

ZORGVERZEKERAARS NEDERLAND

■ Onderzoek Whitebox

Eindrapport

28 oktober 2019

Rapportnummer: 19020.1



WE DO TRUST

The Technology Governance Company

INLEIDING

Digitale uitwisseling van medische gegevens is een belangrijk thema in de zorg. Privacy en security spelen hierin een belangrijke rol. Een groot gedeelte van de burgers geeft toestemming voor uitwisseling van gegevens tussen zorgverleners via het LSP, een deel van de burgers aarzelt om toestemming te geven. Niettemin is er een brede overtuiging dat digitale uitwisseling grote voordelen heeft voor de burger en dat privacy of security geen showstoppers mogen zijn.

Uitwisseling vindt veelal plaats via het Landelijk Schakelpunt (LSP). Sinds 1 januari 2012 is VZVZ verantwoordelijk voor de elektronische uitwisseling van medische gegevens via het LSP. Daarvóór lag die verantwoordelijkheid bij het ministerie van VWS.

Circa 6.000 zorgaanbieders waaronder huisartsen, apothekers en ziekenhuizen zijn aangesloten op het LSP om medische gegevens van burgers digitaal met elkaar te delen. Dat gebeurt alleen na toestemming. Niet alle burgers geven toestemming voor uitwisseling via het LSP. Belangrijke argumenten om geen toestemming te geven zijn zorgen bij burgers over mogelijke privacyschending en gegevensbeveiliging.

Whitebox Systems stelt dat zij met een communicatievorm gebaseerd op indexloze push autorisatie een alternatief biedt met een aantal onderscheidende eigenschappen ten aanzien van security en privacy. Zorgverzekeraars Nederland (ZN) heeft begin 2019 opdracht gegeven om een onafhankelijke vergelijking te maken tussen Whitebox en het LSP.

In de managementsamenvatting van dit rapport treft u een samenvattende vergelijking met betrekking tot onderscheidende eigenschappen van zowel het LSP als Whitebox. Vanuit deze analyse is een advies geformuleerd voor ZN. Tevens hebben wij onze detailbevindingen opgenomen.

Wij bedanken alle betrokkenen van zowel Whitebox Systems, VZVZ, ZN en overige geïnterviewde partijen voor de prettige samenwerking.

Mochten er nog vragen zijn naar aanleiding van dit rapport, dan beantwoorden wij die graag.



ir. J.A.M. Donkers RE



MANAGEMENTSAMENVATTING

ZN heeft begin 2019 opdracht gegeven om een onafhankelijke vergelijking op te stellen tussen de concepten van Whitebox Systems en het LSP voor de uitwisseling van gegevens in de zorg en heeft daarvoor de volgende onderzoeksvraag geformuleerd:

Het doel van het uit te voeren onderzoek is te komen tot een objectieve vergelijking tussen het LSP zoals aangeboden door VZVZ en Whitebox van Whitebox Systems; wat zijn de (onderscheidende) eigenschappen van beide systemen, waarin verschillen zij en welke voor- en nadelen kennen beide?

VZVZ biedt het LSP aan voor gegevensuitwisseling tussen zorgverleners. Het LSP is een infrastructuur waarmee zorgverleners (in principe landelijk) onderling medische gegevens kunnen uitwisselen. Het LSP wordt geïmplementeerd door het zorgveld (LHV, KNMP, NVZ, Ineen, Patiëntenfederatie Nederland e.a.), verenigd in VZVZ. De gegevensuitwisseling vindt plaats via een beveiligd, los van het internet staand netwerk (de AORTA-zorginfrastructuur), waartoe alleen zorgverleners met gebruik van een sterk identificatiemiddel (de UZI-pas) toegang hebben. VZVZ voldoet aan de wettelijke vereisten en met circa 13,5 mln actieve toestemmingen van burgers is er een aantoonbaar groot draagvlak. Een grote groep burgers heeft dus toestemming gegeven voor uitwisseling via het LSP.

Niet alle burgers geven toestemming voor uitwisseling via het LSP. Privacy en security spelen hierin een belangrijke rol. Eén van de bezwaren bij burgers is dat zij de toestemming onvoldoende specifiek kunnen registreren. Binnen het programma Gespecificeerde Toestemming Structureel (GTS) wordt gewerkt aan een praktische oplossing voor het online vastleggen en beheren van deze toestemmingen. Parallel aan GTS wordt gewerkt aan een Online ToestemmingsVoorziening (OTV). Het gaat hier om een portaal dat het burgers gemakkelijker moet maken om zelf toestemmingen vast te leggen en te beheren. Zorgaanbieders kunnen dan op één plek de toestemmingskeuzes controleren. De gespecificeerde toestemming, waar OTV een implementatie van is, blijkt erg ingewikkeld. De uitwerking van OTV is nog volop onder handen en is niet publiek beschikbaar.

Er is een groep burgers die om inhoudelijke redenen geen toestemming heeft gegeven voor uitwisseling via het LSP. Goede voorlichting kan impact hebben op de omvang van de groep want genoemde argumenten zijn niet altijd terecht. Zodra OTV operationeel wordt, zal dit een reducerende impact hebben op de omvang van de groep die geen toestemming geeft. Maar we stellen vast dat een groep die geen toestemming geeft voor het LSP zal blijven bestaan. We onderkennen ook dat sommige personen uit deze groep nooit toestemming gaan geven voor digitale/elektronische uitwisseling. Het bepalen van de omvang van deze groepen valt buiten de scope van dit onderzoek.



MANAGEMENTSAMENVATTING (2)

Whitebox Systems biedt met Whitebox een product met een communicatievorm gebaseerd op indexloze push autorisatie, dat een alternatief biedt voor gegevensuitwisseling via het LSP op basis van een ander vertrouwensmodel. Een belangrijk onderdeel van het LSP is de autorisatiematrix. In deze matrix is vastgelegd welke zorgaanbieder welke informatie kan opvragen. Het LSP baseert vertrouwen naast techniek/software ook op basis van procedures en afspraken waarbij het ongeautoriseerd gebruik maken van toegang door zorgverleners wordt bestraft. Whitebox bouwt vertrouwen op op basis van techniek/software, de betrokkenheid van de huisarts/zorgverlener en fijnmazige, technisch afgedwongen toestemming. Dit biedt verschillen die niet verloren hoeven te gaan bij een meer grootschalige uitrol van Whitebox.

Whitebox Systems vraagt om een open koppelvlak in zorginformatiesystemen op basis waarvan communicatiesystemen naast het LSP ook via een koppeling (API) direct gegevens met HISsen/AISsen etc. kunnen uitwisselen, volgens berichten-standaarden. De Whitebox push autorisatie-standaard kan werken met een lokale API om uitwisselingssystemen (onder voorwaarden) met een XIS te kunnen verbinden om direct gegevens/berichten op te vragen of naar het XIS te versturen. Hiermee krijgen veilige communicatiesystemen naast het LSP een kans om gestandaardiseerd gegevens uit te wisselen en kan door zorgverleners een alternatief worden geboden aan burgers die hebben aangegeven niet via centrale voorzieningen zoals het LSP te willen uitwisselen.

De technologie die in Whitebox gebruikt wordt, is beoogd een standaard te zijn voor gegevensuitwisseling tussen zorgverleners. Whitebox Systems beoogt deze standaard via een onafhankelijke governance organisatie beschikbaar te stellen als open standaard. Hiermee kunnen dan ook andere systemen/leveranciers de technische standaard implementeren.

Whitebox Systems is een start-up. Op basis van de Whitebox-standaard kunnen, volgens Whitebox Systems, dezelfde functionaliteiten worden gerealiseerd als nu door VZVZ via het LSP worden aangeboden. Maar er mag niet aan voorbij worden gegaan dat het LSP al een gevestigde marktpartij is en zowel Whitebox-functionaliteiten als Whitebox Systems nog een ontwikkeling moeten doormaken om te kunnen opschalen.

Het is niet noodzakelijk te kiezen tussen het LSP of Whitebox, technisch gezien kunnen beide systemen naast elkaar draaien. De huisarts/het HIS zou dan zowel via het LSP als via Whitebox kunnen communiceren. Er zijn twee HISsen waar dit al mogelijk is. Dit zou recht doen aan de grote groep burgers voor wie het LSP voldoende waarborgen biedt en het geeft burgers een alternatief als ze vrijwillig afzien van communicatie via het LSP.



MANAGEMENTSAMENVATTING (3)

Dit lost ook het vraagstuk op dat niet de huisarts degene is die de keuze maakt. De patiënt kan samen met de huisarts de keuze maken hoe invulling te geven aan uitwisseling. Dit vergt wel extra inspanning van en kosten voor de huisarts/zorgverlener. Het is aan de zorgverlener of hij/zij de extra dienstverlening van het aanbieden van twee systemen ook wil bieden. Daarnaast brengt dit ook extra inspanningen aan de opvragende kant met zich mee.

Er zal de komende tijd veel veranderen in de uitwisseling van gegevens, zie o.a. ook de derde Kamerbrief elektronische gegevensuitwisseling in de zorg van de minister van 4 oktober 2019 jl. Een aspect is de aankondiging van de minister in de eerste Kamerbrief van 20 december 2018 om het realiseren van verplichte open koppelvlakken te (laten) onderzoeken. Het gaat in dit kader te ver om de impact daarvan mee te nemen in dit rapport, maar het zal er hoe dan ook toe leiden dat er aanpassingen aan systemen nodig zijn. Dit zal impact hebben op de snelheid waarmee XIS-en zouden kunnen meegaan in open communicatie.

Wat is het handelingsperspectief van Zorgverzekeraars Nederland inzake Whitebox?

Beleidsmatig vraagt voorgaande om afwegingen te maken op de volgende terreinen:

- Onderzoek hoe groot de doelgroep van 'weigeraars' is en of Whitebox voor hen daadwerkelijk een alternatief is.
- Onderzoek hoe de alternatieve generieke open koppeling voor ontsluiting ZIBs en andere courante berichtenformaten tussen individuele systemen kan worden vormgegeven.
- Definieer wat ZN wil doen om een generieke open koppeling en Whitebox naast het LSP mogelijk te maken, zowel in financiële zin (kosten gebruik en doorontwikkeling Whitebox door zorgverleners) als in operationele zin (ondersteuning).
- Definieer wat ZN wil doen om zorgverleners (huisartsen/apotheken) te ondersteunen als zij besluiten om de uitwisselingsgraad tussen zorgverleners proberen te verhogen door voor de betreffende groep burgers een alternatief aan te bieden.
- Definieer wat ZN wil doen om IT-leveranciers te ondersteunen bij het aanpassen van hun XIS aan een alternatieve vorm van gegevensuitwisseling.
- Definieer de aan het gebruik van een open koppelvlak te stellen eisen. Whitebox Systems en andere hierop aansluitende systemen moeten immers wel aantoonbaar aan gangbare vereisten voldoen.



MANAGEMENTSAMENVATTING (4)

Wat is het handelingsperspectief van Zorgverzekeraars Nederland inzake Whitebox? (vervolg)

- Ga na of en zo ja welke mogelijkheden er bestaan voor samenwerking tussen Whitebox en VZVZ om één – voor de zorgverlener gebruiksvriendelijke – oplossing te creëren die de voordelen van het LSP en Whitebox bundelt. Whitebox Systems heeft aangegeven voornemens te zijn om alle elementen van het gebruikte protocol: APIs, URL definities, et cetera, alsmede de APIs voor de identity management componenten te beschrijven in open standaard documenten, mogelijk deels voorzien van een (voorbeeld) code.
- Overweeg een proeftuin in de regio Amsterdam om de werkbaarheid in de praktijk te toetsen, waarin meerdere uitwisselingsscenario's naast huisarts-huisartsenpost worden meegenomen.

