Veilige communicatie via het LSP

Ervaringen van een koploper

ZEGEN
ZORGINFORMATIE
NIJMEGEN

Praktijkboek van Stichting ZEGEN
1e druk november 2010; in samenwerking met NICTIZ en mede mogelijk gemaakt door VWS. Oplage 1200
2e druk oktober 2012; in samenwerking met de VZVZ en mede mogelijk gemaakt door de Landelijke Taakgroep EMD-WDH. Oplage 2500

ISBN 978-90-816318-1-5

Redactie Marion Borghuis, Herman Levelink,
Jaap Schreuder, Sabine Verheggen, Willem Regout
Projectcoördinatie en eindredactie Margriet van Aalten
Vormgeving Bureau Ketel, Nijmegen
Drukwerk Drukkerij Efficiënt, Nijmegen

November 2012

Voorwoord

Beloftes zijn er om nagekomen te worden. Dus toen wij in 2005 tijdens de kick-offbijeenkomst van het koploperschap E-communicatie beloofden te zijner tijd onze informatie en ervaringen te delen met andere zorginstellingen, was dat niet 'zomaar' een toezegging. Nu, een aantal jaren verder, zijn we zover. Het is ons gelukt om met vallen en opstaan een werkbare, veilige en betrouwbare vorm van communicatie tot stand te brengen waarvan we veel voordelen ondervinden.
We zijn er trots op dat het onderling raadplegen van medische gegevens binnen onze regio een vanzelfsprekendheid is geworden. Dit verloopt vaak nog via verschillende infrastructuren. Maar daar waar mogelijk communiceren we via het Landelijk Schakel Punt (LSP). Graag willen we met behulp van dit boek onze kennis daarvan overdragen.

Noem het onbescheiden, maar wij zijn ervan overtuigd dat de CIHN en de partners in de Stichting Zorginformatie Nijmegen (ZEGEN) 'op schaal' een standaard hebben neergezet die als voorbeeld kan dienen voor de gehele gezondheidszorg. Juist omdat het project zo 'breed' is uitgerold, terwijl de meeste ICT-projecten op een smalle basis worden uitgevoerd. Het is geen eenvoudige opgave, die aansluiting op het LSP, zeker niet. U wordt geconfronteerd met de nodige misverstanden, u zult wantrouwen weg moeten nemen en draagvlak moeten zien te creëren. Dan is er natuurlijk nog de technische rompslomp waar u zich misschien het liefst compleet afzijdig van houdt. En dan hebben we het niet eens over alles wat erbij komt kijken aan beveilingsprocedures en gedragsregels met betrekking tot privacy. Maar zeg nu zelf: het keurig opslaan van dossiers in een serversysteem dat bij wijze van spreken onder het bureaublad van de doktersassistente past, is toch gewoonweg niet meer van deze tijd? De maatschappij anno 2012 vraagt om verbetering van de informatie en communicatie in de zorg én om verbetering van de veiligheid van de patiënt.

We hebben niet de pretentie een uniform recept te leveren voor aansluiting op het LSP. Want die ís er niet. Ook zijn we de eersten om te zeggen dat dit praktijkboek niet volledig is, verre van waarschijnlijk. Maar al kunnen we maar íets overbrengen van de wijze waarop LSP communicatie in een organisatie en/of praktijk kan worden ingevoerd, dan is onze missie geslaagd. Want hoe meer zorgverleners op het systeem zijn aangesloten en hoe meer medische dossiers opvraagbaar zijn, des te beter het LSP werkt. En dat is geen kwestie van 'scoren', of techniek om de techniek; communicatie via het LSP is geen doel op zich. Uiteindelijk draait het om de kwaliteit van zorg. Dat die er wat betreft veiligheid en privacy op vooruit gaat, dáár boeken we de grootste winst.

Stichting ZEGEN november 2012

Marion Borghuis directeur Stichting ZEGEN en directeur CIHN
Jaap Schreuder huisarts, voorzitter Stichting ZEGEN en voorzitter Huisartsenkring Nijmegen (van 2003 t/m 2010)
Herman Levelink huisarts, bestuurslid Stichting ZEGEN en bestuurslid CIHN
Guido van de Logt lid raad van bestuur CWZ en bestuurslid Stichting ZEGEN
Sander Benraad apotheker, bestuurslid Stichting ZEGEN en voorzitter Stichting OZIS

Met dank aan:
Sabine Verheggen, kwaliteits- en klachtenfunctionaris CIHN
Willem Regout, programmamanager VZVZ
Angelique Schreuder, interimmanager & organisatieadviseur

Inhoud

N.B. In de tekst ziet u verwijzingen naar bijlagen. Deze bijlagen zijn te vinden op een speciaal daarvoor ingericht deel van de website van de CHN. Zie www.cihn.nl/huisartsenposten voor meer informatie.

Introduceren

Introductie

1

1.1 Wat is het doel van het praktijkboek?

We willen u in dit boek laten zien dat het de moeite waard is om met communicatie via het LSP[1] te gaan werken. Dat u net als wij gaat ervaren dat deze innovatie op het gebied van elektronische communicatie een positief en krachtig middel is om de kwaliteit van de zorg te verbeteren. We hopen dan ook een breder draagvlak voor LSP te creëren onder zorgverleners en patiënten. Want hoe groter het vertrouwen, hoe meer zorgverleners, instellingen, maar ook patiënten deelnemen. Alleen een communicatiesysteem waarbij vrijwel iedereen bereikbaar is, is uiteindelijk succesvol.

Tegelijkertijd willen we het werkveld informeren over de wijze waarop LSP communicatie in de organisatie en/of praktijk in te voeren is. Bent u eenmaal overtuigd van het waarom, dan blijft altijd nog die andere grote vraag over: hoe dan?

En *last but not least*: we willen laten zien dat aansluiting op het LSP méér inhoudt dan de implementatie van een communicatiesysteem alleen. Graag geven we inzicht in het totaalpakket aan veranderingen op het gebied van veiligheid, privacy, organisatie, cultuur en gedrag dat de technische realisatie overstijgt.

1.2 Voor wie is het praktijkboek bedoeld?

Dit handboek is bedoeld voor zorgverleners die willen starten met LSP-communicatie. En dan met name die in eerstelijns zorgorganisaties, die in groter of kleiner verband aan de slag willen gaan met het realiseren van LSP

1 *Waar we kortweg spreken over LSP-communicatie bedoelen we de aansluiting op de landelijke infrastructuur voor zorgcommunicatie van zorgverlener tot zorgverlener via het LSP.*

communicatie. Maar ook voor de tweedelijns organisaties die (beter) met eerstelijns organisaties willen communiceren is dit praktijkboek relevant. Het biedt inzichten en handvatten voor professionals, management, projectleiders, teamleiders op huisartsenposten, huisartsenpraktijken, afdelingen spoedeisende hulp van ziekenhuizen en apotheken.
Het praktijkboek kan ook behulpzaam zijn voor andere eerstelijns (paramedische) zorgverleners – zoals verloskundigen, fysiotherapeuten, diëtisten – die daadwerkelijk aan de slag willen gaan met LSP-communicatie (of onderdelen daarvan) in de eerstelijnszorg.
Juíst omdat deze innovatie zo direct het werk en het gedrag van de zorgaanbieders raakt, kan het veranderingsproces ook het beste door de professionals zelf geïnitieerd worden. Laten we in ieder geval zeggen dat ze nauw betrokken moeten zijn bij het nemen van de eerste stappen en de complete uitvoering van het proces.
Op een meer indirect niveau is dit boek te gebruiken door beroepsorganisaties, bij het adviseren van professionals.

1.3 Waar komt ZEGEN zelf vandaan?

Eigenlijk is onze wens heel simpel en helder: er moet meer communicatie mogelijk zijn tussen de verschillende zorgverleners en -instanties. En wanneer die communicatie tot stand is gebracht, dan moet die aan alle kanten beveiligd zijn. Alles om de kwaliteit van zorg te kunnen garanderen. Want daar gaat het uiteindelijk om.

We hebben ons al vroeg actief ingespannen om inzage te faciliteren in relevante medische gegevens van de patiënt tijdens de avond, nacht en weekenden op de huisartsenpost. Waarom? In de beleving van instellingen en beroepsbeoefenaars als de huisartsenpost, de apothekers, ziekenhuizen en de huisartsen – die verenigd zijn in de Huisartsenkring Nijmegen – verliep de uitwisseling van patiëntengegevens tussen zorgverleners (huisartsen, huisartsenpost, apothekers en specialist/ziekenhuis) niet optimaal in de regio Nijmegen. Vooral bij een instelling als de huisartsenpost was zo'n 'gebrekkige' communicatie goed merkbaar. Doordat er geen inzage mogelijk was in de medische gegevens van patiënten bij de eigen huisarts, was het voor professionals soms lastig de juiste zorg aan patiënten te verlenen.

“De belangrijkste reden voor Stichting OZIS om zich aan te sluiten bij Stichting ZEGEN was om een betere samenwerking binnen de gehele lijn te realiseren. Het kunnen beschikken over de juiste medische informatie van de patiënt maakt dat wij, als gehele eerste lijn, in staat zijn ons vak beter uit te oefenen.”

Sander Benraad, apotheker en voorzitter Stichting OZIS

“Je kunt ideeën hebben, plannen en business cases maken en eindeloos discussiëren over de beste aanpak. Uiteindelijk komt het erop neer dat mensen uit de praktijk laten zien hoe het moet. Stichting ZEGEN is op het gebied van elektronische communicatie een voorbeeld voor iedereen die twijfelt aan nut en noodzaak, of niet weet hoe het moet.”

Gert-Jan van Boven, voormalig directeur Nictiz (2002-2012), arts

“In het begin was er weerstand bij de huisartsen. Vanwege het ‘moeten’ veranderen van gewoontes; ook de angst voor het ‘onbekende’ speelde mee. Bovendien kregen ze met die typische kinderziektes te maken, als een systeem dat er vaak uit lag, of traag werkte. Ik vergelijk het wel eens met de weerstand die ik had bij de opkomst van internetbankieren. Ik dacht toen ook: waarom helemaal inloggen op een site als een girobetaalkaart ook werkt? Inmiddels weet ik niet beter.”

Marion Borghuis, directeur CIHN en ZEGEN

“Het systeem wérkt; een heleboel huisartsen zijn gestart om aan te sluiten.
Nu komt het erop aan meer volume krijgen. Hoe meer patiënten aangemeld zijn, hoe meer gegevens er te vinden zijn.”

Jaap Schreuder, huisarts en voorzitter van de Huisartsenkring Nijmegen e.o. (van 2003 t/m 2010)

“Waarschijnlijk was de sleutel tot succes de sterke samenhang tussen de HAP en de huisartsen. Die heeft uiteindelijk geresulteerd in de oprichting van Stichting ZEGEN.”
…“Dat de regio zich zo goed heeft ontwikkeld is voor een groot deel te danken aan de gedrevenheid, passie, maar ook de positief-kritische houding van zowel de HAP als de directie en de betrokken huisartsen.”

Ellen Maat, voormalig programmadirecteur Innovatie & ICT ministerie van VWS

“Toch zijn we er nog lang niet. Zo is er bijvoorbeeld behoefte aan meer tweerichtingsverkeer tussen huisartsen, ziekenhuizen en laboratoria, zodat ook apothekers in staat zijn hun vak (nog) beter uit te oefenen. En de toekomstige ontwikkeling van verder geïntegreerde behandelingen en het ontwikkelen van zorggroepen vergen steeds meer samenwerking.”

