13 oktober 2017

Privacy van patiënten bij elektronische gegevensuitwisseling

Ontwikkeling van een landelijk kader dat de privacy van patiënten in alle redelijkheid en zorgvuldigheid garandeert bij elektronisch gegevensuitwisseling

Project uit het 2e periode-programma 'Regionale Oncologienetwerken'
Rapportage oktober 2017

Dr. H.J. Bloemendal, internist-oncoloog Meander Medisch Centrum/UMC Utrecht
D.I.R. van der Brugge, redacteur
Prof. dr. P.O. Witteveen, internist-oncoloog UMC Utrecht

Regionale Oncologienetwerken

Inhoudsopgave

Inleiding

In deze publicatie vindt u de rapportage van het Citrienproject ‘Privacy van patiënten bij elektronische gegevensuitwisseling’.

Hoofdstuk 1 beschrijft de probleemstelling.
Samenwerking van zorgverleners uit verschillende ziekenhuizen binnen de behandeling van één patiënt veronderstelt dat gegevens over de patiënt, onderzoeksresultaten, behandelplannen en andere dossiergegevens in verschillende ziekenhuizen ingezien en bewerkt kunnen worden.
Doordat er geen systeem is waarbij één centraal patiëntdossier door elke zorgverlener kan worden gebruikt, moeten dossiergegevens van het ene lokale patiëntendossier naar het andere worden gekopieerd.

Hoofdstuk 2 beschrijft welke faciliteiten nodig zijn voor veilig dataverkeer, en wat er nu is. Er is geen landelijke of regionale infrastructuur die de overdrachtsproblemen oplost. Elk ziekenhuis heeft zijn eigen ziekenhuis-EPD, geïntegreerd in een ziekenhuis-informatiesysteem voor planning van onderzoeken, behandelingen en zorgactiviteiten. Die kunnen niet per definitie communiceren met het systeem van collega-zorginstellingen in de regio. Welke deeloplossingen zijn er en wat ontbreekt?
Welke wetten en regels zijn er op dit gebied en (hoe) worden die gehandhaafd.

Hoofdstuk 3 geeft een samenvatting van de bevindingen uit de rondgang die gemaakt is in het kader van dit project. Er worden praktische handreikingen voor zorgverleners gegeven, en terugkoppeling aan de opdrachtgever.

Hoofdstuk 1: Project 'Privacy van patiënten bij elektronische gegevensuitwisseling'

1.1 Aanleiding: zorginnovatie binnen het Citrienfonds

Eén van de grootste beleidsmatige uitdagingen in Nederland is de kwaliteit van de zorg te behouden en zelfs nog uit te bouwen én tegelijkertijd de zorg ook in de toekomst betaalbaar te houden. Daarvoor zijn structurele innovaties nodig.
In opdracht van het Ministerie van VWS heeft ZonMw het Citrienfonds gevormd, waarin de UMC's met andere stakeholders werken aan duurzame en breed inzetbare verbeteringen in de zorg.
De koepelorganisatie van de UMC's, de NFU, is verantwoordelijk voor de uitvoering van Citrien. ZonMw voert de kwaliteitsbeoordeling en monitoring en evaluatie uit van projecten.

De Taskforce Oncologie (bestaand uit NFK, NHG, NVZ, NFU, IKNL en Soncos) werkt met het Citrienfonds aan regionale netwerkvorming in de oncologische zorg. Naast de regionale projecten heeft elk van de UMC-regio's de uitvoering van een landelijk deelproject op zich genomen. Deze publicatie vanuit de UMC Utrecht-regio rapporteert de bevindingen en aanbevelingen van het landelijke project 'Privacy van patiënten bij elektronische gegevensuitwisseling'.

1.2 Oncologische netwerkvorming

Het Koersboek Oncologische netwerkvorming stelt: "Regionale netwerkvorming in de oncologische zorg is noodzakelijk en op veel plekken in Nederland al in gang. Comprehensive Cancer Networks (CCN's) zorgen ervoor dat patiënten met kanker overal, onafhankelijk van de plek waar zij hun zorgtraject starten, kunnen rekenen op optimale oncologische zorg. Op zo kort mogelijke termijn, volgens de laatste stand van de wetenschap, diagnostiek, behandeling en ervaringsdeskundigheid."

Deze zorgconcentratie is geen beweging die zich uitsluitend voltrekt in het domein Oncologie.
In het algemeen zien we dat in de zorg de muren tussen verschillende instellingen en zorgverleners geslecht worden om de uitkomsten voor de patiënten en de doelmatigheid van zorg te maximaliseren. Dat vergt communicatie tussen ziekenhuizen en eerste lijn, apothekers, thuiszorg en verpleeginstellingen.

1.3 Probleemstelling: het optimum tussen snel, veilig en betrouwbaar

Netwerkvorming is, bezien vanuit medisch perspectief, dus allereerst een logische en noodzakelijke ontwikkeling om maximale uitkomsten van de zorg te kunnen realiseren voor en met de patiënt. Waar zorgverlener en patiënt besluiten tot een zorgtraject dat aangeboden wordt in netwerkverband, impliceert dat

gegevensoverdracht tussen zorginstellingen. Die hoort, net als alle andere aspecten van zorg, snel, veilig en betrouwbaar zijn beslag te krijgen.
Die drie criteria krijgen slechts in onderlinge samenhang betekenis als 'kwaliteit'. Primair belanghebbende is daarbij de patiënt; daarna achtereenvolgens de zorgverlener en zorgverzekeraar.

Het handelingskader van de zorgverlener die data uitwisselt, wordt verder afgebakend door de mogelijkheden van ICT-faciliteiten en wet- en regelgeving. Idealiter vormen ICT-inspanningen en het juridisch kader een weerslag van de belangenbehartiging van patiënt en zorgverlener.
We zien, in de nog verre van uitgekristalliseerde praktijk, alle actoren nog worstelen met het samenbrengen van belangen, mogelijkheden en regelgeving.

Ongetwijfeld zal er in de toekomst een mogelijkheid worden gevonden om dossiers in netwerkverband te beheren. Vooralsnog heeft de patiënt echter, in elke instelling die in een regionaal netwerk participeert, zijn eigen dossier en wisselen zorgverleners data uit met instellingen die meestal geen compatibele informatiesystemen gebruiken.
Het project 'Privacy van patiënten bij elektronische gegevensuitwisseling' zoekt het optimum in het spanningsveld tussen snelle, veilige en betrouwbare gegevensuitwisseling, in het 'interbellum' waarin we ons bevinden: de periode waarin nog patiëntgegevens van het ene naar het andere ziekenhuisdossier moeten worden gekopieerd.

