden in beginsel verwerkt met als doel het garanderen van de medicatieveiligheid van de patiënt. Dit is een in principe een gerechtvaardigd doel op grond van art. 21 lid 1 sub a Wbp. De verstrekking van de gegevens vindt zijn grondslag in artikel 6.10 Geneesmiddelenwet, deze wet stelt de verplichting om MDRD-uitslagen aan apothekers te verstrekken in verband met de medicatieveiligheid van de patiënt. De verstrekking is dus gerechtvaardigd. De wijze waarop de gegevens worden verstrekt is echter niet rechtmatig, er worden gegevens verstrekt van patiënten die geen "behandelrelatie" hebben met de regioapotheek. De verstrekking van de uitslagen is dus bovenmatig en onrechtmatig op grond van art. 11 lid 1 Wbp.

Verder worden de gegevens via onbeveiligde e-mail verstrekt aan de Regioapotheek wat extra kwetsbaarheden met zich meebrengt. Aan de hand van een risicobeoordeling is getoetst of de verstrekking niet onnodig veel risico's met zich meebrengt. Aan de hand van een classificatie van de beschikbaarheid, integriteit en vertrouwelijkheid en aan de hand van de mogelijke bedreigingen en kwetsbaarheden is gekeken welke risico's de verstrekking met zich meebrengt en welke beheersmaatregelen benodigd zijn om deze risico's te beperken. De verstrekking van de MDRD-uitslagen is gerechtvaardigd, de wijze waarop deze verstrekking geschiedt is echter niet gerechtvaardigd.

Eisen	Project	Voldaan?
Welke gegevens	MDRD-uitslagen: uitslagen om de nierfunctie van iemand te bepalen. Na/k-uitslagen : uitslagen om problemen met de vochtbalans te bepalen. INR-uitslagen: uitslagen naar de snelheid waarmee het bloed van een patiënt stolt. BSN om aan te gegeven van welke patiënt de uitslag is. Deze uitslagen van alle patiënten worden 's- avonds doorgestuurd naar de Regioapotheek.	De uitslagen vallen onder bijzondere persoonsgegevens in de zin van art. 16 jo. art. 21 Wbp. Het BSN valt onder "algemene" persoonsgegevens in de zin van de Wbp. Het feit dat alle uitslagen van alle patiënten verstuurd worden naar de regioapotheek is niet rechtmatig. Dit is bovenmatig en dus in strijd met art. 11 lid 1 Wbp.

Door middel van welk systeem worden de gegevens verstrekt?	Via e-mail	E-mail is geen beveiligde verbinding en heeft daarom ook niet de voorkeur.
Informatieverplichting aan patiënt	De verstrekking van de labwaarden geschied op grond van een wettelijke bepaling. De patiënten worden daarom niet geïnformeerd over de verstrekking van hun labwaarden aan de Regioapotheek.	Patiënt dienen voorafgaand aan de verzameling van de gegevens op de hoogte te worden gesteld van het doel voor de verzameling, verwerking en de verstrekking. In art. 34 lid 5 is bepaald dat patiënten niet geïnformeerd moeten worden als de verwerking/verstrekking geschied op grond van een wettelijke bepaling.
Welbepaald en uitdrukkelijk doel	Het hoofddoel is het garanderen van de medicatieveiligheid voor de patiënt. Het onderliggende doel is het voorkomen dat de nachtdienst van het laboratorium ’s nachts wordt gewekt om uitslagen door te sturen.	Het doel vloeit voort uit de wettelijke verplichting om de gegevens te verstrekken in het kader van de patiëntveiligheid.
Gerechtvaardigd doel voor verzameling en verwerking van gegevens Rechtvaardigingsgronden art. 8 Wbp (algemene persoonsgegevens) Rechtvaardigingsgronden art. 21 Wbp (medische persoonsgegevens)	Het hoofddoel is het garanderen van de medicatieveiligheid voor de patiënt. Het onderliggende doel is het voorkomen dat de nachtdienst van het laboratorium ’s nachts wordt gewekt om uitslagen door te sturen.	In principe is het garanderen van de medicatieveiligheid een gerechtvaardigd doel, op grond van art. 21 lid 1 sub a Wbp (noodzakelijk voor de goede behandeling van de patiënt). Het is echter niet gerechtvaardigd om bovenmatig veel gegevens te verstrekken, dit is in strijd met art. 11 lid 1 Wbp. Het verstrekken van alle uitslagen van alle patiënten kan niet worden beschouwd als noodzakelijk voor de goede behandeling en zorgverlening van al deze patiënten, zoals bepaald in art. 21 lid 1 sub a Wbp.

Rechtvaardigingsgrond verstrekken bijzondere persoonsgegevens • Toestemming • Directe behandelrelatie • Derde is vervanger van de hulpverlener • Wettelijk vertegenwoordiger van patiënt • Wettelijke bepaling • Conflict van plichten	De bijzondere persoonsgegevens worden verstrekt aan de regioapotheek op grond van een wettelijke bepaling (art. 6.10 Geneesmiddelenwet).	Wettelijke verplichting is een rechtvaardigingsgrond voor de verstrekking van medische gegevens aan derden.
Rechtvaardigingsgrond verstrekken “algemene patiëntgegevens” • Toestemming • Uitvoering overeenkomst • Nakomen wettelijke verplichting • Vrijwaring vitaal belang • Vervulling publiekrechtelijke taak • Behartiging gerechtvaardigd belang	Het BSN van de patiënt wordt verstrekt op grond van een wettelijke bepaling (art. 6.10 Geneesmiddelenwet).	Wettelijke verplichting is een rechtvaardigingsgrond voor de verstrekking van “algemene” gegevens aan derden.
Risicobeoordeling NEN 7512 Classificatie : • Beschikbaarheid • Integriteit • Vertrouwelijkheid	 Hoog Hoog Hoog	Beschikbaarheid: uitval van de gegevensuitwisseling levert omvangrijke gevolgen op voor betrokkenen. Integriteit: onjuistheid of onvolledigheid van de gegevensuitwisseling levert omvangrijke gevolgen op voor de betrokkenen. Vertrouwelijkheid: ongewenste openbaarmaking of verspreiding van de uitgewisselde gegevens levert omvangrijke gevolgen op voor de betrokkene.
Bedreigingen	Vooral uitval van de netwerkverbinding en ongeautoriseerde toegang tot persoonsgegevens van de patiënt.	De kans dat deze bedreigingen optreden is hoog. De kans dat de bedreigingen optreden is waarschijnlijk.
Kwetsbaarheden	Gebruik van e-mail is geen gestructureerde gegevensuitwisseling	