Sander Benraad, apotheker en voorzitter Stichting OZIS

Voor een optimale medicatiebewaking bleek het essentieel om inzage te hebben in het volledige medicatiedossier van de patiënt via betere communicatie met de apothekerssystemen. Bovendien was er verbetering mogelijk op het vlak van informatie-uitwisseling tussen SEH en de CHN enerzijds en de CHN en ambulancedienst anderzijds.

Proefballonnetjes

Feitelijk zijn er – vanuit de huisartsenkring en apothekers – vanaf de jaren negentig al wat proefballonnetjes opgelaten om te komen tot elektronische uitwisseling van medische informatie en medicatiegegevens. Maar het daadwerkelijke startsein voor het project ZEGEN (**Z**orginformatie Nijm**egen**) wordt in 2004 gegeven. ZEGEN is een samenwerkingsverband tussen vier verschillende partijen: CHN, Huisartsenkring Nijmegen e.o., Nijmeegse apothekers (verenigd in de Stichting OZIS) en het Canisius Wilhelmina Ziekenhuis (CWZ). Doel van het project is de uitwisseling van gegevens sterk te verbeteren en versnellen door *state of the art* internettechnologie. Na een oriënterende fase – wat bestaat er eigenlijk al op dit gebied? – wordt gekozen voor een oplossing die feitelijk alleen nog op papier bestaat: de standaarden zoals die door het Nationaal ICT Instituut in de Zorg (Nictiz) zijn vastgelegd.

Projectgroepen

ZEGEN brengt haar opdracht onder in vier projectgroepen die zich richten op elk van de volgende onderwerpen:

- toegang tot medische dossiers van patiënten van alle huisartsen die bij de huisartsenpost zijn aangesloten;
- gegevensuitwisseling tussen de huisartsenpost en de spoedeisende hulp van het CWZ;
- raadpleging van het informatiesysteem met medicatiedossiers van de apothekers;
- verbetering van het berichtenverkeer tussen CWZ, huisartsen en apothekers.

Koplopertraject

ZEGEN wordt in 2005 uitgekozen deel te nemen aan het koplopertraject voor het landelijk EPD. Als koploperproject wordt ZEGEN door het ministerie van VWS en Nictiz gefaciliteerd. (N.B. Die ondersteunende rol van Nictiz en VWS is anno 2012 overgenomen door SCZ).

Binnen het koplopertraject ligt door de aanvankelijk gekozen uitgangspunten en de financiering het accent op communicatie via het LSP. Maar al snel is er het besef dat eigenlijk de hele regionale ICT op een hoger plan getild moet worden. Want met die landelijke aansluiting zijn we er nog niet. Daarom wordt parallel aan landelijke communicatie gewerkt aan communicatievormen op regionaal niveau.

Co-existente oplossing

Huisartsen worden massaal aangesloten op het Edifact-netwerk. Voorts worden de elektronische verwijzingen van huisarts naar ziekenhuis gerealiseerd via het programma Zorgdomein. En om in kortere tijd meer huisartsen te laten communiceren met de huisartsenpost (en zo dus meer dossiers beschikbaar te krijgen) realiseert ZEGEN met steun van de zorgverzekeraars CZ en UVIT communicatie via een eerstelijnsserver die voldoet aan de OZIS-voorwaarden. Op deze manier kan de CHN communiceren met zorgaanbieders die op het LSP zijn aangesloten én met zorgaanbieders die alleen nog met een regionale communicatieserver (kunnen) werken. Deze parallelle ontwikkeling van een eerstelijnsserver die bestaat naast het LSP wordt ook wel aangeduid met de term ‘co-existente oplossing’. Uiteindelijk is de eerstelijnsserver verder ontwikkeld en ingezet voor communicatie in de chronische zorg. Hiermee is mogelijk ook de basis gelegd voor verdere regionale experimenten op het gebied van communicatie in de zorg. De doelstelling is wel om de communicatie die gebaseerd is op OZIS-standaarden geheel te vervangen door communicatie via het LSP. Door de politieke besluitvorming rond het EPD is dit proces gedurende 2011 en 2012 gestagneerd.

Succesvol

Kenmerkend voor de werkwijze van ZEGEN is de pragmatische, resultaatgerichte aanpak; gaandeweg worden oplossingen gevonden, doet men leerervaring op, worden belangrijke keuzes gemaakt en wordt gewerkt aan organisatorische maatregelen en gedragsveranderingen. Met het doel helder voor ogen en met grote betrokkenheid van de beroepsgroep en de overige belanghebbenden is het project geslaagd. Voor een groot deel is dat ook te danken aan een transparante werkwijze en een zekere vasthoudendheid, gecombineerd met een flinke portie geduld en een aardig incasseringsvermogen. Er is veel aandacht besteed aan de wettelijke

“Ik vind dat je verplicht bent zorg te leveren aan je patiënten, ook op de momenten dat je geen dienst hebt. Door je dossiers op orde te hebben en via het LSP beschikbaar te stellen kan er een goede overdracht plaatsvinden.” … “De kennis van chronische aandoeningen of medicatie geeft een veel beter beeld van je patiënt. Dat overzicht heb je nodig om als waarnemer de patiënt goed te kunnen behandelen. Ik denk dat daar de grote winst in zit.”

Han Beekwilder, huisarts te Oosterhout

“Dankzij digitale communicatie weten wij op de post nu eerder wat de patiënt mankeert.”… “In de spanning vergeten mensen wel eens dat ze een chronische aandoening hebben. Iemand die belt en zegt nooit ziek te zijn, blijkt dan bijvoorbeeld toch diabetes te hebben en insuline te spuiten. Het is zó’n onderdeel van zijn of haar leven dat het niet meer gezien wordt als een ziekte, terwijl die kennis voor ons wél van belang is.”

Annette Veenhof, coördinerend doktersassistente

“Je moet je hersens blijven gebruiken. Je kunt niet blind varen op het dossier, maar zult triage moeten blijven doen zoals je dat altijd al deed. Het dossier is niets meer of minder dan een prettig hulpmiddel dat duidelijkheid schept.”

Wendy Breuker, doktersassistente HAP Nijmegen en applicatiebeheerder

“Een grote fout die een arts kan maken is dat hij de hypothesen van zijn voorganger niet toetst, maar klakkeloos overneemt en daardoor relevante informatie over het hoofd ziet. Als arts moet je vooral naar de patiënt blijven luisteren en kijken. Je moet telkens even bij ‘af’ beginnen, zelfs als je zélf de vorige arts was. Met andere woorden: de informatie die je als arts uit E-communicatie haalt, moet kritisch worden beschouwd en niet zonder meer voor waarheid worden aangenomen. Bovendien kun je je afvragen of een EPD überhaupt ooit compleet kan zijn.”

Jaap Schreuder, huisarts en voorzitter van de Huisartsenkring Nijmegen e.o. (van 2003 t/m 2010)

regels en voorschriften en de kwaliteitseisen en criteria die aan de veiligheid en betrouwbaarheid van LSP-communicatie worden gesteld. Het project heeft ruim vijf jaar geduurd en is begin 2010 succesvol afgerond. De elektronische communicatie via het LSP is sindsdien operationeel en verloopt tot volle tevredenheid van de gebruikers en met vertrouwen van patiënten. Nu komt het erop aan de resultaten te monitoren, de kwaliteit en controle te handhaven en zo nodig verbeterplannen uit te voeren.

1.4 LSP, waarom eigenlijk?

De maatschappij vraagt in toenemende mate om verbetering van de informatie en communicatie in de zorg en om verbetering van de veiligheid van de patiënt in de zorg. Dat blijkt uit de wensen van patiëntenorganisaties en politiek, uit het overheidsbeleid en uit de ontwikkelingen in het buitenland. Goede informatie in de zorg is voor alle burgers van wezenlijk belang en wordt ook steeds meer als vanzelfsprekend gezien. Maar nu is de vraag, waarom het LSP? Het antwoord laat zich zorgvuldig, maar toch ook vrij eenduidig formuleren: wanneer een bevoegde zorgverlener in een goed beveiligde ICT-omgeving een beperkte set kan opvragen van betrouwbare medische gegevens en medicatiegegevens over de patiënt met wie hij op dat moment een zorgrelatie onderhoudt, dan verhoogt dat de kwaliteit en veiligheid van de zorg.
LSP (maar ook de eerstelijnsserver) maakt het mogelijk dat zorgverleners onder strikte voorwaarden snel, *realtime* en 24/7 actuele en relevante patiënteninformatie kunnen inzien. Een arts die de actuele probleemlijst en de meest recente medicatielijst tot zijn beschikking heeft, is een arts die snel en doeltreffend kan optreden in de zorg en/of behandeling van de patiënt. Het belang voor de patiëntenzorg is evident. De patiënt is immers afhankelijk van de juiste en actuele informatie over zijn gezondheidstoestand en behandeling. Wanneer er meerdere zorgverleners bij een patiënt betrokken zijn, kan dit soms cruciaal zijn voor de kwaliteit en de veiligheid van de zorg.

Zorgvuldig, eenduidig, betrouwbaar

Communicatie via het LSP of de eerstelijnsserver zorgt voor een verbetering van de continuïteit van zorg; de aansluiting van de dagzorg op de ANW-zorg verloopt zorgvuldiger, eenduidiger en betrouwbaarder. Goede communicatie

kan bijdragen aan de kwaliteit van zorg. Specifiek aan communicatie via het LSP is dat de privacy van de patiënt optimaal wordt veiliggesteld. Het werken met een geverifieerd BSN zorgt ervoor dat de medische gegevens van de juiste persoon opgevraagd worden. Met de UZI-pas is er de garantie dat alleen geautoriseerde zorgverleners toegang hebben tot precies dát deel van medische gegevens van een patiënt waartoe ze bevoegd zijn. Het blijft overigens onverminderd noodzakelijk dat zorgverleners zich kritisch opstellen ten opzichte van informatie van andere zorgverleners. Het is immers nog altijd mogelijk dat die informatie onvolledig is.

Landelijk versus regionaal

Nu is het natuurlijk zo dat verreweg de meeste huisartsen in hun praktijk al langer werken met elektronische communicatie. Het gebruik van ICT in de zorg heeft de afgelopen jaren een hoge vlucht genomen. De diverse zorginstellingen maken daarbij gebruik van een groot aantal oplossingen. Denk daarbij aan landelijk werkende technieken zoals Edifact en Zorgdomein, of lokale en regionale uitwisseling van informatie zoals via de eerder genoemde eerstelijnsserver. Nadeel van deze wijze van communiceren is dat deze veelal beperkt voldoet aan standaarden die vandaag de dag aan veiligheid en privacybescherming van de patiënt worden gesteld. Ook is er niet altijd sprake van communicatie tussen de verschillende ICT-systemen, of verloopt deze communicatie niet soepel. Dat staat het verkrijgen van essentiële informatie over de patiënt in veel gevallen in de weg. Denk daarbij aan die gevallen waarin een patiënt een apotheek, ziekenhuis, of huisarts buiten de regio bezoekt. Waarom dan energie en geld steken in een regionaal systeem, als er ook een landelijke techniek beschikbaar is en de infrastructuur helemaal voor u ligt uitgerold? Vooral als het u ‘slechts’ gaat om toegang tot waarneem- en medicatiegegevens, kunt u besparen op de startinvesteringen, de onderhoudskosten en de organisatorische inspanningen die bij het inrichten van een regionale server komen kijken. Daarmee is overigens niet gezegd dat aansluiting op het LSP het regionale systeem overbodig maakt. Feitelijk kunnen de systemen naast elkaar bestaan. Bovendien is het zo – een bijkomend voordeel van het LSP – dat de regels en procedures die ten grondslag liggen aan de landelijke communicatie ook te integreren zijn in de regionale communicatie (al is dat wel afhankelijk van de technische oplossingen die in een bepaalde

“Het gros van onze achterban is vóór gegevensuitwisseling, vooral wanneer het gaat om de zorg voor chronisch zieken. Diabetespatiënten snappen heel goed dat er één dossier nodig is om gegevens op elkaar te laten aansluiten.
Een ander deel van de achterban is huiverig, omdat zorgverleners óók te maken hebben met GGZ-patiënten die veel vragen stellen over de bescherming en privacy van hun gegevens.”