1.4 Opdracht: ontwikkel handreikingen voor een veilig en werkbaar handelingskader

Nu de praktijk: hoe te handelen als individuele zorgverlener en zorginstelling?
De opdracht aan de projectgroep 'Privacy van patiënten bij elektronische gegevensuitwisseling' is een praktische handreiking te schrijven, die recht doet aan patiëntbelang van snelle, veilige en betrouwbare overdracht van zijn gegevens, met maximale zorg voor privacy en veiligheid, binnen de juridische kaders die van toepassing zijn.

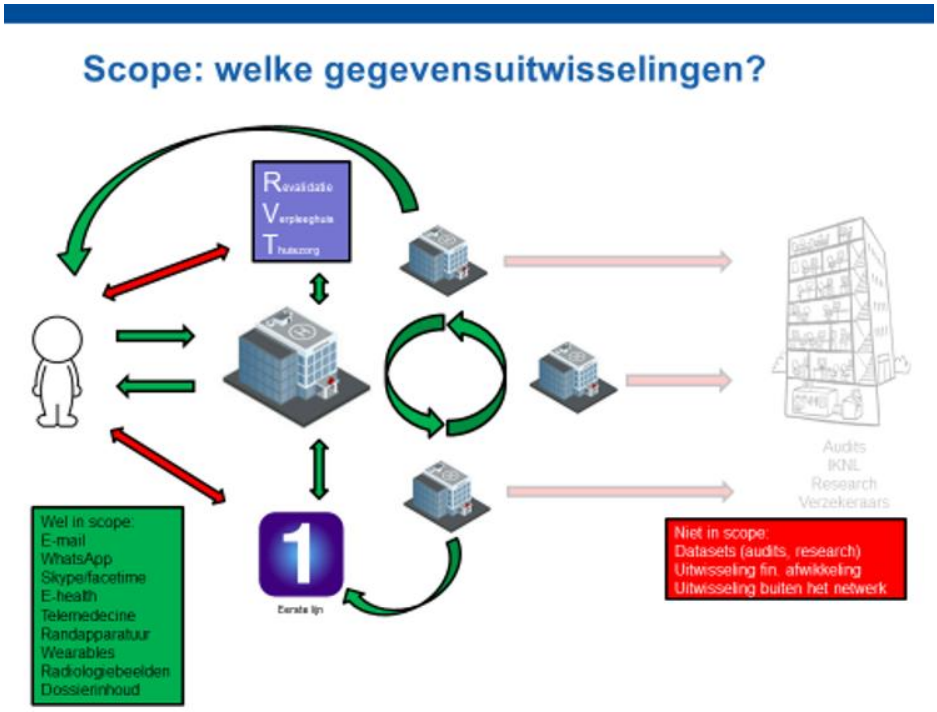
Onvermijdelijk leidt een oriëntatie op de beste handelingsstrategie voor zorgverleners ook tot aandachtspunten voor de inrichting van ICT-systemen in de instellingen die patiënten in netwerkverband behandelen. Die worden in het kader van deze projectrapportage aangestipt, maar niet nader uitgewerkt.

De rapportage gaat in op de situatie van 2017: er zijn netwerksystemen in ontwikkeling, en daarvoor gelden aanbevelingen om de werkbaarheid in de toekomst te garanderen.
Maar we werken nu in een tussenfase. Noch de netwerkontwikkeling, noch de wetgeving rond elektronische gegevensuitwisseling is uitgekristalliseerd. We hebben te maken met verschillende lokale patiëntendossiers en het kopiëren van data van ziekenhuis 1 naar ziekenhuis 2 om collega's adequaat te informeren voordat de patiënt zich daar meldt. Welke praktische handreikingen kunnen we doen aan zorgverleners?

1.5 Aanpak: inventariseren, analyseren en concluderen

In het kader van het project ‘Privacy van patiënten bij elektronische gegevensuitwisseling’ is een inventarisatie gemaakt van wat idealiter nodig is voor veilig dataverkeer, van wat we nu hebben (en wat er dus nog ontbreekt) en van wettelijke regels en richtlijnen die van toepassing zijn op dit moment, in de fase waarin we al wél gezamenlijk patiënten behandelen, terwijl dossiervoering in netwerkverband nog niet gerealiseerd is.

De scope van het project beperkt zich tot dataverkeer tussen zorgverleners in het kader van de behandeling van patiënten. Uitwisseling ten behoeve van audits, research en financiële afwikkeling van het zorgproces, valt buiten het bestek van deze rapportage, maar kent gelijksoortige vraagstukken.



De inventarisatie is gemaakt in een rondgang langs ter zake deskundige en gezag dragende personen en instellingen, zowel met persoonlijke gesprekken als door middel van deskresearch. Een lijst van geconsulteerde personen en instellingen is opgenomen als bijlage 1.
De conclusies die uit de samengebrachte input zijn getrokken, zijn voor verantwoordelijkheid van de rapporterende auteurs.

Deze rapportage biedt professionals die in netwerkverband zorg verlenen aan patiënten een domeinverkenning en een praktische handreiking voor data-uitwisseling. De rapportage bevat tevens aanbevelingen voor bestuurders die de zorgverlening faciliteren.

2. Hoofdstuk 2: Bevindingen

2.1 De noodzaak van overdracht van patiëntgegevens

Behandeling van een patiënt in netwerkverband vereist beschikbaarheid van medische gegevens (en in tweede instantie ook planningsgegevens) voor alle zorgverleners die een behandelrelatie met de patiënt hebben of aangaan. De noodzaak van uitwisseling loopt vooruit op de beschikbaarheid van 100% veilige, accurate en snelle uitwisselingskanalen. Dat is een onderwerp van permanente zorg en aandacht, zowel van zorgverleners als van beleidmakers.

De werkelijkheid waarin een patiënt zo snel mogelijk bij een collega op het spreekuur moet zitten, waarbij de collega adequaat geïnformeerd moet zijn, is vanzelfsprekend zo oud als de ziekenhuiszorg. De noodzaak om gegevens goed over te dragen dus ook, evenals de morele en juridische verplichtingen die zorgverleners in dat verband dragen. Alleen is de zoekgeraakte brief van weleer vandaag een datalek. Aard en omvang van risico's bij gegevensoverdracht zijn veranderd. Met databeveiliging is een heel nieuw kennisdomein gemoeid.

In de dominante beeldvorming onder zorgprofessionals is uitwisseling en overdracht van medische gegevens dan ook aan strenge regels gebonden. Dat kan in de praktijk van de spreekkamer als belemmering worden ervaren voor snelle en adequate zorg. Deze projectrapportage biedt pragmatisch zicht op het stelsel van privacybeschermende wet- en regelgeving. Welke normen en handelingsvoorschriften hebben betrekking op een in de toekomst beschikbaar te stellen netwerksysteem (vergelijkbaar met het politiek gesneuvelde landelijk Elektronisch Patiënten Dossier, EPD)? Bestaat de 'Gouden standaard' die wij als zorgverleners percipiëren eigenlijk wel in real life? En welke regels gelden ten aanzien van wat de zorgverlener vandaag kan en moet doen, opdat zijn netwerk collega morgen goed beslagen ten ijs komt bij de consultverlening aan de patiënt?