Ons advies is om een generiek open koppelvlak dat één-op-één te gebruiken is en ook in zijn algemeenheid bijdraagt aan een betere ontsluiting en interoperabiliteit, naast het LSP te positioneren. Whitebox kan daar dan gebruik van maken. Burgers die bewust afzien van het gebruik van het LSP – vanwege een gebrek aan fijnmazige toestemming of vanwege het vertrouwensmodel van het LSP – krijgen met Whitebox een alternatief dat aan deze bezwaren tegemoet komt. Dat zal bij een groep burgers een belemmering wegnemen voor het uitwisselen van gegevens tussen zorgverleners. Een combinatie van beide oplossingen zou voor de opvragende partij zoveel mogelijk 'onder water' moeten gebeuren, dus bij het opvragen geen extra handelingen moeten opleveren in het zorgproces.

Hierna worden de onderzoeksvragen beantwoord en bieden we een samenvattende analyse van het LSP en Whitebox vanuit het oogpunt van privacy en security. Voordat wij ingaan op de specifieke onderzoeksvragen, gaan we eerst in op de generieke context, mede omdat dit inzicht biedt in de behoefte aan een alternatieve vorm van gegevensuitwisseling.

Dit rapport wordt afgesloten met een toelichting van Whitebox Systems op de uitgangspunten, en een analyse vanuit Whitebox Systems voor extra kosten om een open koppeling Whitebox-breed in Nederland neer te zetten.



INHOUDSOPGAVE

*De WeDoTrust contact-
personen voor dit rapport:*

Hans Donkers

Partner

Tel: +316 53754323
hansdonkers@wedotrust.nl

Jan de Boer

Partner

Tel: +31651546750
jandeboer@wedotrust.nl

Verder betrokken:

Sape Mullender

Tel: +31615850510
samullen@cisco.nl

Brian Peters

Tel: +31653796930
brianpeters@wedotrust.nl

Pagina

Managementsamenvatting

• Onderzoeksvraag	8
• Achtergrond gegevensuitwisseling	9
• Beantwoording onderzoeksvraag	14
• Whitebox concept en praktijk	23
• Het LSP concept en praktijk	28
• Investeren in Whitebox naast het LSP	33



ONDERZOEKSVRAAG

Zorgverzekeraars Nederland heeft ons begin 2019 opdracht gegeven tot een onafhankelijk onderzoek naar de oplossing van Whitebox Systems in vergelijking met het LSP voor de uitwisseling van gegevens in de zorg. Deze onderzoeksvraag betreft:

1) Het doel van het uit te voeren onderzoek is te komen tot een objectieve vergelijking tussen de bestaande systemen voor de zorg, in elk geval het LSP en Whitebox; wat zijn de (onderscheidende) eigenschappen van beide systemen, waarin verschillen zij en welke voor- en nadelen kennen beide?

2) Tevens hebben we gekeken hoe informatie-uitwisseling via Whitebox en het LSP mogelijk is, om een indicatie te verkrijgen wat het voor inspanning van wie gaat kosten als beide systemen geïmplementeerd moeten worden in de zorg, en/of wanneer systemen op elkaar aangesloten moeten worden (wanneer dit technisch kan), met behoud van onderscheidende eigenschappen.

De kernvraag is of het concept van Whitebox daadwerkelijk iets toevoegt en zo ja, wat dan? Op basis van de verkregen inzichten wil Zorgverzekeraars Nederland een advies hoe te handelen. Moeten ze:

- Niets doen. Het concept van Whitebox voegt onvoldoende toe*
- Het concept van het LSP aanpassen? Wat is de impact?*
- Of moeten ze zorgverleners de keuze geven: Het LSP of Whitebox? En wat betekent dat?*
- Of moeten we stoppen met het LSP en over schakelen op Whitebox*

Wij voegen hier een variant aan toe: Of moeten ze zorgverleners de keuze geven het LSP en Whitebox naast elkaar te gebruiken?

Voordat wij ingaan op deze specifieke onderzoeksvraag, gaan we eerst in op de generieke context, mede omdat dit inzicht biedt in de behoefte aan een alternatieve vorm van gegevensuitwisseling.

Een analyse van de vraag hoe groot de groep burgers is voor wie er naast het LSP alternatieven wenselijk zijn, valt buiten de scope van het onderzoek.



ACHTERGROND GEGEVENSUITWISSELING

Gegevensuitwisseling tussen zorgverleners als basis voor goede en toekomstvaste zorg

Patiënten staan veelal niet onder behandeling bij één zorgaanbieder. Daarom is het essentieel om op betrouwbare en soepele wijze digitaal gegevens te kunnen uitwisselen, bijvoorbeeld tussen huisarts en huisartsenpost of tussen huisarts(enpost) en apotheek.

Het belang daarvan groeit onder invloed van een veranderend zorglandschap. De patiënt bouwt daarbij steeds meer een netwerk van professionals (en/of mantelzorgers) om zich heen en dat functioneert alleen als er sprake is van naadloze uitwisseling van gegevens. In algemene zin geldt: betere informatie leidt tot betere inzichten en daarmee ook tot betere (beslissingen in de) zorg.

Er is momenteel dan ook veel aandacht voor landelijke standaarden (informatiestandaarden en ZIB's) en het wettelijk verplichtstellen daarvan. Voor gestructureerde gegevensuitwisseling moeten zowel verzender als ontvanger aan standaarden voldoen. Er staat dan ook veel op het spel: een soepele gegevensuitwisseling is een make-or-break-factor voor het zorglandschap van de toekomst.

De voordelen zijn evident:

- We kunnen patiënten een naadloze uitwisseling van gegevens bieden zodat ze niet meerdere keren een identiek verhaal hoeven te vertellen of meerdere keren een formulier met dezelfde gegevens hoeven in te vullen;
- We kunnen de zorg (veel) efficiënter organiseren door de digitale overdracht van gegevens tussen patiënten, zorgverleners en instellingen te verbeteren;
- We kunnen voorkomen dat patiënten verkeerde diagnoses of behandelingen krijgen – met potentieel dramatische gevolgen – omdat er bij de overdracht wat mis ging in de informatievoorziening.

Belang van privacy en security

Privacy in de zorg is een belangrijk thema, het gaat immers juist in de zorg vaak om gevoelige gegevens. Elk individu heeft hierover andere ideeën. De een is terughoudend in het delen van informatie, de ander juicht informatiedeling juist toe vanuit de gedachte dat dit leidt tot meer gemak en een betere behandeling. Een aanpalend thema is security. Sommigen vinden de inzet van het best beschikbare/breed beschikbare hulpmiddel afdoende. Anderen stellen dat dit niet voldoende is, begrijpen het niet, of kunnen de argumenten niet op waarde beoordelen.



ACHTERGROND GEGEVENSUITWISSELING (2)

Belang van privacy en security (vervolg)

In de huidige discussies rondom privacy en security lopen ratio en gevoel door elkaar. Dat gevoel wordt ook beïnvloed door (media-aandacht voor) incidenten. Het vraagt veel tact en doorzettingsvermogen om te bouwen aan het noodzakelijke vertrouwen, maar het kan met een incident ook weer snel verloren gaan. Dit beïnvloedt de vooruitgang in gegevensuitwisseling in de zorg.

Hoofdvormen uitwisseling gegevens

In Nederland kennen we twee hoofdvormen van gegevensuitwisseling in de zorg:

- **Pull communicatie.** Eén of meerdere bronsystemen stellen gegevens beschikbaar aan groepen zorgverleners in bepaalde regio's, of landelijk. Het LSP en de XDS-systemen zijn representanten hiervan. Geauthentiseerde zorgverleners kunnen via het LSP gegevens opvragen indien de zorgaanbieders hiervoor zijn geautoriseerd. Autorisatie is gecentraliseerd.
- **Push communicatie.** In deze vorm sturen zorgverleners statische berichten naar zorgverleners of naar burgers. Voorbeelden zijn Edifact berichtenverkeer, Zorgmail of beveiligde mail. Maar ook XDS en het LSP bieden deze functionaliteiten.

Whitebox introduceert een derde variant: **indexloze push autorisatie**.

Wat is indexloze push autorisatie?

Push autorisatie zit tussen push en pull communicatie in. Het gaat niet om het sturen van berichten, maar om het sturen van autorisaties naar zorgverleners of zorgaanbieders. Zij kunnen daarmee (delen van) een brondossier en/of een vooraf vastgelegd bericht direct opvragen bij de bron. Brondossiers - zoals het dossier van de huisarts - kunnen via deze push autorisaties worden verbonden, zodat een - decentraal - 'netwerk van toegang' rondom de patiënt ontstaat. Daarover kunnen berichten door geautoriseerde zorgverleners zowel worden opgehaald als verstuurd. De autorisatietechniek werkt via linkjes (URL's) die op verschillende manieren verstuurd kunnen worden. Huisartsen kunnen dit bijvoorbeeld doen als onderdeel van een recept of een (elektronische) verwijsbrief.

Een systeem dat een autorisatie ontvangt, zal die wel ergens in diens database moeten opslaan. Dat zou een index of een tabel genoemd kunnen worden. Het verschil met een centrale index is dat die gebruikt wordt door meerdere zorgaanbieders om patiënten en patiëntgegevens mee te kunnen opzoeken. Er is ook geen centrale/externe infrastructuur nodig of een verantwoordelijke die gegevens van personen verwerkt of ontsluit.



ACHTERGROND GEGEVENSUITWISSELING (3)

Geen alternatieven voor groep weigeraars

Uitwisseling via het LSP mag alleen na toestemming van een patiënt. De opt-in ten aanzien van het geven van toestemming blijft in sommige regio's of groepen (huisartsen) achter. Huisartsen spelen een belangrijke rol in het verhogen van deze opt-in. Er is ook een groep die nooit bij een zorgaanbieder komt en niet eens weet dat er al dan niet toestemming kan/moet worden gegeven.

Maar welke alternatieven heeft een burger in Nederland die geen toestemming geeft en/of bezwaren of zorgen heeft ten aanzien van de huidige LSP-oplossing? De vraag hoe groot deze groep is, valt buiten de scope van dit onderzoek. Maar wij kunnen hierover wel de volgende opmerkingen maken:

Opt-in LSP

VZVZ publiceert de opt-in percentages. De apothekerspercentages liggen gemiddeld rond 80%, de huisartspercentages liggen lager, gemiddeld rond 40%. Er zijn regionale verschillen. In Amsterdam ligt het opt-in percentage voor huisartsen rond 10%.

Enquête CBS

Uit het 'Onderzoek Belevingen 2018' van het CBS kwam naar voren dat van de 80% van de geënquêteerde volwassenen die bekend is met het LSP, de meerderheid (6 op de 10) zegt ook toestemming te hebben verleend voor het delen van medische gegevens via dit netwerk. 14% zegt geen toestemming te hebben verleend voor het delen van medische gegevens via het LSP, en een kwart weet het niet of wil het niet zeggen. Van de volwassenen die aangeven geen toestemming te geven voor het delen van medische gegevens via het LSP, zegt een deel (76%) nooit om toestemming daarvoor gevraagd te zijn. De overige 24% heeft toestemming geweigerd na daarom gevraagd te zijn. Omgerekend geven de onderzoekers aan dat dit 5% van de volwassen bevolking is.