Behandeling risico's	Toepassen van beheersmaatregelen.	Wanneer een bedreiging of risiconiveau te hoog is kunnen beheersmaatregelen worden getroffen.
Beheersmaatregelen	Uitwisselingsovereenkomst; Eisen stellen aan derde partij (SLA); Technische maatregelen voor identificatie en authenticatie van de koppeling; Continuïteitsplan.	Deze maatregelen zijn van belang voor het waarborgen van de kwaliteitseisen. Een beheersmaatregel kan specifiek op één kwaliteitseis of generiek voor meer kwaliteitseisen van toepassing zijn.

6. Het Landelijk SchakelPunt

Het LSP is een uitwisselingssysteem om persoonsgegevens op een snelle en veilige manier uit te wisselen. Het is een infrastructuur waardoor het voor zorgverleners makkelijker wordt om medische gegevens uit te wisselen met andere zorgverleners in de regio. Zorgverleners kunnen hun computersysteem aansluiten op het beveiligd netwerk van het LSP. Zo kan de medisch specialist medische gegevens over de patiënt, via het LSP, opvragen bij de huisarts.

De Vereniging van Zorgaanbieders voor Zorgcommunicatie (hierna: VZVZ) houdt toezicht op het LSP. Zij draagt de verantwoordelijkheid voor het beheer, onderhoud en ontwikkeling van het LSP. De VZVZ is een samenwerkingsverband van vier koepelorganisaties van zorgaanbieders. Deze zorgaanbieders zijn: De Landelijke Huisartsen Vereniging (hierna: LHV), De Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie (hierna: KNMP), Vereniging Huisartsenposten Nederland (hierna: VHN) en de Nederlandse Vereniging van Ziekenhuizen (hierna: NVZ).[78]

In dit hoofdstuk wordt besproken hoe het LSP precies werkt, hoe de beveiliging van de persoonsgegevens gewaarborgd wordt, welke zorgverleners uit de regio zijn aangesloten, welke voor- en nadelen er zijn, welke mogelijkheden het LSP biedt en wat voor gevolgen aansluiting heeft voor het ziekenhuis.

6.1 Werking van het LSP

Alle zorgverleners die aangesloten zijn bij het LSP houden hun eigen dossier bij. Door middel van het LSP kunnen ze bij de andere aangesloten zorgverleners medische gegevens opvragen, als dat nodig is voor de behandeling van de patiënt. De opgevraagde gegevens worden vervolgens doorgestuurd naar de zorgverlener die de gegevens heeft opgevraagd, het is niet zo dat andere zorgverleners hier toestemming voor moeten geven, het systeem stuurt de gegevens automatisch door.

Zorgverleners kunnen alleen gegevens opvragen als ze daarvoor geautoriseerd zijn. De zorgverleners zijn geautoriseerd door middel van een speciale Unieke Zorgverleners Identificatie pas (hierna: UZI-pas), deze is nodig om in te kunnen loggen in het LSP. Via het LSP mogen geen gegevens opgevraagd worden als de patiënt daar geen toestemming voor heeft gegeven. Voorafgaand aan het beschikbaar stellen van de gegevens in het LSP dient de patiënt uitdrukkelijke toestemming te geven voor het beschikbaar stellen en uitwisselen van zijn medische gegevens via het LSP, dit is de zogenaamde opt-in regeling. [79] De toestemming die gegeven wordt met de opt-in regeling, moet niet gezien worden als een generieke toestemming om de persoonsgegevens op te vragen. Iedere zorgverlener moet apart toestemming vragen aan de patiënt om de gegevens in te zien en beschikbaar te stellen.[80] Indien de patiënt toestemming verleent, worden enkel de noodzakelijk geselecteerde gegevens van de patiënt aangemeld bij het LSP door het Burgerservicenummer (hierna: BSN) door te geven aan het LSP. Bij uitbreidingen of aanpassingen is opnieuw of aanvullende toestemming nodig.

De zorgverleners kunnen gegevens opvragen door middel van het BSN- nummer van de patiënt. Het LSP zoekt, op basis van het BSN, welke zorgverleners gegevens over de patiënt beschikbaar hebben. Als er gegevens beschikbaar zijn kan de zorgverlener de gegevens opvragen en inzien. Het LSP houdt bij welke zorgverlener inzage heeft gehad in het dossier van de patiënt en welke zorgverlener de gegevens beschikbaar heeft gesteld. Dit kan de patiënt controleren door het zogenaamde inzage-overzicht op te vragen bij het LSP.

---

[78] 'Wie is verantwoordelijk?', *NVZ*, www.nvz-ziekenhuizen.nl (kies onderwerpen, kies j-l, kies LSP)
[79] 'Toestemming patiënt', *VZVZ*, www.vzvz.nl (zoek op toestemming patiënt).
[80] 'Specifieke toestemming voor gegevensverwerking via het LSP', *VZVZ*, www.vzvz.nl (zoek op specifieke toestemming).

Verder is er voor de patiënt ook de mogelijkheid om een e-mail melding te ontvangen wanneer een zorgverlener medische gegevens van de patiënt beschikbaar stelt of opvraagt. Via het LSP kunnen op dit moment alleen medicatiegegevens en waarnemingen van de huisarts geraadpleegd worden. Ziekenhuizen kunnen dus nog geen gegevens beschikbaar stellen, zij kunnen de beschikbaar gestelde gegevens wel inzien. Gegevens over intoleranties, comorbiditeit[81] en allergieën worden waarschijnlijk binnenkort beschikbaar gesteld. Het is de bedoeling dat in de toekomst meer gegevens volgen die van belang zijn voor snelle en veilige zorg. In de toekomst zullen ook de reden van voorschrijven van bepaalde medicatie en labwaarden worden uitgewisseld via het LSP. Het uitwisselen van de labwaarden is van belang voor de medicatieveiligheid.