Eric Verkaar, directeur Zorgbelang Gelderland

“Het gekke is dat je door zo’n groot traject als aansluiting op het LSP veel meer spin-off krijgt. Vijf jaar geleden had je bij een specialist niet moeten aankomen over standaardisatie van een specialistenbrief. Ze gaven uitgebreide beschrijvingen, begonnen pas aan het einde met hun conclusie en noteerden hun overwegingen. Zaken waar een huisarts niet altijd boodschap aan had. We hebben nu voor elkaar kunnen krijgen dat er voor de specialistenbrief net zo’n standaard is als voor de verwijsbrief. Dit leidt tot meer samenwerking.”

Dick Munsterman, voormalig coördinator huisartsenzaken CWZ

regio voor handen zijn). Op die manier is het mogelijk om regionale communicatie te beveiligen met UZI-pastechnologie, zodat men op alle niveaus veilig en betrouwbaar om kan gaan met patiënteninformatie.

1.5 Wat moet er globaal gebeuren?

Het is een hele onderneming om vanuit de uiteenlopende ICT-systemen in de huidige dagelijkse praktijk over te stappen naar een landelijke communicatiestructuur. Analyseer eerst eens de bestaande technische oplossingen en bepaal of u de mogelijkheden en/of beperkingen accepteert of voor een nieuwe oplossing kiest met bijkomende extra veranderingen. Bedenk verder dat aansluiting op het LSP organisatorische maatregelen vereist en tegelijkertijd veranderingen in gedrag en cultuur. 'Overstappers' krijgen te maken met een complexe en omvangrijke omslag waar veel partijen bij betrokken zijn. Elke regio heeft de eigen belanghebbenden, weerstanden tegen verandering en krachtenvelden die communicatie bevorderen of belemmeren. Samenwerken is hier eigenlijk het toverwoord. Een draagvlak creëren, daar draait het om. In de praktijk zal namelijk blijken dat alles met elkaar samenhangt, iedereen – van de huisarts, via de apotheker tot de huisartsenpost en de eerste hulp – is van elkaar afhankelijk. Aansluiting op het LSP houdt in dat alle partijen zich moeten verenigen. En dat betekent: alle neuzen dezelfde kant op, gezamenlijk prioriteiten formuleren, voor ogen houden wat het gemeenschappelijke doel is van communicatie via het LSP, zich verbinden aan de afspraken die het LSP met zich meebrengt en een routine ontwikkelen in de werkzaamheden ('brengen' en 'halen' van informatie). Probeer niet te verzanden in eindeloze discussies hierover, maar stel vooraf heel concreet vast wat je precies met elkaar wilt communiceren en zorg dat gegevens daadwerkelijk beschikbaar zijn (of worden gesteld). Benoem opgesomde bezwaren en problemen en zie ze als aandachts- of verbeterpunten en niet als 'beren op de weg'. Een project als dit komt pas van de grond als alle partijen ook echt zíen dat het werkt, dat het commitment ook echt tastbaar is. Van daaruit kun je er verder aan 'schaven en doen'.

Veranderen

En verder: de werkprocessen in de organisatie moeten veranderen, u moet ICT-investeringen doen en de infrastructuur geschikt maken om via het LSP te kunnen communiceren. Wil de E-communicatie aan alle eisen voldoen om als veilig, integer en betrouwbaar gekwalificeerd te worden, dan is het zaak op de hoogte te zijn van alle voorwaarden en standaarden die zijn ontwikkeld op het gebied van ICT-voorzieningen in de zorg. Maar het betekent ook dat de werkprocessen in de organisatie moeten veranderen om de kwaliteit van zorg en de privacy van de patiënt te kunnen waarborgen. Verantwoordelijkheden, werkprocessen en verantwoording dienen optimaal geregeld te zijn; dat is van invloed op alle niveaus in de organisatie. Ook is het nodig veranderingen in gedrag en cultuur te bewerkstelligen. Kort gezegd: het zal noodzakelijk zijn bij de overstap bestuurlijke en beleidsmatige keuzes te maken en de juiste organisatorische en financiële condities te creëren.

Informeren

Het hoe en wat van het LSP

2.1 Wat is het LSP?

De infrastructuur voor de communicatie in de zorg bestaat uit een groot aantal elementen die samen een veilige communicatie mogelijk maken. Het schakelpunt daarin is het LSP (Landelijk Schakel Punt). Het begrip LSP wordt als aanduiding gebruikt van de gehele zorginfrastructuur. In het schakelpunt is de verwijsindex opgenomen waarmee de juiste zorgverlener van de patiënt snel kan worden gevonden. Het LSP verbindt alleen; er is geen sprake van het uitwisselen en/of opslaan van de gegevens die kunnen worden ingezien. Het LSP maakt als het ware 'zichtbaar' welke zorgaanbieder in zijn eigen zorginformatiesysteem gegevens heeft vastgelegd over een patiënt. En dat 'zichtbaar' zijn is niet meer dan een vermelding, de gegevens zelf blijven bij de zorgaanbieder. Daarmee is het LSP is nadrukkelijk géén landelijk EPD. Het moet juist gezien worden als een communicatiemiddel. Een extra informatievoorziening met een landelijk bereik die naast de regionale en lokale informatieuitwisseling kan bestaan. Via het LSP heeft een zorgaanbieder volgens wettelijke regels ten aanzien van betrouwbaarheid en veiligheid en onder specifieke voorwaarden toegang tot gegevens die van belang zijn voor de behandeling van zijn patiënt.

2.2 Wie zit er achter het LSP?

De overheid heeft vanuit de wens om meer transparantie en veiligheid in de zorg te bewerkstelligen geïnvesteerd in de hiervoor noodzakelijke infrastructuur voor digitale communicatie. Voorheen lag de uitvoering in handen van het Nationaal ICT Instituut in de Zorg (Nictiz). Per 1 januari 2012 is de verantwoordelijkheid voor de gegevensverwerking door

de overheid overgedragen aan VZVZ (Vereniging van Zorgaanbieders voor Zorgcommunicatie). Deze organisatie is opgericht op initiatief van de koepels van huisartsen (LHV), huisartsenposten (VHN), apotheken (KNMP) en ziekenhuizen (NVZ) in samenwerking met Nictiz en met steun van de Nederlandse Patiënten en Consumenten Federatie (NPCF). VZVZ is opdrachtgever van het Servicecentrum Zorgcommunicatie (SCZ), verantwoordelijk voor het beheer van de infrastructuur. Daarnaast ziet VZVZ toe op een goede werking van het LSP.

2.3 Wat wordt gecommuniceerd via het LSP?

Het beeld is ontstaan dat zorgverleners via het LSP als het ware het EPD konden 'downloaden'. Dit is een misvatting. Doktersassistenten, huisartsen, verpleegkundigen, apothekers en andere zorgverleners nemen niet meer dan een 'kijkje' in een beperkte set medische en/of medicatiegegevens van de patiënt. En dat alléén wanneer zij op dat moment een zorgrelatie onderhouden met de patiënt. Die beperkte set gegevens, bestemd voor de zorgverleners, wordt een professionele samenvatting genoemd. Bij de start van het LSP zijn er twee sets: de huisartsenwaarneemgegevens (HWG) en de medicatiegegevens (MG).
De HWG bevatten een beperkte set van medische gegevens en medicatie uit het dossier van de huisarts en zijn alleen beschikbaar op de huisartsenpost en voor waarnemende huisartsen. De MG bevatten informatie over de door apotheken verstrekte medicatie aan de patiënt en zijn toegankelijk voor iedere zorgverlener die het recht heeft de gegevens in te zien en die deze informatie nodig heeft voor de behandeling van de patiënt.
De medische informatie wordt niet automatisch opgeslagen tijdens of na de LSP-communicatie. Er is dus geen sprake van het verspreiden en/of achterlaten van informatie bij andere zorgverleners. Zorgverleners kunnen er zelf voor kiezen om – indien nodig – delen van de geraadpleegde informatie over te nemen in hun eigen dossier. Door het beveiligingssysteem is altijd te traceren wie inzage heeft gevraagd in de professionele samenvatting.

“Dat er zoveel politieke en maatschappelijke discussies over het LSP zijn gevoerd, begrijp ik best. Het is ook goed. De veiligheid van zo’n omvangrijk ICT-systeem met betrekking tot gevoelige informatie is al even belangrijk als hygiëne bij een operatie. Datahygiëne noemde iemand het pas...” Marion Borghuis, directeur CIHN en ZEGEN

“Wie heeft bedacht om het EPD te noemen weet ik niet. Daarmee is een beeld ontstaan waar iedereen tegenaan loopt. Big Brother is watching you, dat idee... Mensen denken ten onrechte dat heel hun dossier ergens wordt opgeslagen en iedereen met een pasje overal bij kan.” Herman Levelink, huisarts en bestuurslid ZEGEN

“Ik vind het sterk dat ervoor is gekozen het waarnemingsdossier huisartsen (WDH) niet één op één beschikbaar te stellen. De professionele samenvatting is op een dusdanige manier ingericht dat de volgende die ermee verder moet er ook daadwerkelijk wat aan heeft. Dat is niet zo maar data overbrengen, maar informátie overbrengen: ‘Wat is relevant voor een waarnemer om te weten over deze patiënt?’.”

Jan Vesseur, hoofdinspecteur Inspectie voor de gezondheidszorg

“Nu zien wij de kern van het dossier, die gegevens verifiëren we altijd met de patiënt. Patiënten zijn vaak teleurgesteld als ze merken dat wij niet alles kunnen inzien. De discussie over wat je wel of niet mag zien, is vooral een politieke. Mijn ervaring met apothekers: er is meer ‘herrie’ over zaken die niet over de lijn zijn gekomen dan dat er ‘te veel’ over en weer gaat. De dagelijkse realiteit is dat iemand die zorg nodig heeft, wil dat die informatie beschikbaar is.”

Herman Levelink, huisarts en bestuurslid ZEGEN

Verantwoordelijkheid voor een EPD

De huisarts is en blijft de verantwoordelijk beheerder van 'zijn' eigen deel van het EPD van de patiënt, dus de volledige huisartsenwaarneemgegevens (HWG). Zolang de patiënt tot zijn praktijk behoort, draagt hij te allen tijde zorg voor het dossier en is hij verantwoordelijk voor het registreren van medische gegevens (de zogeheten 'dossierplicht' van iedere zorgverlener). Dat wil echter niet zeggen dat andere zorgverleners niets bijdragen aan het EPD. Elke zorgverlener houdt in zijn éigen praktijk medische gegevens bij van zijn patiënten in zijn EPD en zorgt ervoor dat de informatie zo actueel mogelijk is. Een goed voorbeeld hiervan zijn met name de medicatie-gegevens (MG): diverse apothekers hebben een medicatiedossier van een patiënt. Zij dragen allen hun steentje bij aan de volledige inhoud van de MG die opgevraagd worden via het LSP. Om hun 'eigen deel' van het EPD bij te houden, gebruiken zorgverleners hun eigen informatiesystemen, zoals de verschillende HIS-sen (Huisarts Informatie Systeem). Voor LSP-communicatie is vereist dat iedereen die is aangesloten werkt met eenduidige standaarden en geschikte applicaties.

