BORKING CONSULTANCY

ONGEDOLVEN GOUD: VAN DATA NAAR INFO – CONCEPT-ADVIES

KNELPUNTEN, AANBEVELINGEN, BEPERKINGEN

GEBRUIK VAN PRIVACY-BY-DESIGN

7 april 2014
Status: Definitief
Versie:Finaal

Lange Kerkdam 27
NL 2242 BN Wassenaar
Tel.: 062 – 958 2789
Fax.: 070 – 517 8936
Email: jborking@xs4all.nl

KvK Haaglanden dossierno. 27249622
BTW no. NL 0625 24 689 B.01
Bankrekeningno. 62.54.66.608
ABN AMRO Wassenaar

1.2 Versiegeschiedenis

Versie	Versiedatum	Opgesteld door	Samenvatting / aanpassingen
1.0	06-02-2014	J.Borking	1e concept verzonden
	06-02-2014	J.Borking	Overleg 13-02-2014 met T.Hooghiemstra, M. ten Have, M. van Gemert – input docs
1.1	04-03-2014	J.Borking	Verwerken van commentaar Theo Hooghiemstra, Marcel van Gemert; Toevoegingen over technologie
1.2	10-03-14	J.Borking	Toevoegen PbD voor PGD en TTP, uitbreiding aanbevelingen
2.0	13-03-14	J.Borking	2e concept verzonden
Finaal 3.0	31-03-14	J.Borking	Verwerking van commentaar Theo Hooghiemstra 25-03-2014
4.0	07-04-14	J.Borking	Verwerking van commentaar Theo Hooghiemstra 06-04-2014

2. Opdracht

Aan Borking Consultancy (Dr. J.J.F.M.Borking, Lange Kerkdam 27, NL 2242 BN Wassenaar, Tel. 06-2958 2789; Fax. 070- 517 8936; email: jborking@xs4all.nl) is gevraagd ten behoeve van het adviestraject 'Ongedolven Goud: van data naar info' voor de Raad voor de Volksgezondheid en Zorg te Den Haag de volgende werkzaamheden uit te voeren:

A. Het uitvoeren van een studie die de volgende vragen zal beantwoorden:

1. Welke knelpunten rondom privacy signaleert u in de oplossingsrichtingen die worden beschreven in het concept-advies? Het gaat om knelpunten op de middellange termijn, mede in het licht van ontwikkelingen zoals 'big data' en de decentralisatie.
2. In hoeverre kunnen deze knelpunten worden opgelost door 'privacy-by-design'?
3. Welke concrete aanbevelingen volgen uit de geschetste oplossingsrichtingen?
4. Wat zijn de beperkingen van de geschetste oplossingen?

De studie dient een samenvatting van 1 A4 te bevatten en dit is het enige onderdeel dat door de voltallige Raad wordt gelezen. Een concept met globale bevindingen dient uiterlijk 3 februari te zijn ontvangen door de RVZ en de definitieve studie dient uiterlijk 1 maart 2014 te zijn ontvangen door de RVZ.

B. Het becommentariëren van het conceptadvies in de periode februari-mei.

Over de opdracht is met de heer Mr. Drs. T.F.M. Hooghiemstra en mevrouw Dr. M. Ten Have telefonisch en per email overleg gevoerd.

De nota: "Ongedolven goud, van data naar info, concept redeneerlijn ter vaststelling in de raadsvergadering van 19 december 2013 is door de RVZ aan Borking Consultancy ter hand gesteld en daarna is het concept-advies aan hem voorgelegd.

Vervolgens heeft Borking Consultancy op 10 januari 2014 een offerte ten behoeve de bovenstaande werkzaamheden aan RVZ gestuurd, die op 14 januari 2014 door RVZ is geaccepteerd.

3. Aanleiding voor dit advies

De aanleiding voor dit advies is de vraag van de Raad voor de Volksgezondheid & Zorg om antwoord te geven op een viertal vragen te weten:

1. Welke knelpunten rondom privacy signaleert u in de oplossingsrichtingen die worden beschreven in het concept-advies? Het gaat om knelpunten op de middellange termijn, mede in het licht van ontwikkelingen zoals 'big data' en de decentralisatie.
2. In hoeverre kunnen deze knelpunten worden opgelost door 'privacy-by-design'?
3. Welke concrete aanbevelingen volgen uit de geschetste oplossingsrichtingen?
4. Wat zijn de beperkingen van de geschetste oplossingen?

Deze vragen zijn een gevolg van de concept-redeneerlijn in het rapport 'Ongedolven goud, van data naar info'.

De aanbevelingen zijn enerzijds bestemd voor een informatiestelsel rondom de te verwachten persoonlijk gezondheidsdossiers (PGD's), waarin de patiëntengegevens optimaal worden verwerkt ten behoeve van een betere kwaliteit van zorg, terwijl tegelijkertijd de privacy van de patiënt wordt gewaarborgd en anderzijds voor de overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek.

Casuspositie: Grote hoeveelheden data worden verzameld, verwerkt, gedistribueerd en opgeslagen in de zorg. Desondanks worden de patiënt en de burger geconfronteerd met diverse knelpunten doordat hijzelf en diverse zorgprofessionals vaak niet over de informatie en kennis beschikken die zij nodig hebben om een betere gezondheid van patiënten en burgers te realiseren.

Dit heeft geleid tot de beleidsvraag voor het concept-advies: Hoe kan het verwerken van data worden geoptimaliseerd ten behoeve van een betere kwaliteit van de zorg? Het belang van de patiënt en de burger en diens gezondheid dient centraal te staan. Het verwerken van data in de zorg raakt immers ook mensen die nog niet ziek zijn, bijvoorbeeld wanneer het gaat om preventie of onderzoek.
Onder het verwerken van data verstaan we het verzamelen, opslaan, gebruiken en vernietigen van data.
Het concept-advies richt zich tot de actoren die direct of indirect een relatie met de patiënt hebben en belicht het perspectief van actoren die op micro-, meso en macroniveau bijdragen aan een betaalbare en toegankelijke zorg van hoge kwaliteit. Microniveau betreft patiënt en zorgverlener. Mesoniveau betreft organisaties en instellingen, zoals zorgaanbieder, zorgverzekeraar en gemeente. Macroniveau betreft overheid, beleid en wetenschap. Voor een adequate informatievoorziening is de verbinding van micro-, meso- en macroniveau van belang. Het accent wordt gelegd bij de 'governance' van de kennis- en informatiestrategie. Bij het beantwoorden van de beleidsvraag bestrijkt de verwerking van data in de gehele breedte, dus voor preventie, cure en care.

4. Management samenvatting

1. Knelpunten

Bij de bestudering van de concept-advies zijn een aantal knelpunten op middellange termijn voorzien:

1.Verwacht wordt dat de patiënt toegang en beheer van zijn persoonlijk gezondheidsdossier (PGD) krijgt op basis van vrijwilligheid en met de keuze uit meerdere PGD's. In de praktijk zullen niet alle patiënten / cliënten gebruik kunnen en willen maken van PGD's in aanvulling op overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek.

Onder andere door de vergrijzing zullen grotere aantallen 'gemiddelde' (laag opgeleide en bejaarde) patiënten hun PGD niet (meer) willen en/of kunnen controleren en/of beheren. Commerciële (adviserende) diensten zullen het beheer van hen overnemen. Zij zullen de verkregen informatie naast het PGD zelf opslaan en voor data analyses gaan gebruiken. Dit kan tot manipulatie van de patiënt leiden. De visie over de participerende patiënt in het RVZ advies (2013) is te rooskleurig.

2.Bij zorgverleners kan, wanneer patiënten per onderwerp en gegeven mogen bepalen wie in het PGD dossier daar toegang toe krijgt en welke gegevens niet gedeeld mogen worden, twijfel ontstaan over de juistheid en volledigheid van het dossier. Om het risico op medische fouten te verkleinen zullen tests en anamnese worden herhaald, wat de efficiëntie van het PGD zal ondermijnen. Logging van wijzigingen in het PGD is gewenst.

3. Gezien het grote macro-economisch belang van de gezondheidszorg wordt voorzien dat geautomatiseerde aanvallen op de gezondheidsinformatiehuishouding zullen toenemen. Dergelijke aanvallen kunnen door personen met weinig expertise worden uitgevoerd.

4. De ontwikkelingen binnen de gezondheidszorg zullen leiden tot het gebruik van een verscheidenheid aan ICT-technologieën. Bij data volgende-, gegevens koppelende- en informatie ontdekkende en extraherende technologieën spelen persoonsidentiteiten een sleutelrol. Hierbij kunnen er omvangrijke data lekken en privacy inbreuken optreden en kunnen identiteiten van patiënten en hun gegevens op vele (onbekende) plaatsen door commerciële partijen worden opgeslagen met ongewenst gebruik als gevolg. Het gebruik van pseudo-identeiten is noodzakelijk.

5. Bij het meervoudig en secundair (her)gebruik van medische gegevens door vele afnemers en het gebruik van big data zullen aan anonimisering en de-anonimisering zeer hoge eisen moeten worden gesteld, wil identificatie worden voorkomen. Cloud computing vormt een extra risico door de potentiele toegang van de Amerikaanse overheid tot opgeslagen gegevens en het gebruik van opslagtechnieken die ongewild hergebruik van gegevens tot gevolg zou kunnen hebben.

6. De wettelijke vereisten ter bescherming van persoonsgegevens en de boetes bij overtreden zullen aanzienlijk worden verzwaard.

2. Oplossingen door Privacy-by-design

De geconstateerde privacy knelpunten kunnen voor een zeer groot deel worden voorkomen door gebruik te maken van Privacy-by Design (PbD) waarvan de kern bestaat uit Privacy-Enhancing Technologies (PETs). Dit zijn technische maatregelen gericht op het beschermen van de privacy van de patiënt en zorgverlener en andere bij de 'patient-centered care' informatiehuishouding betrokkenen. Het basis ontwerp patroon bestaat uit een of meerdere Identity Protectors en het creëren van meerdere (pseudo)-identiteitsdomeinen en pseudo-identiteiten. Deze aanpak wordt toegepast in een privacy-by-design PGD. De medische en financiële gegevensstromen kunnen

hier door worden gescheiden. Bovendien houden de patiënt, arts en zorgverlener zeggenschap op de toegang tot het PGD en wie welk gedeelte mag inzien. De toepassing van PbD leidt tot een 'end-to-end' beveiliging, identiteits- en toegangsmanagement en een sterke op de functie gebaseerde authenticatie. Controlemogelijkheden, logging en auditing en terugkoppeling worden voor de patiënten ingebouwd. Gezien de complexiteit is het gebruik van privacy management systemen(PMS) noodzakelijk om privacy regels geautomatiseerd afdwingen. Onmisbaar is bij de gegevensuitwisseling de inschakeling van meerdere 'trusted third parties' (TTPs). Encryptie en decryptie zijn hierbij voor alle medische data een sine qua non.
Als PbD, zoals hierboven beschreven, wordt toegepast in PGD's en informatiesystemen in de gezondheidsinformatiehuishouding, dan zullen de medische gegevens van patiënten zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun gegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid.

3.Concrete aanbevelingen
Teneinde PbD te realiseren is het noodzakelijk vooraf:
1. Een PbD expertise centrum op te richten of deze expertise onder te brengen bij bestaande kennis- of standaardisatieinstituten, zoals Nictiz, ter ondersteuning van het PbD proces;
2. Druk vanuit standaarden en – in voorbereiding zijnde - wetgeving uit te oefenen door vast te leggen, dat een privacy risico analyse vooraf dient plaats te vinden en dat PbD 'by default' moet worden toegepast en gebruik gemaakt wordt van de adoptiefactoren. De 'General Data Protection Regulation' van de EU kan bij aanvaarding, vermoedelijk in 2015, voor die druk zorgen;
3. Een multi-actor analyse toe te passen omdat PbD moet voldoen aan een aantal fundamentele functionaliteiten en de 'stakeholders' (veel) specifieke eisen zullen hebben. Het is het wenselijk hen actief bij het besluitvormingsproces te betrekken. Dit zal een breed draagvlak scheppen en de adoptie van de PbD informatiehuishouding vergemakkelijken;
4. Uitvoerige privacy impact analyses (PIA's) te laten uitvoeren om de bedreigingen en risico's die optreden bij de verwerking van medische gegevens in kaart te brengen. Op grond van de resultaten van de PIAs kan bepaald worden welke vormen van PbD gewenst zijn voor de informatiehuishouding;
5. De ontworpen privacy-by-Design architectuur in een pilot te testen;
6. Inzetten van TTP's bij PGD's en overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek;
7. Bij de decentralisatie van zorg naar gemeenten van begin af expliciet risicomanagement en Privacy-by-Design voorschrijven en inzetten;
8. Bij het opzetten van big data projecten zeer nauwkeurig de geanonimiserde data sets te onderzoeken op mogelijke direct en indirect identificerende gegevens;
9 PbD op te nemen in standaarden van PGD's en voor overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek.
10. Bij Cloud computing vooraf een PIA uit te voeren, waarbij tevens vastgesteld moet worden of de beveiliging, transparantie en rechtszekerheid voor de gebruikers goed geborgd zijn en welk rechtstelsel geldt. Wanneer het recht van een staat van de Verenigde Staten van toepassing is, geldt een contra-indicatie.

4. Beperkingen

Voor het realiseren van PbD ontbreken voldoende positieve adoptiefactoren. De wetgeving en de toezichthouder refereren nog niet expliciet aan (preventieve) PbD. Met de invoering van de Europese Privacy Verordening (2015) zal dit veranderen. Een kritische succesfactor is dat ICT systemen en met name IAM (Identity & Access management) systemen robuust moeten zijn en voldoende maturiteit moeten bezitten.

5. Eerste onderzoeksvraag:

Welke knelpunten rondom privacy signaleert u in de oplossingsrichtingen die worden beschreven in de concept advies? Het gaat om knelpunten op de middellange termijn, mede in het licht van ontwikkelingen zoals 'big data' en de decentralisatie.

5.1 Oplossingsrichtingen

De concept redeneerlijn richt qua oplossingsrichtingen zich op:
1. De gedecentraliseerde 'patient-centered care' waarbij patiënt en zijn directe familie centraal staat, hij bij de medisch klinische behandeling en zorg met respect wordt behandeld, rekening wordt gehouden met zijn voorkeuren, behoeften en waarden, zoals zijn privacy en het recht op niet-weten;
2.Het eenmalig registreren van patiënt gegevens aan de bron;
3.Het adequaat en efficiënt verwerken van medische data betreffende patiënt;
4.Het gebruiken van elektronisch patiëntendossiers;
5.Het meervoudig gebruik van door de patiënt en door de zorgverlener in de ruimste zin van het woord, de zorgaanbieder, het wetenschappelijk onderzoek, de zorgverzekeraar en gemeente ten behoeve van de patiënt genereerde medische en zorg gegevens;
6.Een op micro, meso en macro geïntegreerde informatiehuishouding ten behoeve van preventie en de genezing en verzorging van de patiënt op basis van standaardisatie teneinde een flexibele, veilige en betrouwbare informatiehuishouding te bewerkstelligen in plaats van een rigide systeem;
7.De behaalde resultaten onder meer in de vorm van uitkomstindicatoren te gebruiken als terugkoppeling ten behoeve van de kennis en uitvoering in de gezondheidszorg;
8.Het optimaal inzetten van informatie technologie, inclusief internet;
9.Binnen de in het in de oplossingsrichtingen voorziene gezondheidsproces gegenereerde 'big data' gebruiken ten behoeve van de gezondheidsinformatie en het managen van het totale gezondheidsproces.
10. Buiten de oplossingsrichtingen blijft de specifieke positie van de verzekerde versus de verzekeraar. Dit is voor het vaststellen van privacy beschermende maatregelen in de geïntegreerde informatiehuishouding ook niet nodig. Voor de wetgever is wat betreft de privacybescherming het irrelevant of de patiënt verzekerd is

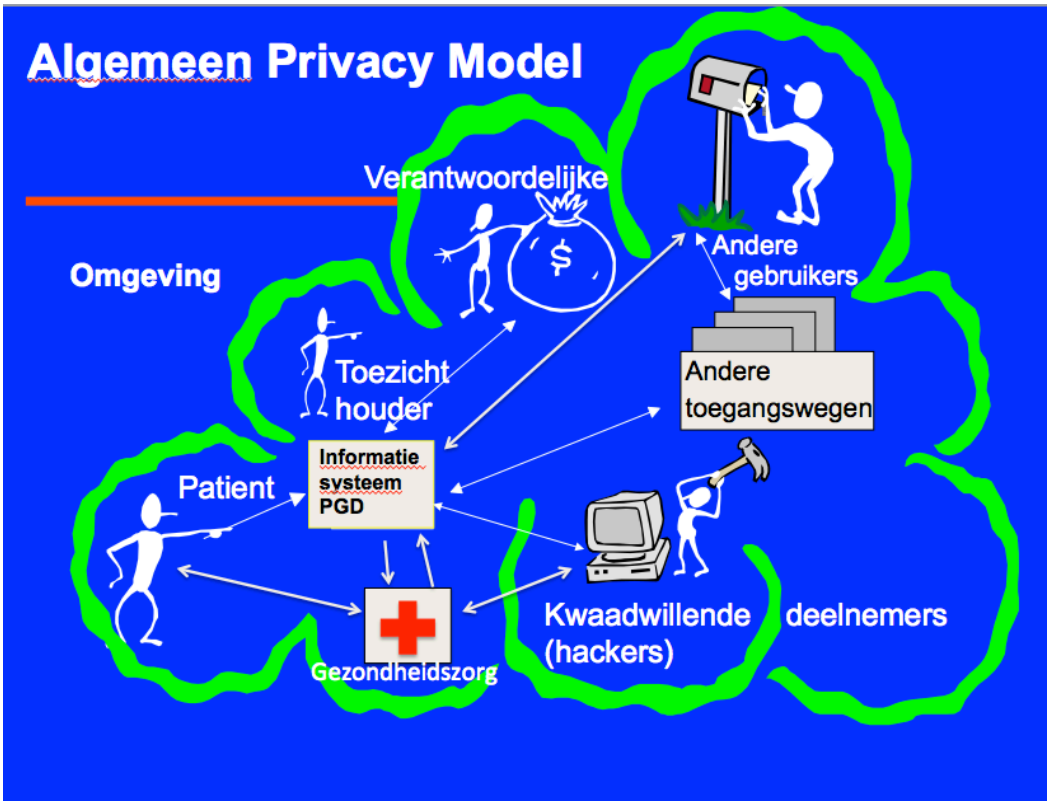
5.2 Algemene privacy knelpunten op middellange termijn

Privacy bescherming en het medisch beroepsgeheim vereist dat de zorgvuldige omgang met vertrouwelijke gegevens van patiënten dient centraal te staan. Vanuit de privacy problematiek gaat het om medische gegevens die door de Wbp als bijzondere en gevoelige direct of indirect identificerende persoonsgegevens worden gekwalificeerd.
De medische zorg-systemen worden steeds meer en meer verfijnd en voorzien van tal van toepassingen, waar niet alleen medische professionals toegang tot hebben, maar ook de boekhouding, de IT afdeling en het administratief personeel.
Uit onderzoek blijkt dat patiënten bezorgd zijn dat hun persoonlijk gezondheidsdossier in de handen van hun werkgevers of overheidsinstanties vallen zonder hun toestemming en kennis en dat de hoeveel informatie die aan zorgverleners en verzekeraars wordt gegeven ongelimiteerd is[1].