Nader onderzoek

Er is een groep burgers die bezwaar heeft tegen de (mogelijkheid) tot bredere uitwisseling van gegevens en landelijke voorzieningen. Een deel van de Nederlands burgers geeft geen toestemming en wil geen uitwisseling via het LSP. Nader onderzoek zou verder inzicht moeten geven in (1) de omvang van deze groep en (2) de vraag of ze wel of anders toestemming zouden geven als het ging om een oplossing als Whitebox.



ACHTERGROND GEGEVENSUITWISSELING (4)

Gespecificeerde Toestemming Structureel (GTS) en Online ToestemmingsVoorziening (OTV)

Alleen met toestemming van de patiënt kunnen gegevens door een zorginstelling beschikbaar worden gesteld aan een groep op voorhand niet bekende zorgaanbieders. Dat is vastgelegd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabgz). Binnen het programma GTS werken koepelorganisaties van zorgverleners en patiëntenfederatie Nederland aan een praktische oplossing voor het online vastleggen en beheren van deze toestemmingen. Deze gespecificeerde toestemming geldt dus alleen voor die situaties waarin gegevens beschikbaar worden gesteld aan een groep op voorhand niet bekende zorgaanbieders of op voorhand niet bekend gebruik.

De stuurgroep GTS concludeerde in december 2018 dat de huidige uitwerking van de wet juridisch en technisch passend is, maar onvoldoende werkbaar en uitvoerbaar is voor burgers, patiënten en zorgaanbieders. Dit is ook de uitkomst van een oriëntatie onder patiënten. Patiënten geven aan regie te willen voeren op de uitwisseling van hun gegevens, maar schrikken van het grote aantal toestemmingsmogelijkheden. Als belangrijkste adoptiefactoren worden overzicht van toestemmingsmogelijkheden en laagdrempelig gebruik genoemd. De stuurgroep GTS heeft de opdracht om een effectieve manier om toestemming te geven te onderzoeken, teruggegeven aan de minister.

Parallel aan GTS wordt gewerkt aan een Online ToestemmingsVoorziening (OTV). Het gaat hier om een portaal dat het burgers gemakkelijker moet maken om zelf toestemmingen vast te leggen en te beheren. Zorgaanbieders kunnen dan op één plek de toestemmingskeuzes controleren. De uitwerking van OTV is nog volop onder handen en is niet publiek beschikbaar.

Uit de beschikbare informatie komt naar voren dat kenmerkend voor de OTV-oplossing is dat op basis van een categorie zorgaanbieders toestemming wordt verleend en dat voor het opvragen algemene regels gelden. De patiënt bepaalt zelf aan welk type zorgaanbieder zijn/haar gegevens beschikbaar worden gesteld.

De patiënt kan daarbij (bepaalde categorieën) uitsluiten en krijgt daarmee meer regie over de gegevensuitwisseling. De zorgverlener krijgt de mogelijkheid om dit voor de patiënt te doen. OTV krijgt een separate toestemmingsmogelijkheid 'Spoedzorg'.

Indien gegevens alléén bij spoedzorg gedeeld mogen worden, dan kan dat hier worden aangegeven. OTV voorziet in 28 'vinkjes'; bij de adviescommissie Toetsing regeldruk bestaat twijfel over de toepasbaarheid en rechtmatigheid van dit gereduceerde aantal toestemmingsmogelijkheden.



ACHTERGROND GEGEVENSUITWISSELING (5)

Gespecificeerde Toestemming Structureel (GTS) en Online ToestemmingsVoorziening (OTV) (vervolg)

OTV dwingt geen logische toegangsbeveiliging af, indien er geen toestemming wordt gegeven, wordt toegang niet geblokkeerd. VZVZ geeft aan dat uitsluitingen of insluitingen voor opvragende partijen (zoals bij Whitebox) geen onderdeel vormen van OTV.

Met de invoering van OTV zal verdere specificatie van toestemming straks ook door het LSP worden aangeboden.

De minister heeft in een recente brief (d.d. 4 oktober 2019) aan de Tweede Kamer aangegeven dat de inwerkingtreding van artikel 15a, lid 2 van de Wabvpz op 1 juli 2020 niet haalbaar is. Hij heeft aangegeven in de eerste helft van 2020 de Kamer een voorstel te doen voor de herijking van de invoering van gespecificeerde toestemming op basis van de in de desbetreffende brief genoemde adviezen.

Hij geeft in deze brief ook aan dat hij 'streeft naar gegevensuitwisseling die bij voorkeur de zorg zelf volgt en niet werkt met beschikbaarheidsstelling vooraf' en dat hij wil dat 'er zoveel mogelijk gezocht wordt naar een (infrastructurele) oplossing voor gegevensuitwisseling wanneer nodig', waarbij de handelrelatie volgens de WGBO de basis vormt. Whitebox Systems stelt dat hun oplossing aan deze wens voldoet.

De minister gaat tegelijkertijd verder met het zoeken naar een oplossing voor uitwisseling van informatie via een elektronisch uitwisselingssysteem specifiek voor spoedzorg. Hij geeft aan hier aan het eind van dit jaar op terug te komen.

VZVZ geeft aan dat OTV begin 2020 operationeel zal zijn.



BEANTWOORDING ONDERZOEKSVRAAG

Het doel van het uit te voeren onderzoek is te komen tot een objectieve vergelijking tussen de bestaande systemen voor de zorg, in elk geval het LSP en Whitebox; wat zijn de (onderscheidende) eigenschappen van beide systemen, waarin verschillen zij en welke voor- en nadelen kennen beide?

- Het LSP is een infrastructuur waarmee zorgverleners (in principe landelijk) onderling medische gegevens kunnen uitwisselen. Bij de (door)ontwikkeling van de infrastructuur zijn de behoeften uit het zorgveld (LHV, KNMP, NVZ, Ineen e.a.) meegenomen. Uitwisseling vindt plaats via een beveiligd, los van het internet staand, Nederlands netwerk (de AORTA-zorginfrastructuur). Alleen zorgverleners met gebruik van een sterk identificatiemiddel (de UZI-pas) hebben toegang. VZVZ voldoet aan alle wettelijke vereisten en een grote groep burgers heeft toestemming gegeven voor uitwisseling via het LSP.
- Whitebox biedt zonder index-gebaseerde (centrale) systemen de mogelijkheid om op basis van fijnmazige, technisch afgedwongen decentrale toegangsverlening beveiligd gegevens uit te wisselen tussen zorgverleners die direct bij iemands behandeling betrokken zijn.

Puntsgewijs zijn hierna de belangrijkste eigenschappen van beide omgevingen weergegeven.

Karakteristieken organisatie en scope ondersteunde uitwisselingen

	VZVZ/LSP		Whitebox Systems/Whitebox	
	Functionaliteit	Voordeel/nadelen	Functionaliteit	Voordeel/nadelen
Organisatie	Staande organisatie		Start-up	
Mate waarin aantoonbaar wordt voldaan aan beveiligingskwalificaties	De organisatie voldoet aantoonbaar aan de beveiligingskwalificatie voor het beveiligd en vertrouwd uitwisselen van medische gegevens conform wettelijke vereisten.	Voldoet aantoonbaar aan beveiligingskwalificaties.	De organisatie beschikt nog niet over externe kwalificaties.	Moet nog inspanningen verrichten om aantoonbaar te voldoen.
Aantallen en aard ondersteunde zorgaanbieders	Apotheek, Huisarts, GGZ, JGZ, Lab, VG instelling, VVT, ziekenhuis, zorggroep etc.	Ruime en brede operationele toepassing oplossing.	Operationeel bij huisartsen en huisartsenposten in specifieke regio's. In pilot bij 1 apotheek (wordt niet door leverancier ondersteund).	Moet nog operationeel opschalen in aantal en aard ondersteunde zorgaanbieders.
Type en formaten patiënt die worden ondersteund	Professionele samenvatting, ICA en medicatiegegevens worden grootschalig gebuikt. Pilots operationeel voor veel gegevensdiensten op uitbreiding datasets.	Professionele samenvatting, ICA en medicatiegegevens grootschalig toegepast.	Standaard informatieset, professionele samenvatting (verschillende varianten), medicatiegegevens. Additioneel vrij te definiëren sets: ook mogelijkheden voor delen van complete dossiers, PDF of beelden.	Delen van vrij te definiëren sets en beelden wordt ondersteund.
Aangesloten XIS-leveranciers	Alle XIS-leveranciers betrokken bij uitwisseling, zijn aangesloten.	Ruime en brede ondersteuning XIS-leveranciers.	Enkele HIS- en HAP-leveranciers kunnen met Whitebox uitwisselen.	Nog lage dekkingsgraad ondersteuning XIS-leveranciers.



BEANTWOORDING ONDERZOEKSVRAAG (2)

Beveiligingsconcept

	VZVZ/LSP		Whitebox Systems/Whitebox	
	Functionaliteit	Voordeel/nadelen	Functionaliteit	Voordeel/nadelen
Beveiliging data tijdens transport	Het LSP vereist in de aansluitvoorwaarden dat de opvragende partij gebruik maakt van gecertificeerde netwerkverbindingen (Goed Beheerd Zorgnetwerk). De afzonderlijke berichten die over de beveiligde verbinding worden verstuurd/uitgewisseld, worden niet aanvullend 'dubbel' beveiligd. Uitwisseling vindt plaats via dit beveiligde, los van het internet staande, netwerk (de AORTA-zorginfrastructuur), waartoe alleen zorgverleners met gebruik van een sterk identificatiemiddel (de UZI-pas) toegang hebben.	Gesloten omgeving, beperkte mogelijkheid voor ongeautoriseerde toegang.	Er worden geen eisen gesteld aan de wijze van transport, dit kan via internet. De individuele berichten worden versleuteld en zijn beveiligd tijdens het gehele transport (end-to-end), ook bij eventuele compromittering van het netwerk waarover de berichten worden getransporteerd.	End-to-end versleuteling van een bericht maakt oplossing niet afhankelijk van de kwaliteit van de beveiliging van datanetwerken. Tevens is de oplossing in theorie schaalbaar buiten de Nederlandse grens (geen fysieke netwerkbeperkingen).
Beveiliging gekoppelde systemen zorgverleners	Het LSP vereist in de aansluitvoorwaarden dat de opvragende partij gebruik maakt van een gecertificeerd Goed Beheerd Zorgsysteem (GBZ).	Alleen op beveiligde, gecertificeerde systemen worden aangesloten.	Whitebox stelt geen eisen aan omgeving opvragende partij, gaat uit van wettelijk verplichte normeringen (o.a. NEN7510).	Geen eisen aan beveiliging systemen opvragende partijen, anders dan wettelijke regels.
Vertrouwensmodel	Uitwisseling op basis van vertrouwensmodel. Zorgverleners zijn alleen bevoegd de gegevens op te vragen als zij een behandelrelatie hebben en dit nodig is voor de behandeling. Zij kunnen echter 'technisch gezien' gegevens opvragen, ook als er geen sprake is van een behandelrelatie.	Burger kan via 'volgmijnzorg' zien welke gegevensuitwisselingen hebben plaatsgevonden.	Uitwisseling op expliciet autorisatie (insluiten). Whitebox staat opvragen toe op het moment dat een expliciet autorisatie is verstrekt. Zorgverleners kunnen geen opvragen doen op het moment dat op basis van de behandelrelatie geen expliciete autorisatie is verstrekt.	Technische controle toestemming voordat informatie wordt uitgewisseld, geen centraal inzicht voor burger op uitwisseling die heeft plaatsgevonden. Mogelijk via portaal (beperkt operationeel) of mogelijk PGO (toekomst).
Gradualiteit beveiliging	De samenvatting uit het huisartsdossier is voor de waarnemend huisarts beschikbaar. De medicatieverstrekkingsinformatie van apotheken en ICA-gegevens zijn ook landelijk toegankelijk voor ziekenhuizen. Een patiënt kan een zorgverlener vragen om (een deel van) de gegevens uit zijn dossier bij de bron af te schermen. De mogelijkheden hiertoe worden mede bepaald door de functionaliteit in het HIS.	Centraal inzicht in toegekende autorisaties. Beperkte gradualiteit mogelijk, de autorisatie wordt beperkt technisch afgedwongen.	De zorgverlener bepaalt in de behandelrelatie samen met de patiënt welke andere zorgaanbieder(s) een samenvatting uit het huisartsdossier en/of medicatie gegevens mogen inzien. De zorgverlener is samen met de patiënt in control om te bepalen welke gegevens worden verstrekt. Zorgverlener kan afhankelijk van het HIS fijnmazig de datasets bepalen die wordt gedeeld en de zorgverleners waarmee de informatie wordt gedeeld.	Patiëntportaal dat inzicht in toegekende autorisaties /toestemmingen per zorgaanbieder gaat bieden is beperkt operationeel. Hoge mate van gradualiteit mogelijk die autorisatietechnisch wordt afgedwongen. Toekomst: huisarts medicatie-overzicht ook landelijk te delen (spoed, verwijzing), mits geautoriseerd (push autorisatie).
Bewerking van gegevens	In steeds meer gevallen treedt het LSP op als intermediair om 'vertalingen' uit te voeren tussen zorgaanbieders die nog niet op dezelfde versie van de uitwisselingsstandaard zitten. De beveiligingsprocessen zijn gecertificeerd.	De gecertificeerde beveiligingsprocessen waarborgen ongeautoriseerde toegang tijdens de bewerking van de gegevens.	Whitebox Systems kent uitsluitend decentrale autorisaties en verwerking van persoonsgegevens. Er is dus geen sprake van centrale bewerking van persoonsgegevens.	Geen externe bewerking van persoonsgegevens, daardoor geen beveiligingsrisico tijdens bewerking.



