Concept, implementatie en evaluatie van een decentraal communicatiesysteem voor de zorg

Guido van 't Noordende, Whitebox Systems, Amsterdam

Definitief verslag waarneempilot Whitebox in Amsterdam, maart 2018

Pilot begeleidingsteam:
Hein Thiel, Huisartsenkring Amsterdam-Almere (HKA)
Cees Dekker, Stichting Eerstelijn (1ste lijn) Amsterdam

Inhoudsopgave

Voorwoord

De pilot heeft ruim twee jaar gelopen. Voor het tot stand komen van een pilot met een systeem zoals de Whitebox, is de inzet van vele mensen en partijen nodig. Niet alleen de huisartsen, maar ook leveranciers en organisaties die bij de implementatie betrokken zijn. Ik dank iedereen die bij het project betrokken was op voorhand, ook hen die niet specifiek hieronder vermeld worden.

Na een start met twee huisartsen om de techniek te onderzoeken, zijn in 2015 de Whitebox en de pilot in Amsterdam aangekondigd via een artikel in Medisch Contact [Thiel et al., 2015]. Vervolgens is er een traject begonnen waarin 20 TetraHIS huisartsen werden aangesloten en waarbij het systeem werd geïntegreerd in de systemen van de huisartsen én het systeem van de huisartsenpost, Call Manager. Daarbij kon het gebruik van het systeem getoetst worden in de productieomgeving van de Huisartsenposten Amsterdam (HpA). De weerslag van de pilot en de daaruit behaalde resultaten en leermomenten zijn te vinden in dit verslag.

Speciale dank gaat uit naar Hein Thiel, die binnen de HKA en daarbuiten hard en consistent heeft gewerkt om de omstandigheden te creëren waarmee de pilot kon plaatsvinden, en altijd tot steun was wanneer zaken tegenzaten. Ook heeft Hein vele testen gedaan en feedback geleverd op alle aspecten die voorbij kwamen, van techniek tot gebruik tot presentatie van informatie in het systeem. Dit heeft het systeem sterk verbeterd. Hein: hartelijk dank voor je inzet, je kritische blik, en niet te vergeten, je geduld!

Stella Zonneveld en David Koetsier hebben zich ingezet binnen het HKA bestuur, en David ook als pilot-deelnemer en tester. Speciale dank gaat ook uit naar Ton Mulder, deelnemer van het eerste uur die veel van de nieuwe functies als eerste heeft uitgetest in zijn praktijk en op de huisartsenpost.

Dank ook Cees Dekker, voor de begeleiding van de pilot vanuit de HAP en kritische feedback; ook jij hebt samen met Hein vele malen geholpen bij het testen van de systemen en het opvragen van (test)dossiers. Marco Stommel, bedankt voor ondersteuning bij dit traject.

Aan leverancierskant gaat dank uit naar TetraHIS en CGM-Labelsoft, specifiek naar Joep Vullinghs, Ab Elzenga, en Rob van den Berg voor hulp bij het realiseren van de technische implementatie.

Diverse partijen zijn in verschillende (voor)stadia van de ontwikkeling van de Whitebox betrokken geweest en hebben het project mede mogelijk gemaakt. Dank gaat uit naar onder meer UvA, COMMIT/, SIDN fonds, RVO, Stichting Nlnet, de LHV Huisartsenkring Amsterdam, en tevens naar Stichting 1elijn Amsterdam en de Huisartsenposten Amsterdam. Bedankt Cliëntenbelang Amsterdam voor evalueren van het informatiemateriaal.

Uiteraard is de pilot ook alleen mogelijk geweest door de belangeloze bijdrage van de huisartsen in de pilot, inclusief de deelnemers aan een tweede pilot met het systeem in Maastricht-Heuvelland, en de huisartsen die aan het ontwerp en de evaluatie van de minimale PS hebben gewerkt.

Ook wetenschappers hebben op verschillende manieren formeel of informeel bijgedragen aan het project. Esmée Schregardus en Margot Oosterwechel hebben meegewerkt aan het onderzoek van de VU naar de minimale PS. Specifieke dank gaat uit naar Luuk Lagerwerf (VU) en Eline Roelofsen, in beide gevallen met speciale waardering voor het uithoudings- en doorzettingsvermogen.

Cees de Laat verdient speciale vermelding vanwege zijn steun vanuit de UvA, toen ik onderzoeker was in zijn groep en het project nog in ideefase was, en bij de stappen daarna die nodig waren om tot realisatie te komen.