6.2 Beveiliging van de persoonsgegevens

De gegevens die worden uitgewisseld via het LSP blijven in het zorginformatiesysteem van de zorgverlener. Het LSP beheert alleen de zogenaamde verwijsindex, het LSP verwijst de zorgverleners naar elkaar door. In de verwijsindex is opgenomen welke persoonsgegevens, in welke zorginformatiesystemen, bij welke zorgaanbieders zijn opgeslagen.[82]

Om de beveiliging van de gegevens te garanderen zijn er verschillende maatregelen genomen. Alle zorginformatiesystemen moeten voldoen aan de eisen voor een Goed Beheerd Zorgsysteem (hierna: GBZ). Een GBZ moet voldoen aan organisatorische en technische eisen.[83] Aangesloten zorgverleners zijn verplicht om een beheerder aan te stellen voor het technische beheer van het zorginformatiesysteem. De beheerder ziet erop toe op de dat de gegevens 24/7 beschikbaar zijn en controleert de logging.

Het LSP houdt bij welke zorgverlener inzage heeft gehad in de gegevens van de patiënt, deze zogenaamde logging wordt geregistreerd. Patiënten kunnen zelf in het inzage-overzicht zien welke zorgverleners gegevens beschikbaar hebben gesteld en ingezien. Hierdoor kan de patiënt ook zelf controle uitoefenen en een melding maken als er sprake is van misbruik. Deze meldingen worden door het LSP doorgegeven aan een van de toezichthoudende organen, het CBP of de Inspectie voor de Gezondheidszorg (hierna: IGZ). Zij nemen vervolgens de mededeling in behandeling en bepalen of er een sanctie moet worden opgelegd en zo ja welke.

Verder wordt ook de toegang tot het LSP beperkt door middel van een UZI-pas en een UZI-servercertificaat. Alleen zorgverleners die beschikken over een UZI-pas of een UZI-servercertificaat kunnen toegang krijgen tot het LSP. De UZI-pas bevat de elektronische identiteit van de pashouder. De pas kan alleen gebruikt worden door middel van het ingeven van een pincode, hierdoor wordt het LSP beveiligd tegen misbruik. De elektronische identiteit van een systeem of applicatie kan worden vastgelegd met een UZI-servercertificaat.

De UZI-middelen worden uitgereikt door het UZI-register, dit is onderdeel van het CIBG (een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport). De UZI-middelen worden alleen verstrekt aan bevoegde zorgverleners. Bij aanvraag wordt de bevoegdheid van de zorgverlener gecontroleerd. Er zijn verschillende UZI-passen hierdoor kan aan de gebruiker meer of minder rechten worden toegekend. Welke pas aan een zorgverlener wordt toegekend, is afhankelijk van de zorgtaak van de zorgverlener. Door middel van de UZI-pas wordt de logging door de beheerder bijgehouden. In Ziekenhuis Rivierenland wordt op de afdeling Radiologie al gewerkt met UZI-passen. Op deze afdeling worden deze passen gebruikt om beelden op te vragen in MammoXL, dit zijn beelden uit het bevolkingsonderzoek naar borstkanker.[84]

---

[81] Comorbiditeit: is het aanwezig zijn van verschillende aandoeningen.
[82] 'Beveiliging', *VZVZ,* www.vzvz.nl (zoek op beveiliging).
[83] Deze eisen van een GBZ worden nader toegelicht in paragraaf 6.5.2.
[84] Zie bijlage 7: Interview Peter Schelling.

6.3 Aangesloten zorgverleners in de regio

Het LSP wordt gebruikt door huisartsen, huisartsenposten, apothekers, ziekenhuisapothekers en medisch specialisten om medische gegevens uit te wisselen. Door consultatiebureaus, schoolartsen en jeugdgezondheidszorg (Hierna: JGZ) wordt het LSP gebruikt om dossiers over te dragen. Bij het LSP zijn per 17 maart 2014, 25 ziekenhuizen aangesloten, 1677 apotheken, 3218 huisartspraktijken en 111 huisartsenposten. Verder waren er 4.911.831 persoonsgegevens aangemeld en 2.934.755 unieke BSN's geregistreerd in het LSP.[85]

In een straal van 10 kilometer rondom Ziekenhuis Rivierenland zijn 12 apotheken, 1 huisartsenpost en 28 huisartsenpraktijken aangesloten bij het LSP. Enkel zorgverleners uit dezelfde regio kunnen elkaars persoonsgegevens inzien.[86] Een huisarts uit Groningen kan bijvoorbeeld geen gegevens inzien van een huisarts uit Eindhoven. Zorgverleners uit een regio kunnen alleen gegevens inzien uit hun eigen regio, tenzij zij zich aansluiten bij een andere regio. Ziekenhuizen kunnen echter wel gegevens uit meerdere regio's opvragen, aangezien zij vaak in meerder regio's opereren.

Het LSP heeft een regio-indeling met 40 verschillende regio's, waaronder de regio Tiel. In de regio Tiel zijn 51 apotheken, 1 apotheekhoudende huisarts, 2 huisartsenposten, 44 huisartspraktijken, 1 JGZ en 6 ziekenhuizen aangesloten.[87]

6.4 Voor- en nadelen

Er zijn voor- en tegenstanders van het LSP. De VP Huisartsen hebben zelfs een rechtszaak aangespannen tegen de VZVZ vanwege het LSP.[88] Zij is van mening dat het LSP in strijd is met het medische beroepsgeheim en een inbreuk maakt op de privacy van de patiënt. De voor- en tegenstanders van het LSP benoemen allemaal verschillende voor- en nadelen van het LSP. In deze paragraaf worden de voor- en nadelen van het LSP uiteengezet.