BEANTWOORDING ONDERZOEKSVRAAG (3)

Traceerbaarheid mutaties in toestemming/uitwisselingen

	VZVZ/LSP		Whitebox Systems/Whitebox	
	Functionaliteit	Voordeel/nadelen	Functionaliteit	Voordeel/nadelen
Traceerbaarheid van mutaties in toestemmingen	Het LSP registreert (mutaties) in toegekende verleende toestemmingen per zorgaanbieder/soort gegevens landelijk.	Centraal inzicht voor burger (in mutaties) in geregistreerde toestemmingen.	Via patiëntportaal kan per zorgaanbieder worden ingezien welke toestemming is verleend op het dossier van de huisarts en wie gegevens heeft opgevraagd/ingezien.	Decentraal inzicht voor burger (in mutaties) in geregistreerde toestemmingen.
Traceerbaarheid van informatie-uitwisselingen	Het LSP registreert voor de patiënt welke zorgaanbieders welke soort gegevens hebben uitgewisseld. Dit geschiedt landelijk.	Centraal inzicht voor burger in uitwisselingen.	Whitebox Systems geeft aan dat Patiëntportaal/App in de toekomst wordt uitgebreid met functionaliteit om informatie-uitwisselingen van meerdere bronnen te raadplegen.	Nog geen centraal inzicht voor burger in uitwisselingen via patiëntportaal.
Toegankelijkheid audit-trail voor patiënt	Zowel de toegekende toestemmingen als de informatie-uitwisselingen zijn toegankelijk voor de patiënt, indien gewenst met actieve signalering bij gebruik.	Toestemmingen en uitwisselingen zijn centraal raadpleegbaar voor de patiënt.	Het patiëntportaal is een nieuwe ontwikkeling en wordt nog niet structureel in de praktijk toegepast. Whitebox Systems geeft aan dat een app is gepland.	Patiëntportaal met decentraal inzicht beperkt operationeel.

Betrouwbaarheid gegevensuitwisselingen

	VZVZ/LSP		Whitebox Systems/Whitebox	
	Functionaliteit	Voordeel/nadelen	Functionaliteit	Voordeel/nadelen
Betrouwbaarheid id	De zorgaanbieder dient te beschikken over en een Goed Beheerd Zorgsysteem (GBZ) gericht op het waarborgen dat beheersmaatregelen zijn getroffen waarmee wordt voorkomen dat gegevens verloren gaan of op cruciale momenten niet toegankelijk zijn voor uitwisseling.	Aansluitingscriteria waarborgen minimale beveiliging omgeving zorgaanbieder.	Whitebox Systems stelt geen eisen aan de betrouwbaarheid en beveiliging van HIS bij de zorgaanbieder anders anders dan wettelijke eisen.	Geen eisen aan beveiliging zorgsysteem, anders dan wettelijke regels.
Betrouwbaarheid netwerk	Uitwisseling via AORTA-zorginfrastructuur. De zorgaanbieder dient te beschikken over en een Goed Beheerd Zorgnetwerk (GZN) gericht op het waarborgen van een goede en veilige communicatie.	Aansluitingscriteria met waarborgen beschikbaarheid zorgnetwerk.	Whitebox Systems stelt geen eisen aan de betrouwbaarheid en beveiliging van het netwerk waarover de uitwisseling gaat plaatsvinden bij de zorgaanbieder.	Geen eisen beschikbaarheid netwerk, anders dan wettelijke regels.
Monitoring	Centrale monitoring op beschikbaarheid vanuit gecertificeerde processen vanuit centrale beheerorganisatie.	Centrale monitoring op basis van gecertificeerde processen.	Whitebox Systems is een start-up organisatie. De bewaking op beschikbaarheid infrastructuur is inmiddels vormgegeven, de processen zijn nog niet gecertificeerd.	Processen voor bewaking zijn (nog) niet geformaliseerd in een SLA en ingebed in gecertificeerde processen.

Schaalbaarheid

	VZVZ/LSP		Whitebox Systems/Whitebox	
	Functionaliteit	Voordeel/nadelen	Functionaliteit	Voordeel/nadelen
Technische schaalbare architectuur qua volumes	De LSP-infrastructuur heeft zich bewezen in de verwerking van hoge volumes aan berichten. De huidige berichtensets (naast huidige 2), nieuwe berichten soorten (bv beeld), opschaling gebruik door zorgaanbieders.	Infrastructuur heeft zich bewezen met grote transactievolumes.	De infrastructuur van Whitebox Systems heeft een decentraal karakter. Hierdoor zullen de volumes voor de infrastructuur per individuele zorgaanbieder beperkt blijven.	Beperkte volumes door decentrale karakter.
Schaalbare regie-organisatie	De LSP-infrastructuur wordt beheerd door een volwassen beheerorganisatie die reeds jaren de infrastructuur landelijk beheert.	Volwassen beheerorganisatie.	Whitebox Systems is een start-up organisatie met een beperkte omvang. Voor een landelijke dekking is een opschaling en een verdere professionalisering van de beheerorganisatie cruciaal.	Verdere professionalisering van de beheerorganisatie is cruciaal.



BEANTWOORDING ONDERZOEKSVRAAG (4)

Eenvoud van implementatie voor zorgverleners

	VZVZ/LSP		Whitebox Systems/Whitebox	
	Functionaliteit	Voordeel/nadelen	Functionaliteit	Voordeel/nadelen
Eenvoud gebruik authenticatie middelen opvragende partijen	De zorgaanbieder dient te beschikken over UZI-middelen: een UZI-servercertificaat en een UZI-zorgverlenerpas.		De zorgaanbieder dient te beschikken over een UZI-zorgverlenerpas.	Geen beheerisen aan infrastructuur zorgaanbieder.
Eenvoud mandatering toegang bij opvragende partijen (Apotheken, Huisartsenposten en ziekenhuizen)	De zorgaanbieder hoeft geen identity (autorisatie) management in te richten voor het beheer van de autorisaties vergt ook minder beheer. tot het LSP voor medewerkers met UZI-middelen op naam.	Minder gradualiteit in autorisatie management	Een zorgaanbieder in de rol van opvragende partij (bijvoorbeeld een Huisartsenpost) moet (behalve bij gebruik van een web browser) de zorgverleners registreren in een (Whitebox) identity management systeem voordat zij toegang kunnen krijgen.	Beheer inspanning is mede afhankelijk van gewenste gradualiteit in toegangsrestricties.
Eenvoud integratie HIS bij opvragende partijen	Het LSP heeft hoge adoptiegraad bij de leveranciers van HIS-systemen, hetgeen de integratie vereenvoudigt.	Hoge adoptiegraad HIS-systemen.	Whitebox is een start-up met beperkte adoptiegraad bij de leveranciers van HIS-systemen. Open standaard en financiering van niet vendor-specifieke (open) koppelvlakken zijn cruciaal om adoptiegraad te realiseren.	Beperkte adoptiegraad HIS-systemen.

Voorzieningen voor ongeplande (spoed) zorg

	VZVZ/LSP		Whitebox Systems/Whitebox	
	Functionaliteit	Voordeel/nadelen	Functionaliteit	Voordeel/nadelen
Gegevensset beschikbaar in geval ongeplande (spoed) zorg	De samenvatting uit het huisartsdossier is voor de waarnemend huisarts (HAP) beschikbaar. De medicatieverstrekkingsinformatie van apotheken en ICA-gegevens zijn ook landelijk toegankelijk voor HAP en ziekenhuizen. Een patiënt kan een zorgverlener vragen om (een deel van) de gegevens uit zijn dossier bij de bron af te schermen, ook bij spoed is daar dan geen toegang toe.	Standaard gegevensset beschikbaar.	Op de HAP is een professionele samenvatting beschikbaar. Bij gebruik van een spoedvoorziening buiten de HAP zijn medicatie, ICA en mogelijk een (beperkte) episodielijst uit het huisartsdossier beschikbaar. Een patiënt kan een zorgverlener vragen om (een deel van) de gegevens uit zijn dossier bij de bron af te schermen, ook bij spoed is daar dan geen toegang toe.	Standaard gegevensset beschikbaar. Mogelijkheid om aanvullende gegevens uit te wisselen.
Voor wie zijn gegevens beschikbaar in geval ongeplande (spoed) zorg	Indien de patiënt toestemming heeft gegeven voor uitwisseling via het LSP, zijn de gegevens beschikbaar voor de HAP aan wie toestemming is verstrekt (eigen regio) en landelijk ziekenhuizen (inclusief SEH) die zijn aangesloten bij het LSP.	Indien vooraf toestemming is gegeven voor uitwisseling via het LSP, zijn mediatie en ICA-gegevens breed beschikbaar. PS beperkt tot huisartsen in regio's waar toestemming voor is gegeven.	Gegevens zijn beschikbaar voor partijen waar vooraf toestemming aan is gegeven en waarmee een technische koppeling bestaat. En daarnaast voor partijen die beschikken over technische mogelijkheden om zich te authenticeren om gegevens in te zien (voorbeeld: web browser en UZI pas).	Mogelijkheid om toegang te geven tot gegevens. Gebruikersvriendelijkheid en gebruiksgemak vergt, afhankelijk van mate van integratie, aandacht.
Voorzieningen als vooraf geen toestemming voor uitwisseling is gegeven/ingericht	Procedure aanwezig om alsnog toestemming te geven voor uitwisseling.	Geen alternatief als geen toestemming wordt verleend.	Mogelijkheden om uit te wisselen, deels beschikbaar maar nog niet in gebruik en niet direct geschikt voor opschaling.	Uitwisseling mogelijk indien dit in het belang van de patiënt is.