Hartelijk dank iedereen die bijgedragen hebben, of nog steeds bijdragen aan de ontwikkeling van de Whitebox, en die geholpen hebben om de Whitebox te brengen waar het nu is.

Amsterdam, maart 2018,

Guido van ‘t Noordende

1 Inleiding: wat is de Whitebox

De Whitebox is een communicatiesysteem voor de uitwisseling van patiëntgegevens dat bedoeld is voor de huisarts en, in de toekomst, voor andere zorgverleners. Het systeem is eigendom van de huisarts. Met dit systeem bepaalt alleen de huisarts wie wel en niet toegang tot gegevens krijgt. Daarom kan niemand anders dan de huisarts – in samenspraak met patiënt - beslissen welke gegevens met wie gedeeld worden. Naast de huisarts kan alleen de patiënt, via een eigenstandige toegang tot de Whitebox, zorgen dat bepaalde gegevens bij bepaalde zorgverleners terecht kunnen komen. Patiënt en huisarts kunnen altijd inzien welke gegevens dit betreft en wie toegang heeft gehad. Patiënt en arts kunnen óók zorgen dat bepaalde gegevens niét bij derden terecht kunnen komen, door het instellen van “filters” die zorgen dat bepaalde gegevens nooit beschikbaar komen voor externe partijen. Dit beschermt het medische beroepsgeheim beter dan welk ander systeem dan ook.

Het doel is om met de Whitebox het meest privacyvriendelijke communicatiesysteem voor de zorg te ontwikkelen. De uitgangspunten van het systeem zijn zo gekozen dat alle vormen van communicatie, zowel nationaal als internationaal – op een eenvoudige en schaalbare, maar altijd door arts en patiënt controleerbare manier – mogelijk is. De Whitebox is eigendom van de huisarts en valt daarom onder de bescherming van het beroepsgeheim. Zo is er géén externe partij die via de Whitebox bij de medische gegevens van een patiënt kan, behalve expliciet door de huisarts of de patiënt geautoriseerde partijen.

1 De zorgverlener centraal, handelingsperspectief voor de patiënt

De huisarts heeft in de Nederlandse gezondheidszorg een centrale functie. De huisarts is poortwachter van de zorg. Bovendien is de huisarts een vertrouwenspersoon voor de patiënt bij zaken rond zowel gezondheid als privacy. Daarom heeft de huisarts in de implementatie van het Whitebox systeem in Nederland een centrale rol. In de meeste gevallen is de huisarts het beginpunt van zorgcommunicatie, maar ook de plek waar gegevens over de behandeling steeds weer terugkomen – denk bijvoorbeeld aan een specialist die een ontslagbrief aan de huisarts terugstuurt waarin de bevindingen van de behandeling worden beschreven of informatie die op het medicatiebeleid betrekking heeft[1]. Zo houdt de huisarts het overzicht over het medische dossier. Gegevens die de huisarts bijhoudt, vallen onder het

1 Apothekers moeten het medicatiebeleid altijd valideren bij de huisarts – (herhaal)recepten worden geautoriseerd door de huisarts. Specialisten die medicatie voorschrijven (die soms verstrekt wordt door de ziekenhuisapotheek), moeten de huisarts ïnformeren over (aanpassingen van) het medicatiebeleid zodat de huisarts goed geïnformeerd is wanneer de patiënt weer behandeld wordt vanuit de eerste lijn, cq wanneer de medicatie verstrekt wordt door de openbare apotheker.

beroepsgeheim. Dit beroepsgeheim zorgt ervoor dat patiënten zich vrij tot een arts kunnen wenden, zonder angst dat gevoelige gegevens zullen uitlekken of bij derden kunnen terechtkomen. Het vertrouwen van patiënten in het beroepsgeheim en daarmee in de zorgverlener is van groot belang voor de maatschappij. Het beroepsgeheim garandeert, zoals dat soms wat zwaarwichtig genoemd wordt, de *toegankelijkheid van de zorg.*

Uiteraard heeft de huisarts niet het exclusieve beheer over alle medische dossiers van een patiënt: ook apothekers, medisch specialisten en in toenemende mate de patiënt zelf heeft medische of gezondheids-gerelateerde dossiers. Deze dossiers kunnen via een Whitebox “persoonlijk netwerk” inzichtelijk worden gemaakt voor relevante zorgverleners in het zorgproces en de patiënt zelf. Al deze dossiers heten brondossiers, en de auteur van deze dossiers heten “brondossierhouders”.