[1]. Rothstein M.A., The Hippocratic Bargain and Health Information Technology, in Journal of Law, Medicine &

Ruotsalainen stelt dat het belangrijkste knelpunt is dat de op de huidige beveiliging en toegangscontrole gerichte implementatie modellen niet het vertrouwen en privacy kunnen te garanderen binnen de alles omvattende rond de patiënt gecentreerde gezondheidszorg. Op technisch vlak worden in de huidige informatiesystemen voor de gezondheidszorg beveiligingsoplossingen gebruikt die vooral organisatorisch en reactief zijn en zijn gebaseerd op statische regels. Deze zijn noch context- of content-bewust, en zijn bedoeld om te worden gebruikt in een gecontroleerde omgeving met vooraf gedefinieerde regels. Er zijn daarom nieuwe informatie systeem architecturen nodig om de kwetsbaarheid drastisch te verminderen.[2] Bij gebrek aan voldoende gerichte research naar privacy-by-design architecturen ontstaat er een belangrijk knelpunt voor de ontwikkelingen van een privacy veilig 'patient-centered' care.

Het algemene privacy model geeft aan welke informatiestromen er tussen de verschillende actoren kunnen bestaan. Knelpunten kunnen bij de actor zelf ontstaan, door veranderingen in de omgeving en door de in de concept-redeneerlijn geïndiceerde informatiestromen.



Figuur 1: algemeen privacy model[3]

Ethics, 2010, p.7-13

[2]Ruotsalainen P. et al., Framework model and principles for trusted information sharing in User Centered Networked Health Care, IOS press, Amsterdam 2011, p.500 e.v.

[3] Bewerking van model van Van Blarkom G.W., Borking J.J., Olk J.G.E., Handbook of Privacy and Privacy-Enhancing Technologies, The Hague, 2003, p.144

De veelheid van informatie en communicatiestromen leggen zware eisen op de beveiliging van informatie, de toegangscontrole en de bescherming van de privacy. In het algemeen geldt dat alle informatie zowel in de elektronisch PGD en de databanken van de zorgaanbieders, als bij verzending over gezondheids- en andere netwerken adequaat (zwaar) versleuteld dient te zijn. Wat betreft de versleuteling en beveiliging is het knelpunt dat het niveau van de beveiliging en bescherming naar de dan (>5 jaar) geldende stand van de techniek niet meer toereikend zal zijn. Deze ontwikkeling vereist voortdurende aanpassing.
Op middellange termijn zal de gezondheidszorg (in toenemende mate) internationaal (EU, mondiaal) georganiseerd zijn en zullen internationale standaarden de privacy veilige architectuur van het medische zorg systemen bepalen.

5.3 Welke knelpunten kunnen bij de patiënt op middellange termijn optreden?

De gemiddelde digitale vaardigheden van de huidige 60-ers (idem: lager opgeleiden, allochtonen en inactieven) met betrekking tot ICT toepassingen is beperkt. Met Internet en email kan worden om gegaan, maar met veel meer dan dat ook niet.[4] Op middellange termijn (5-10 jaar) zal er een sterke toename (verdubbeling) van het aantal bejaarde patiënten plaatsvinden met beperkte aanpassing aan en begrip van de ICT toepassingen. (De human interface problemen kunnen met gebruik van de ergonomisch doordachte symbolen ('icons') problemen verminderen).

In de praktijk zal blijken dat vele patiënten niet of niet meer in staat zullen zijn hun gekwalificeerde toestemming te geven. Op termijn kan of wil de patiënt het beheren van en de controle op de inhoud van zijn elektronisch persoonlijk gezondheidsdossier niet/ niet meer uitoefenen. Vele patiënten missen de kennis om dit te doen. De inzet van persoonsgebonden monitoringsystemen in zogenoemde 'slimme' huizen om de veiligheid van hulpbehoevende bejaarden te kunnen garanderen, zal sterk toenemen.[5] Derden kunnen ten behoeve van de patiënt dan hun (adviserende) diensten daarvoor commercieel aanbieden en zullen de verkregen informatie niet alleen in het PGD op laten slaan, maar ook in hun eigen systemen. Deze informatie kan vervolgens gebruik worden voor data analyses die kunnen leiden tot (ongewenste) aanbieding van andere (al dan niet) gerelateerde medische producten en diensten. Bovendien vergroot dit de ongeautoriseerde verspreiding van medische gegevens.

Er vanuit gaande dat de patiënt die het wil en kan in het 'patient-centered' care systeem zijn eigen medische informatie beheert, kunnen de volgende casusposities voorkomen:

1. De patiënt verandert de door hem kenbaar gemaakte/vastgelegde beperkingen aan het gebruik, de verwerking, bekendmaking en opslag van zijn medische informatie, die hij al dan niet met anderen heeft gedeeld; Dit kan leiden tot authenticatieproblemen en weerstand bij de zorgverleners.
2. De patiënt wenst meer transparantie, terugkoppeling c.q. grotere verificatiemogelijkheid met betrekking tot de verspreiding en het gebruik van zijn persoonlijke informatie;
3. De patiënt wil zijn gegevens meenemen naar een zorgverlener die niet is aangesloten op het informatie systeem dat de persoonlijke gezondheidsdossiers bewerkt en opslaat;

[4] Ingen van E., De Haan J. & M.Duimel, Achterstand en Afstand, SCB Den Haag 2007
[5] Advies van het Europees Economisch en Sociaal Comite over Matschappelijke betrokkenheid van ouderen en hun participatie in de samenleving (initiatiefadvies) (2013/C11/04)

4. De patiënt kan ten onrechte zijn toestemming onthouden worden,; hij kan via internet de nodige (soms onjuiste) informatie gaan verzamelen, medisch consult vragen en gaan 'shoppen' bij zorginstellingen en zorgverleners.

Voor een optimistische visie zie: het RVZ-advies 'De participerende patiënt': http://www.rvz.net/publicaties/bekijk/de-participerende-patientDe gestelde voorwaarden (in 2013) dienen eerst vervuld te zijn, voordat er over de volle breedte van de samenleving sprake kan zijn van een adequaat participerende en geïnformeerde patiënt. Tot nu toe zijn de inspanningen van de betrokken partijen niet voldoende om het beoogde doel te realiseren.

5.4 Knelpunt: Verantwoordelijke

De verantwoordelijke en de participerende actoren kunnen om kostentechnische en commerciële redenen besluiten op middellange termijn het informatiesysteem c.q. de informatiehuishouding dat de persoonlijke gezondheidsdossiers bewerkt en opslaat en de daarmee communicerende systemen niet aan te passen aan de stand van de techniek en de verhoogde privacy- en beveiligingseisen, die mede opgelegd kunnen worden door de toezichthouder. Budgettair zal hier rekening gehouden moeten worden. Het is denkbaar dat commercialisering van de informatiehuishouding tot ongewenste neven-marketing activiteiten leidt, zoals het aanbieden van gerichte 'banners'.
De verantwoordelijke en/of de bewerker (inclusief de Cloud) bevindt zich buiten de EU, waardoor gegevens niet geëxporteerd mogen worden

5.5 Knelpunt: zorgverlener / gezondheidszorg
Zorgaanbieders dienen gebruik te maken van een gestandaardiseerde diagnose rapportage. De correctheid en volledigheid van gegevens is onvoldoende gegarandeerd.[6] Dit gebrek wordt een knelpunt op middellange termijn. Mogelijk treedt er na verloop van tijd weerstand op bij de zorgprofessionals. Rothstein wijst er op, dat als patiënten per onderwerp en gegeven mogen beoordelen wie daar toegang toe krijgt en welke gegevens niet gedeeld mogen worden, het PGD voor de clinici minder waardevol zou kunnen worden en het risico op medische fouten zou kunnen toenemen. Clinici zouden de juistheid en volledigheid van de bestaande informatie in het PGD minder gaan vertrouwen en zouden geneigd zijn om tests en anamnese te herhalen, waardoor de efficiëntie van persoonlijk gezondheidsdossiers zou worden ondermijnd. [7] Logging van wijzigingen in het dossier kan dit voorkomen.

5.6 Knelpunt: Hackers

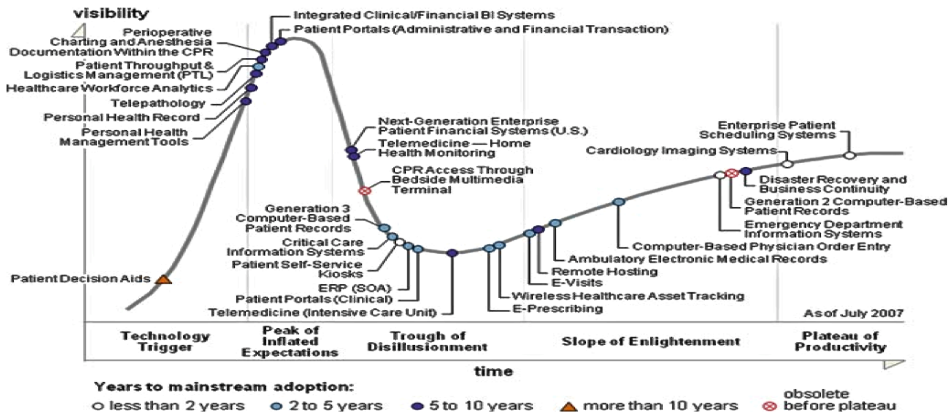
De trend is dat geautomatiseerde aanvallen op gezondheidsinformatiesysteem toenemen. Technieken om die aanvallen uit te voeren worden over het Internet verspreid, waardoor personen met aanmerkelijk minder expertise (de zgn. script kiddies),[8] maar in het bezit van

[6] Medisch Contact 14 mei 2009: M. Katzenbauer, Te vroeg voor landelijk EPD
[7] Rotnstein M.A., The Hippocratic Bargain and Health Information technology, journal of law, medicine & ethics, spring 2010, p.12
[8] Hieronder wordt verstaan een onervaren kwaadwillige hacker, die programma's gebruikt die door andere hackers zijn ontwikkeld om informatiesystemen aan te vallen en websites te bekladden; http://www.honeynet.org/papers/enemy/

generieke PC hardware een aanval kunnen uitvoeren. Het gaat om een automatische methode die in een netwerk of informatiesysteem inbreekt op het niveau van 'point-and-click'.
Deze ontwikkeling houdt in, dat voor een geautomatiseerde aanval weinig expertise is vereist van systemen, er weinig tijd nodig voor is en er ook geen geavanceerde computers gebruikt hoeven te worden voor een dergelijke 'scripted' (geprogrammeerde) aanval. Georganiseerde (criminele) aanvallen op de gezondheidsinfrastructuur voor eigen gewin zullen een knelpunt op middellange termijn vormen. Deze ontwikkeling werd bevestigd door de Europese Commissie tijdens de vergadering over EU Cybersecurity Strategy in Brussel op 28 februari 2014. Cyber aanvallen zijn de afgelopen jaren dramatisch toe genomen. Cyber criminelen zijn steeds moeilijker te traceren. Lybaert van Belgacom deelde mede dat er inmiddels 800.000 aanvallen per dag op Duitse Telekom plaatsvinden. Standaardisatie van systemen waar niet in 'state of the art' beveiliging is voorzien, kan het hackers probleem verergeren.

5.7 Knelpunt: Ontwikkeling Technologie

Bij het inschatten van knelpunten in de gezondheidszorg is de ontwikkeling van de technologie mede bepalend. Hieronder volgt een model over de verwachte ontwikkeling van het PGD.



Figuur 2 Ontwikkeling persoonlijk gezondheidsdossier in Web-Based Applications in A. Lazakidou, Healthcare and Biomedicine, New York, 2010

Op middellange termijn dient rekening gehouden te worden met de ontwikkeling van tele-geneeskunde, 'patient self service kiosks', de inzet van medische Apps via mobiel (smart)telefoons (smart watches) en internet (cloud) connecties, ambient intelligente omgevingen met (geïmplanteerde) sensoren en RFID chips (waarvan de informatie niet in het PGD terecht komt maar bij de commerciële aanbieders), het gebruik en de verspreiding van DNA profielen voor persoonsgericht medicijngebruik en het inzetten van robots en medische software agents.
Het PGD dient met deze ontwikkelingen rekening te houden.
Nu al geldt dat bij opslag van gegevens in een Cloud het risico van ongewenste en onbevoegde toegang (al dan niet door overheden, bijvoorbeeld onder de U.S. Patriot Act), datalekken en

misbruik van data toenemen.[9] De opdracht voor het bouwen, beheer en onderhoud van de gezondheid/zorg verlenende infrastructuur door een Amerikaans moeder of zusterbedrijf maakt dit mogelijk en moet afgeraden worden. De Europese Commissie deelt deze zorgen en heeft een Europese Cloud strategie in 2012 voorgesteld.[10]
De ontwikkelingen in de gezondheidszorg zullen leiden tot een verscheidenheid aan ICT-technologieën, waarvan het gebruik tot knelpunten kan leiden. Gilbert signaleert drie verschillende lagen van technologieën, die steeds meer convergeren en elkaar versterken. Bij deze technologieën spelen persoonsidentiteiten een sleutelrol. De Royal Academy of Engineers onderscheidt als eerste laag de 'Connection technologies', dat zijn technologieën die data volgen, bijvoorbeeld RFIDs en NFC. Als tweede laag gaat het om de 'Disconnection technologies', dat zijn gegevens koppelende technologieën, zoals de SIM kaart in mobiele telefoons en biometrische technologie, die de toegang tot data controleren. De derde laag zijn de 'Processing technologies', dat zijn technologieën die informatie ontdekken en extraheren, zoals data mining, data warehousing, big data en tijd-ruimte "Googleing" die mogelijk zijn door de goedkope massale opslag van gegevens en het Wereld Wijde Web.

Gilbert[11] ziet drie mogelijke scenario's voor de nabije toekomst (2020):

1. 'Big Brother', waarin met name de gegevens ontdekkende technologieën domineren, zoals data mining en data warehousing. In dit scenario leidt de dominante technologie tot gigantische databanken met een zeer sterke speurkracht. Alles is voor eeuwig vastgelegd en digitale patroonherkenning in grote hoeveelheden data kan zeer snel geschieden. Dergelijke databanken worden beheerd, hetzij door de overheid (Big Brother), hetzij door commerciële organisaties. Omdat de kosten van data processing mede door gebruik van clouds scherp zullen dalen, zullen ook individuen in staat zijn om voldoende opslag- en speurcapaciteit voor henzelf en ten nadele van anderen in te zetten. De privacy is in dit scenario verloren.
2. Bij het tweede scenario 'Big mess' domineren de technologieën die data volgen, zoals RFIDs en NFC. De chip in het paspoort, in de OV-chipkaart, in kleding en lichaam maken volledig toezicht mogelijk. Vooral als deze technologieën gecombineerd worden met niet-robuuste technologieën die data aan elkaar koppelen (smart cards, SIMs in mobiele telefoons, biometrische technologieën zoals spreker identificatie) zullen er voortdurend op grote schaal privacy incidenten plaatsvinden. Persoonsgegevens zullen tegen de wens van betrokkenen door data lekken publiek gemaakt worden en er zal op een misdadige manier van toezicht en persoonsgegevens gebruik gemaakt worden.
3. Het derde scenario is 'Little sisters'. In dit scenario domineren de gegevens koppelende technologieën. Persoonsgegevens zullen routinematig versleuteld worden en (digitale)identiteiten zullen worden gefragmenteerd. De sleutels tot deze gefragmenteerde identiteiten zullen beheerd worden door de 'Little sisters". Dat zijn nu de ISPs en creditcard maatschappijen, TTPs en straks zullen dat de 'identity management brokers' zijn, waar veel persoonsgegevens zullen zijn opgeslagen met mogelijke ernstige privacy inbreuken als gevolg. Dit scenario lijkt voor de informatiehuishouding binnen de gezondheidszorg een reële mogelijkheid

[9] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1, 2009
[10] http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
[11] Gilbert N., Dilemmas of privacy and Surveillance: Challenges of Technology change, (presentation and paper), London 2007,p. 14-18

5.8 Knelpunt: Zorg overdracht naar gemeenten

De overdracht van de zorg naar de gemeenten geeft op korte termijn al aanleiding tot bezorgdheid, omdat het beveiligings- en privacy bewustzijn niet naar de stand van de techniek is ontwikkeld. Het is niet duidelijk of de Gemeenten wel een rol kunnen gaan spelen in de 'patient-centered' care. Nu al kunnen vele gemeenten de WMO verplichtingen met moeite aan. Het proces van de verwerking van medische data dient van het begin af aan zeer zorgvuldig te worden opgezet waarbij expliciet risicomanagement en Privacy-by-Design wordt voorgeschreven voor alle systemen binnen de Gemeenten die gezondheidsdata verwerken,[12] op straffe van ernstige datalekken en privacy inbreuken. De overdracht van de jeugdzorg naar de Gemeenten geeft een indicatief beeld van wat er te verwachten valt.[13] De financiële positie van veel Gemeenten is tevens een bron van zorg.[14]

5.9 Knelpunten in concept advies

De in de oplossingsrichtingen voorgestelde aanpak, in combinatie met de bestaande informatiesystemen in de gezondheidszorg betekent niet alleen dat er meer medische gegevens in nieuwe contexten of door aggregatie zullen worden verwerkt, maar dat er ook patiëntgegevens beschikbaar komen voor een veel grotere groep afnemers, zoals verzekeraars, onderzoekers, wetshandhavers, nieuwe gezondheidszorg dienstverleners, etc. Het concept advies introduceert daarmee een nieuw risicoscenario met mogelijk het (niet- beoogd) lekken van medische informatie van en over individuen, indien niet gebruik wordt gemaakt van PbD.