2.2 Wat is nodig voor veilig dataverkeer?

Idealiter is een landelijke elektronische infrastructuur nodig. De volksvertegenwoordiging (i.c. de Eerste Kamer) heeft in 2011 de stekker uit het landelijk EPD getrokken, omdat er twijfels waren over de privacybescherming van patiënten en informatieveiligheid.

Hoe zat het ook alweer met het landelijk EPD?
Het Landelijk Schakelpunt (LSP) dat landelijk uitwisseling van medische gegevenstussen zorginstellingen mogelijk moest maken, was sedert 1997 in opbouw, onder beheer van Nictiz (het expertisecentrum voor eHealth). Op verzoek van de Tweede Kamer is de regie in 2005 overgeheveld naar het Ministerie van WVS.
In 2008 werd de Wet gebruik BSN in de zorg goedgekeurd. Daarmee werd het burgerservicenummer aangewezen als de noemer waarop patiënten geïdentificeerd worden en waarop EPD-data via het LSP zouden kunnen worden uitgewisseld.
In april 2011 trok de Eerste Kamer (unaniem!) de stekker uit het landelijk EPD door de verplichte aansluiting voor zorgverleners en zorginstellingen te schrappen.
Het landelijk EPD werd vooral genekt door twijfels over privacy en informatieveiligheid.
De Tweede Kamer gelastte de Minister later dat jaar om toch een doorstart te faciliteren, maar dan langs private weg. Dan gaat het per definitie om een opt-in-systeem.
Het LSP wordt sedertdien doorontwikkeld door de daartoe opgerichte VZVZ (Vereniging van zorgaanbieders voor zorgcommunicatie). Het patiëntendossier van individuele patiënten berust bij hun behandelaar. Via een opt-in-procedure kan de patiënt toestemming geven voor gegevensuitwisseling met andere zorgverleners, via het LSP. Huisartsen, huisartsenposten en medisch specialisten in ziekenhuizen kunnen na toestemming van de patiënt alleen het medicatieoverzicht van de apotheek zien. Voor uitwisseling van patiëntgegevens in ziekenhuisdossiers is het LSP niet bruikbaar.

De verwachting (en wat de meeste zorgaanbieders betreft: de hoop) is dat er uiteindelijk toch een centraal of ten minste regionaal platform zal komen, waar zorgverleners gezamenlijk een dossier voeren. Zorgverleners kunnen het dossier van hun patiënt dan uitchecken en na gebruik (eventueel aangevuld) terugplaatsen. Zo'n systeem zou dan vanzelfsprekend voorzien zijn van alle veiligheidswaarborgen die in 2011 nog ontbraken en het landelijk EPD politiek fataal werden.

De politieke discussie rond het (landelijk) EPD is in flinke mate gekleurd door lobbyorganisaties. Actieplatforms als Bits of Freedom en Privacy First hebben met hun eisen voor absolute informatieveiligheid het morele gelijk aan hun zijde als het gaat om normstelling. Er is echter ook een ander moreel gelijk: dat van de arts die een patiënt in consult heeft. In het geval van een oncologische patiënt moet vaak met een hoge mate van spoed een adequate behandeling ingezet worden. Ook de arts die met instemming van deze patiënt alle technologie die hem ten dienste staat aanwendt om in gang te zetten wat er gedaan moet worden, heeft eveneens een moreel gelijk. Ook al is er (nog) geen systeem beschikbaar dat aan alle denkbare eisen van veilig dataverkeer voldoet. De confrontatie van deze perspectieven ontbreekt in het politieke debat, en dat wordt door veel zorgverleners ervaren als een essentieel gemis.

Het ontwikkelen van infrastructuur voor data-uitwisseling in de zorg is een omvangrijk proces, zowel technisch, economisch, politiek, en praktisch. Er moet integratie en interoperabiliteit gerealiseerd worden van en tussen verschillende zorg-ICT hardware en software. Dat dataverkeer 'moet' voldoen aan de norm NEN 7510, een door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging voor de zorgsector in Nederland.

Voldoen aan NEN 7510 is echter geen wettelijke verplichting. De NVZ-site meldt: “De norm, in 2011 geactualiseerd, is uitgangspunt voor de maatregelen die ziekenhuizen moeten nemen voor goede informatiebeveiliging. Hierin staat bijvoorbeeld dat ziekenhuizen goed in kaart moeten brengen welke risico’s ze lopen en dat ze bij elk risico passende maatregelen moeten nemen. Daarbij gaat het niet alleen om de informatie op computers, maar ook om de informatie op papier en om het gedrag van medewerkers die met de informatie omgaan. Naast vertrouwelijkheid gaat informatiebeveiliging ook over beschikbaarheid en integriteit van gegevens.”

Zolang er geen centraal patiëntendossier bestaat, moeten instellingen de normen van doelmatigheid, interoperabiliteit en veiligheid zo dicht mogelijk benaderen met de infrastructuur die hen nu ten dienste staat om patiëntgegevens uit hun eigen instellingsdossier ter hand te stellen aan collega-zorgverleners. Het management van een instelling is vanzelfsprekend geen passieve ‘probleemeigenaar’; het bepaalt met beleidsontwikkeling en investeringsbeslissingen immers mede hoe die infrastructuur eruitziet die gebruikt wordt voor data-uitwisseling, zowel intern als in netwerkverband.

2.3 Wat is er nu?

Door zorgconcentratie en netwerkvorming stijgt de behoefte om data te kunnen uitwisselen. Bovendien raken mensen in Nederland er steeds meer aan gewend dat zij e-based kunnen communiceren met de overheid, nutsinstellingen, hun bank, de winkels die zij beklanten… Patiënten verlangen en verwachten dat ook van hun ziekenhuis, en zorgverleners verwachten daarin gefaciliteerd te worden voor hun beroepsuitoefening.
De vraag naar faciliteiten voor gegevensuitwisseling is dus niet gestokt bij het sneuvelen van het landelijk EPD. Het momentum om op nationaal niveau te werken aan een masterplan voor ontwikkeling van eenduidige infrastructuur is gepasseerd toen de Eerste Kamer in 2011 het landelijk EPD afschoot. De doorstart is beperkt tot een opt-in-systeem met private middelen. Zie het kader ‘Hoe zat het ook alweer met het EPD?’. Initiatieven zijn regionaal van aard.

Wat is er nu beschikbaar om die uitwisseling te faciliteren?

I Systemen

Elektronische uitwisselingssystemen
Om zorginformatiesystemen van zorgaanbieders aan elkaar te koppelen of om patiëntgegevens te kunnen delen of uitwisselen zijn systemen nodig. Zoals Edifact digitale gegevensuitwisseling met de huisartsen mogelijk maakt via een beveiligd netwerk, en zoals het LSP bedoeld is voor data-uitwisseling in het EPD. Die uitwisselingssystemen zijn gebaseerd op een standaard, zoals OZIS of XDS.