Een belangrijk idee achter de ontwikkeling van de Whitebox is dat het systeem handelingsperspectief biedt voor mensen (patiënten) die niet willen dat hun gegevens gedeeld worden met een groot aantal zorgverleners. Het gaat dan met name om zorgverleners waarvan de patiënt niet op voorhand weet dat deze bij de behandeling betrokken zijn. Maar tegelijkertijd gaan we ervanuit dat die patiënten wél willen dat hun gegevens met specifieke zorgverleners gedeeld kunnen worden als dat nodig is – maar dan dus zonder onnodige risico’s, en zo veilig mogelijk.

De meeste zorgverleners zijn van mening dat minimaal de actuele gegevens over het medicatiegebruik van de patiënt (en allergieën, contra-indicaties en intoleranties voor medicamenten) beschikbaar moeten zijn voor andere artsen en apothekers ‘in de keten’, oftewel bij alle zorgverleners die bij de behandeling van een patiënt betrokken zijn. Ook de Inspectie voor de Gezondheidszorg (IGZ) stelt dat het beschikbaar stellen van gegevens over het actuele medicatiegebruik in de keten verplicht is[2]. Dit betekent dat het steeds minder realistisch wordt om te veronderstellen dat patiënten elke vorm van uitwisseling van medische gegevens kunnen uitsluiten.

Om te voorkomen dat mensen uiteindelijk toch verplicht worden te accepteren dat hun gegevens via het Landelijke Schakelpunt (LSP) of een ander grootschalig systeem gedeeld worden met partijen in de keten (en daarmee ook met veel partijen die *niet* direct bij de behandeling betrokken zijn), is het van belang dat een communicatiemiddel bestaat waarmee deze gegevens specifiek beschikbaar kunnen worden gesteld aan(uitsluitend) partijen die direct bij de zorgverlening rondom een patiënt betrokken zijn, maar niet aan andere partijen. Het is van belang dat dit kan zonder dat dit betekent dat patiënten toestemming moeten geven om hun gegevens beschikbaar te stellen aan een grote groep

2 Zie https://www.medicatieoverdracht.nl/de-richtlijn , en https://apotheekhoudend.lhv.nl/actueel/nieuws/igz-toezichtkader-2015-focus-op-medicatieveiligheid

zorgverleners, met daaraan verbonden risico's[3] – met name ook het risico dat patiënten/burgers uit vrees voor risico's drempels ervaren bij het vragen van zorg.

Het delen van medische gegevens moet dus kunnen *zonder* dat dit automatisch het delen van gegevens via een grootschalig uitwisselingssysteem impliceert[4]. Tegelijkertijd moeten relevante gegevens wel *kunnen* worden uitgewisseld, als dit nodig is.

Als praktische oplossing voor dit probleem wordt in de huidige implementatie van de Whitebox de huisarts gezien als de belangrijkste brondossierhouder. Deze fungeert als "sleutelbewaarder" tot het huisartsendossier[5], namens en voor de patiënt. De architectuur en het systeem staan andere 'configuraties' toe, inclusief een opzet waarbij de patiënt zelf 'sleutelbewaarder' is, maar praktisch gezien verwachten wij dat de huisarts als sleutelbewaarder in de meeste gevallen een effectieve oplossing is.

De huisarts, als vertrouwenspersoon en regisseur van de meeste zorg in Nederland, wordt met de Whitebox dus sleutelbewaarder tot het dossier, voor en namens de patiënt.

Met deze opzet bieden wij handelingsperspectief voor artsen en patiënten die vinden dat hun gegevens zo kleinschalig mogelijk gedeeld moeten worden, en alleen toegankelijk moeten zijn voor artsen die direct betrokken zijn bij de zorg rondom de patiënt. De huisarts is in een goede positie om deze gegevensuitwisseling te organiseren, vanuit zijn verantwoordelijkheid als regisseur van veel zorg rondom de patiënt.

---

3 Hoe meer zorgverleners aangesloten zijn op een systeem en tot medische gegevens, hoe groter het risico dat gegevens ongeoorloofd kunnen worden opgevraagd – door zorgverleners, óf bijvoorbeeld door hackers die inbreken in het systeem van een arts en van daaruit misbruik kunnen maken van de UZI pas van de arts om, namens die arts, gegevens op te vragen uit het systeem. Zie ook G. van 't Noordende, "Nieuwsoverzicht EPD", Universiteit van Amsterdam. Gearchiveerd op https://dev.mcsr.nl/guido/public_html_uva/epd/news7.html (2017).