2.4 Wat houdt de professionele samenvatting in?

De professionele samenvatting bevat zogezegd onder meer informatie over de belangrijkste gezondheidsproblemen (HWG: huisartsenwaarneemgegevens, in te zien door huisartsen) én informatie over de medicatie (MG: medicatiegegevens, in te zien door huisartsen, apothekers en medisch specialisten). De belangrijkste onderdelen zijn:

- de volledige episodelijst;
- de journaallijst van de laatste vijf consulten. Zijn er in de afgelopen vier maanden meer consulten geweest, dan worden alle journaalregels uit deze periode meegestuurd;
- het medicijngebruik: de actuele medicatie en de historische medicatie van de laatste vier maanden tot acht maanden (de periode waarover het LSP wordt bevraagd, is in veel informatiesystemen zelf in te stellen);

- alle geneesmiddelenintoleranties/-allergieën en contra-indicaties; actuele overdrachtsgegevens.
- de meetwaarden van de laatste vier maanden en memo's uit het HIS (vanaf 2012/2013).

In de toekomst zal het gebruik van LSP-communicatie onder strikte voorwaarden worden uitgebreid met nieuwe onderdelen of meer functionaliteiten.

2.5 Wie heeft toegang tot het LSP?

Niet elke zorgverlener kan 'zomaar' de professionele samenvatting van een elektronisch patiëntendossier raadplegen. Er zijn strikte voorwaarden aan verbonden. LSP-communicatie is alleen toegankelijk voor beroepsbeoefenaars die vallen onder de Wet BIG en die in de curatieve zorg werken als zorgaanbieder of bij een zorgaanbieder in dienst zijn. Welke gegevens een zorgaanbieder kan inzien is afhankelijk van welke functie hij/zij vervult. Alleen huisartsen kunnen de HWG opvragen. En alleen apothekers, specialisten en huisartsen kunnen de MG opvragen. Om dit te regelen moeten zorgverleners beschikken over een UZI-pas (UZI staat voor Unieke Zorgverlener Identificatie). Maar zelfs dat is niet voldoende. Wil een zorgverlener via het LSP communiceren, dan zal hij op het moment van inzage een behandelrelatie met de patiënt moeten hebben. Ook is toestemming vooraf nodig van de patiënt aan de houder van het brondossier om de gegevens op te kunnen vragen. Een zorgverlener of medewerker die onbevoegd patiëntengegevens inkijkt, schendt de privacyregels en is in overtreding (er vindt actief controle hierop plaats aan de hand van logging van alle bevragingen op het LSP, zie hoofdstuk 4). Door de wijze waarop het LSP is ingericht kunnen bedrijfsartsen, verzekeringsartsen, verzekeraars en administratieve organen sowieso niet aansluiten op het LSP.

2.6 Hoe is de toegang beveiligd?

Gebruik van de UZI-pas

Patiënten moeten erop kunnen vertrouwen dat niet zomaar in hun gegevens wordt 'gerommeld'. Alleen bevoegde zorgverleners hebben inzage in hun dossier (zie hierboven). Om deze privacy te garanderen, heeft de overheid de Unieke Zorgverlener Identificatie (UZI)-pas ontwikkeld. Met deze pas kan een zorgverlener zijn identiteit en rol (bijvoorbeeld huisarts of apotheker) in het elektronisch verkeer aantonen en bewijzen. Alleen dan is met zekerheid te stellen dat een zorgverlener is wie hij zegt dat hij is. De pas zorgt ook voor het versleutelen van de informatie die wordt uitgewisseld (tussen zender en ontvanger). Op die manier is op een veilige en betrouwbare wijze via het LSP informatie op te vragen bij andere zorgverleners. Ook wordt zo inzichtelijk gemaakt wie wat op welk moment gedaan heeft.

Gebruik van het BSN

Daarnaast is het gebruik van het burgerservicenummer (BSN) van de patiënt in combinatie met een geldig identiteitsdocument van groot belang. Want óók van de patiënt moet met zekerheid worden vastgesteld of hij is wie hij is; de professionele samenvatting van de patiënt moet matchen met de persoon die een zorgverlener tegenover zich ziet. Via het BSN zijn patiënten te identificeren in het elektronische verkeer. Alleen met dit unieke nummer kan worden vastgesteld van welke patiënt de zorgverlener de professionele samenvatting oproept en de informatie kan inzien. Zorgaanbieders kunnen op eenvoudige wijze via de Sectorale Berichten Voorziening in de Zorg (SBV-Z) het BSN opvragen en controleren.

2.7 Wat is de rol van de patiënt?

De patiënt geeft vooraf toestemming aan elke afzonderlijke zorgaanbieder voor het beschikbaar stellen van zijn gegevens via het LSP. De huisarts registreert die toestemming (ook wel opt-in genoemd) in zijn systeem. Daarna wordt de patiënt aangemeld bij de verwijsindex van het LSP. Indien de patiënt zich later bedenkt, kan hij op elk moment bij de huisarts of apotheek die verleende toestemming weer intrekken.

De patiënt zelf heeft geen directe toegang tot het dossier, maar kan wel op verzoek bij zijn behandelaar het dossier inzien. Bij de VZVZ kan de patiënt opvragen welke zorgaanbieders zijn gegevens hebben aangemeld bij het LSP of hebben ingezien via het LSP. Ook kan de patiënt bij de SBV-Z controleren welke zorgaanbieder of welk indicatieorgaan zijn BSN heeft opgevraagd en/of geverifieerd, wie er zijn persoonsgegevens heeft geraadpleegd en wie het identiteitsdocument heeft gecontroleerd op geldigheid.

Realiseren

Het aansluitproces

Het waarom en wat van het LSP mag nu duidelijk zijn, nu is de grote vraag hoe organiseert u het? Waar te beginnen, wie begint er eigenlijk en met wat, hoe plant u het goed en wat komt er verder bij kijken? In dit hoofdstuk staat een aantal handreikingen die helpen de daadwerkelijke aansluiting op het LSP te realiseren.

3.1 Organisatie

Voor de individuele huisarts, apotheker of huisartsenpost kan het een individuele beslissing zijn om de aansluiting op het LSP te regelen. Doorgaans zal dat niet veel meerwaarde hebben. Die is er pas als meer partijen en dan nog een hoog percentage van de zorgverleners in een regio meedoen. Communiceren doe je met elkaar en overwegend in de eigen regio.

De ervaring heeft geleerd dat bij een dergelijke `innovatieopdracht' in de zorg een *bottom-up* benadering het meeste kans van slagen heeft. Wil zo'n traject slagen, dan is absoluut commitment van zorgverleners in een logisch geclusterde regio noodzakelijk. Het beste is een praktijkgerichte benadering die gebaseerd is op samenwerking en co-creatie van de professionals. Zij zullen het leer- en ontwikkelproces moeten starten, want zij zijn uiteindelijk de eigenaars en regisseurs van het instrument. Verwacht hierbij vooral niet dat het in één keer goed zal (moeten) gaan. Het is vooral een kwestie van beginnen en daarbij een fikse dosis durf aan de dag leggen. Bij deze materie werkt een pragmatische, resultaatgerichte aanpak het beste. Wees gesterkt door de gedachte dat door *trial and error* een organisatie er eigenlijk alleen maar wijzer op wordt.

De rol van het bestuur

Gaan we ervoor, ja of nee? Het is aan de bestuurders in de regio om een missie op te stellen, die goed uit te dragen en het startsein te geven.
De missie kan luiden: met een betere en snellere uitwisseling van gegevens de kwaliteit van de zorg aan patiënten verbeteren.
Concrete doelstellingen: een verhoging van kwaliteit en toegankelijkheid van de zorg; verkorting van de doorlooptijd van zorgprocessen; verbeteren van de patiëntveiligheid en -vriendelijkheid en het realiseren van besparingen door het terugdringen van papierstromen en administratieve lasten. De bestuurders doen er goed aan een analyse te maken van de communicatievormen die reeds bestaan in de regio en de communicatie-vormen die gerealiseerd moeten worden.

Enkele voorbeelden van bestaande of te realiseren communicatie zijn:

- medicatiegegevens apotheek ➔ huisarts en zorginstellingen;
- receptberichten van voorschrijvers ➔ apotheek;
- waarneemgegevens huisartsen ➔ huisartsenpost;
- laboratoriumgegevens en radiologieberichten ➔ huisarts;
- verwijsbrieven en diagnostiekaanvragen ➔ ziekenhuis;
- specialistenbrieven/behandelverslagen ➔ huisarts.

Een project rond gegevensuitwisseling via het LSP raakt maar een deel van de regionale zorginstellingen en een deel van de communicatie die er plaatsvindt. Een keuze voor een project rond LSP-communicatie moet helder gepositioneerd zijn naast andere vormen van gegevensuitwisseling. Bovendien moet het project heldere grenzen kennen. In de startperiode zullen niet alle zorgverleners en patiënten bereikbaar zijn via het LSP en de functionaliteit zal beperkt zijn. Het is een belangrijke taak van het bestuur om het nut van zo'n project met alle voordelen en beperkingen naar alle betrokkenen uit te dragen. Alle betrokken zorgverleners achter het gemeenschappelijke doel krijgen, dát is de kunst. Dit betekent dat het bestuur flink zal moeten investeren in het motiveren en inspireren van de individuele zorgverleners en medewerkers.

“Laat de regio’s in eerste instantie vooral zelf stappen nemen.” … “Daar waar de bereidheid is, moet je bewegen en niet alles laten ‘hangen’ op landelijke ontwikkelingen. Door verschillende regio’s hun eigen tempo te laten volgen, voorkom je dat initiatieven ongewild doodbloeden.” Annemieke van Hees, zorginkoper huisartsenzorg UVIT

“Je hebt in je regio zeker sterke trekkers/believers nodig. Het succes zit ‘m niet zozeer in het technische verhaal, maar in de eensgezindheid en besluitvormingsstructuur om knopen te kunnen doorhakken en een goed beleid uit te zetten.”

Jan Vesseur, hoofdinspecteur Inspectie van Gezondheidszorg

“Het belangrijkste dat we hebben bewerkstelligd is misschien wel een cultuurverandering: iedereen is zich bewust geworden van het belang van privacy en veiligheid. Als medewerkers van de CHN tegenwoordig een waarnemend huisarts zien die ze niet kennen, aarzelen ze niet om naar een identificatie te vragen. In het verleden was dat *not done*.”

Marion Borghuis, directeur CIHN en ZEGEN

“Ik snap goed dat huisartsen er echt niet op zitten te wachten technische problemen op te lossen. Ze zijn zo druk... Als applicatiebeheerder probeer ik samen met de rest van de ICT-afdeling problemen op te lossen, nieuwe versies neer te zetten en te kijken wat beter kan. Huisartsen weten me steeds beter te vinden. Soms fungeer ik als een soort telefonische helpdesk.”

Wendy Breuker, doktersassistente HAP Nijmegen en applicatiebeheerder

Projectmatig werken

Starten in de vorm van een project is het meest voor de hand liggend. Er is een begin en een eind aan de werkzaamheden en het werkproces wordt afgebakend; een project heeft per definitie een tijdelijk karakter. De werkzaamheden zijn ondergebracht in een projectorganisatie die los staat van de staande organisatie. Het project wordt pas succesvol afgerond als de resultaten geïntegreerd zijn in de staande organisatie.