6.4.1 Voordelen

- Makkelijker en sneller huisartsenwaarnemingen en medicatiegegevens van patiënten inzien;
- Het LSP draagt bij aan de verbetering van veilige zorg en patiëntveiligheid;
- Het systeem is goed beveiligd door middel van het gebruik van UZI-middelen;
- Ziekenhuizen kunnen van meerdere regio's gegevens inzien;
- De dossiers blijven bij de zorgverlener, het LSP weet precies welke zorgverlener informatie heeft over welke patiënt;
- De patiënt kan zelf gemakkelijk toezicht houden door middel van het inzage-overzicht;
- In de toekomst, als het LSP verder ontwikkeld is en alle zorgverleners zijn aangesloten, worden andere systemen overbodig en kan dus vanuit één systeem worden gewerkt. Dit zorgt voor eenheid en voor een makkelijkere gegevens uitwisseling.

6.4.2 Nadelen

- Niet alle zorgverleners in de regio zijn aangesloten bij het LSP;
- Als ziekenhuis kun je alleen gegevens inzien, maar nog niet beschikbaar stellen via het LSP;
- Patiënten moeten toestemming gegeven voor aanmelding in het LSP, voor patiënten die geen toestemming geven kan het LSP niet gebruikt worden;

[85] 'Cijfers', *VZVZ* 17 maart 2014, www.vzvz.nl (zoek op feiten en cijfers).
[86] Dit is ook een beveiligingsmechanisme en had ook in paragraaf 6.2 kunnen staan.
[87] 'Lijst regio-indeling', *VZVZ*, www.vzvz.nl (zoek op regio-indeling en kies nr. 31. Tiel).
[88] 'Rechtzaak over verbod op LSP', *VP Huisartsen* 24 maart 2014, www.vphuisartsen.nl (zoek op verbod LSP).

- Het LSP biedt geen garanties tegen onrechtmatige opvraging van gegevens, maar achteraf kan deze onrechtmatige inzage wel achterhaald worden (aan de hand van logging);

6.5 Gevolgen

Aansluiting bij het LSP zal voor Ziekenhuis Rivierenland verschillende gevolgen hebben. Zo zullen er, voordat de aansluiting kan plaatsvinden, verschillende technische en organisatorische maatregelen getroffen moeten worden om de aansluiting te regelen. Deze verschillende maatregelen zullen hierna achtereenvolgens worden besproken.

Allereerst dient gecontroleerd te worden of het zorginformatiesysteem van het ziekenhuis voldoet aan de eisen van een Goed Beheerd Zorgsysteem (GBZ). Voldoet dit systeem niet aan de eisen dan zal het systeem moeten worden aangepast aan de geldende technische en organisatorische eisen voor een GBZ. Deze eisen zijn opgenomen in het programma van eisen voor een Goed Beheerd Zorgsysteem van het Nictiz. Dit programma stelt eisen aan een servicedesk, een toegangslogbeheerder, systeembeheerder, connectiviteit, beveiliging, beschikbaarheid van het systeem, prestaties, in- en uitloggen van de gebruikers, toegangslog en het beheer van zorgapplicaties.[89]

Naast de GBZ dienen werkinstructies te worden opgesteld voor het aanmelden, opvragen van medische gegevens in het LSP en het gebruik van UZI-middelen. Er zal een informatiebijeenkomst c.q. scholing moeten plaatsvinden om medewerkers te informeren over het gebruik van het LSP. Aangezien er nog geen inzage verschaft kan worden in ziekenhuisdossiers is het nog niet noodzakelijk om de patiëntendossiers op te schonen en er voor te zorgen dat de patiëntengegevens eenduidig geregistreerd zijn. Dit zal in de toekomst wellicht noodzakelijk worden als de mogelijkheden van het LSP worden uitgebreid en de ziekenhuisdossiers ook beschikbaar gesteld kunnen worden.

Vervolgens moet het ziekenhuis worden aangemeld als UZI-abonnee bij het UZI-register en moeten de UZI-middelen worden aangevraagd. Als het ziekenhuis UZI-abonnee is kan er een GBZ-aanvraag ingediend worden bij het Servicecentrum van het VZVZ. Na indiening van de GBZ-aanvraag, gaat het aansluitproces op het LSP van start. Het VZVZ Servicecentrum stuurt dan een gebruikersovereenkomst op. Pas nadat de gebruikersovereenkomst is ondertekend, zal de daadwerkelijk technische aansluiting op het LSP plaatsvinden. Als de aansluiting heeft plaatsgevonden, dienen de UZI-middelen te worden geïnstalleerd en dan is het systeem klaar voor gebruik.

Om gebruik te kunnen maken van het LSP dienen de patiënten te worden geïnformeerd en er dient toestemming te zijn verkregen van de patiënten om de gegevens beschikbaar te stellen en uit te wisselen via het LSP. Tot slot zullen afspraken gemaakt moeten worden met collega zorgverleners over welke gegevens via het LSP worden uitgewisseld.

[89] *Programma van eisen organisatie goed beheerd systeem (GBx),* Den Haag*:* Nictiz 2011.

7. Conclusies
In dit hoofdstuk worden de belangrijkste conclusies uiteengezet. Naar aanleiding van het onderzoek kunnen er verschillende conclusies getrokken worden die van belang zijn voor het aanpassen van het privacybeleid van Ziekenhuis Rivierenland.

Juridisch kader
Huidige wet- en regelgeving: de Wbp is van toepassing op de verwerking van persoonsgegevens en de verstrekking van persoonsgegevens. De WGBO is van toepassing op de verstrekking van medische gegevens, gegevens betreffende de gezondheid van een patiënt.

Toekomstige wet- en regelgeving: Door de Europese commissie is een privacyverordening opgesteld in 2012, deze verordening zal ervoor zorgen dat privacyrichtlijn 95/46/EG zal vervallen. Wanneer de verordening zal worden aangenomen en in werking zal treden is nog onduidelijk. De verordening brengt verschillende ingrijpende gevolgen met zich mee. Zoals een ruimere informatieplicht, het recht van de betrokkene om “vergeten te worden”, het verplicht voeren van een privacybeleid, het verplicht melden van datalekken en het opleggen van boetes bij niet-naleving van de verordening.