BEANTWOORDING ONDERZOEKSVRAAG (5)

Welke inspanningen zijn er nodig om beide systemen naast elkaar te gebruiken en/of wanneer op elkaar aan te sluiten (wanneer dit technisch kan), met behoud van onderscheidende eigenschappen?

De conclusies over toepasbaarheid:

- Whitebox kan het LSP niet op korte termijn vervangen voor alle burgers. Daarvoor is het aantal beschikbare koppelingen/ uitwisselingstoepassingen nog te beperkt.
- Het is niet noodzakelijk te kiezen tussen het LSP of Whitebox, technisch gezien kunnen beide naast elkaar draaien. Uitwisselende systemen moeten hiervoor wel worden aangepast.
- Om burgers een keuze te bieden tussen het LSP en een alternatief als Whitebox, is het nodig dat bronhouders (huisartsen en apothekers) uitwisseling mogelijk maken via zowel het LSP als Whitebox en de keuze aan de burger aanbieden.
- Huidige implementaties in Tetra en MicroHIS laten zien dat LSP- en Whitebox-aanmeldingsopties elkaar niet in de weg zitten en aan de opvragende kant (Topicus HAP en Call manager) ook niet.
- Bij de afweging kan niet voorbij worden gegaan aan het feit dat de uitwisselingsmogelijkheden dubbel moeten worden uitgevoerd. Een zorgverlener moet beide aansluitingen hebben. Daarnaast moet voor beide alternatieven (onafhankelijk van elkaar of in samenhang) worden gespecificeerd, ontwikkeld en afgestemd. Er zullen afspraken gemaakt moeten worden hoe dit binnen en tussen governance structuren in te vullen. Om voor de gebruiker en zorgverlener gebruiksvriendelijke oplossingen te creëren, is nadere afstemming tussen VZVZ en Whitebox-systemen noodzakelijk.

De conclusies over inspanningen:

- Voor gebruik van Whitebox moet de bron (bijvoorbeeld huisarts) logisch of fysiek beschikken over een Whitebox of een met de push autorisatie standaard compatibele eigen implementatie van de standaard. Voor een efficiënte integratie moet de opvragende partij (bijvoorbeeld HAP) minimaal beschikken over een met Whitebox compatibel identity management systeem. Dit vergt een eenmalige investering en jaarlijkse licentiekosten.
- Het gebruik van Whitebox vraagt om aanpassingen aan uitwisselende systemen (zoals HIS en HAP) om gegevensstandaarden van/naar Whitebox te ontsluiten. Leveranciers moeten deze koppelingen bouwen en onderhouden.
- Invoering van Whitebox leidt niet tot verlaging van de kosten van het LSP. Dit rapport wordt afgesloten met een toelichting van Whitebox Systems op de uitgangspunten en analyse vanuit Whitebox Systems voor extra kosten om een open koppeling Whitebox-breed in Nederland neer te zetten.



BEANTWOORDING ONDERZOEKSVRAAG (6)

De conclusies over noodzakelijke doorontwikkeling Whitebox Systems en Whitebox

- De organisatie en het product Whitebox hebben de kenmerken van een start-up. Daarmee voldoet Whitebox in de huidige vorm nog niet aantoonbaar aan de te stellen eisen of aan het einddoel. Whitebox Systems heeft aangegeven de benodigde ontwikkelingen zelf te willen financieren.
- Het gaat daarbij om de volgende zaken:
 - In de huidige opzet van Whitebox beheert de zorgverlener (de huisarts) de toegang. Ook burgers kunnen zelf hun instellingen beheren via portaal (beperkt operationeel).
 - Burgers moeten in de toekomst eenvoudig en transparant inzicht krijgen in wie toegang heeft tot hun gegevens (gemaakte keuzes) en wie gegevens heeft opgevraagd. Deze functionaliteit is deels beschikbaar.
 - Uitbreiding van functionaliteiten/koppelingen in het Whitebox-product vraagt aanvullende inspanning van de Whitebox- organisatie.
 - Whitebox functioneert alleen als een bronsysteem gebruik maakt van de Whitebox en andere zorgverleners in de zorgketen (bijvoorbeeld HAP, SEH) Whitebox-autorisaties kunnen gebruiken. Bij lage volumes kunnen ontvangende partijen direct gebruik maken van ontvangen URL's via een viewer (in een browser), maar bij hogere volumes en voor integratie is een gestandaardiseerde koppeling nodig.
 - Een ontvangende partij moet een identity management systeem inrichten. Dit kan een stand-alone component zijn die Whitebox levert, maar ook een eigen implementatie op basis van de (open) Whitebox-standaard, bijvoorbeeld met gebruik van UZI-passen.
 - Opschaling vergt investeringen in marketing/verkoop om alle partijen in de zorgketen, burgers, zorgverleners en leveranciers van systemen te overtuigen en mee te krijgen. Dit vereist onder meer het inrichten van een 'verkoop'-organisatie bij Whitebox. Het ligt daarbij voor de hand te starten met een regionale aanpak zoals Whitebox nu ook doet.
 - Ook een oplossing als Whitebox vereist een volwassen beheer- en supportorganisatie inclusief monitoring van operationele verbindingen, die voldoet aan de gangbare security vereisten, die op efficiënte wijze een groot aantal gebruikers kan bedienen en die softwareleveranciers kan ondersteunen bij de afhandeling van incidenten en wijzigingen. Ook op dit vlak is een verdere ontwikkeling nodig.



BEANTWOORDING ONDERZOEKSVRAAG (7)

Voegt het concept van Whitebox daadwerkelijk iets toe, en zo ja, wat dan?

Conclusie

Whitebox voegt iets toe. Burgers die bewust afzien van het gebruik van het LSP – vanwege een gebrek aan fijnmazige toestemming of vanwege het vertrouwensmodel van het LSP – of die zorgen hebben over het gebruik hiervan krijgen met Whitebox een alternatief dat aan deze bezwaren tegemoet komt. Dat zal bij een groep burgers een belemmering wegnemen voor het uitwisselen van gegevens tussen zorgverleners.

Ons advies aan Zorgverzekeraars Nederland

In de onderzoeksvraag zijn al een aantal alternatieven benoemd hoe mogelijk te handelen indien Whitebox daadwerkelijk iets toevoegt. Nu wij vaststellen dat dit het geval is, adviseren wij een alternatief dat daar niet is benoemd: positioneer Whitebox, op basis van een generieke open koppeling tussen individuele systemen, naast het LSP.

Voorwaarde daarbij is dat ZN beleidsmatig de keuze maakt of zij een behoefte wil invullen voor een groep burgers die nu geen toestemming geeft voor gegevensuitwisseling via het LSP en ruimte wil bieden voor alternatieve oplossingen voor uitwisselingen tussen zorgverleners. Beleidsmatig vraagt voorgaande om afwegingen te maken op de volgende terreinen:

- Onderzoek hoe groot de doelgroep van 'weigeraars' is en of Whitebox voor hen daadwerkelijk een alternatief is.
- Onderzoek hoe de alternatieve generieke open koppeling voor ontsluiting ZIB's en andere courante berichtenformaten tussen individuele systemen kan worden vormgegeven.
- Definieer wat ZN wil doen om een generieke koppeling en Whitebox naast het LSP mogelijk te maken, zowel in financiële zin (kosten gebruik en doorontwikkeling Whitebox door zorgverleners) als in operationele zin (ondersteuning).
- Definieer wat ZN wil doen om zorgverleners (huisartsen/apotheken) te ondersteunen als zij besluiten om de uitwisselingsgraad tussen zorgverleners te verhogen door de betreffende groep burgers een alternatief aan te bieden.



BEANTWOORDING ONDERZOEKSVRAAG (8)

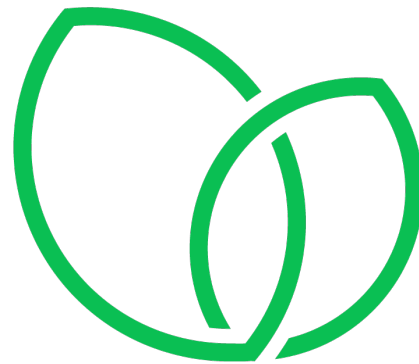
Ons advies aan Zorgverzekeraars Nederland (vervolg)

- Definieer wat ZN wil doen om IT-leveranciers te ondersteunen bij het aanpassen van hun XIS aan een alternatieve vorm van gegevensuitwisseling (al dan niet via een open koppelvlak).
- Definieer de aan het gebruik van een open koppelvlak te stellen eisen. Whitebox Systems en andere hierop aansluitende systemen moeten immers wel aantoonbaar aan gangbare vereisten voldoen.
- Ga na of en zo ja welke mogelijkheden er bestaan voor samenwerking tussen Whitebox en VZVZ om één – voor de zorgverlener gebruiksvriendelijke – oplossing te creëren die de voordelen van het LSP en Whitebox bundelt. Whitebox Systems heeft aangegeven voornemens te zijn om alle elementen van het gebruikte protocol: API's, URL definities, et cetera, alsmede de API's voor de identity management componenten te beschrijven in open standaard documenten, mogelijk deels voorzien van een (voorbeeld) code.
- Overweeg een proeftuin in de regio Amsterdam om de werkbaarheid in de praktijk te toetsen, waarin meerdere uitwisselingsscenario's naast huisarts-huisartsenpost worden meegenomen.

Ons advies is om een generiek open koppelvlak dat één-op-één te gebruiken is en ook in zijn algemeenheid bijdraagt aan een betere ontsluiting en interoperabiliteit, naast het LSP te positioneren. Whitebox kan daar dan gebruik van maken. Burgers die bewust afzien van het gebruik van het LSP – vanwege een gebrek aan fijnmazige toestemming of vanwege het vertrouwensmodel van het LSP – krijgen met Whitebox een alternatief dat aan deze bezwaren tegemoet komt. Dat zal bij een groep burgers een belemmering wegnemen voor het uitwisselen van gegevens tussen zorgverleners. Een combinatie van beide oplossingen zou voor de opvragende partij zoveel mogelijk 'onder water' moeten gebeuren, dus bij het opvragen geen extra handelingen moeten opleveren in het zorgproces.

Hierna geven we onze bevindingen rondom Whitebox en het LSP vanuit het oogpunt van privacy en security. Dit rapport wordt afgesloten met een toelichting van Whitebox Systems op de uitgangspunten en een analyse vanuit Whitebox Systems voor extra kosten om een open koppeling Whitebox-breed in Nederland neer te zetten.





DETAIL BEVINDINGEN

WHITEBOX: CONCEPT EN PRAKTIJK

Whitebox in een notendop

Whitebox is een systeem – hard- en software – voor een beveiligde één-op-één uitwisseling van patiëntgegevens tussen zorgverleners. De huisarts heeft een spilfunctie in deze uitwisseling en heeft de hardware die deze uitwisseling regelt – een witte doos – ook daadwerkelijk (fysiek) in beheer. De voordelen van deze benadering:

- Patiënt en/of arts hebben meer verfijnde controle over welke partij(en) bij gegevens kunnen;
- Het is mogelijk te traceren wie toegang is verleend (autorisatie) en wie deze daadwerkelijk neemt (opvragen van gegevens);
- End-to-end beveiliging (op basis van meerdere typen credentials) is mogelijk.