De privacy gerelateerde knelpunten kunnen optreden daar waar medische gegevens worden gegenereerd, verzameld, verwerkt, verspreid en opgeslagen in de elektronische identiteitsinfrastructuur en de elektronische informatie-infrastructuur met de PGD, verwijsindexen voor het uitwisselen van gegevens, chipkaarten en sensoren.

Extra aandacht zal vergen het meervoudig (her)gebruik van medische gegevens door vele afnemers. Dit knelpunt kan alleen met Privacy-by Design architectuur adequaat worden opgelost. De mogelijkheden tot hacking binnen de op micro, meso en macro niveau geïntegreerde informatiehuishouding, de uitkomstindicatoren (mogelijk een waarschijnlijkheidsinstrument dat de status van onbetwistbaar feit kan krijgen) (zowel voor de patiënt, de zorgverlener, de commerciële en financiële sector) en big data zijn belangrijk aandachtspunten voor knelpunten en bedreigingen. De hoeksteen voor het delen van data en hergebruiken is vertrouwen en dat vertrouwen kan alleen tot stand komen als een onafhankelijke certificatie van systemen aantoont dat de privacy van de patiënt en zorgverleners adequaat is beschermd. Zo'n certificaat voor de gezondheidszorg zou moeten worden voorgeschreven om vertrouwen te krijgen en te houden.

---

[12] Art.1.b Wbp: 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;

[13] Cfr: Bakker J., Golbach I., Nuijen T. Schouten H., ,Over risico's gesproken, Een onderzoek naar risicomanagement van de decentralisatie van de jeugdzorg bij gemeenten , Amsterdam/Den Haag, 2013

[14], Giebels R. & G. Herderschee, Rijk treft zwakste gemeenten, overheveling van taken gaat vooral pijn doen waar de vraag naar zorg het grootst is, p.1, p.10-11 in De Volkskrant, 28 maart 2014

Knelpunt op middellange termijn is tevens de ontwikkeling dat concurrentie tussen zorg aanbiedende instellingen op nationaal en internationaal gebied, de adviesbureaus voor patiënten die niet met hun PGD om kunnen gaan, grensoverschrijdende gegevensstromen (uitwisseling en hergebruik van medische data) tussen EU lidstaten (complicerende factoren: de diversiteit van culturen, talen, beleid, regel- en wetgeving en operationele regelingen)[15] en de verschuiving van artsen in ziekenhuizen naar verplegend en zorg verlenend personeel thuis. Het verplegend en verzorgend personeel zal net zoals bij artsen in een register ingeschreven moeten worden om fraude te voorkomen.

De gekozen technologieën kunnen tot meer specifieke knelpunten en bedreigingen leiden[16].
Dit zal nader onderzocht moeten worden.

5.10 Wettelijke knelpunten: EVRM, General Data Protection Regulation, Wbp, WGMO

Om te beoordelen of de oplossingsrichtingen knelpunten en problemen op middellange termijn gaan opleveren op het gebied van de privacy, dienen de voorstellen in het concept-advies getoetst te worden aan artikel 8 EVRM, de Wet bescherming persoonsgegevens (Wbp) en de andere relevante medische wetgeving, die de privacy van de patiënt, het medisch beroepsgeheim (o.a. Wet op de geneeskundige behandelingsovereenkomst (WGBO)) en de zorgverlener betreffen. [17]
Daarnaast gelden specifieke ISO/CEN/NEN standaarden, die een rol in normatief opzicht spelen, zoals NEN 7510(2011), 7512(2014), 7513(2010), (o.a. toegang tot patiëntgegevens, de grondslagen voor uitwisseling), NEN 8028(2011) over telemedicine, en specifieke standaarden in de gezondheidszorg (bijvoorbeeld: HL7/CDA, ICD-9/10, CPT), die betrekking hebben op de structuur / het formaat van teksten, geluid , foto's, multimedia inhoud, medische codering die een rol spelen in normatief opzicht. Deze standaarden zijn niet in deze studie onderzocht.
Aiguier van EUROCONTROL (European Organisation for the Safety of Air Navigation) deelde dat wijdverbreide standaardisatie als keerzijde heeft dat systemen makkelijker te hacken zijn.[18]
De General Data Protection Regulation (GDPR) kan op termijn knelpunten veroorzaken door de verzwaarde eisen onder meer op het gebied van privacy impact assessment, privacy–by-design en privacy-by-default, data portabiliteit, en het recht om te vergeten. Tevens is in artikel 79 een zware boete van maximaal 5% van de wereldomzet (amendement LIBE) in het vooruitzicht gesteld als niet voldaan wordt aan de privacy-by-design vereisten. Het Europese Parlement aanvaarde op 12 maart 2014 de GDPR met de hoge boeten.
Invoering van de GDPR wordt voor 2015 voorzien en is afhankelijk van de uitslag van de Europese verkiezingen in mei 2014 en de opstelling van de Europese raad.

---

[15] Geissbuhler A et al., Trustworthy reuse of health data: A transnational perspective in international journal of medical informatics 82 (2013) 1–9
[16] Househ M., Sharing sensitive personal health information through Facebook, the unintended consequences, in *User Centred Networked Health Care A. Moen et al. (Eds.) IOS Press, 2011, p.616-620*
[17] Hooghiemstra T.F.M. & Nouwt S, Wet bescherming persoonsgegevens,Den Haag 2011; Article 29 Data Protection Working Party WP 131, Working Document on the processing of personal data relating to health in electronic health records (EHR) (2007); Working Document 01/2012 on epSOS ((European Patients Smart Open Services), 00145/12/EN WP 189, Adopted on 25 January 2012
[18] EU Cybersecurity Strategy in Brussel op 28 februari 2014

Zolang de vertrouwelijkheid, privacy en veiligheid 'state of the art' worden toegepast, zijn er geen grote ethische of juridische problemen te verwachten. Het gebruik van sterke cryptografie is een *sine qua non*.

5.11 Big Data

Het gebruik van 'big data' staat nog in de kinderschoenen. Er lijkt sprake te zijn van overspannen verwachtingen. Lanier stelt dat tot nu toe gebleken is dat "big data schemes eventually fail, for the simple reason that statistics in isolation only ever represent a fragmentary mirror of reality with no supporting scientific theory".[19] Er is weinig bekend over de risico's voor en de attitude van individuen in het algemeen en patiënten en zorgverleners in het bijzonder wanneer zij met de gevolgen van (datamining van) big data (profilering) worden geconfronteerd. Big data lijkt het beste nog te vergelijken met *data warehousing* en *data mining*, maar dan op grotere schaal.

Juridisch gezien is het probleem dat bij de analyse van big data vaak secundair gebruik van data voorkomt, die bij de eerste verzameling niet voorzien was. Hoe kun je daar juridisch mee omgaan? Welke mededeling moeten organisaties afgeven voor een doel dat nog onbekend is? Hoe kunnen mensen uitdrukkelijke toestemming voor datagebruik geven dat op het moment van toestemming onbekend is? Bij gevoelige gegevens zoals medische data klemt dat nog te meer. Het inzagerecht in de gegevens voor het datasubject blijkt bij dit soort operaties illusoir te worden. In ieder geval gelden voor big data de regels betreffende de rechtmatige grondslag, zoals toestemming, de uitvoering van een overeenkomst of gerechtvaardigd belang van de verantwoordelijke. Bij bestandsverrijking dient de verantwoordelijke de betrokkenen in te lichten, uiterlijk wanneer dat het geval zal zijn. In het voorstel van de *General Data Protection Regulation* is tijdens de behandeling in het LIBE committee in het Europese parlement een artikel 3a aangenomen dat het individu het recht op verzet tegen profiling geeft. Er zal wettelijk nog het een en ander moeten gebeuren om zonder problemen over te gaan tot big data analyses.

Er is nochtans een spraakmakend big data project onder auspiciën van de CNIL (de Franse privacy toezichthouder) uitgevoerd, waaruit afgeleid kan worden welke juridische voorwaarden gelden. Het gebruik van privacy-by-design blijkt daarbij cruciaal te zijn. Het gaat om het big data project D4D (data for development) van de telecomaanbieder Orange in Ivoorkust in juni 2012, waarvan de resultaten in mei 2013 zijn bekend gemaakt. Om toestemming van CNIL voor dit project te krijgen, zijn rigoureus alle mogelijke direct of indirect identificerende gegevens geanonimiseerd. Er gold een strikte ethische code zowel bij Orange als bij de researchers en er was een strikte kwaliteitscontrole tijdens de verzameling van data om o.a. datalekken te voorkomen.
Na de de-anonimisering en analyse werden de big data sets per interval van maximaal 15 minuten verwijderd onder toezicht van de CNIL. Het big data project betrof de analyse van het aantal telefoongesprekken per cel (telecom zend/ontvangst antenne), per uur binnen Ivoorkust en dat over een periode van december 2012 tot en met april 2013. De analyse werd door derden gedaan die geen binding met Orange hadden. Een van de uitkomsten van het onderzoek was dat het anonimiseren van big data zeer moeilijk is omdat er grote kans bestaat dat uit de geanonimiseerde data bij 'matching' met andere grote data bestanden toch identificerende informatie kan vrijkomen.
Daarom dient bij het opzetten van big data projecten zeer nauwkeurig de geanonimiserde data sets te worden onderzocht op mogelijke indirect identificerende gegevens. Bijvoorbeeld als een

[19] Lanier J., How Should We Think about Privacy, in Scientific American, November 2013, p.54-55

telefoonsignaal van een mobiele telefoon in plaats A wordt geregistreerd en het zelfde signaal wordt een uur later honderden kilometers verder weer wordt geregistreerd, dan kan dat op iemand duiden die het vliegtuig genomen heeft. De analyse van dit gegeven is dan snel gemaakt door de passagierslijsten te analyseren. Bij het bestuderen van anonimiserings- en de-anonimiseringstechnieken is wetenschappelijk aangetoond waarom de anonimisering van 'multidimensionale databases' (big data) moeilijk is en welke soort technieken niet moeten worden gebruikt. De gebruikte anonimiseringstrategie in het D4D project is zwak gebleken en maakt het een aanvaller niet al te moeilijk om data te her-identificeren en te koppelen.[20]
Bij gebrek aan een robuuste anonimiserings- en de-anominisering methode treedt in 20% van de gevallen ernstige reputatieschade op en is het vertrouwen van de betrokkenen verdwenen.[21] Overleg met de toezichthouders om de voorwaarden voor big data analyse vast te leggen is een vereiste en wordt een knelpunt als dit niet is geschied.

5.12 Cloud computing

Cloud computing bestaat uit een aantal technologieën en service modellen die zich richten op het gebruik van het Internet en de levering van IT-toepassingen, verwerkingscapaciteit, opslag en geheugen. Cloud Computing komt voor in vele vormen. Het Amerikaanse National Institute of Standards and Technology (NIST) omschrijft 'de Cloud' als:

"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[22]

In de omschrijving van het begrip cloud door het NIST ontbreekt het element: virtualisatie. Virtualisatie vormt de basis van Cloud architectuur.[23] Het idee achter virtualisatie is dat de Cloud Service Provider al zijn hardware (servers, netwerk en software) als één geheel beschouwd en hierop verschillende programma's heeft draaien. Als er meer vraag ontstaat, kan er een nieuw 'virtueel' systeem gemaakt worden en hoeft er geen nieuwe hardware te worden geïnstalleerd. Efficiënte data-opslagtechnieken worden in Clouds toegepast, b.v. door in plaats van hetzelfde bestand twee keer op te slaan, het bestand maar één keer op te slaan. Daarbij wordt gebruik gemaakt van 'single instance storage' en data deduplicatie.

Risico's die zich voordoen zijn gebrek aan controle en gebrek aan informatie over de verwerking (transparantie). Als cloud computing een optie is, dan dient er eerst een privacy risicoanalyse (PIA) te worden uitgevoerd. Vastgesteld moet worden of de beveiliging, transparantie en rechtszekerheid voor de gebruikers goed geborgd zijn en welk rechtstelsel geldt.

Een Cloud provider moet de naleving van de EU-wetgeving inzake gegevensbescherming

[20] Sharad K. & G. Danezis, De-anonymizing D4D Datasets, http://petsymposium.org/2013/papers/sharad-deanonymization.pdf
[21] Financieel Dagblad Outlook LIVE 4 februari 2014
[22] Mell P. & T. Grance, The NIST Defintion of Cloud Computing, September 2011, csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf,
[23] Nägele T. & S. Jacobs, 'Rechtsfragen des Cloud Computing', *Zeitschrift für Urheber--- und Medienrecht* vol. 54, 2010, nr. 4, p. 281 – 292.

garanderen. Dit houdt in dat de overeenkomsten met Cloud-providers nauwkeurig bestudeerd moeten worden op voldoende contractuele garanties op het gebied van technische en organisatorische maatregelen met betrekking tot de bescherming van persoonsgegevens . Ook is van belang is dat de cliënt van de Cloud provider verifieert of de Cloud provider de rechtmatigheid van een grensoverschrijdende internationale doorgifte van gegevens kan garanderen. Knelpunt is dat op het ogenblik er geen Europese Cloud providers zijn die grote hoeveelheden gegevens kunnen verwerken. Amerikaanse Cloud providers worden afgeraden omdat de Amerikaanse overheid (NSA) op grond van de Patriot Act toegang tot alle medische/persoonsgegevens hebben en kunnen krijgen en individuen moeilijk hun recht kunnen halen.

5.13 Antwoord op de eerste onderzoeksvraag

Bij de bestudering van de Concept-Advies zijn een aantal knelpunten op middellange termijn voorzien, met name op het gebied van de decentralisatie en big data:
1.Verwacht wordt dat de patiënt toegang en beheer van zijn persoonlijk gezondheidsdossier (PGD) krijgt op basis van vrijwilligheid en met de keuze uit meerdere PGD's In de praktijk zullen niet alle patiënten / cliënten gebruik kunnen en willen maken van PGD's in aanvulling op overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek.
Onder andere door de vergrijzing zullen grotere aantallen 'gemiddelde' (laag opgeleide en bejaarde) patiënten hun PGD niet (meer) willen en/of kunnen controleren en/of beheren. Commerciële (adviserende) diensten zullen het beheer van hen overnemen. Zij zullen de verkregen informatie naast het PGD zelf opslaan en voor data analyses gaan gebruiken. Dit kan tot manipulatie van de patiënt leiden. De visie over de participerende patiënt in het RVZ advies (2013) is te rooskleurig.
2.Bij zorgverleners kan, wanneer patiënten per onderwerp en gegeven mogen bepalen wie in het PGD dossier daar toegang toe krijgt en welke gegevens niet gedeeld mogen worden, twijfel ontstaan over de juistheid en volledigheid van het dossier. Om het risico op medische fouten te verkleinen zullen tests en anamnese worden herhaald, wat de efficiëntie van het PGD zal ondermijnen. Logging van wijzigingen in het PGD is gewenst. In het advies van de RVZ wordt gesteld dat niet iedereen zal willen en kunnen participeren, maar dat degene die dat wel wil en kan geholpen moet worden bij de keuze informatie door zijn zorgverlener via 'shared decision making'[24]
3. Gezien het grote macro-economisch belang van de gezondheidszorg wordt voorzien dat geautomatiseerde aanvallen op de gezondheidsinformatiehuishouding zullen toenemen. Dergelijke aanvallen kunnen door personen met weinig expertise worden uitgevoerd.
4. De ontwikkelingen binnen de gezondheidszorg zullen leiden tot het gebruik van een verscheidenheid aan ICT-technologieën. Bij data volgende-, gegevens koppelende- en informatie ontdekkende en extraherende technologieën spelen persoonsidentiteiten een sleutelrol. Hierbij kunnen er omvangrijke data lekken en privacy inbreuken optreden en kunnen identiteiten van patiënten en hun gegevens op vele (onbekende) plaatsen door commerciële partijen worden opgeslagen met ongewenst gebruik als gevolg. Het gebruik van pseudo-identeiten is noodzakelijk.

[24] De participerende patient, Den Haag 2013, p.7,12 thttp://www.rvz.net/publicaties/bekijk/de-participerende-patient

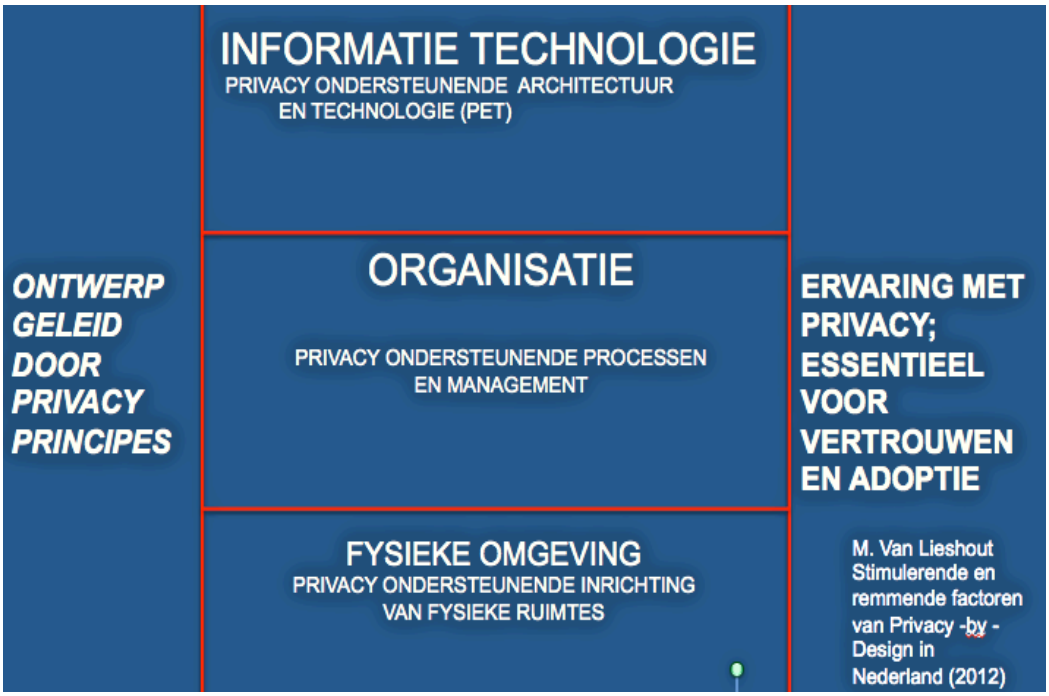
5. Bij het meervoudig en secundair (her)gebruik van medische gegevens door vele afnemers en het gebruik van big data zullen aan anonimisering en de-anonimisering zeer hoge eisen moeten worden gesteld, wil identificatie worden voorkomen. Cloud computing vormt een extra risico door de potentiele toegang van de Amerikaanse overheid tot opgeslagen gegevens en het gebruik van opslagtechnieken die ongewild hergebruik van gegevens tot gevolg zou kunnen hebben.
6. De wettelijke vereisten ter bescherming van persoonsgegevens en de boetes bij overtreden zullen aanzienlijk worden verzwaard.