XDS (Cross-enterprise Document Sharing) is de standaard voor veilige gegevensuitwisseling binnen regionale netwerken. Via de ‘digitale snelweg’ van hun netwerk, kunnen ziekenhuizen patiëntgegevens (tekst, beeld) uitwisselen. XDS wordt ondersteund door het internationale samenwerkingsverband IHE, ‘Integrating the Healthcare Enterprise’.

In veel regio's in Nederland zijn XDS-netwerken geïmplementeerd of in ontwikkeling, waaronder in de acht verschillende regio's rond UMC's. XDS maakt gebruik van een eigen netwerk op de bestaande infrastructuur.

XDS heeft als veilige afspraak rond de gegevensuitwisseling tussen ziekenhuizen geen wettelijk verplichte status. Er zijn ook andere platforms denkbaar en soms worden die ook bepleit. We noemen hier XDS omdat dat het enige systeem is met wereldwijd draagvlak en een ondersteunende infrastructuur om integratie en interoperabiliteit te kunnen realiseren.

Ziekenhuis-EPD's/ZIS
Praktisch alle Nederlandse ziekenhuizen hebben een elektronisch patiëntendossier, in een pakket gecombineerd met een Ziekenhuis Informatie Systeem (ZIS) voor planning, logistiek van patiëntstromen, inzet van zorgverleners en financiële afwikkeling. Die dossiers zijn met name ingevoerd vanwege de interne snelheid en doelmatigheid van werken. In die zin functioneren ze ook. Uitwisseling van gegevens met andere instellingen, die mogelijk deel hebben aan de behandeling van dezelfde zorgvraag van dezelfde patiënt, is geen prominent doel geweest bij de implementatie van die elektronische dossiers. Doorgaans kozen instellingen voor de goedkoopste optie die tegemoet kwam aan de wensen van interne uitwisseling. Er wordt nog altijd niet primair gedacht in termen van (ICT-) netwerkvorming en het aantal mensen in een instelling dat kennis van zaken heeft op het gebied van data-uitwisseling op regionaal of landelijk niveau is zeer beperkt. Het gevolg is dat ziekenhuizen met verschillende systemen en eigen applicaties werken, die niet met elkaar (kunnen) communiceren.

Die situatie toont wel enige kentering. In Nederland waren medio 2016 nog 9 verschillende EPD's in gebruik, maar dat aantal loopt terug. Onderzoek door M&I/Partners in opdracht van Zorgvisie liet zien dat 24 ziekenhuizen bezig waren met de switch naar een ander EPD en zonder uitzondering de aankoop of implementatie van Epic of Chipsoft Hix voorbereidden. Dat wil nog niet zeggen dat het uitwisselingsprobleem zich hiermee vanzelf oplost. De inrichting van Epic of Hix verschilt per ziekenhuis; daarmee zijn ook gelijke systemen nog niet op elkaar aan te sluiten zonder aanvullende applicaties.

II Tools

Er zijn mogelijkheden om de privacy van patiënten bij gegevensuitwisseling zo goed mogelijk te waarborgen. Bij de ontwikkeling van nieuwe ICT-oplossingen wordt het principe 'privacy by design' gehanteerd. Het houdt in dat bij het ontwerp van een informatiesysteem al rekening wordt gehouden met privacy van de patiënt, bijvoorbeeld door data versleuteld op te slaan of te versturen. Dit is de meest gebruiksvriendelijke manier van het waarborgen van privacy. En daarnaast het minst foutgevoelig.

Voorbeelden van systemen die gebruikt worden voor gegevensuitwisseling:

E-mailverkeer, berichtenservices en transferdiensten
In aanvulling op netwerken, of soms ook nog bij gebrek aan netwerken, gebruikt een aantal artsen ook e-mail, berichtenservices en transferdiensten op internet om patiëntgegevens uit te wisselen met collega-behandelaars. Daarmee realiseert men een snelle doorverwijzing of second opinion. In die zin komt dit handelen de kwaliteit van de zorg ten goede. Er wordt evenwel nog lang niet altijd gebruik gemaakt van beveiligde varianten op de bekende communicatiekanalen, waarbij gegevens encrypted worden verstuurd. Dat heeft te maken met onbekendheid en/of met een gebrek aan beschikbaarheid van diensten als Siilo, ZorgMail, Filesender of applicaties als Zivver waarmee men data kan versleutelen. We moeten ook constateren dat er weinig afstemming is tussen instellingen over de diensten die zij selecteren om hun zorgverleners veilig te kunnen laten communiceren binnen bestaande of te vormen samenwerkingsverbanden.

Informatiedragers: USB-sticks, DVD's, hard disks van laptops
USB-sticks en DVD's met patiëntengegevens worden nog veelvuldig gebruikt voor overdracht van patiëntgegevens tussen zorginstellingen. De meeste instellingen stellen het gebruik van beveiligde USB-sticks verplicht; het zijn producten die makkelijk en zonder veel meerkosten verkrijgbaar zijn. Dit beleid wordt echter nauwelijks afgedwongen. De veiligheid van dataverkeer via DVD's wordt bepaald door het brandprogramma dat gebruikt wordt; niet door het medium DVD. Ziekenhuizen kunnen voorzien in brandprogramma's die data versleutelen. We hebben geen zicht op de praktijk ter zake.

Laptops die ziekenhuizen beschikbaar stellen worden weinig gebruikt voor overdracht van patiëntgegevens, maar die mogelijkheid is er in principe wel. Doorgaans zijn ziekenhuis-laptops standaard voorzien van encryptie en toegangsbeveiliging, zodat bij diefstal of verlies van het apparaat geen gegevens op straat liggen.

Niet-elektronische communicatiekanalen: fax, telefoon, postverkeer en koeriersdiensten
Jarenlang was de standaard dat papieren documenten, dvd's of cd-roms aangetekend per post of soms met een (eigen) koeriersdienst werden verstuurd. De foutkans was naar huidige maatstaven groot, maar de gevolgen bij een fail waren beperkt in vergelijking met de risico's van een elektronisch datalek. Deze kanalen voor data-overdracht worden nog altijd gebruikt; een 'gouden standaard' is het niet meer, hooguit een 'best beschikbare oplossing' als er geen betere optie is.

III Personen/functies

Security Officer en Functionaris Gegevensbescherming
Elk ziekenhuis heeft een of meerdere security officers; experts op het gebied van dataveiligheid die onder meer verantwoordelijk zijn voor de beleidsontwikkeling van de instelling ter zake van gegevensuitwisseling en de facilitering daarvan door de instelling. Zij beoordelen programma's en tools, adviseren het instellingsmanagement over investeringen op dat vlak en fungeren als vraagbaak en instructeur voor de zorgprofessionals van hun instelling.