Verwerking
De persoonsgegevens van patiënten worden geheel of gedeeltelijk geautomatiseerd verwerkt of niet-geautomatiseerd verwerkt. Er wordt binnen Ziekenhuis Rivierenland gebruik gemaakt van zowel elektronische als papieren dossiers. Voor de verwerking van persoonsgegevens wordt gebruik gemaakt van verschillende systemen die verschillen per afdeling.

De persoonsgegevens van patiënten worden binnen Ziekenhuis Rivierenland rechtmatig verwerkt op grond van art. 8 lid 1 sub b jo. art. 21 lid 1 Wbp. Op grond van de zorgovereenkomst en als basis voor een goede behandeling voor de patiënt is het noodzakelijk om persoonsgegevens te verzamelen en te verwerken. Binnen Ziekenhuis Rivierenland geschiedt dit op een behoorlijke en zorgvuldige wijze met inachtneming van de wet. De doeleinden voor de verwerking van persoonsgegevens binnen Ziekenhuis Rivierenland voldoen aan de wettelijke vereisten, ze zijn welbepaald, uitdrukkelijk omschreven en rechtmatig.

Beveiliging verwerkte persoonsgegevens
De beveiliging van de persoonsgegevens wordt gewaarborgd door de ten uitvoer gelegde technische en organisatorische maatregelen. Aan de hand van de NEN 7510 norm is de beveiliging van persoonsgegevens ingericht. Bijna alle handelingen die ten aanzien van de persoonsgegevens worden verricht worden gelogd, echter kunnen nog niet alle systemen loggen, waardoor op dit moment nog niet alles gelogd wordt. Verder zijn de systemen beveiligd door middel van inlogcodes. De beveiliging van verwerkte persoonsgegevens is binnen Ziekenhuis Rivierenland voldoende gewaarborgd.

Er zijn nog wel verbeterpunten op het gebied van autorisatie binnen het ziekenhuis. Op dit moment kunnen alle zorgverleners in alle digitale dossiers, ook in de dossiers van patiënten waarmee geen behandelrelatie bestaat. Dit wordt in de meeste systemen wel gelogd, waardoor achteraf sancties kunnen volgen voor zorgverleners die zich onrechtmatig toegang hebben verschaft tot het dossier. In principe gaat Ziekenhuis Rivierenland er van uit dat alle medewerkers zich aan de gedragscode houden en zich alleen toegang tot een dossier verschaffen als zij een directe behandelrelatie hebben met de patiënt. Op dit moment wordt er binnen Ziekenhuis Rivierenland gewerkt aan een nieuw autorisatiebeleid, dit moet ervoor zorgen dat de toegang tot de dossiers verder wordt afgeschermd en niet alle medewerkers toegang hebben tot alle digitale dossiers.

Een groter probleem is de beveiliging van papieren dossiers, als de dossiers worden uitgeleend aan een afdeling wordt er vervolgens geen toezicht meer gehouden op wie het dossier inziet, bij de papieren dossiers vindt dus geen logging plaats. Ziekenhuis Rivierenland gaat er van uit dat haar medewerkers weten dat zij zich geen onrechtmatige toegang mogen verschaffen tot een dossier en zij zich dienen te houden aan de gedragscode.

Verstrekken persoonsgegevens
De persoonsgegevens worden in beginsel verstrekt aan derden indien dit noodzakelijk is voor de goede behandeling van de patiënt en de uitvoering van de behandelovereenkomst. Voor het verstrekken van gegevens aan derden is in beginsel uitdrukkelijke toestemming van de patiënt vereist. Deze toestemming is niet vereist indien: de derde een directe behandelrelatie heeft met de patiënt, de derde als vervanger optreedt voor de zorgverlener, de derde wettelijk vertegenwoordiger is van de patiënt, zij op grond van een wettelijke bepaling verplicht zijn gegevens te verstrekken aan derden of in een conflict van plichten.

Om te kijken of de verstrekking van persoonsgegevens door Ziekenhuis Rivierenland aan derden voldoet aan de wet- en regelgeving moet per geval gekeken worden of de verstrekking voldoet aan de wettelijke vereisten. Aan de hand van twee casussen is gekeken of aan deze vereisten is voldaan.

Het doorbraakprogramma CVRM voldoet aan de bepalingen uit de Wbp en WGBO. De gegevens worden verzameld met een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. Verder voldoet het programma aan de vereisten van uit de NEN 7512 norm. Het doorbraakprogramma CVRM kan worden gekwalificeerd als een veilige gegevensuitwisseling, die voldoet aan de wet- en regelgeving.

De verstrekking van MDRD-uitslagen door het laboratorium aan de regioapotheek is in beginsel rechtmatig op grond van art. 6.10 Geneesmiddelenwet. Art. 6.10 Geneesmiddelenwet verplicht het ziekenhuis deze uitslagen te verstrekken aan de apotheek van de patiënt in het kader van medicatieveiligheid. Er worden echter bovenmatig veel gegevens verstrekt aan de Regioapotheek. Het laboratorium verstrekt namelijk ook gegevens van patiënten die de Regioapotheek niet als voorkeursapotheek hebben opgegeven. Dit is in strijd met art. 11 lid 1 Wbp, de gegevensverstrekking is bovenmatig en niet gerechtvaardigd gezien het doel waarvoor de gegevens zijn verkregen.

Beveiliging verstrekte persoonsgegevens
Ziekenhuis Rivierenland verstrekt persoonsgegevens via beveiligde verbindingen. Deze beveiligde verbindingen voldoen aan de vereisten uit de wet en de NEN normen en garanderen een veilige en betrouwbare gegevensuitwisseling. Op grond van de NEN 7512 norm dient gekeken te worden of de ontvanger van de gegevens betrouwbaar is, aan de hand van deze norm kan bepaald worden of er sprake is van een betrouwbare en veilige gegevensverstrekking. Er worden ook gegevens verstrekt via onbeveiligde e-mail, fax en telefoon. Dit voldoet niet aan de beveiligingsstandaarden. De veiligheid van de verstrekte gegevens kan niet worden gewaarborgd als de gegevens via onbeveiligde e-mail, fax of telefoon worden verstrekt. De privacy van de patiënt kan op dat moment niet gewaarborgd worden, gegevens verstrekking via onbeveiligde e-mail, fax en telefoon moet worden voorkomen, indien de gegevens bedoeld zijn om opgenomen te worden in een bestand.