Whitebox is een relatief nieuwe en regionaal gebruikte oplossing. In de regio's Amsterdam en Maastricht wordt de Whitebox-implementatie van indexloze push autorisatie al enige tijd gebruikt in de context van huisartswaarneming.

Uitbreiding naar meerdere zorgverleners, in het bijzonder naar de apotheek en naar ketenzorg (KIS) vanuit de huisarts, wordt voorzien. Voor (bovenregionale) uitwisseling van gegevens zoals met SEH's is een oplossing ontwikkeld/geïmplementeerd, maar nog niet uitgerold.

Kernpunten concept Whitebox:

- Whitebox hanteert het concept indexloze push autorisatie. Het biedt daarmee decentrale controle (zowel technisch als beleidsmatig) over de toegang tot medische gegevens, ingesteld en uitgevoerd bij en door de arts en de patiënt zelf, bij voorkeur binnen het zorgproces door de brondossierhouder(s) zelf zodat de toegang niet groter wordt dan binnen dat proces nodig. De sleutel wordt bewaard door een beroepsgeheimhouder/arts.
- Whitebox baseert vertrouwen op de betrokkenheid van de huisarts/zorgverlener, techniek/software en fijnmazige toestemming. Dat is een verschil met het gangbare model waarin vertrouwen meer wordt gebouwd op procedures en afspraken. De indexloze push autorisatie speelt in op privacy-eisen en wensen van burgers die fijnmazig toegang tot hun gegevens willen regelen. Een potentieel voordeel van het decentrale concept van Whitebox is dat het systeem voor het gevoel 'dicht op de eigen zorgverleners zit' en geen landelijke voorzieningen nodig zijn (geen 'L van LSP'). Dat kan bij een bepaalde groep burgers een zorg wegnemen en vertrouwen wekken.



WHITEBOX: CONCEPT EN PRAKTIJK (2)

- Push autorisatie heeft - mits uiteraard goed geïmplementeerd - de eigenschappen die nodig zijn om wantrouwen weg te nemen of te minimaliseren, omdat het nooit meer doet dan nodig is, en omdat de 'root of trust' hier de (huis)arts is, in algemene zin: de brondossierhouder, die de burger moet vertrouwen.
- Whitebox geeft de huisarts (of andere zorgverlener zoals apotheker) een rol als 'spin in het zorgweb van de patiënt'. De huisarts, of de andere beheerder van de medische gegevens regelt technisch de toegang met goedkeuring van en namens de patiënt. De burger kan inzien welke gegevens zijn ingesteld. De zorgverlener beheert de autorisaties op het dossier van de burger. Dat vraagt wel een extra inspanning van de arts/apotheker. De patiënt kan ook zelf autorisaties uitgeven, of 'drager' zijn van een autorisatie(code), die de patiënt zelf kan afgeven bij de (door patiënt) beoogde partij.

Technologie en beveiliging

- Technisch gezien zijn voor de elektronische uitwisseling van patiëntgegevens een aantal aspecten relevant: Representatie van de gegevens, Registratie van de plaats waar ze zijn opgeslagen (een URL) en Autorisatie van de toegang. Whitebox combineert 2 en 3: een geautoriseerde partij krijgt via een Whitebox een URL die in een klap twee dingen doet: de URL brengt je bij de gegevensbron en de URL codeert (cryptografisch) de autorisatie die je hebt gekregen. Door koppeling van een URL aan een authenticatie token/credential (bijv. UZI pas, identity management systeem), wordt voorkomen dat de URL door een niet-geautoriseerde partij kan worden gebruikt/misbruikt.
- End-to-end beveiliging is bij Whitebox versleuteling van het hele pad van begin tot eind, op transportniveau, direct van/naar (tussen) bron en opvrager. Dit gaat via een bi-directioneel geauthenticeerde TL-verbinding, eventueel aangevuld met geauthenticeerde requests via authenticatietokens.
- Als een landelijk goed beveiligd systeem te maken krijgt met een beveiligingslek, kan een grote hoeveelheid patiëntgegevens op straat belanden. Dit kan leiden tot een beschadiging van het vertrouwen in het systeem en – bij patiënten - in de artsen die het systeem gebruiken. Bij een decentraal systeem als Whitebox zal de schaal van een lek beperkter zijn. De toegang is cryptografisch beveiligd en de sleutels zijn voor elk beveiligd object onafhankelijk gegenereerd. Dus mocht een sleutel worden gecompromitteerd, dan is de schade beperkt tot de gegevens die door die specifieke sleutel worden beveiligd. Bij gebruik van moderne tamper-resistant crypto hardware, wordt het risico op sleutelverlies nog verder verminderd.



WHITEBOX: CONCEPT EN PRAKTIJK (3)

Technologie en beveiliging (vervolg)

- Whitebox Systems levert het product Whitebox voor ontsluiting van gegevens aan de bronkant, en identity management/autorisatie registratie software en hardware voor ontvangende partijen. Whitebox Systems is voornemens om alle elementen van het gebruikte protocol: APIs, URL definities, et cetera, alsmede de APIs voor de identity management componenten te beschrijven in open standaard documenten, mogelijk deels voorzien van een (voorbeeld) code. Deze documentatie beschrijft de push autorisatie standaard.
- De technologie van Whitebox maakt uitwisseling binnen het behandelteam mogelijk zonder specifieke toestemming van de patiënt. De opzet van het LSP vereist dat die toestemming er altijd is. Bij gebruik van Whitebox zou de huisarts vanuit patiëntbelang kunnen besluiten om gegevens uit te wisselen.

Waar staat Whitebox in de praktijk

- Alleen de koppeling 'Huisarts-Waarneming (HAP)' is operationeel bij enkele HIS-leveranciers. Er is nog geen ziekenhuis of apotheek operationeel. Wel wordt gewerkt aan autorisatiecodes om ziekenhuis/SEH of apotheek (via een browser) toegang te geven tot gegevens. Whitebox Systems geeft aan dat in Q4 2019 een apotheekaccount word uitgerold ten behoeve van medicatieverificatie door de eigen apotheek.
- Patiënten hebben inzicht in instellingen en uitgewisselde berichten via het Whitebox-portaal. Aan een app wordt gewerkt. XIS-Leveranciers moeten inspanning leveren om hun systemen compatibel te maken en te houden. Operationalisering verder dan HAP vraagt aanvullende inspanning. Functionaliteiten zijn nog in (door)ontwikkeling, zie toekomstige toepassingen.
- De zorgverlener/huisarts legt de gegeven toestemmingen/autorisaties vast in de Whitebox/HIS. Indien de huisarts kiest voor 'continu toegang voor alle waarnemende artsen op de HAP', komt de fijnmazigheid van het concept niet tot zijn recht. Dit stelt dan eisen aan logische toegangsbeveiliging binnen het systeem van de zorgverlener (HAP).
- Ondanks het decentrale concept moet ook Whitebox beheerd worden, dit vindt nu meer pragmatisch plaats, centraal punt met bevoegdheden. De realisatie van het beoogde auditbare 'published source' model en reproducible builds vereisen nog inspanning.
- Flexibiliteit en klantgerichtheid van Whitebox Systems worden nu als sterke punten ervaren. Volwassenheid van de beheer-organisatie vraagt om aanvullende inspanning. Maar grootschaligheid vraagt extra inspanningen en een andere organisatievorm.



WHITEBOX: CONCEPT EN PRAKTIJK (4)

Voorzieningen voor ongeplande (spoed) zorg

Whitebox zet niet (primair) in op spoed, de toegevoegde waarde van de Whitebox-autorisatietechniek ligt meer in de planbare zorg waarbij zorgverleners binnen het zorgproces actief gegevens (autorisaties) met andere zorgverleners delen.

Echter, de Whitebox heeft wel een aantal voorzieningen voor ongeplande/spoed/acute zorg. Deze voorzieningen hebben, op één na, uitdrukkelijk geen 'pull' karakter. Dit omdat deze zich nu juist richten op mensen die – ondanks eventuele indicatie dat het nuttig kan zijn om gegevens beschikbaar te stellen voor spoedsituaties – niet willen dat hun gegevens via een pull infrastructuur voor een groep (categorie) zorgverleners beschikbaar wordt gesteld.

De Whitebox standaard is uitdrukkelijk ontworpen om ook via de infrastructuur van een derde te kunnen functioneren en is (dus) onafhankelijk van de infrastructuur die een patiënt wil gebruiken. Dit biedt ook voordelen bij ongeplande zorg, bijvoorbeeld buiten Nederland.

Whitebox Systems werkt aan de verdere doorontwikkeling van de oplossing, met onder meer de onderstaande functies, die nu nog niet structureel in de praktijk worden toegepast.

- **Een dedicated 'pull' spoedvoorziening** met behulp van de Whitebox standaard. Met Whitebox is een index te maken, waarop (met toestemming) Whiteboxen patiënten/URL's van spoed-geïndiceerde patiënten aanmelden. Patiënten zijn opzoekbaar door – voor deze dienst – geautoriseerde zorgverleners met een UZI-pas. Dit zou een dedicated 'spoed index' zijn. Deze kan alleen voor spoed worden gemaakt, de server geeft autorisaties uit aan zorgverleners, die daarmee direct naar een bron linken. Transport van medische gegevens gaat niet over een voorgeschreven infrastructuur.
- **Controleerbare, niet-pull spoed voorzieningen.** Een dienstdoende huisarts op de huisartsenpost – waarbij patiënten met een spoedindicatie geacht kunnen worden aangemeld te zijn - kan een autorisatie-URL of een autorisatiecode doorsturen als een door-autorisatie (zie volgende slide). Bijvoorbeeld naar een SEH die meer informatie wil. Zo kan de formele vervanger van de huisarts tijdens ANW-diensten een arts op een spoedeisende hulp toegang geven tot relevante informatie. De geautoriseerde arts kan met een UZI-pas deze (kort geldige) autorisatie gebruiken om in een browser een spoeddossier (AMO + eventueel episodelijst) op te vragen; deze kan bij integratie ook in het XIS van de SEH worden ingelezen via bevraging van de URL.



WHITEBOX: CONCEPT EN PRAKTIJK (5)

- **Patiënt in control.** De patiënt, of een mantelzorger/familielid van de patiënt, zou een functionaliteit kunnen krijgen om zelf via een Whitebox-portaal of app een 'spoedautorisatie' aan te maken die hetzelfde soort toegang biedt als hiervoor bedoeld. Bovendien kan ook een vooraf aangemaakte nood-"emergencycode" op een pasje worden gedrukt/opgeschreven, die altijd vindbaar is bij een noodsituatie. Hiermee kan inzage in het spoeddossier bij de huisarts worden verkregen.

Whitebox URL's kunnen ook geregistreerd worden in een PGO. Hiermee kan de patiënt zelf in een PGO een autorisatie-URL aanmaken en uitgeven aan een zorgverlener, en eventueel ook zelf een autorisatiecode aanmaken die hij/zij kan opslaan in diens telefoon (in de 'SOS'-sectie) of op een pasje in de portemonnee, zoals hierboven beschreven.

Het gebruik van al bovenstaande autorisaties is identiek aan de wijze van gebruik/bevraging van andere autorisatie-URL's die in de Whitebox standaard worden gebruikt.