4 Er zijn reeds situaties gerapporteerd waarbij patiënten de facto gedwongen werden toestemming te geven omdat een apotheker anders niet kon instaan voor medicatieveiligheid, zie bijv. EénVandaag Radio 1 en NPO 1, 12 mei 2017. https://eenvandaag.avrotros.nl/item/zonder-patientendossier-moeizaam-of-geen-medicatie/

5 In de toekomst kan de huisarts mogelijk ook toegang geven tot andere relevante dossiers, zoals het medicatiedossier bij de eigen apotheek, wanneer deze bij de huisarts aangemeld zijn.

2 Waarom hardware? De Whitebox als fysiek apparaat

De Whitebox een kastje dat fysiek op de huisartsenpraktijk staat. Dit kastje vormt de interface (of "gateway") tussen de binnenwereld van de huisarts met het dossier waarin de huisarts de patiëntendossiers bijhoudt, en de buitenwereld, van waaruit verzoeken om informatie geïnitieerd kunnen worden. Plaatsing op de praktijk maakt voor iedereen zichtbaar dat de huisarts eigenaar van het systeem is, en dat de huisarts verantwoordelijk is en verantwoordelijkheid neemt voor de uitwisseling van gegevens.

Plaatsing in de praktijk heeft ook daadwerkelijk betekenis: geen externe partij – geen systeembeheerder, geen eigenaar van een datacentrum – kan buiten Whitebox Systems of het zicht van de arts om, software installeren of aanpassingen aan het systeem doen.
De huisarts kan de Whitebox uit elkaar schroeven en de software en data op het kastje (laten) analyseren om te controleren dat de software doet wat het belooft[6]. De huisarts heeft dus zelf controle, en kan alles letterlijk overzien.

Wanneer toegang eenmaal geautoriseerd is kunnen op elk moment, 24/7 de meest actuele gegevens worden opgehaald, rechtstreeks uit het systeem van de huisarts zonder tussenkomst van de huisarts, uitsluitend door de vooraf geautoriseerde zorgverlener. Zo is de Whitebox niet alleen een zeer veilig, maar ook een modern, schaalbaar en flexibel systeem dat praktisch is en goed aansluit op de zorg.

3 Positionering Whitebox in de markt: product en standaard

Whitebox Systems baseert zijn business model bewust op hardware en software (onderhoud), niet op data. Dit is essentieel. Het betekent namelijk dat wij het bedrijf niet afhankelijk maken van hoe vaak het systeem gebruikt wordt, of van het exploiteren van data die in het systeem wordt opgeslagen. Medische data zijn geen handelswaar.

Wij vinden dat de keuze om wel of niet data uit te wisselen bij de arts en de patiënt ligt: geen enkele andere partij mag hier invloed op (kunnen) uitoefenen. Daarom willen we ook dat de huisarts de Whitebox zelf uit lopend budget kan betalen. De Whitebox wordt gelicenseerd voor een jaarlijks bedrag (fixed-fee) met een eenmalige borg.[7] Het moet voor elke arts mogelijk zijn een Whitebox te kopen,

6 Whitebox gaat werken met een published-source model in een combinatie met een reproduceerbaar build systeem, zodat de code op de Whitebox relatief eenvoudig te verifiëren is.

7 De borg is een soort emballage: het systeem is modulair ontworpen en het grootste deel van de hardware is herbruikbaar.

zelfs als hier geen vergoeding van de zorgverzekeraars tegenover staat.

De Whitebox is een product waar specifieke producteigenschappen gekoppeld worden, zoals het hardware model en beveiligingseigenschappen. Intern in de Whitebox wordt echter gebruik gemaakt van een communicatie standaard die onafhankelijk beheerd zal gaan worden[8], zodat voor het implementeren en het gebruik van de standaard niet altijd Whitebox hardware nodig is. Ook huisarts informatie systemen (XISsen) moeten de standaard kunnen implementeren.

Het doel van de waarneempilot is om patiëntgegevens beschikbaar te stellen voor de huisartsenpost. De Whitebox kan inmiddels echter veel meer dan koppelen met de huisartsenpost alleen. De onderliggende standaard is ontworpen als een schaalbaar autorisatiesysteem dat diverse (medische) toepassingen kan ondersteunen. Zo bestaat er inmiddels een inzagemogelijkheid voor de patiënt (waarmee deze onder meer logging – de historie van autorisaties en opvragingen m.b.t. zijn/haar dossiers - kan inzien en koppelingen met andere systemen zoals patiëntenportalen kan regelen en terugsturen), een visitetoepassing, en een toepassing voor onderlinge waarneming (vakantie/dagwaarneming).