Het LSP
Het LSP is een uitwisselingssysteem dat het mogelijk maakt voor zorgverleners om makkelijk en snel medische gegevens uit te wisselen. Enkel met toestemming van de patiënt worden gegevens aangemeld en opvraagbaar via het LSP. Aansluiting bij het LSP brengt zowel voor als nadelen met zich mee.

Zo kunnen er op dit moment alleen nog maar huisartswaarneemgegevens en medicatiegegevens worden aangemeld en ingezien via het LSP. Het LSP is opgedeeld in verschillende regio's, zorgverleners kunnen alleen gegevens opvragen uit hun eigen regio.

Aansluiting bij het LSP heeft verschillende voor- en nadelen. Voordelen van het LSP zijn, het makkelijker inzien van huisartswaarneemgegevens en medicatiegegevens van patiënten, het draagt bij aan veiligere zorg en patiëntveiligheid, goede beveiliging door middel van uzi-middelen, het inzien van gegevens van meerdere regio's en in de toekomst wordt het mogelijk om meer gegevens in te zien en beschikbaar te stellen via het LSP. Nadelen van het LSP zijn dat niet alle patiënten toestemming gegeven, niet alle zorgverleners zijn aangesloten en de aansluiting vraagt veel inspanningen van de organisatie.

Het LSP is volop in ontwikkeling en in de toekomst zullen de mogelijkheden van het LSP steeds groter worden. De beveiliging en het toestemmingsvereiste van het LSP voldoen aan vereisten uit de wet. De patiënt dient uitdrukkelijk toestemming te gegeven voor het aanmelden en inzien van zijn gegevens, deze toestemming dient per zorgverlener en per aanmelding van gegevens te worden gegeven. Indien een patiënt geen toestemming geeft worden zijn gegevens niet aangemeld en kunnen zijn gegevens niet worden ingezien via het LSP. De beveiliging wordt gewaarborgd door de strenge eisen van een GBZ voor het computersysteem van de zorgverlener en het gebruik van UZI-middelen voor de identificatie van zorgverleners.

Informatieverstrekking patiënten
Patiënten van Ziekenhuis Rivierenland worden onvoldoende ingelicht over de doeleinden waarvoor hun persoonsgegevens worden verwerkt en verstrekt. Verder worden zij ook niet voldoende ingelicht over de wijze waarop hun persoonsgegevens worden verwerkt binnen het ziekenhuis en worden verstrekt aan derden. Het privacyreglement voldoet niet aan de huidige wet- en regelgeving en de informatiefolders omtrent de rechten van patiënten zijn niet up-to-date.

Toestemmingsvereiste
Het verstrekken van persoonsgegevens is in beginsel altijd gerechtvaardigd als patiënten daarvoor hun uitdrukkelijke toestemming hebben gegeven. Als patiënten toestemming geven voor het verstrekken van hun persoonsgegevens aan derden kan Ziekenhuis Rivierenland makkelijker en sneller gegevens verstrekken aan derden. Als patiënten hun uitdrukkelijke toestemming geven voor de verstrekking, is de verstrekking van persoonsgegevens gerechtvaardigd. Daarom is het van belang dat er toestemming wordt verkregen van patiënten.

8. Aanbevelingen

In dit hoofdstuk worden naar aanleiding van de conclusies, aanbevelingen gedaan aan Ziekenhuis Rivierenland omtrent het verwerken en verstrekken van persoonsgegevens betreffende patiënten. Door middel van de aanbevelingen kan het privacybeleid van Ziekenhuis Rivierenland verbeterd worden.

Verwerken

De verwerking van persoonsgegevens binnen Ziekenhuis Rivierenland dient op basis van een privacyreglement te geschieden. Op basis van een reglement kunnen medewerkers geïnformeerd worden over wat wel en niet mag, en hoe de verwerking precies dient te geschieden. Verder kan in een privacyreglement precies worden vastgelegd hoe het privacybeleid van Ziekenhuis Rivierenland eruit ziet. Hierdoor kan Ziekenhuis Rivierenland de privacy van patiënten garanderen en aantonen dat hun beleid voldoet aan de wet- en regelgeving. Het reglement is zowel van belang voor het eenduidig voeren van een privacybeleid binnen Ziekenhuis Rivierenland als voor het informeren van patiënten over het privacybeleid. Omdat het huidige privacyreglement niet meer voldoet aan de geldende wet- en regelgeving en dus niet meer toereikend is, is het van belang dat er een nieuw privacyreglement wordt opgesteld. Verder wordt het voeren van een privacybeleid en het hebben van een privacyreglement verplicht als de nieuwe privacyverordening wordt ingevoerd. Een concept privacyreglement is opgenomen als bijlage 14.

Verstrekken

Aan de hand van de opgestelde toetsingsmatrix[90] dient bepaald te worden welke gegevens aan welke derden mogen worden verstrekt. Alvorens de persoonsgegevens betreffende een patiënt te verstrekken aan een derde dient afgewogen te worden aan de hand van de toetsingsmatrix of de verstrekking rechtmatig is en niet te veel risico's met zich meebrengt. Elke gegevensverstrekking dient te berusten op toestemming van de patiënt of op een van de rechtvaardigingsgronden uit de wet.

De gegevensverstrekking van het laboratorium aan de Regioapotheek is niet rechtmatig, er worden bovenmatig veel gegevens verstrekt. Omdat Ziekenhuis Rivierenland verplicht is de gegevens te verstrekken op grond van een wettelijke bepaling moet gekeken worden hoe de gegevensverstrekking rechtmatig kan geschieden. Er moet gekeken worden hoe de gegevens kunnen worden verstrekt aan de regioapotheek zonder dat er bovenmatig veel gegevens worden verstrekt. Dit kan bijvoorbeeld door een speciaal portaal te maken waarin apothekers medicatiegegevens van hun patiënten kunnen inzien. Aansluiting bij het LSP zou hier in de toekomst eventueel ook een uitkomst voor bieden, doordat het in de toekomst mogelijk wordt om labuitslagen van de patiënt beschikbaar te stellen via het LSP.