Overige ontwikkelingen

Daarnaast werkt Whitebox Systems aan de volgende functies.

- **Patiëntportaal.** Via dit portaal kan de patiënt inzien welke autorisaties zijn verleend op zijn/haar dossier van de huisarts. Daarnaast kan de patiënt zelf autorisaties delen met zorgaanbieders en zorgverleners. De informatie over het daadwerkelijk gebruik van de autorisaties door zorgaanbieder en zorgverleners is beschikbaar en wordt volgens Whitebox Systems in Q4 ook ontsloten in het patiëntportaal.
- **Ad-hoc toegang management.** In de uitwisseling tussen de huisarts en de huisartsenpost beschikt de huisartsenpost over een zogenaamde HAP-box. Whitebox Systems heeft een viewer-functionaliteit ontwikkeld voor zorgverleners om via een account of via een eenmalige autorisatiecode per patiënt toegang te krijgen tot (een beperkt deel van) het dossier van de huisarts, bijvoorbeeld bij verwijzing.
- **Door-autoriseren.** Whitebox werkt aan de mogelijkheid dat een zorgverlener op de huisartsenpost een zorgverlener in de keten ook kan autoriseren voor toegang tot de patiëntgegevens in het dossier van de huisarts. De waarnemende huisarts kan via deze functionaliteit aan een derde zorgverlener/zorgaanbieder die betrokken is bij de behandeling van de patiënt autorisaties verstrekken om een deel van het dossier van de huisarts te raadplegen.



HET LSP: CONCEPT EN PRAKTIJK

Het LSP voldoet met haar vorm van communicatie aan de wettelijke bepalingen

De Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) beheert het Landelijk Schakelpunt (LSP). VZVZ zorgt ervoor dat de uitwisseling van medische gegevens via dit 'netwerk' technisch en organisatorisch goed verloopt, verzorgt de regie over de uitwisselingsketen en bewaakt de snelheid, betrouwbaarheid en veiligheid van het systeem.

Via het LSP worden dagelijks miljoenen berichten tussen zorgverleners door het hele land uitgewisseld. De functionaliteiten van het LSP zijn beschreven en terug te vinden op www.vzvz.nl.

Voor het beschikbaar stellen van medische gegevens voor raadpleging door andere zorgverleners via het LSP, is vooraf expliciete toestemming van de patiënt nodig. Deze toestemming kan de patiënt geven en intrekken via zijn zorgverleners of zelf direct. Met circa 13.5 mln actieve toestemmingen is er een aantoonbaar groot draagvlak, hoewel dat niet voor alle zorggegevens in dezelfde mate geldt: apotheken hebben – voor de ontsluiting van het medicatiedossier – meer toestemmingen verkregen dan huisartsen.

Uitwisseling vindt plaats via een beveiligd, los van het internet staand netwerk (de AORTA-zorginfrastructuur), waartoe alleen zorgverleners met gebruik van een sterk identificatiemiddel (de UZI-pas) toegang hebben. De beveiliging van de gegevensuitwisseling voldoet aantoonbaar aan de eisen voor het beveiligd en vertrouwd uitwisselen van medische gegevens die daar wettelijk aan zijn gesteld (AVG, Wet op de geneeskundige behandelingsovereenkomst, Wabpvz, diverse AMvB's, NEN 7510, 7512 en 7513 etc.).

Toestemming geven of een inzage-overzicht bekijken is ook mogelijk via www.volgjezorg.nl, waar burgers na DigiD-authenticatie toestemming regelen en kunnen volgen wat er met hun medische gegevens gebeurt. Het geeft inzicht in welke gegevens via het Landelijk Schakelpunt zijn gedeeld, door welke zorgaanbieder(s) de gegevens zijn bekeken en wanneer.

Het LSP ontwikkelt zich verder

De doorontwikkeling van het LSP staat niet stil. VZVZ en het LSP zijn nauw betrokken bij de ontwikkelingen als bouwstenen (ZIB's), OTV, behandel/mandaattoken, SDS, inzagefunctie voor burgers, et cetera.



HET LSP: CONCEPT EN PRAKTIJK (2)

Mate van gedetailleerdheid van toestemming geven

Een patiënt geeft toestemming aan de zorgverlener om zijn gegevens beschikbaar te stellen via het LSP. Zorgverleners kunnen via het Landelijk Schakelpunt alleen de belangrijkste medische gegevens bekijken.

Een belangrijk onderdeel van het LSP is de autorisatiematrix. In deze matrix is vastgelegd welke zorgaanbieder welke informatie kan opvragen. Als voorbeeld: een huisarts kan de professionele samenvatting, ICA en medicatiegegevens opvragen. Deze zijn beveiligd met UZI-middelen, gekoppeld aan de rol van de zorgverlener, zoals vastgelegd in het BIG-register.

De huisarts stelt dus een gedeelte van het huisartsdossier van de patiënt beschikbaar. Dat gedeelte mag en kan alleen door huisartsen worden opgevraagd, niet door andere zorgaanbieders. De apotheker stelt een overzicht van de aan de patiënt verstrekte medicatie beschikbaar: het medicatieverstrekkingsoverzicht.

Een specialist in het ziekenhuis of een andere zorginstelling kan alleen gegevens over medicijnen, allergieën en overgevoeligheid bekijken. Dat geldt ook voor een andere apotheek of een apotheek in een instelling.

Om privacy te beschermen, kan de patiënt ervoor kiezen om gegevens uit het huisartsdossier of medicatie-overzicht af te schermen voor uitwisseling via het LSP. Zorgverleners zijn verplicht om hieraan mee te werken. Andere zorgverleners kunnen deze afgeschermdede gegevens niet opvragen via het Landelijk Schakelpunt. Het afgeschermdede gedeelte is dan voor hen niet zichtbaar.

Op dit moment is de patiënt nog beperkt in het specificeren van de (type) zorgaanbieders die gegevens mogen inzien tot hetgeen in de autorisatiematrix al is geregeld. VZVZ is betrokken bij het programma Gespecificeerde Toestemming Structureel (GTS) en de ontwikkeling van OTV.

Zolang binnen het LSP de huidige autorisatiemethode niet is vervangen door een systeem waarbij bepaalde (categorieën) zorgaanbieders kunnen worden uitgesloten op basis van gespecificeerde toestemming/OTV, is fijnmazigere toestemming niet mogelijk. Wanneer dit wel het geval is, is deze (op categorieën gebaseerde) oplossing voor gespecificeerde toestemming nog steeds anders van aard dan de specifieke toestemming/autorisatie die Whitebox biedt.



HET LSP: CONCEPT EN PRAKTIJK (3)

Uitwisselen volgens het vertrouwensmodel

Het LSP is een landelijk uitgerolde zorginfrastructuur waarbinnen regionaal medische gegevens worden uitgewisseld. Daarvoor is het netwerk onderverdeeld in 44 regio's. Zorgverleners kunnen in beginsel alleen binnen een regio gegevens uitwisselen. Zorgaanbieders die burgers uit meerdere regio's behandelen, kunnen ook in die regio's worden opgenomen. Ziekenhuizen kunnen landelijk medicatiegegevens opvragen.

Niet alle zorgverleners kunnen alle beschikbare gegevens van de patiënt bekijken. De gegevens uit het huisartsdossier zijn alleen beschikbaar voor waarnemend huisartsen, bijvoorbeeld op de huisartsenpost. De gegevens uit het medicatie-overzicht van de apotheek zijn beschikbaar voor meerdere zorgverleners: (Dienst)apotheken, ook in ziekenhuizen, (Waarnemend) huisartsen en Medisch specialisten in ziekenhuizen en andere instellingen.

Deze zorgverleners zoeken met het BSN van de patiënt naar beschikbare medische gegevens via het Landelijk Schakelpunt. Na een succesvolle bevraging van het Landelijk Schakelpunt, kunnen zij de beschikbare medische gegevens van de patiënt inzien. Alle zorgverleners die op deze wijze toegang hebben gekregen kunnen 'technisch gezien' gegevens opvragen. Echter, zij zijn hier alleen toe bevoegd als zij een behandelrelatie hebben met de patiënt én als dit nodig is voor de behandeling van de patiënt. Er is dus sprake van een 'vertrouwensmodel'.

Het LSP logt bij welke zorgverlener op welk moment welke gegevenssoort is opgevraagd. De patiënt kan via www.volgjezorg.nl altijd controleren of opvragingen gerechtvaardigd zijn geweest. Vanaf medio augustus is de naam van de (mandaatgevende) zorgverlener niet meer zichtbaar op het overzicht Uitwisselingen. De naam van de zorgaanbieder blijft wel getoond worden op het overzicht. Wie wil weten welke zorgverlener gegevens heeft bekeken, kan dit navragen bij de zorgaanbieder. De zorgaanbieder is verplicht deze informatie te verstrekken.



HET LSP: BEVEILIGDE VERBINDINGEN

Zoals aangegeven, vindt uitwisseling met het LSP plaats via een beveiligd, los van het internet staand netwerk (de AORTA-zorginfrastructuur), waartoe alleen zorgverleners met gebruik van een sterk identificatiemiddel (de UZI-pas) toegang hebben. Binnen het LSP wordt end-to end encryptie, een methode om de uitwisseling van (afzonderlijke) berichten van begin tot eind van een keten volledig versleuteld te laten verlopen, niet toegepast.

VZVZ maakt die keuze bewust. Men kiest voor **beveiliging van de componenten van de verbinding in de keten, niet de afzonderlijke berichten van begin tot eind.**

In het LSP meldt een opvragende partij (zorgverlener) zich altijd vanaf een gecertificeerd Goed Beheerd Zorgsysteem (GBZ) bij VZVZ via een gecertificeerde, beveiligde verbinding, met een sterk identificatiemiddel (de UZI-pas). Het verzoek om gegevens ('de opvraging') wordt doorgezonden naar de bronsystemen via een gecertificeerde, beveiligde verbinding. Indien er relevante gegevens beschikbaar zijn in het brondossier, dan worden deze over diezelfde gecertificeerde versleutelde verbindingen verzonden naar de opvragende zorgverlener, met het schakelpunt als beveiligd tussenstation.

End-to-end encryptie op de afzonderlijke berichten zou praktisch gezien moeten plaatsvinden op de communicatieserver van de zorgaanbieder.

In het geval van het LSP zijn er zo'n 6.000 aangesloten zorgaanbieders. Het LSP beperkt zich tot de veilige uitwisseling en niet de toegang tot de lokale systemen waarin deze gegevens worden afgeleverd. De lokale systemen dienen te voldoen aan NEN 7510. Uitgaande van het communicatieserverniveau bestaat er een beveiligde verbinding (TLS) op basis van een UZI-servercertificaat, die zorgdraagt voor de versleuteling van het transport.

De kans is reëel dat er zich onder deze 6.000 zorgaanbieders op enig moment 'onveilige' systemen bevinden. De kans dat er zich een beveiligingsincident voordoet bij een zorgaanbieder schat VZVZ hoger in dan de kans dat zich een beveiligingsincident op het LSP voordoet. Om die reden is gekozen voor beveiliging van de verbinding.

Het LSP en de toegang tot informatie-uitwisseling via het LSP is beveiligd, met het idee dat een hack bij een zorgaanbieder niet leidt tot een beveiligingsrisico voor alle andere zorgaanbieders. Bij een hack bij een zorgaanbieder zouden wel de gegevens opgevraagd kunnen worden van de vanuit deze zorgverlener opvraagbare patiënten, waarbij het (theoretisch) mogelijk is dat een aanzienlijk aantal patiëntgegevens op straat komen te liggen.