Draagvlak creëren

Hoe groter het draagvlak is en hoe meer wederzijdse belangen worden gedeeld, des te effectiever er gewerkt kan worden en des te beter de kwaliteit van het beoogde resultaat zal zijn. De missie en de doelen spelen een cruciale rol. Begin allereerst enthousiasme binnen de beroepsgroep te kweken. Een kritische huisartsenkring, een evenzeer kritische groep huisartsen die betrokken zijn bij aansturing of bestuur van de huisartsenpost en het regionale departement van de KNMP (of apothekersvereniging), vormen een goede basis voor nieuwe ontwikkelingen. Belangrijk is dat de zorgverleners onderling solidair zijn en goed samenwerken. Hanteer het zwaan-kleef-aan-principe; begin met een groep early adopters en bouw het van daaruit uit. Zorg ook voor draagvlak bij patiëntenorganisaties, zorgverzekeraars en gemeenten.

Hoe u draagvlak creëert? Hieronder enkele voorbeelden:

- Houd presentaties in de reguliere vergaderingen van de verschillende beroepsgroepen.
- Zorg voor scholing over ADEMD-/ADEPD-registratie voor huisartsen en praktijkmedewerkers.
- Vergroot niet alleen de kennis om beter te registreren, maar maak ook zichtbaar wat communicatie in gaat houden. Bied ruimte aan discussies over de zin en onzin van communicatie.
- Organiseer een kickoff-bijeenkomst. Presenteer bijvoorbeeld tijdens een ‘diner pensant’ of rondetafelgesprek met besturen en management succesvolle voorbeelden uit de praktijk. Of giet het in de vorm van een brainstormlunch met patiëntenorganisaties, of een demonstratie van het LSP op dvd in de koffiepauze.
- Organiseer bij de start van LSP-communicatie instructiebijeenkomsten voor alle betrokkenen (behalve zorgverleners ook bijvoorbeeld

baliemedewerkers en chauffeurs) waarbij u aandacht besteedt aan privacy, opt-in en informatiebeveiliging. Dit om het draagvlak voor organisatorische veranderingen, opt-in en het gebruik van en zorgvuldig omgaan met UZI-middelen te vergroten.

- Verstuur regelmatig nieuwsbrieven of e-mails aan alle betrokkenen om ze te informeren over successen en op de hoogte te houden van de voortgang.

Samenwerkingen aangaan

Bij complexe veranderingen zoals bij gegevensuitwisseling via het LSP is goede samenwerking met andere betrokken partijen uit de regio een vereiste. Als het project alleen gaat over huisartsenwaarneemgegevens is de groep een andere dan wanneer ook medicatiegegevens 'meedoen' in het project.

Start het project met een beperkt aantal partijen uit het zorgveld en patiëntenvertegenwoordigers met bewezen enthousiasme voor samenwerking op het gebied van elektronische communicatie en ICT-ontwikkeling. Communiceer de aanpak naar andere partijen en geef aan dat als de technische en implementatieproblemen overwonnen zijn alle belanghebbenden kunnen participeren.

Stem de plannen en de voortgang af met andere regionale organisaties zoals zorgverleners/-partners, instellingen, beroepsverenigingen, patiëntenorganisaties en eventueel gemeente.

Werk samen met de bestaande ICT-leveranciers of kies voor enthousiaste en innoverende ICT-leveranciers met nieuwe ICT-oplossingen die de processen ondersteunen.

Randvoorwaarden creëren

Zorg dat aan alle randvoorwaarden is voldaan. Het gaat niet om commitment en draagvlak creëren alleen. Ook de volgende rand-voorwaardelijke zaken moeten geregeld zijn:

- Maak de begrotingen op orde en bereken de personele inzet;
- Wees alert op (nieuwe) financierings- of subsidiemogelijkheden;
- Maak plannen voor scholing en training;
- Zorg voor deskundige medewerkers of trek zo nodig externe medewerkers /adviseurs aan.

3.2 Praktijkvoorbeeld: project ZEGEN

Stichting ZEGEN is een samenwerkingsverband tussen vier verschillende partijen: CHN, Huisartsenkring Nijmegen e.o., Nijmeegse apothekers (verenigd in Stichting OZIS) en het CWZ. Het project ZEGEN is (deels) tot koploperproject uitgeroepen. Zo is destijds ook de financiering rondgekomen.

Lerend veranderen

In het project ZEGEN is er gewerkt vanuit het principe 'al lerende komen we verder'. 'Lerend veranderen' is een manier van werken waarbij met inachtneming van de wettelijke kaders in een proces van co-creatie nieuwe systemen, werkwijzen en nieuw gedrag worden gerealiseerd. Wanneer deze stijl van werken aansluit op de bestaande opvattingen en ervaringen in de regio is er een goede basis voor het samenwerkingsproject.

Projectorganisatie

Om de doelstellingen succesvol te realiseren is een slagvaardige projectorganisatie ingericht waarin verschillende samenwerkende partijen participeren. De projectorganisatie ziet er als volgt uit:

1. Stuurgroep, bestaande uit de bestuurlijke vertegenwoordigers van de samenwerkende organisaties;
2. Projectmanagement, aangewezen door de stuurgroep;
3. Projectleider/coördinator, aangewezen door het projectmanagement;
4. Projectgroepen, met vertegenwoordigers en deskundigen vanuit de verschillende organisaties.

In de stuurgroep nemen de volgende partijen plaats: vertegenwoordigers van een van de ziekenhuizen; apothekers die tevens betrokken zijn bij het OZIS-communicatienetwerk voor apotheken; bestuursleden van de huisartsenkring en de huisartsenpost; de directeur van de huisartsenpost. In de startfase is ervoor gekozen om bij het project een beperkt aantal partijen te betrekken die al actief zijn op het gebied van elektronische communicatie in de eerste lijn. Op een kick-offbijeenkomst zijn de andere regionale zorginstellingen uitgenodigd en zijn het doel en de beperking van het project toegelicht.

Er is een projectgroep voor de ICT voor de huisartsenpost, een projectgroep voor het aansluiten van huisartsen en apothekers en een projectgroep patiëntinformatie. Die laatste groep is nodig omdat in de koploperfase de communicatie naar patiënten nog vanuit het project loopt.

Het projectmanagement is ingevuld door de directie van de huisartsenpost. Twee projectcoördinatoren (later één coördinator) worden ingehuurd vanuit een extern adviesbureau.

De verschillende projectgroepen en/of de coördinator hebben het volgende takenpakket:

- zorgaanbieders stimuleren en motiveren mee te doen;
- overeenkomsten sluiten tussen project en deelnemers;
- overleg plegen met leveranciers over voortgang in de relevante informatiesystemen;
- overeenstemming bereiken over de financiering van de verschillende onderdelen;
- patiënten(organisaties) en zorgverleners informeren over de (deel)projecten;
- monitoren van de aansluiting van systemen op het LSP (Nictiz, nu SCZ);
- scholing en instructies voor de gebruikers van de systemen;
- monitoring van het functioneren van de communicatie via het LSP;
- procedures opstellen voor het omgaan met privacy, autorisatie en logging;
- een vervolgtraject uitstippelen voor de uitrol naar meer gebruikers/systemen en andere toepassingen;
- de PR en communicatie verzorgen over de voortgang en tussentijdse rapportage over de resultaten.

Plan van aanpak

Stimuleren en motiveren

Voorafgaand aan het project is er een informatiebijeenkomst met alle geïnteresseerde zorginstellingen uit de regio. In de startfase is een kick-offbijeenkomst georganiseerd voor huisartsen en andere professionals. Het onderwerp is bij herhaling geagendeerd op reguliere bijeenkomsten van zorgverleners.

Overleg met leveranciers over de voortgang

Er is regelmatig overleg met leveranciers over de voortgang van prepareren van de systemen voor aansluiting op het LSP. Bij gebrek aan voortgang in het HAP-systeem is besloten te kiezen voor een andere leverancier. Daarnaast is gekozen voor een 'co-existentie oplossing' waarbij een eerstelijnsserver is ingericht omdat de uitwisseling via het LSP stagneert.

Financiering

In de regio ontbreken financieringsmogelijkheden voor discipline-overstijgende communicatieprojecten. Deelname aan de koploperprojecten stelt de financiering veilig.

Informatie over voortgang

Periodiek is een nieuwsbrief uitgegeven. Deze nieuwsbrief informeert de betrokken partijen over de voortgang. Ook is er een website opgericht.

Aansluitingen monitoren

Aan de hand van navraag bij praktijken en informatie vanuit Nictiz (nu SCZ) en leveranciers wordt zo goed mogelijk gemonitord wat de voortgang van de aansluiting op het LSP is.

Scholing

Bij de start van het project is scholing verzorgd voor huisartsen en assistentes. Na een algemene uitleg over gegevens opvragen via het LSP wordt per HIS ingegaan op de ADEPD-richtlijnen. Op het moment dat de eerste dossiers op de huisartsenpost beschikbaar komen, ligt in een cursus voor medewerkers van de huisartsenpost de focus op werken met het systeem, privacy en gegevensbeveiliging. Daarnaast zijn de hoofdlijnen van de ADEPD-registratie herhaald. Doktersassistenten krijgen ook nog een aanvullende cursus ICPC-registreren. Huisartsen en praktijkmedewerkers volgen in groten getale dezelfde cursus. Daarbij is aangegeven dat een herhaling van een praktijktraining per HIS mogelijk is.

Privacy, informatiebeveiliging en logging

De bouw van een nieuw informatiesysteem geeft de mogelijkheid een aantal aspecten rond privacy en gegevensbeveiliging te verankeren in de software. Daarnaast zijn diverse procedures uitgewerkt (zie hoofdstuk 4).

PR en communicatie

Goede PR en communicatie zijn van groot belang, ook vanwege de aard van het koploperschap in de ontwikkelingsfase van het project. Kennis en ervaringen vanuit het project worden zoveel mogelijk gedeeld met de uitvoeringsorganisaties van VWS en Nictiz (nu SZC). Koepelorganisaties van beroepsgroepen krijgen actief informatie over de voortgang en knelpunten. Een deel van de PR is gericht op de eigen regio. Als regionale successen of de landelijke gebeurtenissen (of discussies daaromheen) daartoe aanleiding geven, wordt contact gezocht met de regionale pers om ze te informeren over de inhoud en voortgang van het project.

Ondersteuning

Wanneer de aansluiting van de huisartsen op het LSP stagneert, worden ze ondersteund met adviezen of is contact opgenomen met leveranciers of organisaties die betrokken zijn bij de aansluiting op het LSP. Dezelfde service wordt verleend aan huisartsen die na afsluiting van het koplopertraject in het kader van de landelijke uitrol aansluiten op het LSP.

3.3 Technische realisatie

Het is aan te raden om te inventariseren waar u staat. Welke voorwaarden zijn al ingevuld en wat moet er gerealiseerd worden? Uw huidige ICT-leverancier kan inzicht geven in de stand van zaken. Misschien voldoet ‘uw’ hardware, maar is uw softwareprogramma nog niet in staat te communiceren met het LSP (dan zit er soms niets anders op dan ‘wachten’ op het moment dat uw leverancier klaar is voor de aansluiting). Of misschien is de BSN-registratie volledig op orde, maar heeft u geen enkele UZI-pas in huis. Er zijn praktijken waarbij de server bij wijze van spreken nog onder de balie staat. Dat levert bijvoorbeeld problemen op bij het voldoen aan de eisen voor een Goed Beheerd Zorgsysteem (GBZ).

Maatwerk

Welke stappen u in uw specifieke situatie precies moet ondernemen, is afhankelijk van wat uw ICT-leverancier u uit handen neemt. Het aanpassen en/of installeren van de benodigde soft- en/of hardware wordt meestal volledig door de ICT-leverancier uitgevoerd, maar bij bepaalde pakketten kunnen sommige taken wél op uw to-do-list komen te staan. Hoe het ook zij; als u de ICT aan een béétje professionele partij heeft uitbesteed, dan zult u zien dat u sowieso al een eind op weg bent. Het traject van aansluiten op het LSP is maatwerk en zal er voor de een heel anders uitzien dan voor de ander.