6.De Tweede onderzoeksvraag:
In hoeverre kunnen deze knelpunten worden opgelost door 'privacy-by-design'?

6.1 Wat is privacy-by-Design?

Bij PbD wordt de bescherming van de privacy van personen over wie gegevens verzameld worden (bijvoorbeeld patiënten en cliënten) al bij het (vroegste) ontwerp van een systeem meegenomen, er wordt gebruik wordt gemaakt van organisatorische maatregelen om toegang tot en omgang met persoonsgegevens te regelen volgens bepaalde afspraken en voorschriften en technische maatregelen worden toegepast zoals versleuteling om toegang tot en omgang met persoonsgegevens af te schermen of te verhinderen.

Deze opvatting wordt in figuur 1: weergegeven:



Figuur 3 Bouwstenen voor Privacy by Design,

De toelichting is als volgt:
In figuur 1 zijn de bouwstenen gegeven die onderdelen vormen van *Privacy by Design*. Er wordt onderscheid gemaakt tussen instrumenten voor de ontwerpfase (zoals een *Privacy Impact Assessment* en een ontwerpmethode waarin privacy is opgenomen), technische instrumenten (zoals versleuteling en instrumenten om de transparantie van de gegevensverwerking te vergroten), organisatorische instrumenten (zoals het aanstellen van een functionaris gegevensbescherming (*privacy officer*) en het maken van afspraken over toegang en gebruik van gegevens), ontwerpfactoren voor de ruimtelijke dimensie (zoals de ruimtelijke scheiding van gegevensregistratie en gegevensgebruik) en de ervaring van privacy die de personen over wie gegevens verzameld worden zelf hebben.

Er zijn twee belangrijke functionaliteiten van *Privacy by Design* te onderscheiden: *privacy governance* en *privacy protection*. Ieder van deze functionaliteiten is te benaderen vanuit twee dimensies: een organisatorische en een technische. *Privacy governance* richt zich op het realiseren van een (organisatie-)beleid rond privacy waarbij verantwoordelijkheid en transparantie centraal staan in de verzameling, bewerking, verspreiding, opslag en vernietiging van persoonsgegevens. Startpunt hierbij is het betrekken van privacy- overwegingen bij het initiëren van nieuwe diensten en nieuwe organisatie activiteiten.
Privacy protection richt zich op afscherming, versleuteling, anonimisering en minimalisering van persoonsgegevens die worden verzameld, bewerkt, etc. De organisatorische dimensie richt zich op processen en methoden die een organisatie kan invoeren voor *privacy governance* en voor *privacy protection*. Dit is bijvoorbeeld het instellen van auditprocedures, het aanstellen van functionarissen gegevensbescherming (*Privacy Officers)* met bepaalde taken en verantwoordelijkheden, en het opstellen van regels en richtlijnen rond een Privacy Impact Assessment. De technische dimensie richt zich op tools en methoden die ingezet kunnen worden voor de technische realisering van *privacy governance* en *privacy protection*. Dit is bijvoorbeeld het gebruiken van protocollen en procedures van dataminimalisering, of het inzetten van cryptografische technieken voor anonimisering van gegevens.

Het rapport hanteert de volgende definitie: “Privacy by Design heeft als doel privacy schendingen zoveel mogelijk te vermijden door privacybescherming vanaf het begin van een proces waar verzameling en verwerking van persoonsgegevens onderdeel van uitmaakt en tijdens de gehele levenscyclus van de gegevensverwerking systematisch ‘in te bakken’ in de organisatie en in de informatiesystemen die gebruikt worden. Het gaat bij *Privacy by Design* niet alleen om technische maatregelen maar ook om maatregelen in de bedrijfsvoering en de organisatie en om inbreng van de ervaring en houding van eindgebruikers (consumenten).”
Dit concept benadrukt dat privacy niet alleen kan worden gewaarborgd door de naleving van de regelgeving, maar moet worden ingebed in de operationele systeemontwerpen van de betrokken organisaties. Internationale aanpak van PbD is essentieel, omdat op het gebied van overdracht van gezondheidsgegevens over de elektronische netwerken (zoals het internet), is er een kenniskloof is en een gebrek aan synchronisatie tussen geografische gebieden (bijvoorbeeld de EU en Noord-Amerika). Een internationale empirische en vergelijkende benadering zou deze kloof te overbruggen.
Om persoonsgegevens adequaat te beschermen, dient duidelijk te zijn welke privacy risico’s er ontstaan bij het verwerken van persoonsgegevens en het introduceren van nieuwe informatiesystemen en netwerken in de samenleving. PbD en een voorafgaande privacy risico/privacy impact assessment (PIA) horen als een Siamese tweeling bij elkaar. Het spreekt dan ook vanzelf dat Pbd niet zonder een voorafgaande PIA kan worden uitgevoerd. Daardoor kan het PbD systeem de privacy risico’s adequaat kan mitigeren of elimineren.

6.2 Privacy-Enhancing technologies (PETs)

PETs maakt deel uit van PbD. Onder PETs wordt verstaan: Een systeem van maatregelen in de database, toepassing en proces, waarmee de informationele privacy wordt beschermd en vertrouwen wordt geschapen door het verminderen en elimineren van identificeerbare of herleidbare persoonsgegevens en/of voorkomen van onrechtmatige verwerking. Het kent twee basis elementen: de Identity Protector en de (pseudo) Identiteitsdomeinen. In ISO 15408 zijn de basis uitwerkingen vastgelegd:
1. Anonimiteit, waarbij er geen identificeerbare data (meer) aanwezig zijn;

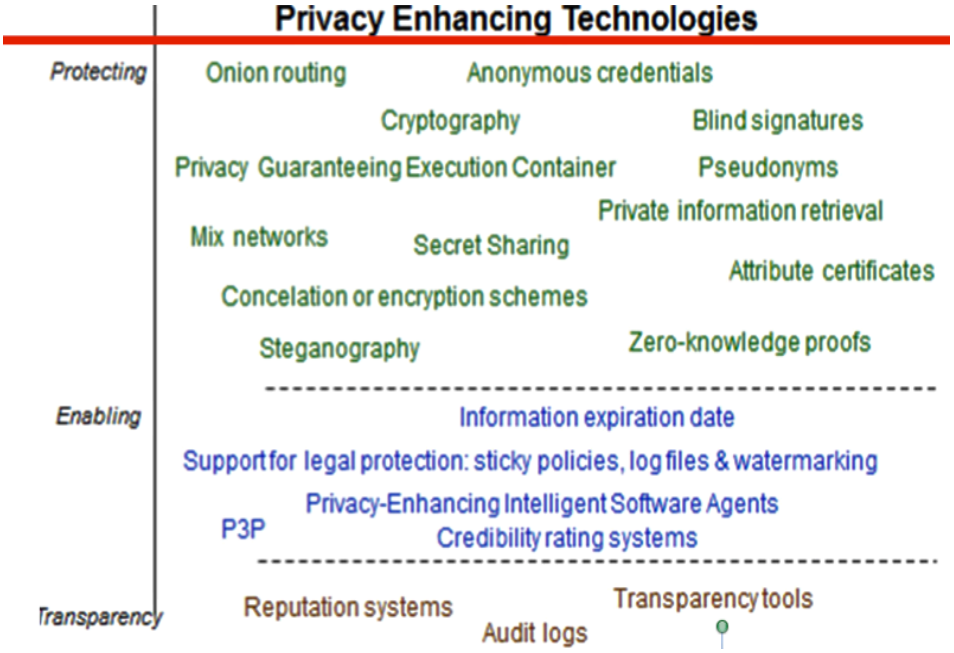
2. Pseudonimiteit, waar identificatie alleen mogelijk is voor geautoriseerde gebruikers;

3. Niet traceerbaarheid, waarbij er geen identificerend middel (b.v. BSN nummer) een verbinding/relatie met het informatiesysteem kan leggen;

4. Niet zichtbaar zijn, tot het moment dat identificatie vereist is.

Doel van een pseudo-identiteit is, dat de identiteit kan niet worden herleid aan de hand van persoonsgegevens en dat de persoonsgegevens kunnen niet gevonden worden aan de hand van de identiteit. (hacker proof criterium)

Hieronder volgt een overzicht van beschikbare PETs.



Figuur 4 Overzicht PETs in Van Lieshout 2012

6.3. Door de wet a contrario onderkende privacy bedreigingen

De volgende niet limitatieve opsomming van bedreigingen voor de persoonsgegevens en de persoonlijke levenssfeer zijn reëel bij het overtreden van privacy regel- en wetgeving:

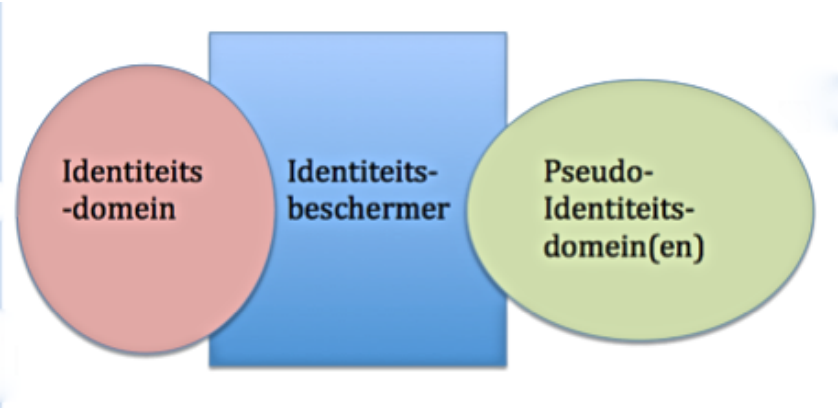
- Bedreiging 1: Geheim bezit van of controle over persoonsgegevens.
- Bedreiging 2: Geheime verwerking van persoonsgegevens door gebrek aan transparantie en gebrek aan toestemming.
- Bedreiging 3: De verwerking van persoonsgegevens vindt plaats in strijd met de privacy voorkeuren van de betrokkene of de verantwoordelijke beperkt de verwerking zich niet tot het opgeven doel van de verwerking (doelbinding);

- Bedreiging 4: Onrechtmatige verwerking van persoonsgegevens in strijd met de wet of is onrechtmatig (illegaal);
- Bedreiging 5: Gebrek aan gegevensminimalisatie.
  De verzameling van persoonlijke informatie wordt niet tot een strikt minimum beperkt. Er wordt meer verzameld en verwerkt dan strikt noodzakelijk is voor de realisering van het doel waarvoor de persoonsgegevens zijn bestemd;
- Bedreiging 6: De excessieve identificatie van het individu.
  De identificatie duurt langer dan conform de doeleinden van de verwerking van de gegevens noodzakelijk is. De inrichting van het informatiesysteem is zodanig dat de identificatie, observering en traceerbaarheid van het desbetreffende individu niet wordt beperkt;
- Bedreiging 7: Verkeerde beslissingen.
  Beslissingen vinden plaats op basis van onjuiste of verouderde gegevens. De persoonsgegevens worden niet correct, niet accuraat, ontoereikend, niet te zake dienend verzameld en verwerkt;
- Bedreiging 8: Verantwoordelijke is onvindbaar of weigert transparantie. Personen over wie gegevens worden verzameld, krijgen niet de mogelijkheid om hun persoonsgegevens in te zien, te verbeteren, aan te vullen, te verwijderen of af te schermen of bezwaar te maken tegen de verzameling en verwerking van hun persoonsgegevens;
- Bedreiging 9: Ernstige privacy inbreuken en onzorgvuldig data management.
  Er zijn geen passende technische en organisatorische maatregelen genomen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking of om onnodige verzameling en verwerking van persoonsgegevens te voorkomen;
- Bedreiging 10: Gebrek aan vertrouwelijkheid van de communicatie.
  De vertrouwelijkheid van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten wordt niet gerealiseerd;
- Bedreiging 11: De gegevens worden te lang opgeslagen.
- Bedreiging 12: Niet toegestane verwerking buiten de EU.
  Verzending van persoonsgegevens vindt plaats naar een land, dat geen (adequate) bescherming biedt zoals die geldt binnen de EU en EEA. [25]

6.4. Basis PbD ontwerp patroon

Aan de hand van de PIA en door de Wbp onderkende bedreigingen dient een PbD systeem ontworpen te worden. Sinds de publicatie van het rapport over PETs van de Registratiekamer, de voorloper van het CBP, in 1995 is ligt aan ‘privacy by design’ naast het vereiste van gegevensminimalisatie twee ontwerpbeginselen ten grondslag, te weten de Identiteitsbeschermer (IP) en het scheiden van gegevens door het scheppen van een identiteitsdomein en een of meer pseudo-identiteitsdomeinen. Dit leidt tot het volgende ontwerppatroon:

[25] Borking J.J.F.M., Privacy is Code, Over de toepassing van Privacy Enhancing Technologies, Deventer 2010, p.142



Figuur 5. Schematische weergave van een basaal ontwerppatroon om persoonsgegevens te scheiden

Scheiding van gegevens houdt in dat persoonsgegevens wel worden verwerkt, maar dat de identificerende persoonsgegevens worden losgekoppeld van de overige persoonsgegevens. Er worden ten minste twee domeinen gecreëerd: een identiteitsdomein waarin bijvoorbeeld de naam en adresgegevens worden verwerkt en één of meer pseudo-identiteitsdomeinen waarin overige gegevens als lidmaatschap of opsporingsgegevens worden verwerkt. De scheiding tussen beide domeinen wordt aangebracht en beheerd door een identiteitsbeschermer.
De IP draagt op vier manieren bij aan de versterking van de bescherming van de persoonlijke levenssfeer:

1. hij kan de identificeerbaarheid voorkomen of verminderen;
2. hij kan ingesteld zijn op het voorkomen van de verdere verwerking van persoonsgegevens;
3. hij kan gericht zijn op het ondersteunen van de privacy verwerkelijkingsbeginselen;
4. hij kan de controle van het individu vergroten over zijn eigen persoonsgegevens. [26]

In de praktijk is een IP een deel van een programma dat op een server kan staan. In het informatiesysteem kan de IP gerealiseerd worden in de vorm van, bijvoorbeeld: een aparte functie geïmplementeerd in het informatiesysteem of informatieproces. Ook kan de IP een apart informatiesysteem zijn, dat onder controle van de gebruiker of de burger (bijvoorbeeld via een smartcard) staat of onder controle staat van een door de dienstverlener (bijvoorbeeld de overheid) en de gebruiker vertrouwde partij ('trusted third party of TTP').
In veel gevallen kent een informatiesysteem verschillende typen gebruikers en mag iedereen maar een beperkt aantal gegevens inzien. In dat geval kunnen verschillende pseudo-identiteitsdomeinen worden ingericht. In ieder pseudo-identiteitsdomein wordt dan een deel van de informatie over een persoon verwerkt. Om privacy inbreuken te voorkomen moet natuurlijk de IP wel betrouwbaar zijn, dus gecontroleerd worden. Dat kan geschieden door een organisatie (bijvoorbeeld Europrise GmbH) die certificaten afgeeft waarin de betrouwbaarheid van de IP wordt gegarandeerd na het uitvoeren van een evaluerende privacy audit.
Wanneer een organisatie statistisch onderzoek wil doen, ontbreekt veelal de noodzaak om de identiteit van de individuele burgers vast te leggen, ook al wil men wel aan de burger gerelateerde

[26] Hes R. & J. Borking, Privacy Enhancing Technologies: The Path to Anonymity, The Hague 2000, p. 13

gegevens gebruiken. In dat geval kan worden volstaan met het verwerken van de gegevens uit het pseudo-identiteitsdomein.
De burger/patiënt kan zelf de identiteitsbeschermer beheren en daarmee de koppeling tussen de domeinen. Deze vorm van scheiding van gegevens kan worden gebruikt in het geval een partij (de overheid) wel zekerheid wil hebben over iemands identiteit, maar deze identiteit niet wil of mag vastleggen. Dit is bijvoorbeeld het geval bij kiezen op afstand. Wanneer burgers hun stem elektronisch uitbrengen wil de overheid wel de zekerheid hebben dat de burger stemgerechtigd is en slechts eenmaal stemt, maar mag de identiteit van de burger in relatie tot de uitgebrachte stem absoluut niet worden vastgelegd om te voorkomen dat de vereiste anonimiteit van de stem verloren gaat. Ook bij het opzetten van een e-ID kaart kan deze aanpak met succes toegepast worden.
Deze PET-vorm kan ook andersom worden gebruikt. De overheid legt alleen het identiteitsdomein vast en alleen de burger beschikt over het pseudo-identiteitsdomein. Ook nu beslist de burger over het feit of de overheid de koppeling kan en mag maken tussen de twee domeinen. Hierbij moet wel worden opgemerkt dat een chipkaart een beperkte opslagcapaciteit heeft en dat daar bijvoorbeeld geen complete gegevensverzameling op bewaard kan worden. Dat is ook niet verstandig in verband met het risico van verlies van de kaart. In veel gevallen zal op de chipkaart een verwijzing zijn opgenomen naar de locatie waar de gegevensverzameling wordt bewaard of de instelling die de gegevens in bewaring heeft. Een voorbeeld hiervan is dat een burger geen PGD bij zich draagt, maar dat op zijn chipkaart bijvoorbeeld is opgeslagen wie zijn huisarts is en andere zorgverleners. Bij een ongeval kan de behandelend arts contact opnemen met de huisarts over medische bijzonderheden uit het verleden.