Beveiliging verstrekking

De persoonsgegevens die bedoeld zijn om opgenomen te worden in een bestand, die via onbeveiligde e-mail, fax of telefonisch worden verstrekt aan derden zijn niet voldoende beveiligd. De verstrekking van die gegevens via onbeveiligde e-mail en fax moet geminimaliseerd worden. Enkel met specifieke toestemming, voor het verstrekken van gegevens via onbeveiligde e-mail of fax, van de patiënt kunnen gegevens worden verstrekt via onbeveiligde e-mail of fax. Deze toestemming kan worden verkregen met een toestemmingsformulier, dat kan worden voorgelegd in situaties waarin het van groot belang is dat de gegevens met spoed worden verstrekt aan de derde. Het telefonisch verstrekken van gegevens moet niet worden toegestaan, omdat hiermee de beveiliging van de persoonsgegevens en de privacy van de patiënt niet kan worden gewaarborgd.

[90] Zie bijlage 12

Bewustwording medewerkers
Om een goed privacybeleid te voeren en te volgen, is het van belang dat medewerkers zich bewust zijn van de privacy van een patiënt. Medewerkers dienen ingelicht te worden over het nieuwe privacyreglement. Ze dienen te worden ingelicht over welke gegevens zij wel en welke gegevens zij niet mogen verstrekken aan derde en aan welke derde zij deze mogen verstrekken.

Landelijk schakelpunt
Aansluiting bij het LSP zou een goede ontwikkeling zijn voor Ziekenhuis Rivierenland. Door aan te sluiten kunnen huisartswaarneemgegevens en medicatiegegevens van een patiënt gemakkelijk worden opgezocht. Aansluiting bij het LSP bevordert de patiëntveiligheid.

Informatieverstrekking patiënten
Het is van groot belang dat patiënten weten welke persoonsgegevens over hen worden verwerkt en dat er persoonsgegevens worden verstrekt aan derden. Om patiënten te informeren is het van belang dat de informatiefolders voor patiënten worden aangepast zodat zij voldoen aan de geldende en toekomstige wet- en regelgeving. De informatiefolder over het inzage-, kopie- en vernietigingsrecht dient aangepast te worden aan de Wbp, de folder is nu nog gebaseerd op de WPR.

Toestemmingsvereiste
Indien de patiënt ondubbelzinnige toestemming verleent voor de verstrekking van zijn persoonsgegevens, kunnen hulpverleners makkelijker en sneller persoonsgegevens verstrekken aan derden. Omdat de verstrekking van persoonsgegevens in beginsel enkel geschiedt indien dit noodzakelijk is voor de goede behandeling van de patiënt, is het noodzakelijk dat patiënten weten dat de verstrekking enkel en alleen in hun belang geschiedt. Het is van belang dat patiënten toestemming geven voor het verstrekken van hun gegevens. Om patiënten zover te krijgen dat ze ook daadwerkelijk toestemming geven voor de verstrekking van hun gegevens dient er een informatiefolder te worden gemaakt over het geven van toestemming voor de verstrekking van gegevens. In de folder dient uitgelegd te worden aan welke zorgverleners gegevens kunnen worden verstrekt, op welke voorwaarden, wat de voor- en nadelen zijn en waarom dit van belang is voor de patiënt. Verder dient er te worden uitgelegd hoe de patiënt toestemming kan gegeven, bijvoorbeeld via de site of via een toestemmingsformulier.

Evaluatie

In dit hoofdstuk wordt teruggeblikt op de verloop van het onderzoek. Zowel het proces als het product zullen worden geëvalueerd. Bij de evaluatie van het proces wordt ingegaan op de totstandkoming van het onderzoeksrapport, wat er goed is verlopen en wat er minder goed is verlopen. Bij de evaluatie van het product wordt gekeken of de conclusies en aanbevelingen die voortvloeien uit het onderzoek voldoende antwoord geven op de centrale vraag en de deelvragen.

Proces

Het onderzoeksplan is steeds de rode draad geweest voor de uitvoering van het onderzoek. Het onderzoeksplan is gedurende het onderzoek op een paar punten gewijzigd. Zo bleek het niet haalbaar om vragenlijsten te verspreiden onder alle ziekenhuizen die aangesloten zijn bij het LSP. Verder is er geen vergelijking gemaakt met het beleid van twee andere ziekenhuizen. Ik heb wel een interview afgenomen in het St. Anna Ziekenhuis en een vragenlijst toegestuurd aan het MMC maar ik heb de resultaten uit deze interviews niet verder verwerkt in het onderzoeksrapport. Wel hebben deze interviews geholpen bij het opstellen van het concept privacyreglement. Verder heb is de voorgenomen hoofdstuk indeling en deelvragen op een paar kleine punten gewijzigd.

Met betrekking tot de interviews kan vastgesteld worden dat de medewerking van alle partijen een groot voordeel heeft gehad voor het onderzoek. Door middel van de interviews heb ik de meeste informatie over de verwerking en verstrekking van persoonsgegevens in de praktijk in beeld kunnen brengen. De opgenomen interviews zijn geautoriseerd door de geïnterviewden.

Product

Het onderzoek is voornamelijk gericht op de verstrekking van persoonsgegevens aan derden. In belang van het onderzoek was het echter noodzakelijk om ook de wijze van verwerking in kaart te brengen, om te kunnen beoordelen of de gegevensverstrekking van Ziekenhuis Rivierenland aan de nu en in de toekomst geldende privacywetgeving voldoet. Uiteindelijk heeft de toetsing van de huidige wijze van verwerking en verstrekking aan het juridisch kader geleid tot de belangrijkste conclusies en aanbevelingen. De toetsing van de twee casussen is van belang om het onderzoek concreet te maken en om aan te tonen of Ziekenhuis Rivierenland daadwerkelijk voldoet aan de wet- en regelgeving. Om de leesbaarheid van de tekst te ondersteunen is ervoor gekozen om de uitgewerkte casussen in de toetsingsmatrix op te nemen in de hoofdtekst.