'Aftikken'

Feit is dat het systeem waarmee u tot dusver heeft gewerkt (als er als sprake was van een systeem) aan een aantal randvoorwaarden moeten voldoen om aansluiting te krijgen op het LSP. Die randvoorwaarden staan hieronder beschreven. Vervolgens moeten verschillende stappen doorlopen worden. In de praktijk zal het zeker niet zo zijn dat u elk van die randvoorwaarden en/of stappen moet 'aftikken'. Als zorgverlener heeft u liever niets te maken met de technische specificaties van ZSP's, XIS-sen en wat dies meer zij. Toch zult u in het proces van aansluiting hier en daar geconfronteerd worden met de technische rompslomp en hoe de organisatie zich daar stapsgewijs doorheen 'ploegt'. Sowieso kunt u een flinke stapel formulieren verwachten waar u uw handtekening onder dient te zetten. Dan is het wel handig te weten wat een en ander inhoudt en waarom u er eigenlijk mee te maken krijgt.

Betrokken organisaties

U zult zien dat allerlei instanties en organisaties bij de aansluiting op het LSP zijn betrokken. Zo zijn er VZVZ (verantwoordelijk voor de gegevensverwerking in het LSP), Nictiz (verantwoordelijk voor de standaarden en specificaties van de landelijke infrastructuur AORTA) en SCZ (verantwoordelijk voor beheer, onderhoud en ontwikkeling van de infrastructuur voor zorgcommunicatie en aansluiten van zorgaanbieders op de zorginfrastructuur). Verder kunt u niet om het CIBG heen (verantwoordelijk voor het UZI-register en de SBV-Z). Tenslotte zijn de koepel- en brancheorganisaties van zorgaanbieders en de ICT-leveranciers van zorginformatiesystemen nauw betrokken bij alle voorbereidingen op de landelijke invoering.

Voor 80% rond

Wilt u voor uzelf het proces zo eenvoudig mogelijk houden, dan komt u al een heel eind als u zich tot het loket op www.sczorg.nl (zie 'zorgaanbieders') richt. Voor (technische) ondersteuning kunt u terecht bij uw ICT-leverancier. Daarmee heeft u de support al voor ongeveer tachtig procent geregeld. Ook kunt u gebruik maken van het stappenplan verderop in dit hoofdstuk.

Randvoorwaarden

Om berichten met het LSP te kunnen uitwisselen moet aan de eisen van een Goed Beheerd Zorgsysteem (GBZ) worden voldaan.

De GBZ-eisen

De juiste XIS-type kwalificatie

Om gegevens te kunnen uitwisselen met het LSP moet het zorginformatie-systeem (ook wel aangeduid met de term XIS, een generieke afkorting voor zorginformatiesystemen als HIS, AIS, ZIS) de aansluiting met het LSP ondersteunen. Het pakket moet daarvoor zijn goedgekeurd door Nictiz en de juiste versie(s) van een XIS-type kwalificatie hebben.

Beveiligde verbindingen

Om gegevens te kunnen uitwisselen met het LSP moet er sprake zijn van een beveiligde verbinding via een ZSP (Zorg Service Provider). Dit is een leverancier die voldoet aan GBZ-eisen en gekwalificeerd is voor communicatie met het LSP. Bijvoorbeeld E-zorg, of Zorgconnect van KPN. Ook veel ASP-leveranciers die hun diensten leveren aan de eerste lijn zijn gekwalificeerd als ZSP.

Technische eisen

De voor de XIS-applicatie benodigde hard- en software moet geschikt zijn om te kunnen communiceren met het LSP. Het gaat hier over de mate van beschikbaarheid, snelheid en capaciteit om gegevens op te slaan en om het tijdig aan kunnen melden van wijzigingen in patiëntendossiers. Bij ASP-oplossingen vult de leverancier van het systeem die voorwaarden in. Indien een instelling of samenwerkingsverband van zorgverleners een gezamenlijk of geclusterd systeem in eigen beheer aansluit aan het LSP, is overleg met hard- en softwareleverancier nodig om te beoordelen of aan de eisen wordt voldaan.

“De registratie van de codes vergt behoorlijk wat tijd. Kun je snel de juiste code vinden? Schrijf je de code bij de goede episode weg? Vroeger was het voldoende als je zelf in ieder geval maar je aantekeningen begreep; nu moeten anderen het ook snappen. Daarom zijn die ADEMD-trainingen georganiseerd.”…
“Uiteindelijk heb je er toch zelf plezier van. De gegevens zijn overzichtelijker gerangschikt en het is gemakkelijker dan voorheen om iets terug te vinden.”

Jaap Schreuder, huisarts en voorzitter Huisartsenkring Nijmegen e.o. (van 2003 t/m 2010)

“Goed coderen is vooral bij vage klachten in de praktijk vaak erg moeilijk. Als we de combinatie willen maken tussen een goede werkwijze en elektronische communicatie, dan moeten we ook zorgen dat er codes zijn. De techniek kan veel; het is een uitdaging om de inhoud van de berichten eenduidig te krijgen. Als ontvanger van een bericht heb ik er last van als er niet volgens ICPC-codering wordt geregistreerd.”

Han Beekwilder, huisarts te Oosterhout

“Zorg voor overzicht en daarmee een goed beheer van de UZI-passen. Als coördinator vraag ik voor nieuwe medewerkers UZI-passen aan. Medewerkers zijn zelf deels verantwoordelijk voor de aanvraag en het verdere verloop, maar met behulp van een Excel-bestand heb ik het totaaloverzicht. Zo weet ik precies wanneer bijvoorbeeld de pas van een AIOS moet worden ingetrokken.”

Franceska Hubers, secretaresse en coördinator procedure UZI-passen

Toestemming patiënt (opt-in)
Op grond van een Europese richtlijn en de Wet bescherming persoonsgegevens (Wbp) moet elke patiënt aan elke zorgaanbieder vooraf toestemming geven voor grootschalige uitwisseling van medische gegevens. Die toestemming betreft ook de opname van gegevens in de verwijsindex (BSN van de patiënt in combinatie met de namen van zorgaanbieders die een dossier voor gegevensuitwisseling hebben aangemeld). Er zijn verschillende manieren om de patiënt hierover te informeren en de toestemming te verkrijgen. De zorgaanbieder kan de patiënt ernaar vragen bij een bezoek aan de praktijk. Ook is het mogelijk mailingen mee te zenden met de griepoproep, of bij bezoek aan de huisartsenpost een toestemmingsformulier te laten invullen voor de eigen huisarts. Een andere optie is een mailing te sturen aan alle patiënten, al dan niet op basis van regionale acties en ondersteund door acties in de regionale pers.

De patiënt kan mondeling toestemming geven, of dit schriftelijk doen, via een formulier (zoals meegestuurd in een mailing, of beschikbaar op praktijk of post, of te downloaden via www.vzvz.nl). Eind 2012 kan de toestemming ook via een landelijke website gegeven worden. De zorgaanbieder moet de toestemming op de juiste manier registreren in het systeem. Voor kinderen tussen twaalf en zestien jaar is toestemming van een van de ouders en het kind zelf vereist.

Op www.vzvz.nl is een aparte informatiesectie speciaal bedoeld voor patiënten. Zorgaanbieders kunnen hun patiënten middels posters, wachtkamerfolders en flyers informeren over de aansluiting op het LSP. Dit materiaal is eveneens verkrijgbaar via www.vzvz.nl.

Adequate registratie
Om gegevens via het LSP zo volledig en juist mogelijk uit te kunnen wisselen, is een adequate registratie van de zorg van belang. Voor huisartsen en huisartsenposten liggen die vast in de ADEMD-/ADEPD-richtlijnen van het NHG. Het is ook zaak om af te spreken hoe om te gaan met incomplete dossiers. Vaak ontbreken gegevens uit het verleden. Recente medisch relevante zaken kunnen eveneens ontbreken omdat ze (nog) niet opgenomen zijn in het dossier van de huisarts. Het is aan de voorschrijvers en apothekers het medicatiedossier actueel te houden. Scholing en continue aandacht en feedback op deze gebieden zijn vereist.

Stappenplan techniek en ICT-leveranciers

In onderstaand overzicht gaan we in op de stappen die voor huisartsen, huisartsenposten en apotheken het meest relevant zijn als het gaat om techniek en ICT-leveranciers.

Stap 1

Informeer bij uw software-leverancier of de door u gebruikte XIS-software versie de XIS-type kwalificatie heeft. Op www.sczorg.nl staat een overzicht van alle ICT-leveranciers die een zorginformatiesysteem aanbieden dat aan alle applicatie-eisen voldoet.

Stap 2

Inventariseer in overleg met uw systeembeheerder of ICT-leverancier of uw computersysteem en de verbindingen voldoen aan de technische GBZ-eisen. Zijn ze niet helemaal *state of the art*, ga dan na wat nodig is om wél te kunnen voldoen aan de genoemde eisen. Overweeg of het zinvol is uw applicatie professioneel te laten beheren door een ASP-provider of schaf de benodigde hard- en software aan en maak afspraken voor installatie.

Stap 3

Sluit een aansluitovereenkomst af met uw softwareleverancier. De meeste leveranciers ondersteunen u vervolgens deels of zelfs volledig bij de hierna volgende stappen.

Stap 4

U dient u meerdere aanvragen in.

Via www.uzi-register.nl:

- Aanvraag registratie als UZI-abonnee (zie bijlage 1: UZI-passen en mandatering).
- Aanvraag UZI-servercertificaat. Voor deze aanvraag dient u zich eenmalig op het postkantoor te identificeren.
- Aanvraag UZI-middelen:
  - Voor de aanvraag van passen voor u en uw medewerkers dient u een kopie van het legitimatiebewijs en pasfoto's in te leveren van iedere medewerker. De afhaalbewijzen worden toegestuurd, maar ieder moet persoonlijk de UZI-pas op het postkantoor afhalen.

- Handel zo veel mogelijk aanvragen ineens af. Dat beperkt het aantal tochten naar het postkantoor. Gebruik een paspoort of identificatiekaart omdat daarop alle voornamen voluit zijn geschreven.

Via www.sczorg.nl:

- Aanvraag GBZ indienen voor aansluiting op het LSP. Daarna ontvangt u van SCZ een gebruiksovereenkomst.

Op de site www.sczorg.nl staan praktische checklists, zoals 'Aansluiten op het LSP', 'Ingebruikname LSP' en 'GBZ beheer'.

Stap 5

Tijd voor de aansluiting zelf:

- Installatie UZI-paslezers en instructie UZI-pas gebruik;
- Registratie van uw UZI-passen in het XIS;
- Invoer van de vereiste mandateringen in het XIS;
- Technische aansluiting door de leverancier en testen van de verbindingen;

Dit eenmalige proces duurt ongeveer twee uur, waarna uw aansluiting een feit is. De aanmelding kan alleen geschieden als u een UZI-pas gebruikt.

Stap 6

Praktijken met meer dan één arts of apotheker hadden al vanaf 2002 de verplichting om hun geautomatiseerde administratie te melden bij het CBP. Is dit niet gebeurd, dan is het elektronisch toegankelijk maken van het dossier via het LSP is een goede aanleiding dit alsnog te doen (zie www.cbpweb.nl).

Tip

Het aanmeldingsformulier op www.cbpweb.nl is vrij complex. Bij de paragraaf over vrijstelling van individuele beroepen in de gezondheidszorg vindt u teksten met handige voorbeelden voor het invullen van het formulier.