Maximale gegevensbescherming wordt gerealiseerd wanneer de identiteitsbeschermer wordt beheerd door de persoon wiens gegevens zijn vastgelegd. Alleen hij bepaalt dan wanneer en aan wie zijn ware identiteit bekend wordt gemaakt. De situatie waarbij de identiteitsbeschermer onder controle staat van de betrokkene zelf wordt ‘persoonsgegevens in eigen beheer’ genoemd en is in feite een specifieke verschijningsvorm van scheiding van gegevens. Een persoonlijke chipkaart en (online) gegevenskluisje zijn voorbeelden hiervan.
De ontwerper wordt, bij de realisatie en implementatie van de identiteitsbeschermer, niet beperkt in zijn keuze voor het toepassen van speciale technieken. Hij kan in zijn ontwerp bijvoorbeeld gebruik maken van (blinde) digitale handtekeningen,[27] en het gebruik van digitale certificaten (‘credentials’). [28]

6.5 Privacy-by-Design vereisten voor het persoonlijk gezondheidsdossier

Persoonlijke gezondheidsdossiers (PGD’s) kunnen worden opgeslagen in de PC van de patiënt, op een website of elders De patiënt, die dat wil kan zijn PGD beheren en kan daar zelf en anderen, die daartoe geautoriseerd zijn, gezondheidsgegevens registreren. Het is de bedeling dat bepalen met wie hij zijn gezondheidsgegevens wil delen. Het PGD wordt gekoppeld aan elektronische dossiers in databanken van zorgaanbieders. Alle gegevens in het PGD en binnen de gezondheidsinformatie huishouding dienen te zijn versleuteld. Logging van alle wijzigingen dient in de PGD’s plaats te vinden.
Teneinde een privacy veilig (Privacy-by-Design) PGD te realiseren dient het PGD in twee

[27] Chaum, D. Achieving Electronic Privacy, in *Scientific American* August 1992, p. 96-101
[28] Brands S.A., Rethinking Public Key Infrastructures and Digital Certificates, Building in Privacy, Cambridge (MA) 2000

gescheiden verzamelingen te worden opgedeeld. In de eerste verzameling, het identiteitsdomein, worden de persoonsgegevens inclusief een patiëntnummer opgeslagen, de zorgrelatie en de vastlegging van de functionele autorisatie.
In de tweede verzameling, een verzameling van pseudo-identiteitsdomeinen, worden de medische, diagnostische en behandelgegevens opgeslagen. Het dossier bevat aparte tabellen voor alle logisch bij elkaar horende gegevens, zoals een tabel voor de anamnese, voor medicatie, voor het behandelplan, de afspraken met zorgverleners, de opname in ziekenhuizen, de chirurgische behandeling, de laboratorium uitslagen, de verstrekkingen van gegevens aan derden (huisarts, tandarts, apotheker, laboratorium etc.), etc.
Elke tabel in de twee gescheiden verzamelingen is voorzien van een primaire sleutel. Elk onderdeel van het persoonlijk gezondheidsdossier is dus ondergebracht in een eigen tabel waarbij de waarde van de primaire sleutel per tabel verschilt, ook al heeft zij betrekking op een en dezelfde patiënt, het zelfde persoonlijk gezondheidsdossier etc.
De tabel Patiënt bevat alle persoonsgegevens, de tabel ‘agenda_afspraak’ bevat de feiten rond het consult en niet meer dan dat. Tussen de tabellen zijn wel logische verbanden maar niet fysiek aanwezig in het dossier.
De gegevens voor het PGD worden opgehaald uit de databanken van de zorgaanbieders (zorgverleners en zorginstellingen ook op gemeentelijk niveau)

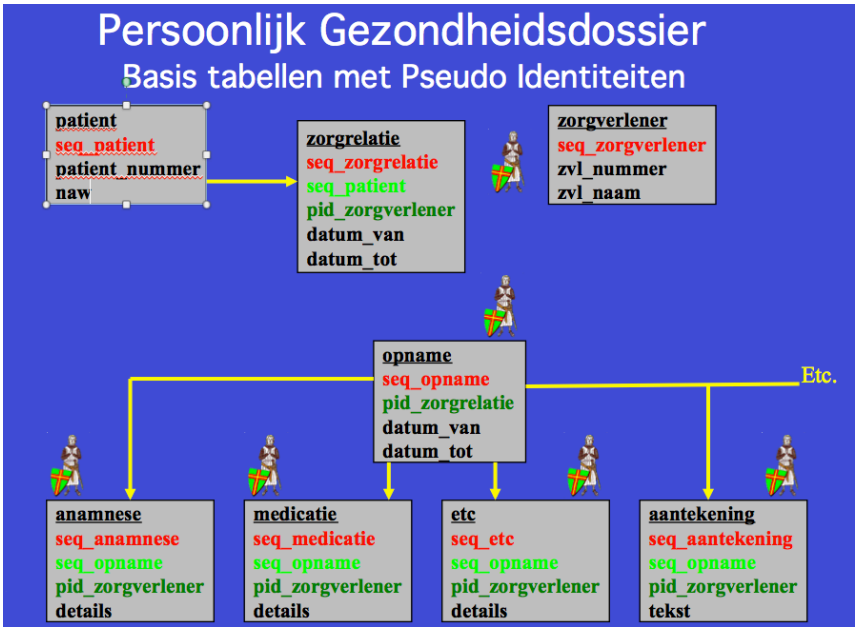
Het patiëntnummer in het identiteitsdomein (eerste verzameling) en in de pseudo-identiteitsdomeinen (tweede verzameling) niet aan elkaar gelijk zijn, omdat iedereen dan de koppeling tussen de identificerende en niet-identificerende gegevens zou kunnen maken. Om de mogelijke koppeling te voorkomen, wordt het patiëntnummer uit het identiteitsdomein versleuteld. Dit versleutelde nummer wordt als patiëntnummer gebruikt in een specifiek pseudo-identiteitsdomein. Met behulp van de ‘Identity Protector’ kan het versleutelde patiëntnummer worden ontcijferd en wordt de koppeling met het identiteitsdomein gemaakt. Op deze wijze kunnen alleen degenen die de beschikking hebben over de ‘Identity Protector’, de twee domeinen met elkaar in verband brengen. Er kunnen in de database even zo veel pseudo-identiteiten per patiënt zijn als het aantal tabellen.
Het beheer van het PGD vereist authenticatie- en autorisatiemanagement. Wanneer het toekennen (autoriseren) en het uitreiken van de authenticatiemiddelen niet zorgvuldig gebeuren, kunnen ongeautoriseerde personen onrechtmatig toegang verkrijgen tot de patiëntgegevens. Hiermee wordt het voordeel van PbD geheel tenietgedaan.

Om een koppeling te maken tussen de tabellen, moet eerst vastgesteld worden of er een geldige zorgrelatie met de patiënt is. Het unieke kenmerk van de betrokken patiënt is bekend. De applicatie versleutelt dit vervolgens tot unieke kenmerkgegevens van de gewenste zorggerelateerde tabel. Deze versleutelde kenmerken stellen de toepassing vervolgens in staat de benodigde gegevens in het dossier te benaderen, te verzamelen en in het PGD weer te geven.

De tabellen zijn voorzien van een extra kolom waarin de pseudo-identiteit wordt vastgelegd, die gebruikt wordt als toegangssleutel tot de gewenste informatie in het PGD.

In PGD bestaat voor elke tabel een uniek encryptie protocol. Daarmee is bereikt dat elke zorggerelateerde tabel voor een en dezelfde patiënt een unieke sleutel bezit. De relaties tussen

de tabellen worden onderhouden door middel van beschreven 'constraints'[29] voor het bewaken van de referentiële integriteit[30] van het dossier om te voorkomen dat gegevens kunnen worden verwijderd. Het is hierdoor ook niet mogelijk om toegang te geven aan een niet-geregistreerde zorgverlener.
In figuur 6 zijn de relaties tussen de verschillende tabellen vervangen door 'Identity Protectors' (weergegeven door het symbool van de kruisridder), die de pseudo-identiteiten tot stand brengen.

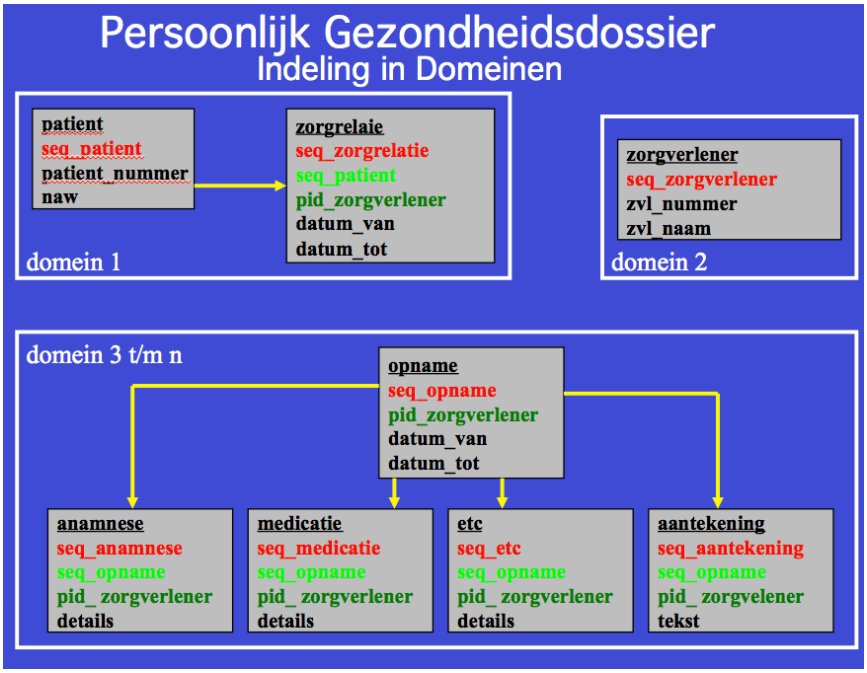


Figuur 6 voorbeeld Basis tabellen waarin de relaties zijn vervangen door Identity protectors; De kruisridders staan symbolisch voor de Identity protectors. Pid staat voor pseudo-identiteit

Om een ongeautoriseerde gebruiker of hacker het niet mogelijk te maken persoonsgegevens te koppelen aan het gezondheidsdossier, dat in tabellen is opgesplitst, zijn tussen de tabellen geen 'constraints' gedefinieerd. Ook zijn er geen verborgen tabellen aanwezig waarin een relatie wordt gelegd tussen de primaire sleutel die binnen de twee dossierdelen in gebruik zijn. Het PGD omvat tabellen die als startpunt worden gebruikt voor een applicatiefunctie nadat de patiënt is geselecteerd. Deze tabellen zijn voorzien van een extra kolom waarin de pseudo-identiteit wordt vastgelegd, die gebruikt wordt als toegangssleutel tot de gewenste informatie in PGD. Er is hier sprake van de invoering van de 'Identity Protector', die de identiteit van de zorgverlener en patiënt afschermt.

[29] Een constraint in een database is een vastgelegde voorwaarde, bedoeld om de integriteit of logica van de opgeslagen gegevens te bewaken. Een constraint zorgt er voor dat er een foutmelding wordt gegeven als de betreffende regel overtreden dreigt te worden.
[30] Referentiële integriteit in een PGD is het uitgangspunt dat de interne consistentie tussen de verschillende tabellen binnen dit dossier wordt gewaarborgd. Dat betekent dat er altijd een primaire sleutel in een tabel bestaat als er in een sleutelveld in een andere tabel naar wordt verwezen.

De client-software biedt de mogelijkheid op basis van de primaire sleutel van een aanvrager een pseudo-identiteit samen te stellen met behulp van encryptie-technologie. Het encryptieprotocol kent drie parameters:
a. de primaire sleutel;
b. de encryptie sleutel van 256 bits of hoger;
c. een unieke tabel 'identifier'.
Het encryptieprotocol gaat bijvoorbeeld als volgt: de seq_patient is 34, de unieke 'identifier' voor de tabel medicatie is 47 en de encryptiesleutel is 263447432356645391.
De uit deze bewerking resulterende pseudo-identiteit wordt opgenomen in een tabel van het PGD en wordt gebruikt voor de toegang tot die tabel. Elke tabel binnen het PGD krijgt zijn eigen pseudo-identiteit toegewezen. Om een afspraak met een zorgverlener te kunnen maken uitgaande van een gegeven in het PGD, bestaat ook de mogelijkheid om softwarematig vanuit de pseudo-identiteit de primaire sleutel van de patiënt te produceren. Door het gebruik van de 'Identity Protectors' worden zoveel als nodig identiteit- en pseudo-identiteitsdomeinen gecreëerd. In figuur 7 zijn de gecreëerde domeinen aangeven als rechthoeken, waarbinnen zich de specifieke tabellen bevinden.



Figuur 7: Domeinindeling in het persoonlijk gezondheidsdossier. Domein 3 t/m n kan voor wetenschappelijk onderzoek worden gebruikt en bevat geen identificerende gegevens

De gekozen oplossing maakt het mogelijk, dat alleen de behandeld arts, zorgverlener of specialist en de patiënt inzage in het hele dossier hebben. De administratie, het laboratorium en de verpleegkundigen hebben slechts inzage in die gegevens uit het PGD die van belang zijn voor het uitvoeren van hun functies.
De in deze toepassing te gebruiken encryptiesleutels dienen te worden beheerd door middel van een TTP (trusted third party), want voorkomen moet worden, dat als een hacker zich toegang zou

kunnen verschaffen tot de computers, dat hij de sleutel op de 'client' van de zorgverlener zou kunnen ophalen en dan alsnog het dossier en de informatiehuishouding zou kunnen binnendringen.
De communicatie tussen client en server zorgt voor de geautoriseerde ontsluiting van de tabellen en gegevens. Een client is een applicatie of een computersysteem met toegang tot een ander systeem, de server, via een netwerk. Men spreekt hierbij van een client-servermodel. De client neemt initiatief tot communicatie met de server met als doel bijvoorbeeld het opvragen van gegevens, het overdragen van gegevens of het uitvoeren van een actie op de server. De dialoog tussen de client (PC van de patiënt) en de servers, waar gezondheidsgegevens van de patiënt zijn opgeslagen.

1. login met patiënt naam;
2. geeft naam van patiënt aan de server;
3. controleer de naam van de patiënt in de tabel 'patiënt';
4. geef de seq_patient (uit een sequentie van nummers) aan de client;
5. versleutel deze op de client naar pid (pseudo-identiteit) van de patiënt;
6. geef de pid_patient aan de server;
7. doorzoek de gewenste tabellen op pid_patient en geeft de daarbij behorende resultaten aan de client.

Voor de zorgverlener bestaat een analoge procedure maar hij zal ook de pid_patient bij het ophalen van de medische gegevens moeten meenemen om bij de gegevens van de patiënt te kunnen komen. Dat kan alleen als er in de tabel zorgrelatie de relatie tussen de zorgverlener en de patiënt is vastgelegd.

De gekozen oplossing maakt het mogelijk, dat alleen de behandeld arts, zorgverlener of specialist en de patiënt inzage in het hele dossier hebben. De administratie, het laboratorium en de verpleegkundigen hebben slechts inzage in die gegevens uit het patiëntendossier die van belang zijn voor het uitvoeren van hun functies.[31]

6.6 De Trusted Third Party (TTP)

Er van uitgaande dat encryptie bij PGD's en in de gehele gezondheidsinformatiehuishouding op micro, meso en macro niveau moet worden toegepast, zal het inzetten van een of meerdere 'trusted third parties' (TTPs),[32] noodzakelijk zijn voor het beheer en de uitwisseling van de encryptiesleutels en digitale certificaten die gebruikt worden voor de vercijfering en ontcijfering van de persoonlijke gezondheidgegevens en andere medische gegevens en het secundair gebruik van gegevens op meso- en macroniveau binnen de informatiehuishouding mogelijk maken. Digitale certificaten zullen in de informatiehuishouding een cruciale rol spelen bij het faciliteren van betrouwbare en vertrouwelijke elektronische communicatie en transacties. Voor het gebruik van digitale certificaten is een zogenaamde public-key infrastructure (PKI) nodig. Een belangrijke rol binnen zo'n infrastructuur spelen trusted third parties (TTP's). Zij vergewissen zich

[31] Blarkom G. W. van, Guaranteeing requirements of data-protection legislation in a hospital environment with privacy-enhancing technology in *BJHCIM (The British Journal of Healthcare Computing & Information Management*), May 1998, Vol.15 number 4
[32] Duthler A.W., Met Recht een TTP!, (proefschrift) Rijksuniversiteit Leiden 22 september 1998, Deventer 1998. Voor de privacy aspecten van een TTP: Versmissen J.A.G., Sleutels Van Vertrouwen, TTP's, digitale certificaten en privacy, (A&V) (Achtergronden en Verkenningen) Nr. 22, Den Haag, 2001

van de identiteit of andere attributen van iemand en geven ter bevestiging daarvan vervolgens een digitaal certificaat uit.
Om privacy inbreuken te voorkomen moet natuurlijk de identity protector wel betrouwbaar zijn, dus gecontroleerd worden. Dat kan geschieden door een organisatie die certificaten afgeeft waarin de betrouwbaarheid van de identity protector wordt gegarandeerd. Het zelfde geldt ook voor de TTPs, teneinde het DigiNotarincident[33] te voorkomen.

6.7 Eerste praktijk voorbeeld: De Privacy Incorporated Database® (PID)

De hierboven besproken aanpak voor een privacy veilig medisch dossier van de patient is uitgewerkt door ICL/SIAC in 1996/7 en resulteerde in de X/Mcare-database gebaseerd op een Oracle relationele database en client-server structuur. De eerste keer is dit toegepast in het psychiatrisch ziekenhuis Veldwijk /Meerkanten in Ermelo. Het patiënt-identificatienummer uit alle tabellen in ziekenhuisinformatiesysteem verwijderd. Vervolgens is het ziekenhuis informatiesysteem in twee identiteitsdomeinen opgedeeld. Het ene domein bestaat uit de persoonsgegevens van de ingeschreven patiënten, de zorgrelatie en de vastlegging van de functionele autorisatie.
Het tweede pseudo-identiteitsdomein omvat de medische gegevens en de medisch dossiers van de patiënten. Elk dossier bevat onder meer de anamnese, medicatie, behandelplan, afspraken met zorgverleners, chirurgische behandeling, laboratorium uitslagen, en verstrekkingen van gegevens aan derden (huisarts, tandarts, apotheker, laboratorium etc.).
In het X/Mcare systeem zijn alle logisch bij elkaar horende gegevens opgeslagen in aparte tabellen.

Om een koppeling te maken tussen de tabellen, moet eerst vastgesteld worden of er een geldige zorgrelatie met een geselecteerde patiënt is. In dat geval is het unieke kenmerk van de betrokken patiënt bekend. De applicatie versleutelt dit vervolgens tot unieke kenmerkgegevens van de gewenste zorg gerelateerde tabel. Deze versleutelde kenmerken stellen de toepassing vervolgens in staat de benodigde gegevens in de database te benaderen.
In de X/Mcare database bestaat voor elke tabel een uniek encryptie protocol. Daarmee is bereikt dat elke zorg gerelateerde tabel voor een en dezelfde patiënt een unieke sleutel bezit. De relaties tussen de tabellen worden onderhouden door middel van beschreven ‘constraints’ voor het bewaken van de referentiële integriteit van de database om te voorkomen dat gegevens van een bestaande patiënt kunnen worden verwijderd. Het is hierdoor ook niet mogelijk om een behandeling te laten uitvoeren door een niet-geregistreerde zorgverlener.