Daarnaast hebben ziekenhuizen sedert juli 2017 ook de verplichting een FG (Functionaris Gegevensbescherming) aan te stellen: een interne toezichthouder op de verwerking van persoonsgegevens. De functie van een Functionaris Gegevensbescherming is die van een onafhankelijk, intern toezichthouder, die zorgt voor naleving van de privacywetgeving. Deze persoon houdt toezicht op en adviseert over de verwerking van persoonsgegevens binnen de organisatie.
Hij of zij kan als contactpersoon door artsen, afdelingen of managers worden geraadpleegd met betrekking tot verwerking van persoonsgegevens. Ook is hij of zij intermediair richting de toezichthouder, de Autoriteit Persoonsgegevens.

ICT-afdeling
De ICT-afdeling draagt zorg voor doorontwikkeling en innovatie en implementeert de systemen voor gegevensuitwisseling. De afdeling is veelal mede-bepaler van gekozen oplossingen. De medewerkers van de ICT-afdeling zijn ook de kenners van de tools, en kunnen de security officer ondersteunen. Het is van belang dat op deze afdeling kennis bestaat van het primaire proces, en besef van de noodzaak om gegevensuitwisseling in netwerkverband te faciliteren.

Dossiervoerder
De hoofdbehandelaar is de dossiervoerder. Bij een wisselend hoofdbehandelaarschap wisselt dus ook de verantwoordelijkheid en aansprakelijkheid voor een goede dossiervoering, inclusief de overdracht van patiëntgegevens aan collega-zorgverleners.

IV Organisaties

IHE, Integrating The Healthcare Enterprise
Dit is een internationaal en wereldwijd samenwerkingsverband van gebruikers en leveranciers van ICT in de zorgsector. IHE is opgericht in 1998 in de VS. Primaire doel is de zorgprocessen, waarbij informatie-uitwisseling onontbeerlijk is, zonder problemen te laten verlopen. IHE promoot het gecoördineerd gebruik van gevestigde zorg- en ICT standaarden, om optimale patiëntenzorg ook daadwerkelijk te kunnen realiseren in de kliniek. IHE heeft dus alles te maken met (het testen van) integratie en interoperabiliteit van en tussen verschillende zorg ICT hardware en software. Systemen die zijn ontwikkeld volgens gelijke specificaties communiceren beter met elkaar, zijn eenvoudiger te implementeren en maken het zorgverleners mogelijk om informatie effectiever te gebruiken. IHE beijvert zich voor het vaststellen van op brede schaal haalbare specificaties.

IHE is een platform dat bij ziekenhuizen die (willen) samenwerken stimuleert en eventueel ook controleert of zij ICT-systemen en apparatuur (tools) hebben met gelijke ‘werkprofielen’, zodat communicatie makkelijk verloopt. Dat hoeft niet per definitie te betekenen dat de instellingen dezelfde programma’s gebruiken. Bv kunnen ziekenhuizen die verschillende EPD’s (EPIC, Chipsoft) hebben toch goed met elkaar communiceren zonder dat er met fax machines data uitgewisseld moet worden om het vervolgens weer in EPD ‘te plakken’.

2.4 Welke opdrachten liggen er om veilig(er) dataverkeer te faciliteren?

a) *Voor zorgverleners en patiënten*

Awareness: zorgverleners en patiënten(vertegenwoordigers) moeten zich bewust zijn van het belang van veilige overdracht, kennis van veilige communicatiemiddelen en inspanning doen om volgens een duidelijk protocol het optimum te kiezen tussen snel, veilig en betrouwbaar.

Beide groepen zouden hun eigen belangen actief moeten behartigen. Artsen doen dat door nadrukkelijk van hun RvB te verlangen dat ICT-beleid in regionaal verband gevoerd wordt en dat de RvB de noodzakelijke tools beschikbaar stelt in de instelling.

Patiënten kunnen hun individuele belang behartigen door een serieuze afweging te maken van hun verlangens ten aanzien van de zorg die zij ontvangen, en de keuzes die daaruit voortvloeien voor gegevensoverdracht. Patiënten in georganiseerd verband behartigen hun belangen door zich als vereniging of koepel uit te spreken over de noodzaak van betrouwbare data-uitwisseling zonder hick-ups die te wijten zijn aan incompatibiliteit van systemen. Bovenal zouden (koepels van) patiëntenorganisaties aandacht moeten opeisen voor de patiënten die vandaag in zorg zijn en die met hun zorgverleners afwegingen moeten maken tussen een soepel lopend zorgproces en optimale privacy waarborgen.

b) *Voor RvB's van zorginstellingen*

De RvB's formuleren het beleid om verwijzing van patiënten en de informatie-overdracht die daarvoor nodig is, te faciliteren. Gezien de noodzaak van dat dataverkeer is dat faciliteren geen dichotome beleidskeuze. Beleid veronderstelt in dit verband: prioritering van het beschikbaar maken van veilige communicatiekanalen (denk bijvoorbeeld aan beveiliging van mailservers), en up-to-date houden van dat aanbod. Durven investeren, bij voorkeur in netwerkverband, in technologische oplossingen die volgens het privacy-by-designprincipe zijn ontwikkeld. En haalbaar implementatiebeleid voeren.

Ziekenhuizen hebben een hoger niveau van awareness nodig ten aanzien van hun eigen beperkte expertise op ICT-gebied. Zij doen vooral waar zij goed in zijn: steeds betere behandelingen ontwikkelen en doorvoeren. Netwerkontwikkeling is een voorwaarde voor een volgende kwaliteitstap. Ziekenhuizen hebben wel de expertise om scherpe visies op zorg te ontwikkelen, maar kennis en inzicht in ICT-faciliteiten die nodig zijn voor implementatie daarvan, berust bij enkelingen in de omvangrijke ziekenhuisorganisaties. Dit zijn bovendien veelal geen zorgverleners met kennis van het zorgproces, maar staffunctionarissen.

De slagvaardigheid waarmee netwerken worden opgezet gaat voorbij aan de lacunes in de faciliterende ICT-omgeving die daarvoor nodig is. Er wordt op of over de grens gewerkt van wat verantwoord is, met betrekking tot de zorg voor privacy en betrouwbaar dataverkeer.

Tevens heeft de RvB de taak regie te voeren (of te laten voeren door ICT-professionals, security officers en FG) met de ziekenhuizen waarmee in regionaal netwerkverband wordt samengewerkt aan de behandeling van patiënten.

c) *Voor de brancheorganisaties NVZ en NFU.*
Brancheorganisaties moeten regie nemen en aangesloten instellingen adviseren, zodat de zorginstellingen kunnen werken aan een masterplan, waarbij naast privacy en informatieveiligheid ook compatibiliteit en doelmatigheid van dataverkeer leidende principes zijn. Er komen steeds meer commerciële partijen die apps aanbieden waarmee gegevens eenvoudig kunnen worden uitgewisseld. Het risico bestaat dat er een versnipperd landschap ontstaat van apps en mailprogramma's … die onderling weer niet compatibel zijn. Het kost de instellingen op termijn een fortuin om dat recht te trekken als er nú niet op gestuurd wordt.