Stap 7

Bij uitwisseling van gegevens zoals via het LSP: breng uw patiënten ervan op de hoogte dat u gegevens uitwisselt via het LSP. Dit kan bijvoorbeeld met behulp van posters en brochures (aan te vragen via www.vzvz.nl). Als u gegevens wilt uitwisselen, moet u de patiënt vooraf om toestemming vragen.

Stap 8

Volg het verloop van de LSP-communicatie. Vooral in het begin is het van belang de rapportages van de zorgapplicatie in de gaten te houden. U kunt overwegen dit te laten uitvoeren door de beheerder. Kijk of u fouten in de communicatie ontdekt en het (her)aanmelden van dossiers wel helemaal lukt. Meld de problemen bij de leverancier of bij SCZ. Zorg dat u ook de logging van uw eigen informatiesysteem regelmatig monitort. Ga na of er sprake is van onverwachte opvragingen van medische dossiers. Dit om eventueel misbruik door medewerkers in een vroeg stadium op te sporen (zie ook hoofdstuk 4).

Werkt het?

Na de eerste aansluitingen in de regio Nijmegen op het LSP begin 2010 blijkt dat het aantal berichten lang niet zo hoog is als verwacht. 25% van de patiënten is aangemeld bij het LSP (medio 2012 is dit gestegen naar 40%), er wordt maar voor 13% van de patiënten via het LSP een professionele samenvatting op de post ontvangen. Bovendien blijkt dat na ontvangst van een professionele samenvatting slechts in 75% van de gevallen een waarneemretourbericht wordt verzonden. Analyse laat zien dat dit te maken heeft met veel factoren. De belangrijkste punten zijn:

- **Techniek**
  - Technische fouten en onhandigheden in de programmatuur.
  - Bereikbaarheidsproblemen van de achterliggende informatiesystemen.
- **Gedrag**
  - Er worden regelmatig UZI-passen 'niet op naam' gebruikt, omdat men de eigen pas is vergeten, of omdat de zorgverlener nog in afwachting is van zijn pas.
  - Mandatering van de passen verloopt niet goed.
  - De identiteit van de patiënt wordt niet geverifieerd, wat wel verplicht is voor een succesvolle opvraging via het LSP.
- **Structuur**
  - Het BSN is niet beschikbaar (bijvoorbeeld van patiënten uit Duitsland).
  - Toestemming van de patiënt ontbreekt.

In september 2010 is het succespercentage van de waarneem-retourberichten gestegen van 75% naar 82%. Medio 2012 is 40% van de patiënten aangemeld bij het LSP. Het succespercentage van de waarneemretourberichten is verder gegroeid naar 92%. Uitbreiden kan alleen door verwerven van een opt-in. Patiënten zonder opt-in zullen in 2013 uit de index worden verwijderd.


Beschermen

Veiligheid en betrouwbaarheid

Goed, nu is er die toegang tot al die medische gegevens. De vraag is nu: hoe gaat u er verantwoord mee om? Hoe worden de gegevens beheerd en beschermd, hoe is in de gaten te houden wie waarom en hoe vaak inlogt? Hoe zorgt u ervoor dat gevoelige informatie niet zomaar wordt 'gedeeld' en dat iedereen 'schoon' en volgens dezelfde normen of standaarden werkt? Met andere woorden: hoe zorgt u voor een goede datahygiëne, door eigenlijk heel de organisatie heen? Het gaat erom de gegevens dusdanig te bewerken, beheren en af te schermen dat elk risico op welke datalek dan ook wordt voorkomen. Natuurlijk is een en ander ingebed in het technische systeem. Geen toegang immers tot het LSP zonder UZI-pas. En heeft een zorgverlener geen 'relatie' met een patiënt, dan is er sowieso geen reden in zijn of haar dossier te zoeken. Sterker nog, hij komt er niet eens 'bij'.

4.1 Gedrags- en cultuurverandering

E-communicatie in de zorg moet voldoen aan de hoogste beveiligings-standaarden, niet alleen aan de harde infrastructurele kant, maar ook aan de zachte organisatorische kant. Want uiteindelijk gaat veilige uitwisseling van gegevens slechts voor tien procent om techniek en voor negentig procent om gedrag. Het grootste risico in de ICT-beveiliging zit tussen het toetsenbord en de stoelzitting, wordt weleens gezegd.

Het omgaan met zeer persoonlijke gegevens van mensen vraagt om een optimale privacybescherming, zoals dat eigenlijk al 2500 jaar geleden omschreven is in de Eed van Hippocrates. Nu zijn zorgverleners al vanaf hun opleiding en tijdens hun carrière van dat gedachtegoed doordrongen. De toegang tot de professionele samenvatting van de patiënt via beveiligde

ICT brengt echter nóg meer verantwoordelijkheid met zich mee. Feitelijk 'triggert' het gebruik van LSP-communicatie een complete gedrags- en cultuurverandering, bij de professionals én de medewerkers. Het gaat bij informatiebeveiliging namelijk niet alleen om de elektronische communicatie, maar ook om zorgvuldige omgang met papieren documenten en andere informatiedragers, openstaande computerschermen en de mondelinge communicatie over patiëntengegevens. Gegevensverlies of juist continue beschikbaarheid van gegevens, het voorkomen van storingen, goede procedures; informatiebeveiliging kent veel facetten.

Het is zaak volop aandacht te hebben voor het klimaat en de omgeving waarin vertrouwelijke gegevens beschikbaar worden gesteld. Het gaat om het ontwikkelen van een nieuwe 'houding'. En dat heeft ingrijpende gevolgen voor de bedrijfsvoering, de gedragsregels en de onderlinge verhoudingen. Het is de opdracht en verantwoordelijkheid van elke zorgverlener en iedere zorgorganisatie om de communicatie op veilige, integere en betrouwbare wijze te laten verlopen. Men moet van elkaar weten wat wel/niet is toegestaan, welke functies, procedures en protocollen nodig zijn om alles in goede banen te leiden. Kortom: dat vraagt om een goede begeleiding, waarbij het belangrijk is weloverwogen en stapsgewijs te werk te gaan.

4.2 Richtlijnen, normen en certificering

Voorheen was het mogelijk op basis van goed vertrouwen en gezond verstand ad hoc afspraken te maken met de professionals en alle medewerkers: niet zomaar vertrouwelijke informatie mondeling 'delen', geen cd's of usb-sticks op het bureau laten rondslingeren, geen printjes in de oudpapierbak dumpen, vastleggen wie wel of niet toegang heeft tot het serverhok of het systeem.
Inmiddels bestaan er echter voor veilige elektronische gegevensuitwisseling verschillende eisen en richtlijnen. Om aan te sluiten op het LSP moet de zorgaanbieder ervoor zorgen dat het zorginformatiesysteem voldoet aan het programma van eisen voor een goed beheerd zorgsysteem (GBZ),

“Op basis van praktijkervaringen in Nijmegen kunnen we stellen dat de lat hoog ligt als het gaat om beveiliging van het LSP. Die strenge beveiliging heeft er soms wel toe geleid dat het daadwerkelijk uitwisselen van gegevens niet direct eenvoudig en werkbaar was. Inmiddels kunnen we zeggen dat het LSP goed functioneert, ook wanneer er op grote schaal gegevens worden uitgewisseld.”

Bertus Buitenhuis, operationeel directeur Protopics

“Door de invoering van het LSP heeft het privacybewustzijn een grote sprong voorwaarts gemaakt. Ik had niet verwacht dat er zoveel attitudeverandering zou ontstaan. Er wordt op de werkvloer ook minder gepraat over patiënten dan vroeger, namen worden minder genoemd en het dossier wordt er minder snel bijgehaald.”

Herman Levelink, huisarts en bestuurslid ZEGEN

“NEN dwingt je om alles op papier te zetten. Je komt erachter dat er toch nog blinde vlekken zijn. Dat verscherpt de discussie. Neem het thuiswerken; daarbij werden weliswaar geen patiëntgegevens geraadpleegd, maar wel andere gegevens van vertrouwelijke aard. Dan ga je je afvragen of het echt nodig is dat deze gegevens buiten de muren van je instelling komen.”

Sabine Verheggen, kwaliteits- en klachtenfunctionaris CHN

inclusief de organisatorische eisen (www.sczorg.nl). In ontwikkeling is de Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ). De Gedragscode maakt duidelijk wat koepels van zorgverleners met elkaar hebben afgesproken om in elke (praktijk)situatie aan de wettelijke regels met betrekking tot privacy en beroepsgeheim te voldoen. De code wordt gedragen door de koepelorganisaties KNMG, KNMP, LHV, NHG en VHN en zal voorgelegd worden aan het College bescherming persoonsgegevens (CBP). Als de Gedragscode definitief is, wordt hij gepubliceerd op de websites van de genoemde organisaties (zie ook bijlage 14).

NEN-certificering

Naast het volgen van de Gedragscode is het mogelijk volgens een systematische aanpak de normen voor informatiebeveiliging in de zorg te implementeren (NEN 7510). Met name voor grotere organisaties zoals huisartsenposten kan een dergelijke certificering een goede route zijn om op een professionele manier te werken aan informatiebeveiliging. De CHN heeft er destijds bewust voor gekozen het traject van aansluiting op het LSP parallel te laten lopen aan het behalen van de NEN-certificering volgens de 7510-norm (toen nog NEN 7511; in oktober 2011 zijn NEN 7511 en NEN 7510 samengevoegd in een nieuwe versie van NEN 7510. De CHN is overigens gecertificeerd door Lloyd's Register Quality Assurance).

Hoe werkt het?

Beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens staan aan de basis van NEN-certificering. Om een beeld te geven van wat die NEN-certificering inhoudt: er vinden risico-inventarisaties plaats van kritische processen als telefonie, patiëntenregistratie, internetverkeer en ICT-applicaties. Werken de telefoon- en internetlijnen optimaal? Maakt de geavanceerde hard- en software het onbevoegden onmogelijk het systeem in te gaan? Ook het bewustzijn en het gedrag van de medewerkers worden aan een kritische blik onderworpen. Is iedereen – van de chauffeur en de baliemedewerker tot aan de doktersassistent en huisarts – ervan doordrongen dat de patiëntengegevens vertrouwelijk zijn en dus ook als zodanig moeten worden behandeld? Zelfs de contracten met de leveranciers van alle diensten (internet, telefonie) gaan onder de loep. Na een aantal audits volgt de officiële certificering. Daarna wordt op regelmatige basis geaudit.

Met behulp van een (extern) adviseur en onder leiding van de kwaliteitsfunctionaris en een projectgroep zijn de voorbereidingen voor NEN-certificering te treffen. Inventariseer wat er nodig is of moet gebeuren om met vertrouwen de audits tegemoet te zien.
De vertaling van de NEN-norm 7510 naar de praktijksituatie voor huisartsen en apothekers is te vinden in de NHG PraktijkWijzer voor informatiebeveiliging en de KNMP richtlijn 'Informatiehuishouding en -beveiliging'.

4.3 Beleid uitstippelen

Zo'n NEN-certificering is uiteraard geen 'must'. En toch, als u ervoor kiest op uw eigen manier de veiligheid en betrouwbaarheid te waarborgen, dan zult u iets van een 'beleid' moeten hebben waarin gedragsregels ten aanzien van privacygevoelige informatie zijn uitgewerkt. Bij het opstellen van zo'n beleid (dat resulteert in een plan) zou u oog moeten hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid van (patiënten-) informatie binnen de organisatie. 'Vertrouwelijkheid' staat daarbij voor het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Het nastreven van 'integriteit' binnen de organisatie houdt in dat de correctheid en de volledigheid van informatie en verwerking is gegarandeerd. En met 'beschikbaarheid' gaat het erom te waarborgen dat geautoriseerde gebruikers op het juiste moment toegang hebben tot informatie en middelen.