Koppelingen met andere partijen zoals apothekers – voor medicatiecontrole – (lokale) ketenpartners, en ziekenhuizen zijn in ontwikkeling. We willen hier in 2018 stappen mee zetten.

Het bijzondere van de Whitebox waarneemkoppeling is dat dit een één-op-één koppeling met de huisartsenpost is waar niets - geen systeem en geen persoon - tussen zit. Dit maakt de eigenschappen van deze koppeling goed begrijpelijk voor arts en patiënt. Bovendien biedt dit handelingsperspectief voor mensen die niet willen dat zij meteen aangemeld worden bij een grootschalig extern systeem waarmee in potentie veel zorgverleners toegang tot hun gegevens krijgen, zoals het LSP. Bij de Whitebox is volledig instelbaar welke gegevens beschikbaar worden gesteld, en is zowel tijdelijke als permanente ontsluiting van gegevens mogelijk. Dit maakt het systeem goed uitlegbaar en aan te passen aan de patiënt.

8 De beste wijze van governance voor deze standaard wordt op dit moment onderzocht.

4 Motivatie voor de pilot

De directe motivatie voor de ontwikkeling van de Whitebox en het opzetten van een pilot met dit systeem ligt bij een survey die de Huisartsenkring Amsterdam (HKA) in 2014 onder haar leden uitzette met de vraag of huisartsen het LSP wilden gebruiken of liever een regionaal alternatief. Deze survey kreeg een hoge respons, waarbij een overgrote meerderheid van de respondenten – inclusief een ruime meerderheid van de artsen die reeds het LSP gebruikten – aangaf dat ze liever een regionaal alternatief zouden gebruiken. Dit legde de basis voor het idee om een decentraal systeem te ontwikkelen dat wel aan de bezwaren en wensen van huisartsen tegemoet kon komen. Op basis van deze vraag is vervolgens de Whitebox ontwikkeld in een spin-off van de UvA, Whitebox Systems.

De verder terugliggende achtergrond achter de ontwikkeling van de Whitebox ligt in de behandeling van de wet-EPD (31.466) in 2008-2011, waar de latere oprichter van Whitebox Systems, Guido van 't Noordende als beveiligingsonderzoeker bij betrokken was. Dit wetgevingstraject was ingezet om het Landelijke Schakelpunt (LSP) te voorzien van een wettelijk kader, dat tot doel had om het LSP verplicht in te voeren onder de naam "Landelijk Elektronisch Patiëntendossier (L-EPD)". Een belangrijke eigenschap van de wet was dat mensen automatisch in het systeem meededen, tenzij ze bezwaar maakten (een zogeheten "opt-out" systeem). Dit wetsvoorstel is in 2011 *unaniem* door de Eerste Kamer afgewezen, onder meer vanuit zorgen over de mate van (mogelijk onnodige) centralisatie van het ontwikkelde landelijke systeem, over de privacybescherming en veiligheid, en over de mogelijkheid van potentieel toekomstig gebruik/misbruik van de infrastructuur op een wijze die in strijd kan zijn met de oorspronkelijke uitgangspunten van het ontwerp.

In het traject na de afwijzing van de wet-EPD zijn er moties aangenomen in de Eerste Kamer die opriepen tot standaardisering ten behoeve van regionale uitwisseling van gegevens[9], een motie die oproept om *privacy-by-design* toe te passen bij de ontwikkeling van nieuwe systemen door de overheid, en een motie die de minister verdere financiële en beleidsmatige bemoeienis met het LSP verbood.

Gezien het Whitebox systeem expliciet kiest voor proportionele, *privacy-by-design* gegevensuitwisseling, doet de Whitebox als veiliger alternatief eigenlijk precies waar de Eerste Kamer toe opriep[10].

9 De motie Tan 31.466 Y (2011) riep op "te komen tot […] standaarden standaarden voor […] ontsluiting als de overdracht van gegevens […] teneinde veilig digitaal transport van gegevens (zowel pull als push) mogelijk te maken tussen zorgverleners binnen een regio".

10 Motie-Tan c.s., 31466 Y, Motie-Franken 31466, 2011. Zie tevens moties 33 509 R en T (2016).

5 Onderzoek marktvraag: wensen van patiënten en artsen

Aan het begin van de pilot hebben een aantal voorbereidende onderzoeken plaatsgevonden om het draagvlak voor de Whitebox te onderzoeken.