Het verdient aanbeveling ook brancheorganisaties van eerstelijnsdisciplines bij die regievoering te betrekken. Met een toenemende zorgconcentratie in de oncologie ligt het immers voor de hand dat eerstelijnspraktijken in de woonplaats of regio waar de patiënt woont, steeds meer zullen participeren in zorgtrajecten en mogelijk op termijn ook aan samenwerkingsverbanden worden toegevoegd.

d) *Voor de landelijke overheid*
De overheid dient landelijke regie/coördinatie te voeren op dit onderwerp. Sinds het landelijk EPD in de politieke koelkast verdween, heeft de markt het richting geven aan ontwikkelingen op het gebied van veilig dataverkeer overgenomen. Hoewel het Ministerie het zelf liever anders had gezien, is deze strategie welbewust ingezet. Dat heeft een lappendeken van niet compatibele tools opgeleverd en tot aanzienlijke kosten geleid om zorgprocessen toch doorgang te kunnen doen vinden. Het is niet te laat om fouten te herstellen: te sturen op specificaties en eisen van interoperabiliteit en compatibiliteit wettelijk te verankeren.

2.5 Juridisch kader voor veiligheidszorg binnen de huidige mogelijkheden

Rond privacy van patiënten is de volgende wet- en regelgeving van toepassing:

Wet op de Geneeskundige Behandelingsovereenkomst (WGBO)
De WGBO is in werking getreden in 1995 en maakt deel uit van het Burgerlijk Wetboek (BW). De WGBO beoogt de positie van de patiënt te versterken.
De WGBO is in dit verband vooral van belang vanwege de vastgelegde geheimhoudingsplicht. Zonder toestemming (of in uitzonderlijke gevallen: veronderstelde toestemming) van de patiënt is het een hulpverlener in beginsel niet toegestaan aan anderen dan de patiënt inlichtingen over de patiënt dan wel inzage in of afschrift van het medisch dossier te geven.
Naast geheimhoudingsplicht regelt de WGBO ter zake van met medisch dossier ook onderwerpen als het recht van patiënten op toegang tot hun dossier, het recht op afschrift daarvan, het recht gegevens te laten verwijderen, een eigen verklaring toe te voegen, e.a.

Wet(svoorstel) Cliëntenrechten bij elektronische verwerking van gegevens
Het eerste deel van deze wet is op 1 juli 2017 in werking getreden. Zorgverleners die elektronische patiëntgegevens willen uitwisselen met andere behandelaars moeten daarvoor voortaan toestemming vragen aan de patiënt. Volgens planning wordt in 2020 regelgeving van kracht rond *specifieke* toestemming (ontwikkeld door VWS, Nictiz en 'het werkveld'). De cliënt moet bij het verlenen van toestemming specifiek aan kunnen geven of hij of zij voor alle of bepaalde gegevens toestemming geeft en aan welke (categorieën van) zorgaanbieders die gegevens beschikbaar mogen komen. Ook het recht op elektronische inzage in dossiers door de patiënt zelf zal nog volgen. Inzage kan altijd (krachtens WGBO), maar niet per se digitaal. Invoering van deze regel ondervond vertraging vanwege problemen met inlog/authenticatie. Er is een nieuw authenticatiesysteem in ontwikkeling (in testfase): Idensys.

Wet Bescherming Persoonsgegevens (WBP)
De Wet bescherming persoonsgegevens (WBP) is - kort samengevat - van toepassing op het verwerken van persoonsgegevens. De WBP en de WGBO vullen elkaar aan. Als deze wetten conflicteren, dan geldt als uitgangspunt dat de WBP 'voorrang heeft'.

De WBP bepaalt dat de burger weet met welk doel zijn persoonsgegevens worden verwerkt. Persoonsgegevens over iemands gezondheid mogen alleen worden verwerkt door 'hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene […] noodzakelijk is'. Daarbij geldt bovendien het medisch beroepsgeheim.

In artikel 13 WBP is bepaald dat 'de verantwoordelijke' voor het dossier ook verantwoordelijkheid draagt voor passende beveiliging tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Sinds januari 2016 zijn organisaties verplicht om datalekken te melden bij de Autoriteit Persoonsgegevens. Deze meldplicht valt onder de Wet bescherming persoonsgegevens. Het niet (tijdig) melden van een lek kan zorgen voor een flinke bestuurlijke boete (oplopend tot 820.000 euro of 10% van de jaaromzet). Voor zover bekend hebben alle ziekenhuizen hun medewerkers gewezen op de plicht en bij een vermoeden van een datalek een melding te doen bij de security officer van de instelling, zodat deze de melding kan doorzenden naar de Autoriteit Persoonsgegevens.

De werking van de WBP eindigt op 25 mei 2018.

Algemene Verordening Gegevensbescherming (AVG)
Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De Wet Bescherming Persoonsgegevens (WBP) geldt dan niet meer.

Als de Algemene Verordening Gegevensbescherming (AVG) van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er komt meer nadruk op accountability; het is aan de ziekenhuizen om hun systemen zodanig in te richten dat zij hun verantwoordingsplicht kunnen nakomen. Zorgverleners kunnen

merken dat er kleine wijzigingen in software en procedures worden doorgevoerd. Zolang zij 'binnen de lijntjes kleuren' met de overdracht van dossiergegevens aan collega's in andere instellingen blijft het daarbij. Wie buiten de aangewezen systemen om snel data doorgeeft aan collega's kan wel met de nieuwe wetgeving te maken krijgen. Zo kunnen patiënten niet alleen verzoeken om gegevens uit hun dossier te verwijderen, zij kunnen daarnaast eisen dat 'het ziekenhuis' de verwijdering doorgeeft aan alle andere instellingen die deze gegevens hebben gekregen.

Wet op de Beroepen in de Individuele Gezondheidszorg (Wet BIG)
De Wet BIG is in het kader van de vorming van regionale oncologienetwerken van belang in geval ook zelfstandige praktijkhouders zich bij het regionetwerk zouden aansluiten. Dan gaan zij immers delen in de gegevensuitwisseling en wordt afstemming noodzakelijk van de juridische kaders waarbinnen zorginstellingen en zelfstandige praktijkhouders werken.

2.6 Wat is er NIET (wettelijk) geregeld?

XDS heeft als standaard voor gegevensuitwisseling tussen ziekenhuizen geen wettelijk verplichte status. Evenmin is de NEN 7510-norm wettelijk vastgelegd.
De belangrijkste wettelijke verplichting met betrekking tot de veiligheid van gegevensuitwisseling is een inspanningsverplichting.

De Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ) geeft handvatten aan zorgaanbieders om aan die inspanningsverplichting te voldoen. De gedragscode EGiZ bevat geen nieuwe regels, maar helpt zorgaanbieders en samenwerkingsverbanden onder andere bij het geven van een goede invulling aan patiënten rechten rond informatieverstrekking en toestemming en verheldert verantwoordelijkheden. De code is inmiddels mede onderschreven door ziekenhuizen in zeven samenwerkende regio-organisaties (o.a. GERRIT, EZDA).

Bij gebrek aan centrale sturing worden op verschillende plaatsen verschillende oplossingen gegenereerd. Die voldoen weliswaar aan eisen van zorgvuldige gegevensuitwisseling, maar zijn niet per definitie compatibel met elkaar. Bezien vanuit het perspectief van de zorgaanbieder: het ziekenhuis kan in verschillende netwerken zitten. De ziekenhuisnetwerken van samenwerkende partners in de regio hoeven ook niet compatibel te zijn.

Voor wat betreft het gebruik van veilige alternatieven voor veelgebruikte applicaties moeten we vaststellen dat de stand van zaken per ziekenhuis en per regio verschilt.

2.7 Controle op naleving van regels

Hoewel zorgverleners veelal (terecht) een strikt kader percipiëren van regels en richtlijnen, wordt hun handelen nauwelijks wettelijk beperkt met het oogmerk problemen te voorkómen. Wanneer zich daadwerkelijk een probleem manifesteert is er wel een meldplicht en staan er sancties op verzaking daarvan. Ook is er waakzaamheid van overheidswege als het gaat om de veiligheid van

persoonsgegevens binnen instellingen; het toenmalige College Bescherming Persoonsgegevens (voorloper van de huidige Autoriteit Persoonsgegevens, AP) publiceerde in 2013 een kritisch onderzoeksrapport over instellings-EPD's.

Bij nalatigheid in de sfeer van slordige omgang met vertrouwelijke gegevens ('dossier mee naar huis nemen, tas in de trein laten staan…') is het de instelling die sancties oplegt en de plicht draagt de AP te verwittigen. Ook zijn er meerdere tuchtzaken geweest over onzorgvuldige omgang met medische gegevens (verzuimd data te vernietigen, te ruime inzage). Die gelden echter niet het gebruik van afdoende beveiligde infrastructuur of informatiedragers. Controle daarop is een taak van de Functionaris Gegevensbescherming (FG). De FG heeft echter geen sanctiebevoegdheid. De AP blijft eindverantwoordelijk, maar stelt zelf: […] de Autoriteit Persoonsgegevens stelt zich terughoudend op bij organisaties met een FG.
Bij overtreding van wetten treedt de AP op. De AP geeft aan alleen achteraf te toetsen, bij melding van klachten. Wanneer aan de toestemmingsvereisten is voldaan, is er nauwelijks een wettelijk vastgelegd beletsel voor data-overdracht: wanneer de best beschikbare technologie is gebruikt heeft de zorgverlener zijn verantwoordelijkheid genomen. Een concreet wettelijk toetsingskader is niet voorhanden.
Het verbaast dan ook niet dat er geen jurisprudentie ter zake bestaat: nog nooit is een arts (of andere zorgverlener) door de AP gedaagd vanwege het gebruik van te mager beveiligde manieren van dataverkeer.

Hoofdstuk 3: Samenvatting, handreikingen en aanbevelingen

3.1 Bevindingen van onze domeinverkenning: samenvatting

De domeinverkenning van het project 'Privacy van patiënten bij elektronische gegevensuitwisseling' levert in hoofdlijn de volgende bevindingen op.

- Met het niet invoeren van het (of ten minste één) landelijk EPD heeft de overheid de regie over de ontwikkeling van eenduidige infrastructuur uit handen gegeven. De markt heeft vervolgens de vraag naar platforms en tools overgenomen, wat tot versnippering en hoge kosten heeft geleid.
- Er rust geen wettelijke verplichting op het toepassen van belangrijke veiligheidsnormen (NEN 7510) of standaards (XDS).
- De relatieve onbekendheid van zorgbestuurders (RvB's) met ICT heeft ertoe geleid dat het merendeel van de instellingen standalone beleid heeft ontwikkeld, vaak ogenschijnlijk met de hand op de knip. Nu er oplossingen moeten worden geïmplementeerd voor vraagstukken ter zake van integratie en interoperabiliteit, zijn er miljoenen gemoeid met de aankoop van softwarelicenties om zorgverleners veilig en doelmatig te kunnen laten communiceren met collega's in instellingen waarmee netwerkverbanden zijn aangegaan voor behandeling van patiënten.
- Security officers van ziekenhuizen leggen de lat hoog, op het niveau van de best mogelijke beveiliging. Aangezien die niet wettelijk af te dwingen is en regionale beleidscoördinatie op RvB veelal onvolkomen is, is naleving van de gestelde normen lang niet altijd haalbaar in de werkpraktijk van zorgverleners.
  De dagelijkse praktijk rond samenwerking tussen zorgverleners in verschillende ziekenhuizen kent dan ook veel onveilig dataverkeer. Bij gebrek aan centraal beleid op gegevensuitwisseling, kiest de zorgverlener nu voor niet gevalideerde oplossingen ("je moet toch wat").
- Het ontbreken van een landelijke, maar ook regionale masterplannen voor zorgcommunicatie zet een rem op efficiëntie van gegevensoverdracht en schaadt de kwaliteit van zorg.
- Datzelfde geldt voor de focus op privacy, als er geen realistische afweging wordt gemaakt met het belang van efficiënte gegevensuitwisseling tussen zorgverleners.
  Netwerkontwikkeling is noodzakelijk om de zorg verder te kunnen verbeteren. Doordat het inzicht in geneeskunde zoveel groter is dan het inzicht in ICT, bestaat de neiging om vernieuwingen door te voeren waarvan verantwoorde governance eigenlijk nog niet gewaarborgd kan worden. Op operationeel niveau leidt dat tot hoge kosten om noodverbanden aan te leggen of tot (eigenlijk onverantwoorde) risico's ten aanzien van de betrouwbaarheid van het dataverkeer.

3.2 Handreikingen voor de praktijk van de zorgverlener

Wat is nu het consigne voor zorgverleners die vandaag een patiënt in hun spreekkamer hebben, waarmee zij samen besluiten dat die patiënt morgen gezien zou moeten worden door een collega uit een andere instelling van hun regionaal netwerk?

1) Het belang van de patiënt dient te allen tijde voorop te staan.
2) Zorgverleners zijn ertoe gehouden om de veiligst beschikbare optie te gebruiken om gegevens over te dragen met de snelheid die vereist is voor optimale medische zorg.
3) De patiënt dient betrokken te zijn bij de keuze voor de wijze van overdracht (wanneer er keuze is). Zorgverleners brengen het aspect privacy en informatieveiligheid in als gespreksonderwerp en leggen afspraken vast.