Het ziekenhuisinformatiesysteem is zo ontworpen dat wanneer een ongeautoriseerde gebruiker of hacker een naam van een patiënt vindt, hij geen koppeling kan maken met welk ander gegeven dan ook gerelateerd aan die patiënt. Omgekeerd is het zo dat mocht bijvoorbeeld de laboratorium uitslag worden onderschept, dan kan van daaruit geen relatie met de patiënt of de zorgverlener worden gelegd. De ‘Identity Protector’, schermt de identiteit van de zorgverlener en patiënt af.

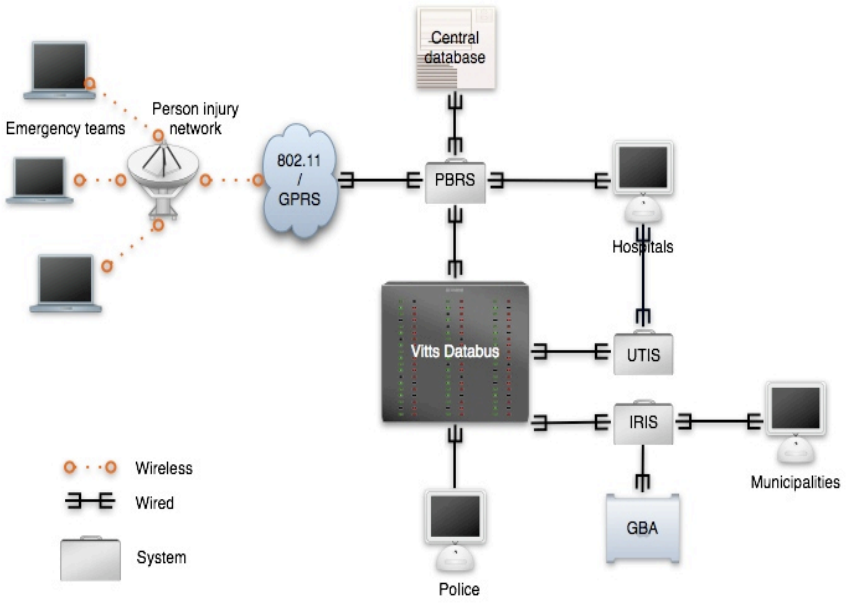
De communicatie tussen client en server zorgt voor de geautoriseerde ontsluiting van de tabellen
Deze toepassing is als de ‘Privacy Incorporated Database’ geoctrooieerd.[34] De in deze toepassing te gebruiken encryptiesleutels dienen te worden beheerd door middel van een TTP

[33] www.onderzoeksraad.nl/nl/onderzoek/1094/het-**diginotarincident**
[34] European Patent: EP0884670 (G.van Blarkom, inventor, ICL 1997)

(trusted third party), want voorkomen moet worden, dat als een hacker zich toegang zou kunnen verschaffen tot de computers, dat hij de sleutel op de 'client' van de zorgverlener zou kunnen ophalen en dan alsnog het systeem zou kunnen binnendringen.

6.8 Tweede praktijk voorbeeld: Het Victim Tracking and Tracing System

Een aanmerkelijk complexere uitwerking van het hierboven behandelde ziekenhuis informatiesysteem is het Victim Tracking and Tracing System (ViTTS) dat uit het Nederlands Trauma Informatie Systeem (NTIS) is voortgekomen.
In het ViTTS gaat het om een digitaal registratiesysteem voor traumapatiënten met zwaar acuut letsel die geholpen worden op de afdeling Spoed Eisende Hulp. De 'emergency teams' (zie figuur 8 hieronder) geven de levende en niet-levende slachtoffers een uniek identificerend ongeval nummer (Unique Identifying Casualty Number: UICN), dat wordt ingevoerd in de ViTTS databank. Aan dit nummer zijn medische gegevens gekoppeld over het slachtoffer, de plaats en tijdstip waar het ongeluk gebeurde en naar welk ziekenhuis het slachtoffer is gebracht en wordt behandeld.
Niet-geïdentificeerde slachtoffers krijgen eveneens een UICN. De Gemeente waar dit slachtoffer zich feitelijk bevindt, poogt het slachtoffer te identificeren op basis van ontvangen informatie van familieleden of anderen die het slachtoffer kennen en die hebben laten registeren dat zij familieleden vermissen. Slachtoffers, die verplaatst worden, kunnen met hun UICN nummer voortdurend worden gevolgd. Gegevens kunnen later ook gebruikt worden om analyses van rampen uit te voeren.
De sterk vereenvoudigde ViTTS architectuur ziet er als volgt uit:



Figuur 8 ViTTS architectuur: 802.11 / GPRS betreft een 'blue tooth' verbinding; PBRS staat voor patiënt barcode registratie systeem. 802.11 of Wi-Fi verwijst naar de gebruikte standaarden voor draadloze netwerken (Wireless LAN) bij ViTTS. GPRS betekent General Packet Radio Service en is een techniek om in het GSM-netwerk

berichten sneller te verzenden. UTIS betekent Utrechts Trauma Informatie Systeem. IRIS staat voor Internet Registratie systeem. GBA is de Gemeentelijke Basis Administratie

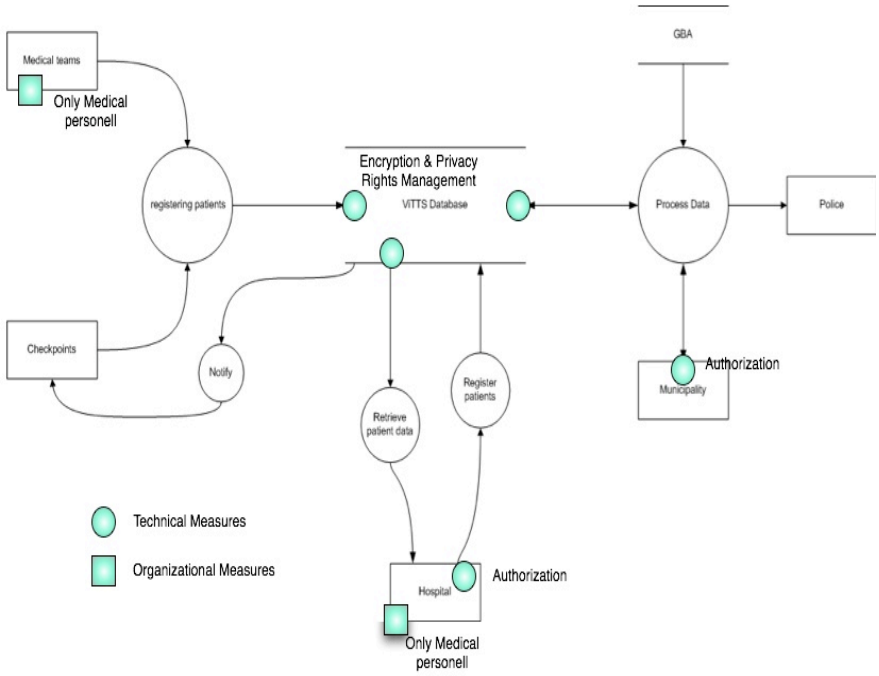
Het verzamelen van gegevens waaraan een UICN wordt gekoppeld, geschiedt met een mobiele RFID/barcode lezer: het patiënt barcode registratie systeem (PBRS) (zie figuur 8). De gegevens worden direct via een beveiligde lijn verzonden en opgeslagen in de PBRS databank die gekoppeld is met de ViTTS databank. Het ziekenhuis waar het slachtoffer verblijft, kan via een internetverbinding contact opnemen met het Utrechts Trauma Informatie Systeem (UTIS) om meer informatie over de ramp te verkrijgen.

Omdat bij een ramp de verantwoordelijkheid voor de afwikkeling van de ramp mede wordt gedragen door de Gemeente waar de ramp heeft plaatsgevonden, wordt de verkregen informatie ook naar de desbetreffende Gemeente en Politie gezonden. De Gemeenten gebruiken het Internet Registratie systeem (I-RIS) om de bevolking te informeren over het aantal gewonde mensen en om de familieleden in te lichten waar het slachtoffer zich bevindt. De Gemeenten en de Politie krijgen uitsluitend de informatie waartoe zij gerechtigd zijn. De Gemeente Basis Administratie (GBA) valideert de informatie. De politie ontvangt slechts informatie als een persoon is overleden.

Artsen, verpleegkundigen en assistenten hebben op basis van functionele autorisatie toegang tot dit systeem. Door de elektronische vastlegging en uitwisseling van medische gegevens kan een efficiëntere en effectievere hulpverlening aan de patiënt worden geboden en de ramp beter beheerst worden. Tevens worden de uiterst gevoelige medische patiëntgegevens en behandelmethoden anoniem geanalyseerd zodat men de behandelmethoden kan verbeteren, de patiënten beter kunnen worden geholpen en de kans op overleven groter wordt. Het spreekt vanzelf dat gezien de privacy gevoeligheid van de medische gegevens, technische maatregelen zijn genomen om alle gegevens vanaf het moment van verzamelen te versleutelen. De communicatie gaat over beveiligde lijnen en de gegevens worden versleuteld in de database zijn opgeslagen.

Omdat het ViTTS systeem privacy gevoelige informatie over slachtoffers verwerkt en deze gegevens door het ziekenhuispersoneel, de medische staf, de Gemeenten en Politie geraadpleegd kunnen worden, is het van groot belang de privacy bedreigingen het hoofd te bieden, door optimale bescherming aan de persoonsgegevens te verlenen en overtreding van de privacywetgeving te voorkomen. Privacyvraagstukken binnen de gezondheidszorg zijn complex. Hiervoor moeten organisatorische en technische maatregelen worden getroffen. Tijdens de rampenbestrijding is het van het grootste belang dat de netwerkverbinding niet uitvalt. Hier is organisatorisch in voorzien door drie radiografische netwerken te creëren, zodat bij uitval van het ene netwerk het andere netwerk de communicatie kan overnemen.

Figuur 9 laat zien een vereenvoudigd gegevensstroomdiagram en geeft aan waar technische (PET) en/of organisatorische beveiligingsmaatregelen zijn genomen. De cirkels in het diagram verwijzen naar een reeks van PET-maatregelen. De organisatorische maatregelen (in figuur 9 vierkanten) die genomen zijn, betreffen onder meer de functionele autorisatie van het medisch personeel.



Figuur 9: Organisatorische en technische maatregelen in ViTTS gebaseerd op PET-maatregelen

Sterke beveiliging wordt toegepast door een verfijnde functionele autorisatiestructuur, waarbij de rol van de gebruiker bepaalt tot welk deel van het systeem hij toegang heeft. Deze oplossing is ook in het ziekenhuis informatiesysteem toegepast (de privacy incorporated database). Alleen het medisch personeel kan inloggen, informatie invoeren over de triage bij de ramp, gegevens opvragen waarbij encryptie en privacy management technieken worden gebruikt en versleuteld informatie verzenden. Geautoriseerde zorgverleners maken gebruik van digitale certificaten die op chipkaarten zijn opgeslagen of van chipkaarten met biometrische gegevens om zich uniek te identificeren. Andere gebruikers maken gebruik van softwarecertificaten, maar daarmee krijgt men geen toegang tot de medische gegevens.

Ook hier vindt scheiding van gegevens plaats, waarbij de medische gegevens en NAW-gegevens in verschillende tabellen zijn opgeslagen. De NAW-gegevens zijn versleuteld, zodat de medische gegevens voor ongeautoriseerde personen (bijvoorbeeld systeembeheerders) niet zijn te herleiden tot een natuurlijk persoon. De database met medische gegevens is opgeslagen bij een vertrouwde derde partij, de 'Trusted Third Party' (TTP), die stringente fysieke en logische beveiligingsmaatregelen heeft getroffen en hierop regelmatig wordt geaudit.

Bovendien vindt minimalisatie van gegevens plaats die worden uitgewisseld met andere informatiesystemen.

De voorloper van ViTTS was Nederlands Trauma Informatie Systeem (NTTS). In NTTS worden een beperkt aantal gegevens verstrekt aan een systeem waarmee de Regionaal Geneeskundig Functionaris (RFG) kan zien welke personen uit zijn gemeente betrokken zijn bij een ramp. Naast de NAW-gegevens wordt uitsluitend een classificatiecode verstrekt. De classificatiecode geeft informatie over de zwaarte van het letsel, maar de RGF krijgt geen inzage in de medische gegevens. Dit systeem bevat een tijdelijke database en de NAW-gegevens blijven hierin niet

bewaard. De functionaris kan de gegevens evenwel exporteren naar zijn eigen computer en dat kan bij onzorgvuldig handelen privacy risico's opleveren.

Om persoonsgegevens te beschermen worden de volgende organisatorische en technische maatregelen ter ondersteuning van de 'Identity Protectors' in ViTTS toegepast:

1.Ten behoeve van de bescherming van persoonsgegevens bij het registeren van slachtoffers op de plaats van de ramp zijn de technische maatregelen:

a. het opzetten van drie speciale (slachtoffer) netwerken in geval er een uitvalt;

b. bij het verzenden van informatie naar ViTTS wordt de data over een versleutelde lijn verzonden. De genomen organisatorische maatregel bij het verzamelen van informatie over slachtoffers is dat het alleen aan het medisch personeel is toegestaan (medische) gegevens te verzamelen over slachtoffers van de ramp conform de vereisten ex artikel 8 van de Richtlijn 95/46/EG.

2.Wat betreft het opvragen van informatie over slachtoffers/patiënten zijn de volgende technische maatregelen genomen:

a) Ziekenhuizen kunnen de web interface van het Utrecht trauma informatie systeem (UTIS) gebruiken om contact te maken met het ViTTS system. In het UTIS zijn strikte functionele autorisatietechnieken geïmplementeerd, die bij het inloggen door de techniek aan de gebruiker dwingend worden opgelegd;
b) Encryptie en privacy management systemen zorgen er voor dat alleen het medisch personeel gegevens kan opvragen;
c) Encryptie technieken zorgen er voor dat alleen het medisch personeel informatie kan toevoegen en terugzenden.

3.Bij het registeren van de slachtoffers met UICN wanneer zij in het ziekenhuis worden opgenomen, zijn bij het inloggen, het invoeren van data en het verzenden van informatie dezelfde organisatorische en technische maatregelen genomen n.l. functionele autorisatie en encryptie.

4.Wat betreft het verwerken van data (inloggen in I-RIS om de identiteit van het slachtoffer vast te stellen, het opvragen en verzenden van informatie) zijn eveneens technisch afdwingbare autorisatie technieken, encryptie en privacy management toegepast.

6.9 Privacy beleid geautomatiseerd uitvoeren

Naast privacy rechten van de patiënt en zorgverlener bestaan er ook privacy plichten van de verantwoordelijke(n). Met het gebruik van privacy management systemen (PMS) kan het naleven van privacy regels worden afgedwongen.

Het betreft hier programmatuur die als het ware als een schil om de verwerkingsprocessen van persoonsgegevens heen ligt en automatisch toetst of het verwerkingsproces plaatsvindt conform het vastgelegde privacybeleid geldend voor de desbetreffende database of het informatiesysteem. Het PMS zorgt er voor, dat er automatisch een inventarisatie plaatsvindt van persoonsgegevens in de databases van de verschillende legacy informatiesystemen, van de rollen (functies) toegekend in de 'directory services' en van de verwerkingsprocessen vastgelegd in de transactie logbestanden.

Het privacy beleid en de verwerkingsprocessen worden door middel van een gestandaardiseerde elektronische privacy taal in de PMS programmatuur ingevoerd.[35] Deze privacy taal werkt met specifieke privacy begrippen, begrippen en daarop gebaseerde privacy ontologieën. In het privacy management systeem worden de volgende privacy parameters gebruikt: 'actor(en)'; 'gegeven(s)' (speciale groepen van gegevens); 'activiteit(en)'; 'conditie(s)', 'doel(en)', 'attributen' en 'verplichtingen'.

Met deze parameters kan een organisatie zijn privacy beleid en de manier van verwerking beheren en modelleren. Bijvoorbeeld: toestemming van de betrokkene kan met een voorwaardelijke parameter worden gemodelleerd.

Toestemming is een belangrijk concept in de privacy wetgeving. Betrokkenen moeten expliciet en ondubbelzinnig toestemming geven alvorens de persoonsgegevens van de betrokkenen voor een specifiek doel mogen worden verwerkt. De toestemming van de betrokkene wordt bijvoorbeeld vastgelegd in een toestemmingenbestand. Dit bestand wordt gecombineerd met de doelbinding die is opgeslagen in een of meerdere informatiesystemen. De inrichting van de verwerking dient zodanig te zijn, dat naleving automatisch wordt afgedwongen. Dit gebeurt door 'privacy statements'.

Een voorbeeld van een 'privacy statement' in het PMS is: (cursief tussen haakjes staan de PMS elementen):
[ABC ziekenhuis] (*PMS element: actor*) [mag] (*PMS element: conditie*) [patiënt telefoonnummer] (*PMS element: gegevens*) [openbaar maken] (*PMS element: acties*) aan [XYZ verzekeraar] (*PMS element: actor*) voor [het aanbieden van nieuwe diensten] (*PMS element: conditie*) [als patiënt ABC ziekenhuis toestemming heeft gegeven voor het telefonisch aanbieden van nieuwe diensten] (*PMS element: conditie*).

Privacy beleid en verwerkingsprocessen gedefinieerd en vastgelegd in de hierboven beschreven privacy statements (in specifieke programmeertaal) gaan een integraal deel uitmaken van de geautomatiseerde gegevensverwerking van organisaties. De elektronische privacy statements kunnen ook worden gebruikt om verwerkingsprocessen te controleren en/of de naleving van het privacy beleid in het informatiesysteem te volgen.

Met behulp van logging en controle kan achteraf worden vastgesteld of het geïmplementeerde PMS adequaat functioneert. Hiervoor is het belangrijk om alle handelingen met betrekking tot persoonsgegevens die onder toezicht van de verantwoordelijke plaatsvinden, vast te leggen en te controleren. Een voorbeeld hiervan is om op persoonsniveau vast te leggen aan welke organisaties gegevens zijn verstrekt (inclusief waarom en wanneer). Er ontstaat daardoor een 'audit-trail' (wie deed wat, wanneer, waar en waarom) waardoor de bewerkingen controleerbaar zijn en er vastgesteld kan worden of het privacy beleid wordt opgevolgd en de genomen PET-maatregelen goed werken.

Met de regelmatige analyse van de logbestanden kunnen 'lekken' in PMS worden opgespoord en vervolgens gedicht worden. Op deze wijze draagt ook logging en controle bij tot het voorkomen van onrechtmatige verwerking van persoonsgegevens.