Uit de enquête in 2014 van de HKA, voorafgaand aan de beslissing om een pilot met de Whitebox te starten, bleek dat 73% van de 97 respondenten niet was aangesloten op het LSP. Van de huisartsen die wel op het LSP waren aangesloten, gaf 73% aan de voorkeur te hebben voor een regionaal alternatief in plaats van het LSP. Dit gaf aan dat er onder Amsterdamse huisartsen een sterke voorkeur was voor een kleinschalige manier van uitwisselen van gegevens.

Pogingen van zorgverzekeraars om via contractering het LSP alsnog indirect verplicht te stellen voor zorgaanbieders (in het bijzonder, huisartsen en apothekers) hebben in 2013 geleid tot een kort geding en vervolgens tot een bodemprocedure tegen VZVZ die de rechtmatigheid van het LSP bestreed, door de Vereniging Praktijkhoudende Huisartsen (VPH). VPHuisartsen vraagt namens haar achterban al jaren expliciet om mogelijkheden om zelfstandig fijnmazig toegang in te kunnen regelen, met gebruik van end-to-end beveiliging, op een manier die rekening houdt met de voorwaarden van de Wet op de geneeskundige behandelovereenkomst (Wgbo). Dit is wat de Whitebox biedt.

Een andere indicatie dat het ontwerp van de Whitebox een stap in de goede richting is zijn recente uitspraken vanuit het Europese parlement dat end-to-end beveiliging verplicht zou moeten worden bij alle communicatie van persoonsgegevens. Dit sluit aan bij steeds strikter wordende Europese databeschermingsregelgeving[11].

Daarnaast is in recente discussies in de Eerste Kamer in het kader van de Wet cliëntenrechten zorg, een motie aangenomen die expliciet aangeeft dat de toegang tot medische dossiers decentraal via bij de zorgaanbieder vastgelegde toestemmingen en autorisaties en toestemmingen mogelijk moet blijven[12]. Dit is wat de Whitebox doet.

Whitebox Systems en de HKA hebben in navolging van presentaties op de Huisartsenbeurs in 2015 een kleinschalige actie georganiseerd waarmee huisartsen konden aangeven dat zij geïnteresseerd waren in de Whitebox. In totaal zijn hierop ruim 200 aanmeldingen binnengekomen, een groot deel uit Amsterdam. Uit een recent “belrondje” door de Amsterdamse regio-organisatie EZDA, blijkt dat inmiddels ca. 94 van de ca. 258 praktijken in Amsterdam op het LSP is aangesloten; 65 zitten in het

11 http://www.tomshardware.com/news/european-parliament-end-to-end-encryption-communications,34809.html (June 16, 2017)

12 Motie-Teunissen, 33 509 T, https://www.eerstekamer.nl/motie/gewijzigde_motie_teunissen_pvdd_c

aansluitproces. Ca. 38% van de huisartsen ziet het LSP niet zitten. Pas nu komt de Whitebox voor een deel van de huisartsen (die gebruik maken van TetraHIS of MicroHIS) beschikbaar. Tenminste een deel van deze groep huisartsen is geïnteresseerd in de Whitebox. Inmiddels hebben zich zo'n 100 Amsterdamse praktijken zich actief bij Whitebox Systems gemeld als geïnteresseerde, waaronder ook een deel dat reeds het LSP in de praktijk heeft.

In opdracht van de UvA heeft in 2014-2015 een (kwalitatief) onderzoek plaatsgevonden dat de opvattingen over elektronisch uitwisselen van medische gegevens vanuit de huisartsenpraktijk onder artsen en patiënten onderzocht[13]. Dit onderzoek wordt in hoofdstuk 3 besproken.

Een deel van de artsen en een deel van de patiënten denkt dat de voordelen van het LSP opwegen tegen nadelen, zoals onder meer mogelijke privacyschade, terwijl een andere groep denkt dat de nadelen opwegen tegen de voordelen. Belangrijker is dat er onder de patiënten duidelijke groepen te onderscheiden zijn die het ene of het andere systeem prefereren. Het bestaan van deze groepen onderschrijft de stelling dat het bieden van een Whitebox én een LSP binnen de huisartsenpraktijk belangrijk is.

Overigens werd zelfs onder de categorie "medisch kwetsbare" patiënten aangegeven dat zij kozen voor het LSP omdat er geen alternatief was, maar liever een alternatief zouden zien waarbij zij (bijvoorbeeld met een PIN code) hun gegevens beter kunnen beschermen. Whitebox werkt aan een dergelijke oplossing.