Uit het onderzoek zijn bruikbare onderzoeksresultaten voortgevloeid voor Ziekenhuis Rivierenland. Aan de hand van de toetsingsmatrix en de concept privacyreglement kunnen zij hun privacybeleid vorm gaan geven. Het onderzoekrapport is van grote waarde voor Ziekenhuis Rivierenland. Het rapport schept meer duidelijkheid omtrent de wettelijke bepalingen en dient als startpunt om het privacybeleid verder vorm te gaan geven binnen de organisatie.

Literatuurlijst

Bannier e.a. 2008
F.A.W. Bannier e.a., *Beroepsgeheim en verschoningsrecht,* Den Haag: SDU Uitgevers 2008.

Berkvens & Prins 2007
J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk,* Deventer: Kluwer 2007.

Hooghiemstra & Nouwt 2013
T.F.M. Hooghiemstra & J. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers 2007.

Huydecoper & Gardeniers 2006
S.M. Hydecoper & H.J.M. Gardeniers, *Wet bescherming persoonsgegevens en ICT*, Den Haag: Sdu Uitgevers 2006.

Koekkoek 2000
A.K. Koekkoek, *De grondwet: een systematisch en artikelsgewijs commentaar*, Deventer: Tjeenk Willink, 2000.

Leenen & Gevers 2011
H. leenen & S. Gevers, *Handboek gezondheidsrecht: deel 1*, Den Haag: Boom Juridische uitgevers 2011.

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

Thole, Van der Jagt & Roerdink 2010
E. Thole, F. van der Jagt & H. Roerdink, *50 vragen over privacy,* Deventer: Kluwer 2010.

De Vries & Rutgers 2001
H.H. de Vries & D.J. Rutgers, *Actualiteiten Sociaal Recht. Wet bescherming persoonsgegevens. Toepassing in arbeidsverhoudingen,* Deventer: Kluwer 2001.

Witmer & De Roode 2004
J.M. Witmer & R.P. de Roode, *Van wet naar praktijk. Implementatie van de WGBO. Deel 4 Toegang tot patiëntgegevens,* Utrecht: KNMG 2004.

<u>Rapporten en richtlijnen</u>

College Bescherming Persoonsgegevens 2008
Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm, College bescherming persoonsgegevens, 2008.

College Bescherming Persoonsgegevens 2011
Informatieblad geheimhouding van medische gegevens, College bescherming persoonsgegevens, 2011.

College bescherming persoonsgegevens 2013
CBP Richtsnoeren: Beveiliging van persoonsgegevens, college bescherming persoonsgegevens, 2013.

College Bescherming Persoonsgegevens 2013
Toegang tot digitale patiëntendossiers binnen zorginstellingen, College bescherming persoonsgegevens, 2013.

KNMG 2010
Richtlijnen inzake het omgaan met medische gegevens, KNMG, Utrecht: 2010.

KNMG & Nictiz 2013
Gedragscode Elektronische gegevens uitwisseling in de Zorg, KNMG & Nictiz, 2013.

Nederlands Normalisatie-instituut
Norm NEN 7510, Nederlands Normalisatie-instituut, 2011.

Nederlands Normalisatie-instituut
Norm NEN 7512, Nederlandse Normalisatie-instituut, 2005.

Nederlands Normalisatie-instituut
Ontwerp norm NEN 7512, Nederlands Normalisatie-instituut, 2013.

NICTIZ 2011
Programma van eisen organisatie goed beheerd systeem (GBx), Nictiz, 2011.

Sauerwein & Linnemann 2002
L.B. Sauerwein en J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens,* Ministerie van Justitie, Den Haag: 2002.

Artikelen

Engelfriet
A. Engelfriet, 'Wat te verwachten van de privacyverordening?', *ICT & Recht* 2014, p. 4-6.

Lassche
M. Lassche, 'Wet- en regelgeving', *ICT & Recht* 2014, p. 9.

Veereschild 2012
S. Veereschild, Normen: Vrijheid, Verantwoordelijkheid en Veiligheid, *Zorg en Financiering* 2012.

Elektronische bronnen

'Wie is verantwoordelijk?', *NVZ*, www.nvz-ziekenhuizen.nl (kies onderwerpen, kies j-l, kies LSP)

'Toestemming patiënt', *VZVZ*, www.vzvz.nl (zoek op toestemming patiënt).

'Specifieke toestemming voor gegevensverwerking via het LSP', *VZVZ*, www.vzvz.nl (zoek op specifieke toestemming).

'Beveiliging', *VZVZ,* www.vzvz.nl (zoek op beveiliging).

'Cijfers', *VZVZ* 17 maart 2014, www.vzvz.nl (zoek op feiten en cijfers).

'Lijst regio-indeling', *VZVZ*, www.vzvz.nl (zoek op regio-indeling en kies nr. 31. Tiel).

‘Rechtzaak over verbod op LSP’, *VP Huisartsen* 24 maart 2014, www.vphuisartsen.nl (zoek op verbod LSP).

Patiëntenpas en identificatieplicht, www.zrt.nl (zoek bij patiënten → patiëntenpas en identificatie).

<www.cbpweb.nl>
<www.nvz-ziekenhuizen.nl>
<www.vzvz.nl>
<www.nen.nl>
<www.zrt.nl>

Jurisprudentie

HR 9 september 2011, ECLI:NL:HR:2011:BQ8097.

CBP 21 mei 2003, z2003-00214.

CBP 22 april 2003, z2003-00284.

CBP 26 februari 2004, z2003-01597.

Centraal Tuchtcollege voor de Gezondheidszorg 10 februari 2005, 2004/161.

Europese richtlijnen

Richtlijn 95/46/EG (*PbEG* 1995 L 281/31).

Voorstel verordening van het Europees Parlement en de Raad nr. 2012/0011.

Kamerstukken

Kamerstukken II 1997/98, 25 892, 3 (MvT).