[35] Koorn R., et al, Privacy Enhancing Technologies, Witboek voor Beslissers, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Den Haag, 2004, p.36-37

Een bijkomend voordeel van logging en controle is dat voldaan kan worden aan de informatieplicht naar de burger/consument. Een burger kan aan een organisatie vragen welke gegevens de organisatie over hem heeft vastgelegd en aan wie deze informatie is verstrekt. Met behulp van de logbestanden kan de organisatie aantonen dat de informatie in het geheel niet is verstrekt of dat de informatie alleen maar is verstrekt aan geautoriseerde instanties of personen.

De logbestanden moeten wel afgeschermd blijven. Daarnaast moeten de logbestanden periodiek worden beoordeeld door bijvoorbeeld de beveiligingsfunctionaris of de functionaris gegevensbescherming (privacy officer), en moet het management hierover periodiek worden geïnformeerd. Een belangrijk aandachtspunt bij logging en controle is dat de logbestanden natuurlijk ook PET-proof moeten zijn.

Uit ervaring in Canada blijkt dat privacy managementsystemen het vertrouwen van de burger aanzienlijk vergroten en het inzicht van het management in de verwerking en controle van gegevens doen toenemen. Vooral de geautomatiseerde handhaving is een belangrijk pluspunt en voorkomt kostbare privacy-audits om de naleving te controleren.[36]

Hewlett Packard Labs in Bristol heeft om dergelijke en andere privacy plichten goed te beheren het *Obligation Management System* (OMS) ontworpen**.** Dit systeemcomponent regelt en ondersteunt het beheer, planning, handhaving en monitoring van de privacy plichten betreffende de persoonsgegevens binnen het informatiesysteem. De privacy plichten in dit systeem bestaan uit een reeks van beperkingen voortvloeiend uit de privacy en andere wetgeving die op de verzamelde persoonsgegevens moeten worden toegepast, met daarnaast de wensen van de eindgebruikers en van de medewerkers die zich met de bescherming van de persoonsgegevens bezighouden. De privacy plichten dwingen softwarematig een privacy bewust en privacy veilig levenscyclusbeheer van persoonsgegevens binnen de informatiehuishouding af. [37]

6.10 Antwoord op de tweede onderzoeksvraag

De geconstateerde privacy knelpunten kunnen voor een zeer groot deel worden voorkomen door gebruik te maken van Privacy-by Design (PbD) waarvan de kern bestaat uit Privacy-Enhancing Technologies (PETs). Dit zijn technische maatregelen gericht zijn op het beschermen van de privacy van de patiënt en zorgverlener en andere bij de 'patient-centered care' informatiehuishouding betrokkenen. Het basis ontwerp patroon bestaat uit een of meerdere Identity Protectors en het creëren van meerdere (pseudo)-identiteitsdomeinen en pesudo-identiteiten. Deze aanpak wordt toegepast in een privacy-by-design PGD. De medische en financiële gegevensstromen kunnen hier door worden gescheiden. Bovendien houden de patiënt, arts en zorgverlener zeggenschap op de toegang tot het PGD en wie welk gedeelte mag inzien. De toepassing van PbD leidt het tot een 'end-to-end' beveiliging, identiteits- en toegangsmanagement en een sterke op de functie gebaseerde authenticatie. Controlemogelijkheden, logging en auditing en terugkoppeling worden voor de patiënten ingebouwd. Gezien de complexiteit is het gebruik van privacy management systemen(PMS) noodzakelijk om privacy regels geautomatiseerd afdwingen. Onmisbaar is bij de gegevensuitwisseling de inschakeling van meerdere TTPs. Encryptie en decryptie zijn hierbij voor

[36] Rooij J.de, Privacymanagement en Enterprise Privacy Manager, *Privacy & Informatie,* 6e jaargang nummer 5, oktober 2003 p. 206-212.
[37] Casassa Mont M., Privacy Models and languages: Obligation Policies in in Camenish J.,R.Leenes, D.Sommer, Digital Privacy, Berlin, 2011, p.332- 361

alle medische data een sine qua non. Als PbD wordt toegepast in het PBD en informatiesystemen in de gezondheidsinformatiehuishouding dan zullen de medische gegevens van patiënten zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun gegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid.

7. Derde onderzoeksvraag: Welke concrete aanbevelingen volgen uit de geschetste oplossingsrichtingen

7.1 Eerste aanbeveling: Zorg dat Privacy-by Design beschikbaar komt

Een geleidelijke invoering van PbD zorgt voor het voortduren van privacy onveilige situaties voor de patiënt, de erosie van zijn privacy en het afnemen van het vertrouwen in de rechtmatige verwerking van zijn medische gegevens. Dit is ongewenst. De toepassing van PbD in PGD's en bestaande (bron) systemen in de gezondheidszorg dient via standaarden door iedereen ingevoerd te worden en mag niet vrijblijvend zijn. Daar voor is inhoudelijk een gecombineerde expertise nodig van privacy juristen en PbD ICT experts.
Empirisch onderzoek leidt tot de conclusie dat PbD/PET vaker zou kunnen worden geïmplementeerd als de toepassing van PbD zichtbaar is (door middel van certificering), door de steun van het management en sleutelfiguren in de samenleving, door de stimulerende rol van voorlichtende instanties, de druk van de privacywetgeving en medische wetgeving en door effectief toezicht.[38] Voorlichting over privacy-by-design is dringend noodzakelijk, zowel aan de ICT industrie als aan de stakeholders in de medische wereld en aan de patiënten. Een specifiek PbD expertise centrum voor de medische wereld zou moeten worden opgericht, dat experts/ consulenten kan inzetten, dan wel dit expertise centrum onder te brengen bij een bestaand instituut, zoals Nictiz.

7.2. Tweede aanbeveling: Voer de druk op vanuit de wetgeving

De druk vanuit standaarden en wetgeving is noodzakelijk, anders blijft alles te vrijblijvend. Druk vanuit de wetgeving zal zeker ontstaan als *General Data Protection Regulation* (GDPR)[39] in Europese Unie van kracht wordt. Artikel 79 van de GDPR maakt het mogelijk een hoge administratieve boete op te leggen bij het niet-voldoen aan de vereisten van de Verordening. De geconsolideerde onofficiële versie van het Europese Parlement gaat uit van sancties tot 100 miljoen of 5% wereldwijde jaaromzet! Het Europese Parlement heeft op 12 maart 2014 de GDPR met de hoge boeten aanvaard. De Europese Raad moet nog beslissen of zij de Regulation in zijn huidige vorm zal aanvaarden.

Lid 2 van dit artikel refereert uitdrukkelijk aan het nalaten van het nemen van technische en organisatorische maatregelen voortvloeiend uit artikel 23. Dit zal er voor zorgen dat "privacy-by-design" en "privacy by default" (PbD) op de management agenda komen te staan en de noodzaak om door PbD de in de privacy risico analyse gesignaleerde risico's te voorkomen sterk toe zal nemen. Bovendien betekent dit voor accountants dat er voor de organisatie waarvoor zij de financiële verslaglegging en controle doen een materieel risico is ontstaan dat in de rapportage moet worden meegenomen.[40]

In de GDPR wordt ook de privacy impact analyse verplicht gesteld. In de Wbp is het vooraf uitvoeren van een privacy risico analyse (impliciet) verplicht gesteld in artikel 13.

Het meest optimistische scenario is dat de GDPR, nu deze op 12 maart 2014 in het Europese Parlement is aangenomen, de Europese Raad gaat onderhandelen over de verschillen tussen de

[38] Borking, 2010, p. 312-326
[39] General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (COM(2012) 11 Final
[40] Borking J.J., Privacy-by-Design, Haute couture of Confectie? 2013/4 p. 186-195

Raad en het Parlement. Vermoedelijk levert dit een vertraging van een jaar op, zodat in de loop van 2015 de GDPR van kracht zou kunnen worden. Dit zal grote invloed gaan hebben om het introduceren van PbD in het PGD.

Na het van kracht worden kan privacy toezichthouder op grond van de GDPR de noodzakelijke controle op de implementatie van PbD uitvoeren en bij verzuim, nalaten of wanprestatie hoge boeten opleggen.

7.3. Derde aanbeveling: Voer vooraf een multi-actor analyse uit

Op basis van het onderzoek naar het gebruik van PET binnen de Nederlandse overheid, constateert RAND Europe in 2003 dat invoering van PET een multi-actorprobleem is. Dat wil zeggen: "een probleem waarbij de besluitvorming over de invoering, de uitvoering en de beschikbare middelen over de betrokken belanghebbenden (centrale overheid, afzonderlijke instanties en afdelingen, data-eigenaren en klanten) is verdeeld."[41]

Omdat PbD moeten voldoen aan een aantal fundamentele functionaliteiten en de 'stakeholders' (veel) specifieke eisen kunnen hebben, is het wenselijk hen actief bij het besluitvormingsproces te betrekken. Dit zal een breed draagvlak scheppen en de adoptie van PbD vergemakkelijken. Als er geen draagvlak is en alle partijen zich niet voor de volle honderd procent inzetten zal de invoering van de voorgestelde informatiehuishouding mislukken. Sterker nog: de betrokken partijen zullen tegenwerken als er geen rekening wordt gehouden met hun eisen en wensen en hun belangen als die door de invoering van PbD worden geschaad. [42]

7.4 Vierde aanbeveling: Voer een uitvoerige privacy impact analyse (PIA) uit

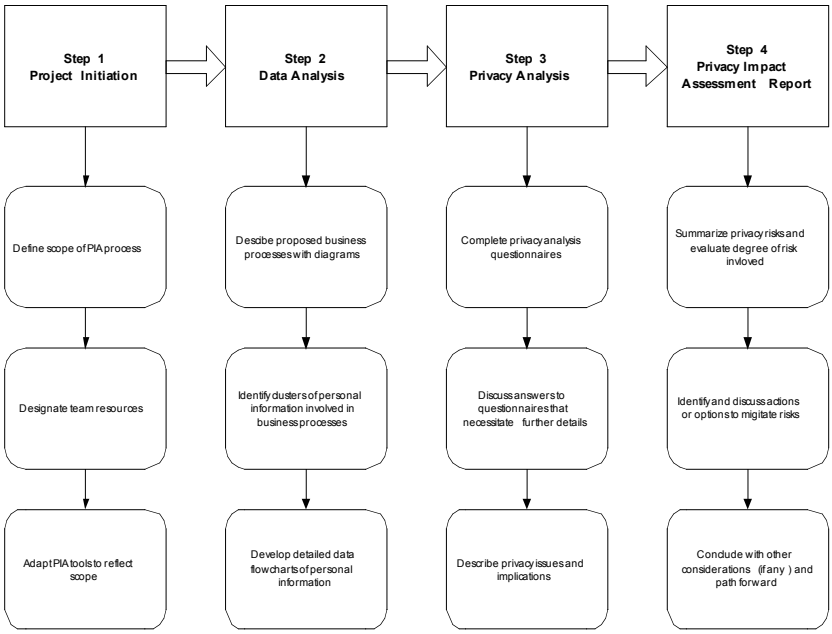
Voordat met PGD's en nieuwe (bron)systemen wordt begonnen dient een uitvoerige privacy impact analyse (PIA) te laten uitvoeren, waarbij gebruik wordt gemaakt van de Canadese model PIA (het meest uitgebreide en beproefde model in de wereld), om de bedreigingen en risico's die optreden bij de verwerking van persoonsgegevens in kaart te brengen. Op grond van de resultaten van de privacy impact(risico)analyse kan bepaald worden welke vormen van bescherming gewenst is voor de informatiehuishouding.

De PIA onderzoekt op basis van het bepaalde in de privacywetgeving of voldaan wordt aan de wettelijke eisen en of er privacy problemen (te verwachten) zijn. Het is een gestructureerde manier om de essentiële componenten van het informatiehuishouding en de stromen van persoonsgegevens in kaart te brengen. Het zorgt er voor dat privacyvraagstukken gedurende het (her)ontwerp van systemen en programmatuur niet veronachtzaamd worden. Zoals uit het onderstaande model (figuur 10) blijkt, bestaat het Canadese PIA proces uit vier basiscomponenten: de project initiatie, de data analyse, de privacy analyse en het privacy effect rapport. De PIA is niet eenmalig, maar volgt de ontwikkeling van het informatiesysteem gedurende zijn bestaan. De PIA leidt tot een privacy risico management plan, dat onder meer een beschrijving geeft van de geïdentificeerde privacy risico's, een analyse van de mogelijkheden om de privacy risico's te ondervangen of te verminderen, een lijst van overgebleven risico's die niet

[41] Horlings E., e.a., Werkbare vormen van Privacy Enhancing Technologies, Rand Europe in opdracht van het Ministerie BZK, Den Haag 2003, p.65

[42] Enserink, B., e.a., Policy Analysis of Multi-Actor Systems, 2010 , The Hague

opgelost kunnen worden en een analyse van de mogelijke gevolgen van deze risico's voor wat betreft de reactie van het publiek en het succes van het voorgestelde beleidsprogramma.



Figuur 10: De stappen in het PIA proces in Canada; Treasury Board of Canada, 2007

De motie Franken[43] verplicht de Rijksoverheid vooraf bij het ontwerpen van informatiesystemen of diensten waar mogelijk beperkingen op het grondrecht tot bescherming van de persoonlijke levenssfeer optreedt, een privacy impact assessment uit te voeren teneinde vast te stellen dat welke risico's de te nemen maatregel met zich meebrengt.

7.5 Vijfde aanbeveling: Maak een functioneel PbD Ontwerp en test het ontwerp in een pilot

Na de PIA kan worden vastgesteld hoe PbD en PETs kunnen worden toe gepast om de gegevensbescherming binnen de informatiehuishouding bij te dragen. De organisatie zal een balans moeten vinden tussen enerzijds de organisatorische en procedurele maatregelen en anderzijds de technische maatregelen waaronder PET-maatregelen. Technische maatregelen hebben sterk de voorkeur. Uit de bevindingen van de PIA zal blijken waar er sprake is van identiteitsrijke (identificerende persoonsgegevens vereist), identiteitsarme (identiteit eenmalig nodig, maar één persoonskenmerk zoals leeftijd of beroep volstaat) of identiteitsloze processen (geen identiteit nodig). Bij identiteitsrijke processen zijn met name de algemene PET-maatregelen toepasbaar: encryptie, toegangsbeveiliging, functionele autorisatie, biometrie en privacy managementsystemen. Bij identiteitsarme processen zijn scheiding van gegevens in identiteit- en pseudo-identiteit domeinen, algemene PET-maatregelen en privacy-management-systemen goed toe te passen. Bij identiteit loze processen zijn scheiding van gegevens in (pseudo)identiteitsdomeinen en het anonimiseren de aangewezen PET-vormen.

[43] Franken H. c.s., 1e Kamer Kamerstukken 2010–2011, 31 051, D

Vervolgens maakt de systeemontwerper onder meer een procesmodel van de gegevensstromen binnen het informatiehuishouding. Koppelingen en uitwisselingen met andere organisaties worden hier ook bij betrokken. [44]
Daarna volgt het functionele ontwerp waarin de benodigde functies van het informatiesysteem /huishouding in hun onderlinge verband worden beschreven. De scheiding van identiteit- en pseudo-identiteit domeinen heeft directe gevolgen voor het gegevensmodel en voor de koppelingen tussen de (pseudo)-identiteitsdomeinen en tussen eventuele andere informatiesystemen die gegevens onttrekken aan de gegevens van de informatiehuishouding.
De geselecteerde PET-vorm wordt vervolgens geïntegreerd in het technisch ontwerp van het informatiesysteem. De PET-vorm is immers geen los toe te voegen component en daarom kan het technisch ontwerp van PET niet los worden gezien van het technisch ontwerp van het gehele informatiehuishouding. Het geheel resulteert dan in een privacy-by-Design architectuur, die in een pilot moet worden getest.

7.6 Zesde aanbeveling: Zet 'trusted third parties' (TTPs) in

In paragraaf 6.6 is reeds gesteld dat encryptie bij PGD's en in de gehele gezondheidsinformatiehuishouding op micro, meso en macro niveau moet worden toegepast, waardoor het inzetten van TTP's bij PGD's en overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek noodzakelijk is;

7.7 Zevende aanbeveling: Voorschrijven van Risicomanagement en PbD bij Gemeenten

In paragraaf 5.8 is erop gewezen dat bij de decentralisatie van zorg naar gemeenten van begin af aan (dus niet achteraf) expliciet risicomanagement en Privacy-by-Design moet worden voorgeschreven en ingezet;

7.8 Achtste aanbeveling: Zorg voor sluitende anonimiseringstechnieken bij Big Data

In paragraaf 5.11 is aangegeven dat het gebruik van 'big data' nog in de kinderschoenen staat. Er is weinig bekend over de risico's voor en de attitude van individuen in het algemeen en patiënten en zorgverleners in het bijzonder wanneer zij met de gevolgen van (datamining van) big data (profilering) worden geconfronteerd. Juridisch gezien is het probleem dat bij de analyse van big data vaak secundair gebruik van data voorkomt, die bij de eerste verzameling niet voorzien was. Het anonimiseren van big data is zeer moeilijk gebleken, omdat er grote kans bestaat dat uit de geanonimiseerde data bij 'matching' met andere grote data bestanden toch identificerende informatie kan vrijkomen.
Daarom dient bij het opzetten van big data projecten zeer nauwkeurig de geanonimiserde data sets te worden onderzocht op mogelijke indirect identificerende gegevens.

7.9 Negende aanbeveling: Neem Privacy by Design op in standaarden

Uit het onderzoek naar de adoptiefactoren (zie paragraaf 8.1) voor PET blijkt, dat de druk van standaardisering, de wet- en regelgeving en van de toezichthouders belast met de bescherming

[44] Borking J.J.F.M., 2010, p. 378-380

van persoons/medische gegevens een positieve invloed hebben op de beslissing van organisaties om PbD/PET-maatregelen te nemen. [45]
Om vrijblijvendheid van de verantwoordelijken in de gezondheidszorg met betrekking tot PbD te voorkomen, is het noodzakelijk om PbD op te nemen in standaarden van PGD's en voor overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek.

7.10. Tiende aanbeveling: Controleer bij het gebruik van Clouds op wettelijk regime

In paragraaf 5.12 is gesteld dat er zich risico's voordoen bij het gebruik van opslag in de Cloud. Bovendien is er gebrek aan controle en gebrek aan informatie over de verwerking (transparantie) van gegevens. Voordat Cloud computing wordt overwogen, dient eerst een privacy risicoanalyse (PIA) te worden uitgevoerd. Vastgesteld moet worden of de beveiliging, transparantie en rechtszekerheid voor de gebruikers goed geborgd zijn en welk rechtstelsel geldt.