Tevens heeft in 2015 een onderzoek plaatsgevonden naar de behoefte aan en ideeën van artsen over een *minimale professionele samenvatting* die minder privacy-invasief is en tevens minder aanleiding kan geven tot *informatie overload* op de huisartsenpost. Dit mede naar aanleiding van een onderzoek van waaruit bleek dat huisartsen op de huisartsenpost Almere vaak vonden dat het daar beschikbare dossier teveel informatie bevatte [vdGeest]. Ook tijdens de behandeling van de wet-EPD in 2010-2011, werd het risico op "information overload" vaak benoemd[14].

Het idee was dat een opvragende partij zijn werk minder goed zou kunnen doen als deze (mogelijk aangezet door overwegingen met betrekking tot aansprakelijkheid bij fouten) een lang dossier van een

13 Eline Roelofsen, "Opvattingen over elektronisch uitwisselen van medische gegevens vanuit de huisartsenpraktijk – welke voorkeuren hebben huisartsen en hun patiënten ten aanzien van de wijze waarop het elektronisch uitwisselen plaatsvindt?" Onderzoek in opdracht van de Universiteit van Amsterdam, september 2015.

14 Expertmeetings wet-EPD, Eerste Kamer 2010/2011, zie https://www.eerstekamer.nl/wetsvoorstel/31466_elektronisch .

andere arts zou moeten doorlezen. Qua privacybescherming speelt verder dat consultinformatie (in de vorm van journaalregels die huisartsen als vrije tekst in hun systeem invoeren) allerlei gevoelige gegevens kan bevatten. Bijvoorbeeld over relatieproblemen, problemen op het werk, of psychische problemen.

Verder is relevant dat Europese regelgeving en de Wet bescherming persoonsgegevens (Wbp), en binnenkort de vervanger van Wbp, de Algemene Verordening Gegevensbescherming (AVG), eisen stelt aan noodzakelijkheid en, daaruit volgend, minimaliteit van gegevensuitwisseling. Het is dus relevant om te zien of de professionele samenvatting aan deze eisen voldoet.

Deze aspecten zijn de basis geweest voor het ontwerp van de *minimale PS* welke in de periode 2015-2017 is ontworpen en onderzocht. Deze PS wordt besproken in hoofdstuk 4.

2 Techniek: concept, werking en toepassing

De Whitebox is een decentrale architectuur. Dit betekent dat de brondossierhouder de regie kan houden over welke gegevens met wie gedeeld worden. Zo kan een huisarts waarborgen dat een arts of apotheker die een autorisatie krijgt, alleen juiste en noodzakelijke gegevens te zien krijgt[15] .

1 Uitgangspunten architectuur

In de architectuur van de Whitebox is het decentrale aspect – eigenaarschap en controle bij de (huis)arts, met van daaruit controle en zeggenschap voor patiënt - consequent doorgevoerd. De Whitebox is een kastje dat van de huisarts is en dat verbonden is met het lokale[16] huisarts informatie systeem (HIS). Verzoeken om informatie komen binnen op de Whitebox, en worden vervolgens geautoriseerd en geverifieerd op basis van door de huisarts instelbare autorisatieregels, voordat de Whitebox een verzoek beantwoordt. Vervolgens wordt een professionele samenvatting geretourneerd die de Whitebox bij het HIS heeft opgevraagd. Deze is instelbaar door huisarts en patiënt. Het gegevenstransport is volledig end-to-end, van een (geautoriseerde) opvragende partij tot aan de bron (de huisarts) beveiligd (versleuteld).

Push autorisatie

De Whitebox introduceert het principe van “push autorisatie”: de huisarts *pusht* autorisaties, waarmee (alleen) de geautoriseerde partij gegevens kan ophalen. De verzendende huisarts neemt het initiatief voor de verzendingvan een autorisatie; een ontvanger kan dus nooit zichzelf autoriseren door zelf een autorisatie “naar zich toe te trekken”.

---

15 EK expertmeetings I en II, 2010 en 2011 (via https://www.eerstekamer.nl/wetsvoorstel/31466_elektronisch) en beroepsprocedure tegen het LSP, Vereniging Praktijkhoudende Huisartsen, http://www.vphuisartsen.nl/nieuws/de-rechtszaak-inzake-stopzetting-lsp-alles-op-een-rij/ en http://www.vphuisartsen.nl/over/lsp/

16 De Whitebox kan ook verbonden worden met een HIS dat gehost is, zoals één van de vele APS HIS-sen. Dit maakt voor het uitgangspunt van de architectuur niet uit: ook een ASP HIS is volledig eigendom van de arts, en de vertrouwelijkheid van de gegevens in het HIS is daarmee gewaarborgd vanuit de Wbp en de Wgbo (beroepsgeheim). Het enige verschil is dat in dit geval de hosting partij cq de ASP leverancier in theorie bij gegevens van patiënten zou kunnen komen door zich fysiek toegang te verschaffen tot de server/database buiten het zicht van de huisarts. De keuze voor een kastje dat bij de huisarts staat maakt duidelijk dat dit bij de Whitebox onmogelijk is.