Ad 1
Elke zorgverlener is vrij om met haar of zijn patiënt een besluit te nemen over behandeling in netwerkverband. Er zijn geen wetten die de snelste of doelmatigste voortgang van het zorgproces in de weg staan.

Ad 2
Waar tools, kanalen en informatiedragers beschikbaar zijn die patiëntgegevens versleuteld overdragen, dienen zorgverleners die te gebruiken: Siilo, ZorgMail, Filesender of applicaties als Zivver versleutelen data. Wanneer deze tools niet beschikbaar zijn, kan een zorgverlener zich behelpen met de traditionele kanalen, die voor dit doel eigenlijk minder geschikt zijn. Hij/zij moet de patiënt wijzen op deze omstandigheden en het onderwerp 'beschikbaarheid van tools voor veilige gegevensoverdracht' in werkoverleg van de maatschap, vakgroep of zorgpadteam agenderen. De Functionaris Gegevensbescherming (FG) van de instelling kan zo nodig adviseren.

Ad 3
Sinds 1 juli 2017 moeten patiënten toestemming geven voor overdracht van hun gegevens. Wanneer dit onderwerp toch aan de orde is, al is het als formaliteit, is het goed om aan te geven op welke manier de patiëntgegevens worden overgedragen. Als er wat te kiezen valt, is het goed om de patiënt bij de keus te betrekken.
De Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ) geeft handvatten aan zorgaanbieders voor elektronische uitwisseling van patiëntgegevens met andere zorgaanbieders. De gedragscode EGiZ bevat geen nieuwe regels, maar helpt zorgaanbieders en samenwerkingsverbanden onder andere bij het geven van een goede invulling aan patiëntenrechten rond informatieverstrekking en toestemming en verheldert verantwoordelijkheden.

3.3 Aanbeveling aan de opdrachtgever

In paragraaf 2.4 is uiteengezet dat zorg voor privacy van patiënten bij elektronische gegevensuitwisseling in regionetwerken georganiseerd wordt in een beleidsketen. Die loopt van patiënt en zorgverlener, via instellingen, hun brancheorganisaties NFU en NVZ, naar de landelijke overheid. Er is al veel werk verzet om veilig dataverkeer te faciliteren. Echter, op dit moment wordt de snelle verwijzing van patiënten en de daarbij behorende dataoverdracht in netwerken gehinderd door slecht communicerende datasystemen. Het komt er nu op aan de barrières in dataoverdracht die optimale zorg in regionale netwerkvorming in de weg staan snel te slechten en dit probleem een prominente plaats te geven in goed geregisseerde beleidsontwikkeling. Daar profiteren vanzelfsprekend niet alleen de oncologienetwerken van, maar alle zorgnetwerken.

Het Citrienfonds is de aangewezen partij om daarin het voortouw te nemen.
Het kan invulling geven aan de regietaak van de overheid.
Aanbeveling aan de opdrachtgever is dan ook een vervolgproject in te stellen om een masterplan op te zetten van ICT beleid, investeringsbeleid en protocollering van dataverkeer in zorgnetwerken. Hierbij dienen vanzelfsprekend alle veldpartijen betrokken te worden.

Bijlage 1: Lijst van geconsulteerde personen en instellingen

Drs. Menno Mostert	Docent Gezondheidsrecht	Julius Centrum UMC Utrecht
Mr.dr. Hester de Vries	Advocaat Voorzitter Vereniging Privacy Recht	Kennedy Van der Laan Advocaten
Mr. Maarten Goudsmit	Advocaat	Kennedy Van der Laan Advocaten
Dr. Pauline Evers	Beleidsmedewerker Medicijnen	NFK
Drs. Arja Broenland	Directeur-bestuurder	NFK
Paul Schüren	Projectleider Oncologie en IHE-XDS	UMCG
Drs. Ric Exterkate	Werkgroep Digitale Gegevensuitwisseling	UMC Utrecht
Drs. Vincent van Luling	Director Digital ICT	Meander MC
Heleen Reijerse	Security Officer	Meander MC
Drs. Evert Sanders	Radioloog Bestuurder (co-chair)	Amphia Ziekenhuis Breda IHE
Tie Tjee MSc	Expert datastorage zorgmarkt Bestuurder (vendor-chair) IHE	E-Storage
Drs. Christine Bennink	Manager Projectleider XDS-uitrol	Amphia Zh Breda/Erasmus MC Citrienfonds, regio Rotterdam
Mr. Alex Commandeur	Hoofd Toezicht Publieke sector	Autoriteit Persoonsgegevens
Floor Terra	Senior inspecteur ICT	Autoriteit Persoonsgegevens
Mr. Laura Ghirlanda	Senior inspecteur jur. zaken	Autoriteit Persoonsgegevens

Bijlage 2: Brondocumenten

Cover
Regionale oncologienetwerken
https://www.oncologienetwerken.nl/

Hoofdstuk 1
Koersboek oncologische netwerkvorming
http://koersboek-oncologische-netwerkvorming.nl/

Hoofdstuk 2
Nictiz
https://www.nictiz.nl/

De norm NEN 7510
https://www.werkenmetnen7510.nl/

XDS
https://www.nictiz.nl/standaarden/xds

Artikel Zorgvisie EPD-overzicht 2016: twee spelers blijven over (9 juni 2016)
https://www.zorgvisie.nl/epd-overzicht-2016-twee-spelers-blijven-over/

IHE
https://www.ihe-nl.org/

Wet op de Geneeskundige Behandelingsovereenkomst (WGBO)
https://www.knmg.nl/advies-richtlijnen/dossiers/behandelingsovereenkomst.htm

Wet(svoorstel) Cliëntenrechten bij elektronische verwerking van gegevens
https://www.knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht/per-1-juli-2017-nieuwe-regels-uitwisseling-medische-gegevens.htm

Idensys
https://www.idensys.nl/

Wet Bescherming Persoonsgegevens
http://wetten.overheid.nl/BWBR0011468/2017-03-10

Meldplicht datalekken
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Algemene Verordening Gegevensbescherming (AVG)
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming

Wet BIG
http://wetten.overheid.nl/BWBR0006251/2016-08-01

Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGIZ)
https://www.nictiz.nl/publicaties/gedragscode-elektronische-gegevensuitwisseling-in-de-zorg-egiz

CBP-rapport 'Toegang tot digitale patiëntendossiers binnen zorginstellingen' (2013)
https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-zorginstellingen.pdf

AP-informatie 'Functionaris voor de Gegevensbescherming'
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming

Regionale Oncologienetwerken
p/a UMC Utrecht
Heidelberglaan 100
3584 CX Utrecht

088 755 5555
H.J.Bloemendal@umcutrecht.nl

'Regionale Oncologienetwerken'

Regionale
Oncologienetwerken