Hieronder geven we aan wat onderdelen zouden kunnen zijn van zo'n beveiligingsbeleid (zie bijlage 2: Informatiebeveiligingsbeleid CHN i.o.).
Het kwaliteitsmanagement kan ervoor zorgen dat zo'n beleid wordt vastgelegd en uitgewerkt in procedures en protocollen die de professionals en medewerkers worden geacht na te leven.

N.B. Voor de meeste regels, procedures, matrixen et cetera uit de bijlagen geldt dat deze, al dan niet met wat aanpassingen, bruikbaar zijn voor huisartsenpraktijk en apotheek.

“Informatiebeveiliging gaat om meer dan digitale communicatie alleen. Onze grootste uitdaging betreft waarschijnlijk ons eigen gedrag; kun je de verleiding weerstaan iemand op te zoeken? En kun je ook je mond houden als je iets van iemand weet? We gaan niet uit van kwaadwilligheid bij medewerkers, maar meer van onbedoeld nieuwsgierig zijn, of anders gezegd: van ‘meer opvragen dan strikt genomen nodig is voor je werk’.
Ga steeds bij jezelf na: wil de patiënt wel dat ik deze gegevens nu opvraag?”

Sabine Verheggen, kwaliteits- en klachtenfunctionaris CHN

“Medewerkers zijn zich nu veel meer bewust van de privacyprocessen, daar hebben we vanuit de organisatie veel aandacht aan besteed. Ga niet onnodig patiënten oproepen, want daar loggen wij op, ‘neusgedrag’ tolereren wij niet. Het reikt ook verder dan IT; geen briefjes laten liggen, printer nalopen na de dienst; dit staat ook in protocollen en richtlijnen.” Lisette Willems, locatiemanager Boxmeer en beheerder Protopics (op beide posten)

“Wat ik belangrijk vind, is dat de assistentes beschermd worden door dit systeem. Een tijdje terug belde een patiënt dat ze een assistente ging aanklagen die ongeoorloofd dossiers zou hebben ingekeken en gegevens zou hebben gedeeld. Onderzoek wees uit dat de assistente de dossiers niet ingezien kón hebben. Nu kun je het dankzij logging goed uitzoeken, ik weet niet hoe we het vroeger zouden hebben gedaan...”

Annette Veenhof, coördinerend doktersassistente

“Wat we vooral van de loggingcontroles hebben geleerd, is om onszelf vragen te stellen: ‘wat zien we nu precies?’ en ‘wat kunnen we daaruit afleiden?’ Als we bijvoorbeeld zien dat iemand een bevraging via het LSP niet compleet of correct heeft afgerond, zoeken we dat uit. De rapportages geven overigens niet aan of die persoon de informatie op het scherm ook echt heeft gelezen. En ook niet of er misschien nog iemand anders meekeek.”

Sabine Verheggen, kwaliteits- en klachtenfunctionaris CHN

Contouren beveiligingsbeleid

- Geef aan aan welke wettelijke eisen de organisatie al voldoet en nog moet voldoen. Stel uzelf de vraag: waar staat u voor als organisatie?
- Stel instructies op voor gebruik, verlies en beheer van de UZI-pas (zie bijlage 1 en bijlage 3: Gebruikersreglement UZI-pas).
- Zorg dat u inzicht krijgt in de risico's ten aanzien van kritische processen (telefonie, patiëntenregistratiesysteem, de internetverbinding en eventueel de fysieke toegankelijkheid) en hoe deze risico's in te perken of acceptabel te maken zijn. Denk goed na over de risico's die privacygevoelige data kunnen lopen: door middel van risicoanalyses komt u daarachter (zie bijlage 4: Beschrijving risicoanalysemethode en/of bijlage 5: Risico-analyses NEN 7511-2).
- Ontwikkel een systeem om bedrijfsprocessen, informatiesystemen en informatie die vastgelegd is in documenten te classificeren (zie bijlage 6: Classificatie van beveiligingsrisico's). Op basis van classificatie kunnen prioriteiten voor beveiliging worden gesteld, 'beveiliging op maat' dus. Aan de hand van een classificatiesysteem zijn verschillende beveiligingsniveaus te definiëren en per klasse specifieke minimumregels te stellen voor de beveiliging van bedrijfsprocessen, informatiesystemen en informatie.
- Bescherming van privacygevoelige data staat hoog op de agenda. Daar hoort bij dat u nadenkt over bewaartermijnen van patiëntenformatie, maar ook een beleid uitstippelt voor het beschermen/bewaren van de gegevens die gebruikt worden bij onderzoeken, klachten, financiën, personeel. Hoe lang worden de gegevens bewaard, en waar? Welke gegevens mogen het pand wel verlaten en welke niet? Mogen patiëntdata de deur uit? Staat u thuiswerken en gebruik van usb-sticks toe? Worden wachtwoorden per mail verstuurd? Bij grootschalig beschikbaar stellen van patiëntgegevens voor inzage is toestemming vooraf nodig (opt-in) en bezwaarmogelijkheid (per regel) bij verzenden van gegevens. Transparantie naar patiënten is een vereiste (zie bijlage 7: Gedragsregels t.a.v. privacygevoelige informatie en bijlage 8: Procedure bewaartermijnen).
- Stel de fysieke toegankelijkheid veilig van privacygevoelige informatie: hoe zit het met de toegankelijkheid van afgesloten kasten en de computergegevens? Want niet alleen de toegang tot het centrale XIS-systeem moet gewaarborgd

zijn, maar ook die tot de serverruimte. Die is in te richten als een 'kluis' waar slechts een beperkt aantal gekwalificeerde medewerkers toegang tot heeft. Denk aan een inbraak- en branddetectiesysteem, maar ook bijvoorbeeld aan de elektriciteitsvoorziening (overschakelen op noodaggregaat indien nodig). Maak de serverruimte nog eens extra brandveilig. En verder moeten er natuurlijk voorzieningen getroffen worden voor het maken van back-ups en het uitvoeren van onderhoud.

- Stel een continuïteitssplan op: wat te doen als er calamiteiten zijn, welke maatregelen moeten er dan getroffen worden? Juist een organisatie als de HAP is voor het leveren van ANW-zorg extreem afhankelijk van telefonie, internet en de juiste werking en beschikbaarheid van het patiëntregistratiesysteem (zie bijlage 9: Continuïteitsplan ANW).
- Stel een beleid vast voor WID-controle (WID is het wettelijk identiteits-document, zorgverleners moet hun patiënten hiernaar vragen). Met name bij visiterijden (relevant voor HA of HAP) is het handig één lijn te trekken. Binnen de beroepsgroep kan er weerstand ontstaan om bij ernstig zieke mensen, ouderen, crisissituaties, et cetera naar een paspoort te vragen, terwijl dit wel verplicht is. De juiste medische gegevens moeten immers met zekerheid aan de juiste persoon gekoppeld worden.
  De 'vergewisplicht' volstaat meestal bij visiterijden, pas bij twijfel over de identiteit van de patiënt wordt overgegaan op WID-controle.
- Leg alle belangrijke processen vast in een middelenmatrix (zie bijlage 10: Middelenmatrix veilige infrastructuur).
- Bespreek hoe er omgegaan dient te worden met beveiligingsincidenten. Registreer wat er is gebeurd en stel verbeterplannen op. Maak achteraf analyses om incidenten te voorkomen.
- Organiseer voorlichtingsbijeenkomsten voor personeel, huisartsen en anderen (bijvoorbeeld chauffeurs, cliëntenraad) en vergeet daarbij het kantoorpersoneel niet!
- Zorg voor een 'heldere' organisatie: wie doet wat? Hoe zijn de taken en bevoegdheden voor wat betreft informatiebeveiliging verdeeld over de diverse medewerkers? Geef ook aan welke taken op regelmatige basis terugkeren per medewerker (zie bijlage 11: Taakomschrijving rollen NEN informatiebeveiliging en bijlage 12: Procedure autorisatie en controle toegangsrechten).

- Bewustwording van gedrag vertoont ook belangrijke raakvlakken met het personeelsbeleid: screenen van nieuwe personeelsleden, wat te doen als iemand uit dienst gaat (blijven de inlogcodes dan gelijk?), welke sancties hangen iemand boven het hoofd als hij of zij over de schreef gaat? En van welke werkafspraken moeten nieuwe medewerkers op de hoogte zijn om te voorkomen dat ze per ongeluk een beveiligingsincident veroorzaken? (zie bijlage 13: Personeelsbeleid in kader van informatiebeveiliging).

Beleid communiceren

Belangrijk is zo'n beleid goed te communiceren; iedereen moet van het beveiligingsbeleid doordrongen zijn. Daarom is het een idee (verplichte) informatieavonden te organiseren over de gevolgen van de aansluiting op het LSP en het gebruik van de UZI-pas en logging (zie hieronder). Informatiebeveiliging is de verantwoordelijkheid van alle medewerkers – of zij nu doktersassistent, baliemedewerker of chauffeur zijn. Iedere medewerker of lid van een bijvoorbeeld een HAP dient zich in het functioneren en het gedrag hiernaar te richten. Door middel van voorlichting wordt dit bewustwordingsproces opgestart, gestimuleerd en gecontinueerd. Vervolgens kan de kwaliteitsfunctionaris bijvoorbeeld erop toezien dat de regels worden nageleefd. Bovendien is het een idee de uitvoering van zo'n plan jaarlijks te evalueren.

4.4 Controleren

Iedere week maakt het management uitdraaien die zicht geven op de wijze waarop het waarneemretourbericht van de patiënt naar de eigen huisarts is verzonden: via het LSP of OZIS. Bij problemen wordt onmiddellijk actie ondernomen. Het management kan ook aan pro-actieve logging doen om te kijken of er geen misbruik wordt gemaakt van de inzage. Informeer de medewerkers hierover: 'neusgedrag' is na te gaan, verbind er als directie consequenties aan. Check of professionals die een dossier inkijken op dat moment een zorgrelatie met de patiënt hebben. Wees attent op patiëntencontacten die niet gefiatteerd zijn; er lijkt dan immers geen sprake te zijn van een zorgrelatie.

Tot slot

Het is een hele klus, die aansluiting op het LSP. Ongetwijfeld zijn er na het trouw (op)volgen van alle aanbevelingen, adviezen en stappenplannen nog altijd wat losse eindjes. Grote kans bijvoorbeeld dat de stabiliteit tussen de verschillende systemen in de gehele keten (bijvoorbeeld van HIS-LSP-HAP) te wensen over laat. Of dat de schaalgrootte nog omhoog kan (meer zorgverleners zich zouden moeten aansluiten) om écht profijt te hebben van inzage in patiëntendossiers. Of misschien valt het succespercentage opvragen en verzenden van waarneemberichten ietwat tegen. Enfin, er komen ongetwijfeld (nieuwe) hobbels op uw pad. Laten we zeggen dat het hierna op de finetuning aankomt. Het belangrijkste is dat de elektronische communicatie via het LSP in grote lijnen is uitgezet.
Vergeet vooral niet dat ICT en een tot in detail uitgewerkt informatie-beveiligingsbeleid weliswaar prachtige middelen zijn, maar geen doel op zich. Waar het werkelijk om draait, is kwaliteit in de zorg. Hopelijk komt u er – net als wij – achter dat u wat dat betreft een enorme sprong voorwaarts heeft gemaakt. Is dat niet alle tijd en moeite dubbel en dwars waard geweest?

ISBN 978-90-816318-1-5