HET LSP: BEVEILIGDE VERBINDINGEN (2)

End-to-end encryptie van elk afzonderlijk bericht beperkt functionaliteiten die momenteel worden aangeboden

Beveiliging van de afzonderlijke berichten heeft als nadeel dat de inhoud daarvan niet samengevoegd, vertaald of anderszins bewerkt kan worden, voordat het bij de opvrager terechtkomt. In steeds meer gevallen treedt het LSP (of aparte generieke componenten daarvan) als intermediair op om 'vertalingen' uit te voeren tussen zorgaanbieders die (nog) niet op dezelfde (versie van) een uitwisselingsstandaard zitten.

In concreto: bij het opvragen van medicatiegegevens kunnen deze uit verschillende bronnen (huisarts, apotheken) afkomstig zijn, die niet 'dezelfde taal/eenheid van taal' hanteren. Dit levert in zowel praktische als technische zin al een uitdaging op. Bij toepassing van end-to-end encryptie op de afzonderlijke berichten, wordt het onmogelijk om deze vertaalslag te maken.

Oplossing voldoet aan de vereiste beveiligingsverplichtingen

De algemene beveiligingsverplichting is voor de Nederlandse gezondheidszorg uitgewerkt in de NEN-normen, waarvan de naleving wettelijk verplicht is gesteld. In de AVG is voorgeschreven dat persoonsgegevens alleen verwerkt mogen worden als door passende technische en organisatorische maatregelen een passende beveiliging wordt gewaarborgd. In het Besluit elektronische gegevensverwerking door zorgaanbieders (Stb 2017-446) is voorgeschreven, dat zorgaanbieders daartoe NEN 7510, 7512 en 7513 dienen na te leven. NEN 7512 bevat de voorschriften die relevant zijn voor de beveiliging van communicatie in de zorg. Door NEN 7512 wordt geen end-to-end encryptie voorgeschreven. Er zijn meerdere manieren om tot een sterke beveiliging te komen, waaronder de beveiliging van de verbinding –van begin tot eind- en die ruimte biedt de norm dus ook.

Het restrisico is bekend

VZVZ geeft aan dat het risico dat overblijft na het versleutelen van de verbindingen tussen GBZ (zorgaanbieders) en het LSP, het kunnen 'inzien' is door 'het LSP' (als systeembeheerder) van de berichten op het moment dat deze zich binnen het LSP bevinden. Om dit te voorkomen, zijn technische en organisatorische maatregelen getroffen. Dit wordt gemonitord en met regelmaat vindt er een audit plaats (NEN7510). Er is geen realtime inzage mogelijk. Verder is toegang tot het LSP voorbehouden aan een beperkt aantal personen en subverwerkers. Subverwerkers die ingeschakeld worden, werken op basis van een verwerkersovereenkomst die voldoet aan de eisen uit de AVG.

Door VZVZ is geconcludeerd dat de inspanningen en kosten die gemoeid zijn met het end-to-end encrypten van het berichtenverkeer niet op wegen tegen dit restrisico.



INVESTEREN IN WHITEBOX NAAST HET LSP

Uitgangspunten en vraagstelling vanuit Whitebox Systems:

- Uitgangspunt voor Whitebox Systems is dat Whitebox een meerwaarde biedt, de alternatieven voor communicatie rondom burgers verhoogt en de uitwisseling verhoogt. Daarbij hoort volgens Whitebox Systems een vergoeding voor zorgverleners en leveranciers die in verband met de meerwaarde zelf de keuze maken om ook via Whitebox uit te wisselen ten behoeve van de keuze van hun patiënt. Dit als stimulans voor zorgaanbieders en ten behoeve van de realisatie van een (enigszins) gelijk speelveld.
- Whitebox Systems geeft aan geen behoefte te hebben aan (rechtstreekse) financiering van ZN, anders dan voor het opstellen van voorlichtingsmateriaal of standaardisatie, kosten die bovenop de reguliere activiteiten van het leveren van hun product komen. Whitebox Systems geeft aan geen verlengstuk te willen zijn van zorgverzekeraar of overheid en ook niet die schijn te willen wekken. Zij stelt dat een vrije markt voor uitwisselings-/communicatiesystemen innovatie van standaarden stimuleert. Een level playing field, ook financieel, maakt dat mogelijk.
- De koppeling moet via een gestandaardiseerd (beveiligd) koppelvlak (API) werken. Whitebox Systems wil helpen deze API te ontwikkelen. Via deze API dienen alle courante berichtformaten voor de informatie uit het XIS beschikbaar te worden gemaakt voor (geautoriseerde) systemen. Het 'open koppelvlak' (leveranciers) kan zodanig worden gerealiseerd dat dit herbruikbaar is voor gebruik door meerdere systemen; uiteraard wel op een goed beveiligde (controleerbare) manier. Denk aan: afsprakenstelsel, acceptatie als onderdeel van het duurzaam informatiestelsel.
- Whitebox Systems zou graag een vergoeding zien voor leveranciers (HIS, HAP, AIS) om een 'open' koppeling te realiseren voor het opvragen van alle courante berichtformaten (inclusief LSP HL7v3/FHIR en ZIB's) en het terugsturen (bijvoorbeeld berichten uit medicatieproces 9.0). Leveranciers zijn gewend om vergoedingen te ontvangen voor het ontwikkelen van koppelingen en deze te onderhouden. Whitebox Systems wil het initiatief nemen op deze 'open' koppelvlakken, deze specificeren en deze eventueel 'herbruikbaar' aanbieden aan andere aanbieders.
- Whitebox Systems vraagt dat de gebruikers van de Whitebox (huisarts, HAP, apotheek of andere zorgaanbieders) die voor het product betalen uit eigen budget daar aanvullend budget/subsidie voor krijgen. LSP-gebruikers krijgen ook een vergoeding/subsidie voor de aanschaf en het 'gebruik' van het LSP en dus zullen zorgverleners dit uiteindelijk ook voor alternatieven, zoals Whitebox, gaan verwachten. Zeker als de meerwaarde van de Whitebox voor burgers met een sterke(re) privacybehoefte breder wordt geaccepteerd.



INVESTEREN IN WHITEBOX NAAST HET LSP (2)

- Ziekenhuizen en andere partijen met (commerciële) marges zullen uiteindelijk, wanneer push autorisatie breder geadopteerd wordt, goeddeels (op realisatie open koppelvlak na) voor eigen kosten hun software moeten laten aanpassen, met name als het gaat om de integratie van push autorisatie in de opvragende rol.
- Een vergoeding voor de huisarts is volgens Whitebox Systems gewenst om te zorgen dat er concurrentietechnisch een level playing field ten opzichte van het LSP ontstaat. Beoogd is om tot de helft van de kosten te vergoeden. Overige vergoedingen die LSP-klanten krijgen en die los staan van Whitebox dienen ook voor Whitebox beschikbaar te zijn. Denk aan (generieke, infrastructuur en uitkomst-onafhankelijke) vergoedingen, UZI-passen voor de praktijk en eventuele vergoedingen voor de inspanning voor het vragen van toestemming.
- Er is een aantal situaties waarbij de zorgverzekeraar permissie moet geven voor specifieke IT-uitgaven, waaronder de huisartsenposten Amsterdam. Whitebox Systems vindt het van belang dat in die gevallen de zorgverzekeraar daar toestemming voor geeft.

Beoogde vergoedingen

- Whitebox Systems denkt aan de volgende vergoedingen voor zorgverleners en leveranciers:
 - Voor huisartsen een eenmalige vergoeding van 750 Euro en jaarlijks een vergoeding van 375 Euro (50% van de kosten).
 - Voor HAP 500 Euro (gelijk aan kosten) en jaarlijks een vergoeding van 1.000 Euro (gelijk aan kosten).
 - Voor Apothekers een eenmalige vergoeding van 500 Euro (gelijk aan kosten) en jaarlijks een vergoeding van 500 Euro (50% van de kosten).
 - Voor ziekenhuizen een eenmalige vergoeding van 500 Euro (gelijk aan kosten) en jaarlijks een vergoeding van 1.000 Euro (50% van de kosten).
 - Voor zelfstandige klinieken en overige, een eenmalige vergoeding van 500 Euro (gelijk aan kosten) en jaarlijks een vergoeding van 500 Euro (50% van de kosten).
 - Voor leveranciers, een eenmalige vergoeding van 75.000 Euro voor het bouwen van een 'open' koppeling en jaarlijks een vergoeding van 15.000 Euro voor het onderhouden daarvan.



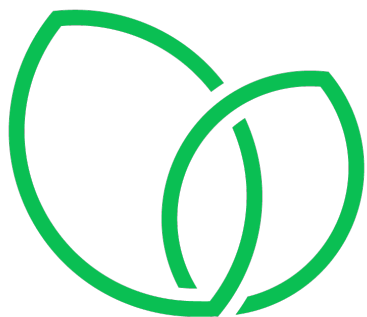
INVESTEREN IN WHITEBOX NAAST HET LSP (3)

- Ter illustratie zijn door Whitebox Systems een aantal scenario's naast elkaar gezet voor de gewenste ondersteuning door ZN. Deze zijn hierna weergegeven.

Case: 100 huisartsen in Amsterdam, 1 HAP en drie HIS systemen				
Eenmalige investering				375.500
Jaarlijks kosten				98.500
Case: 100 huisartsen in Amsterdam+Maastricht, twee HAP en drie HIS systemen				
Eenmalige investering				451.000
Jaarlijks kosten				114.500
Case: 100 huisartsen in ASD+Ma'cht, 2 HAP, 40 Ap, 3 HIS, 2 HAPIS, 1 AIS				
Eenmalige investering				545.000
Jaarlijks kosten				147.500
Case: 500 huisartsen door het land, 10 HAP, 150 Ap, 5 HIS en 2 HAP systemen, 1 AIS				
Eenmalige investering				1.055.000
Jaarlijks kosten				355.000
Case: 1.000 huisartsen door het land, 10 HAP, 250 Ap, 5 HIS en 2 HAP systemen, 2 AIS				
Eenmalige investering				1.555.000
Jaarlijks kosten				582.500
Case: 2.000 huisartsen in door het land, 40 HAP, 40SEH, 500 Ap, 5 HIS, 2 HAP systemen, 2 AIS				
Eenmalige investering				2.465.000
Jaarlijks kosten				1.090.000
Case: 3.500 HA, 40 HAP, 1.000 Ap, 100 ZH/SEH+250 klinieken+overige orgs, 20 leveranciers				
Eenmalige investering				4.820.000
Jaarlijks kosten				2.127.500

- Meer dan 2.000 huisartsen worden naar verwachting van Whitebox Systems in Nederland nooit bereikt omdat de grote HIS-leveranciers liever zelf de (open) standaard/koppeling zullen implementeren bij zulke getallen en zo de implementatie onder eigen controle houden.
- Daarmee komt Whitebox in de berekeningen erop dat de 'stimuleringsfase' tot dat aantal circa 2.5M Euro eenmalige kosten en een kleine 1M Euro per jaar inclusief de kosten voor de HIS-leveranciers bedraagt, waarvan een deel een generieke investering betreft, voor het open koppelvlak.





© 2019 WeDoTrust

WeDoTrust B.V. is ingeschreven bij het
handelsregister in Nederland onder
KvK nummer 65568346.

www.wedotrust.nl