Een Cloud provider moet de naleving van de EU-wetgeving inzake gegevensbescherming garanderen. Dit houdt in dat de overeenkomsten met Cloud-providers nauwkeurig bestudeerd moeten worden op voldoende contractuele garanties op het gebied van technische en organisatorische maatregelen met betrekking tot de bescherming van persoonsgegevens. Nu al is gebleken, dat bij opslag van gegevens in een Cloud het risico van ongewenste en onbevoegde toegang (al dan niet door overheden, bijvoorbeeld onder de U.S. Patriot Act) plaatsvindt, en het risico op datalekken en misbruik van data toeneemt.[46]

Daarenboven wordt de opdracht voor het bouwen, beheer en onderhoud van de gezondheid/zorg verlenende infrastructuur door een Amerikaans moeder of zusterbedrijf afgeraden, omdat die bedrijven onder het regime van de Patriot Act vallen, zelfs als een dochterbedrijf gevestigd is binnen de EU.
De Europese Commissie deelt deze zorgen en heeft een Europese Cloud strategie in 2012 voorgesteld. Het is een *sine qua non* om bij Cloud computing vooraf een PIA uit te voeren, waarbij tevens vastgesteld moet worden of de beveiliging, transparantie en rechtszekerheid voor de gebruikers goed geborgd zijn en welk rechtstelsel geldt

7.11 Antwoord op de derde onderzoeksvraag

Teneinde PbD te realiseren is het noodzakelijk vooraf:

1. Een PbD expertise centrum wordt opgericht ter ondersteuning van het PbD proces en dat voorlichting kan geven en geconsulteerd kan worden. Privacy-by-Design experts dienen bij het ontwerp te worden betrokken.
2. Wettelijke druk uit te oefenen en vast te leggen, dat een privacy risico analyse vooraf dient plaats te vinden en dat privacy-by-design moet worden toegepast teneinde privacy-by-default te

[45] Borking J.J., Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time in Gurwirth S., e.a. Computers, Privacy and Data Protection: an Element of Choice, Dordrecht, 2011 p. 309-341
[46] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1, 2009

realiseren. De General Data Protection Regulation van de EU kan bij aanvaarding voor die druk zorgen;
3. Een multi-actor analyse uit te voeren, omdat PbD moet voldoen aan een aantal fundamentele functionaliteiten en de 'stakeholders' (veel) specifieke eisen zullen hebben, is het noodzakelijk hen actief bij het besluitvormingsproces te betrekken. Dit zal een breed draagvlak scheppen en de adoptie van de PbD informatiehuishouding vergemakkelijken en de adoptie van de PbD informatiehuishouding vergemakkelijken. Als er geen draagvlak is en alle partijen zich niet voor de volle honderd procent inzetten zal de invoering van de voorgestelde informatiehuishouding mislukken. Sterker nog: de betrokken partijen zullen tegenwerken als er geen rekening wordt gehouden met hun eisen en wensen en hun belangen als die door de invoering van PbD worden geschaad.
4. Een uitvoerige privacy impact analyse (PIA) te laten uitvoeren om de bedreigingen en risico's die optreden bij de verwerking van medische gegevens in kaart te brengen. Daarvoor kan gebruik wordt gemaakt van de Canadese model PIA (het meest uitgebreide en beproefde model in de wereld), om de bedreigingen en risico's die optreden bij de verwerking van persoonsgegevens zichtbaar te maken. Op grond van de resultaten van de PIA kan bepaald worden welke vormen van PbD gewenst zijn voor de informatiehuishouding;
5. Na de PIA het functionele ontwerp te laten volgen, waarin de benodigde functies van het informatiehuishouding (inclusief *identity and access management*) in hun onderlinge verband worden beschreven. De scheiding van identiteit- en pseudo-identiteit domeinen heeft directe gevolgen voor het gegevensmodel en voor de koppelingen tussen de (pseudo)-identiteitsdomeinen en tussen eventuele andere informatiesystemen die gegevens onttrekken aan de gegevens van de informatiehuishouding. Het geheel resulteert dan in een privacy-by-Design architectuur, die in een pilot moet worden getest.
6. TTP's in te zetten bij PGD's en overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek;
7. Bij de decentralisatie van zorg naar gemeenten van begin af aan expliciet risicomanagement en Privacy-by-Design voor te schrijven en in te zetten;
8. Bij het opzetten van big data projecten zeer nauwkeurig de geanonimiseerde data sets te onderzoeken op mogelijke direct en indirect identificerende gegevens;
9 In standaarden van PGD's en voor overige (bron)systemen in de informatiehuishouding van de gezondheidszorg op micro- meso – en macroniveau van zorgaanbieders, zorgverzekeraars, gemeenten en instituten voor beleids- en wetenschappelijk onderzoek PbD vereisten op te nemen.
10. Bij Cloud computing vooraf een PIA uit te voeren, waarbij tevens vastgesteld moet worden of de beveiliging, transparantie en rechtszekerheid voor de gebruikers goed geborgd zijn en welk rechtstelsel geldt. Wanneer het recht van een staat van de Verenigde Staten van toepassing is, geldt een contra-indicatie.

8. Vierde Onderzoeksvraag: Wat zijn de beperkingen van de geschetste oplossingen?

8.1 Adoptieproblemen

Voor het verwezenlijken van PbD bestaat een grote variëteit aan oplossingen. Tot nu toe is er nog geen algemeen geaccepteerde (gestandaardiseerde) methode hoe privacy bescherming (die verder gaat dan louter informatiebeveiliging) en de handhaving daarvan in hard- en software kan worden ingebouwd.[47] Van Rest stelt dat om PbD een effectief middel te laten zijn, er gericht onderzoek moet worden gedaan naar welke PbD architectuur patronen privacy risico's voorkomen of mitigeren en welke middelen en methoden privacy bescherming optimaliseren. Dit moet bij gebrek aan economische prikkels niet aan de markt worden overgelaten, want dat zal het innovatieproces te traag doen verlopen. [48] Hier ligt een belangrijke taak voor de Europese en nationale overheid om de reikwijdte van PbD concreter te maken en om PbD per applicatie domein (b.v. gezondheidszorg) te specificeren.

Het werkelijke probleem is echter de afwezigheid van voldoende positieve adoptiefactoren voor PbD en de onderliggende PETs. Ondanks de vele malen aantoonbare technische haalbaarheid van PbD/PET-maatregelen, maken organisaties nog vrijwel geen gebruik van PbD/PET, maar vertrouwen zij voornamelijk op klassieke organisatorische en technische informatiebeveiligings-maatregelen. Het blijkt dat een groot aantal factoren organisaties beïnvloeden bij hun beslissing om wel of niet PbD/PET toe te passen. Positieve factoren stimuleren de toepassing van PbD/PET en negatieve factoren zijn duidelijke belemmeringen om PbD/PET te implementeren. De overheid, die zich toch in de motie Nicolaï (in 1999 bij de behandeling van de Wbp) verplicht heeft om het voortouw te nemen bij het inzetten van PET in hun eigen gegevensverwerkende en gegevensdragende systemen, past PET structureel niet toe. Dit is het gevolg van het gebrek aan politieke wil en gebrek aan voldoende kennis over de voordelen die PbD/PET bij privacybescherming kan bieden. Volgens het Rand Europe onderzoek is er sprake van een vicieuze cirkel ten gevolge van de opvatting: zolang PET zich niet hebben bewezen, acht de overheid het risico van mislukking te groot; zolang men het risico te groot vindt, worden PET niet toegepast en kunnen PET zich niet bewijzen.[49]

Rogers heeft aangetoond dat een relatief voorspelbaar en constant ontwikkelingspatroon bestaat bij de acceptatie en verspreiding van een innovatie (PbD/PET is een innovatie). Bepalend is hoe de direct betrokkenen binnen de omgeving, waarin de innovatie wordt geïntroduceerd, de innovatie beoordelen. Rogers noemt vijf attributen die de mate van adoptie bepalen:

1. het relatieve voordeel;
2. de compatibiliteit;
3. de complexiteit;
4. de testbaarheid;
5. de zichtbaarheid.[50]

Van Lieshout deed in 2012 in opdracht van het Ministerie ELI een onderzoek naar de acceptatie

[47] Borking J.J., Privacy-by-Design, Haute couture of confectie? In Computerrecht 2013/ 4 - p. 186-195
[48] Van Rest J., e.a., Designing privacy-by-design, paper Annual Privacy Forum, 10-11 October, 2012, Limassol, p. 3,7
[49] Horlings E., et al, 2003, p.64
[50] Rogers, 2003, p. 36 Rogers E.M., Diffusion of Innovations, 5th edition New York 2003

van PbD in het bedrijfsleven. Hij stelt vast dat organisaties een onafhankelijk en op bedrijven gericht platform missen, dat informeert over beste aanpakken en dat ervaringen over invoering en toepassing van PbD kan delen. Daar hoort ook informatie over de interpretatie van het wettelijk kader bij en een uiteenzetting van professioneel opdrachtgeverschap rond privacyvraagstukken.
Dat pleit voor het oprichten van een PbD expertise centrum voor de medische sector. De geïnterviewde bedrijven geven aan dat de toezichthouder een geringe rol speelt bij de beslissing van de organisatie om PbD toe te passen, omdat de toezichthouder te weinig ondersteuning biedt rond praktische aangelegenheden. Ook ervaren zij geen positieve prikkels vanuit de toezichthouder die het aantrekkelijk maken om in PbD te investeren.
De hoofdconclusie van het onderzoek is dat er op het moment van het onderzoek in 2012 bij het bedrijfsleven duidelijk meer remmende dan stimulerende factoren aanwezig zijn voor de invoering en toepassing van *Privacy by Design.*[51]
Het van kracht worden van de Algemene Verordening gegevensbescherming (GDPR) door de Europese Raad en het Europese Parlement, die op zijn vroegst in 2015 wordt voorzien, zal daarin verandering brengen.

Onderzoek toont aan dat afgezien van de wettelijke verplichtingen waaraan bedrijven moeten voldoen, zij vooral in PbD/PET lijken te willen investeren om reputatieschade te vermijden. De geïnterviewde bedrijven zien omzetverlies en potentiële reputatieschade als de grootste risico's van een privacy inbreuk/ datalek. Een dergelijke reputatieschade vermijden is zelfs één van hun grootste zorgen.[52] Daarop zou door toezichthouders op de gezondheidszorg kunnen worden ingespeeld.

Uit het onderzoek naar de adoptiefactoren voor PET blijkt tevens, dat de druk van standaardisering, de wet- en regelgeving en met name van de toezichthouders belast met de bescherming van persoons/medische gegevens een positieve invloed hebben op de beslissing van organisaties om PbD/PET-maatregelen te nemen. [53]

Fairchild & Ribbers stellen dat om PET in een organisatie te kunnen implementeren het noodzakelijk is dat binnen de organisatie structureel 'identity and access management' (IAM) wordt toegepast. Immers, zonder IAM-processen is het niet mogelijk het gebruik van en de toegang tot (gevoelige) persoonsgegevens te controleren. Bovendien is een bepaald maturiteitsniveau van de betreffende IAM-processen en de ICT systemen noodzakelijk. Verscheidene maturiteitsmodellen zijn door Nolan Norton, CMMi, en INK ontwikkeld voor specifieke onderzoekgebieden zoals het gebruik van IT binnen organisaties, softwareontwikkeling, privacybescherming en informatiebeveiliging. Het is zeer onwaarschijnlijk dat onvolgroeide organisaties overgaan tot implementatie van PET.[54]

[51] Van Lieshout M., L. Kool, G. Bodea, J. Schlechter, B. van Schoonhoven, Stimulerende en remmende factoren van Privacy by Design in Nederland, TNO-rapport 2012 R10006, Delft 2012, p.49
[52] Borking J.J., Privacyrecht is code, over het gebruik van privacy Enhancing Technologies, proefschrift Leiden, Deventer 2010 p. 337-339
[53] Borking J.J., Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time in Gurwirth S., e.a. Computers, Privacy and Data Protection: an Element of Choice, Dordrecht, 2011 p. 309-341
[54] Fairchild A. & P.Ribbers, Privacy-Enhancing Identity Management in Business in Camenish J.,R.Leenes, D.Sommer, Digital Privacy, Berlin, 2011, p.107-138

Onderzoek moet worden wat het niveau van de maturiteit is van de ICT en IAM systemen in de gezondheidszorg. Zonder voldoende maturiteit van de ICT en IAM systemen is een hoog beschermingsniveau van medische gegevens door middel van PbD problematisch.

8.2 Antwoord op de vierde onderzoeksvraag

Het antwoord op de vierde onderzoeksvraag: Hoewel er al vele malen is aangetoond dat technologische oplossing van privacy problemen goed mogelijk is, blijkt het werkelijke probleem te zijn de afwezigheid van voldoende positieve adoptiefactoren voor PbD en de onderliggende PETs. Het vermijden van reputatieschade is een belangrijke stimulus om PbD toe te passen. Druk van de wetgever/ toezichthouders is een belangrijke voorwaarde om PbD geïmplementeerd te krijgen. Daar ontbreekt het nu volledig aan. De wetgeving refereert niet expliciet aan PbD/toepassing van PETs. Met de invoering van de EU Algemene Gegevensbescherming Verordening kan dit op middellange termijn veranderen. Het CBP oefent geen preventieve en repressieve druk uit om PbD /PETs te stimuleren. Een kritische succesfactor is dat ICT systemen en met name IAM (Identity & Access management) systemen robuust moeten zijn en voldoende maturiteit te bezitten.

9. Referenties

Advies van het Europees Economisch en Sociaal Comite over Matschappelijke betrokkenheid van ouderen en hun participatie in de samenleving (initiatiefadvies) (2013/C11/04)
Article 29 Data Protection Working Party WP 131, Working Document on the processing of personal data relating to health in electronic health records (EHR) (2007)
Bakker J., Golbach I., Nuijen T. Schouten H., Over risico's gesproken, Een onderzoek naar risicomanagement van de decentralisatie van de jeugdzorg bij Gemeenten, Amsterdam/Den Haag, 2013
Blarkom G. W. van, Guaranteeing requirements of data-protection legislation in a hospital environment with privacy-enhancing technology in *BJHCIM (The British Journal of Healthcare Computing & Information Management*), May 1998, Vol.15 number 4
Blarkom Van G.W., Borking J.J., Olk J.G.E., Handbook of Privacy and Privacy-Enhancing Technologies, The Hague, 2003,
Borking J.J.F.M., Privacyrecht is code, over het gebruik van privacy Enhancing Technologies, proefschrift Leiden, Deventer 2010
Borking J.J., Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time in Gurwirth S., e.a. Computers, Privacy and Data Protection: an Element of Choice, Dordrecht, 2011
Borking J.J., Privacy-by-Design, Haute couture of Confectie? In Computerrecht 2013/ 4
Brands S.A., Rethinking Public Key Infrastructures and Digital Certificates, Building in Privacy, Cambridge (MA) 2000
Casassa Mont M., Privacy Models and languages: Obligation Policies in in Camenish J., R.Leenes, D.Sommer, Digital Privacy, Berlin, 2011
Chaum, D. Achieving Electronic Privacy, in *Scientific American* August 1992
Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1, 2009
Cloud computing, http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
Diginotar incident www.onderzoeksraad.nl/nl/onderzoek/1094/het-**diginotarincident**
Duthler A.W., Met Recht een TTP!, (proefschrift) Rijksuniversiteit Leiden 22 september 1998, Deventer 1998.
Enserink, B., e.a., Policy Analysis of Multi-Actor Systems, 2010 , The Hague
EU Cybersecurity Strategy Verslag, Brussel op 28 februari 2014
European Patent: EP0884670 (G.van Blarkom, inventor, ICL 1997)
Fairchild A. & P.Ribbers, Privacy-Enhancing Identity Management in Business in Camenish J., R.Leenes, D.Sommer, Digital Privacy, Berlin, 2011
Financieel Dagblad, Big Data, Outlook LIVE 4 februari 2014
Franken H. c.s., 1e Kamer Kamerstukken 2010–2011, 31 051, D
Geissbuhler A et al., Trustworthy reuse of health data: A transnational perspective in international Journal of medical informatics 82 (2013)
General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (COM (2012) 11 Final)
Gilbert N., Dilemmas of privacy and Surveillance: Challenges of Technology change, (presentation and paper), London 2007
Hes R. & J. Borking, Privacy Enhancing Technologies: The Path to Anonymity, The Hague 2000
Hooghiemstra T.F.M. & Nouwt S, Wet bescherming persoonsgegevens,Den Haag 2011
Horlings E., e.a., Werkbare vormen van Privacy Enhancing Technologies, Rand Europe in opdracht van het Ministerie BZK, Den Haag 2003

Househ M., Sharing sensitive personal health information through Facebook, the unintended consequences, in *User Centred Networked Health Care A. Moen et al. (Eds.) IOS Press, 2011*
Ingen van E., De Haan J. & M.Duimel, Achterstand en Afstand, SCB Den Haag 2007
Katzenbauer M., Te vroeg voor landelijk EPD in Medisch Contact 14 mei 2009:
Koorn R., et al, Privacy Enhancing Technologies, Witboek voor Beslissers, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Den Haag, 2004
Lanier J., How Should We Think about Privacy, in Scientific American November 2013
Lazakidou A., Healthcare and Biomedicine, New York, 2010
Lieshout Van M., L. Kool, G. Bodea, J. Schlechter, B. van Schoonhoven, Stimulerende en remmende factoren van Privacy by Design in Nederland, TNO-rapport 2012 R10006, Delft 2012,
Mell P. & T. Grance, The NIST Definition of Cloud Computing, September 2011, csrc.nist.gov/publications /nistpubs/800-145/SP800-145.pdf,
Nägele T. & S. Jacobs, 'Rechtsfragen des Cloud Computing', *Zeitschrift für Urheber--- und Medienrecht* vol. 54, 2010, nr. 4,.
Rest Van J., e.a., Designing privacy-by-design, paper Annual Privacy Forum, 10-11 October, 2012, Limassol
Rogers E.M., Diffusion of Innovations, 5th edition New York 2003
Rooij J.de, Privacymanagement en Enterprise Privacy Manager, *Privacy & Informatie,* 6e jaargang nummer 5, oktober 2003
Rothstein M.A., The Hippocratic Bargain and Health Information Technology, in Journal of Law, Medicine & Ethics, 2010
Ruotsalainen P. et al., Framework model and principles for trusted information sharing in User Centered Networked Health Care, IOS press, Amsterdam 2011
Sharad K. & G. Danezis, De-anonymizing D4D Datasets, http://petsymposium.org/2013/papers/sharad-deanonymization.pdf
Versmissen J.A.G., Sleutels Van Vertrouwen, TTP's, digitale certificaten en privacy, (A&V) (Achtergronden en Verkenningen) Nr. 22, Den Haag, 2001