Het verschil met gewoon “push” verkeer is wel dat de geautoriseerde partij na ontvangst van een autorisatie, met die autorisatie gedurende een gegeven periode in staat is om *live* actuele gegevens bij het systeem van de autoriserende partij – het *bronsysteem* – op te halen. Dit lijkt op “pull” maar het verschil is dat maar één partij de gegevens kan opvragen.

Een push autorisatie is een door de Whitebox gegenereerde unieke URL die als *autorisatie* naar een specifieke partij gestuurd kan worden.

In principe werkt bij de Whitebox elke aanmelding van gegevens als een *push autorisatie* naar een specifieke *target.* Deze target kan op voorhand bekend zijn (bijv. een huisartsenpost of de eigen apotheek), of pas op het moment van autoriseren. Het is bij de Whitebox dus niet zo dat een patiënt “bij de Whitebox” wordt aangemeld. Elke autorisatie is namelijk een unieke autorisatie die logisch is in het zorgproces.

Het is ook belangrijk te melden dat push autorisatie in principe geen Whitebox aan de ontvangende kant vereist[17]: de Whitebox kan ervoor zorgen dat de ontvangende kant gegevens kan inzien door een linkje (de autorisatie heeft de vorm van een web-link, een URL) kan openen met een UZI pas.

De eisen die aan het systeem en de onderliggende standaard worden gesteld, zijn gedefinieerd in Appendix C.

Statische en dynamische koppelingen en binding.

De Whitebox biedt mogelijkheden voor autorisatie van specifieke zorgverleners door het opsturen van een autorisatie-URL. *Hoe* een autorisatie bij een zorgverlener aankomt, op een veilige manier, hangt af van de situatie. Belangrijk daarbij is dat de URL uiteindelijk gekoppeld moet zijn aan de geautoriseerde zorgverlener of zorgaanbieder, zodat de URL alleen geopend kan worden door die zorgverlener of (een zorgverlener van) die zorgaanbieder. Het proces van koppelen van een URL aan een zorgaanbieder of zorgverlener heet *binding.*

Binden kan op voorhand, of op het (eerste) moment van gebruik van de URL.

- Op voorhand binden *(pre-binding).* Dit impliceert dat de (cryptografische sleutel, c.q. het certificaat van) die zorgverlener op voorhand bekend moet zijn;
- Op het eerste moment van gebruik (*late binding).* Dit impliceert dat de URL een periode (nog)

17 Ook aan de verzendende kant kan in principe zonder een Whitebox gewerkt worden; we werken aan een (open) standaard, waardoor leveranciers ook zelf push autorisatie kunnen implementeren.

niet gebonden is, en dat moet worden voorkomen dat een willekeurige persoon of zorgverlener de URL kan gebruiken en dus binden. Er moet in dit scenario een *veilig pad* zijn om de URL naar de uiteindelijke geautoriseerde zorgverlener te krijgen. Hier zijn verschillende methodes voor.

In het geval van de waarneemkoppeling is de autorisatie die naar een huisartsenpost gestuurd wordt altijd *pre-bound,* dus op voorhand gekoppeld aan de huisartsenpost zodat alleen huisartsen[18] op die huisartsenpost de gegevens kunnen inzien.

Een URL kan gebonden worden aan de UZI pas van een zorgverlener of aan de cryptografische sleutel van een systeem dat bij een zorgaanbieder staat. Dit laatste is het geval bij de koppeling met de huisartsenpost, waar een *identity management* systeem staat die een lijst van zorgverleners van die organisatie (en hun credentials, bijv. UZI nummers) bevat. Wanneer een URL die door een Whitebox is uitgegeven via een Hapbox wordt gebruikt door een huisarts met een UZI pas, controleert de Whitebox die bevraagd wordt eerst bij de Hapbox of de betreffende UZI pas daar bekend is, dat wil zeggen, of de betreffende huisarts bij de HAP werkt en de URL mag bevragen.

Hoe de koppeling te leggen is met een identity management systeem zoals die welke onderdeel is van de Hapbox, of alternatief hoe een binding met een zorgverlener (late of pre-bound) gelegd kan worden, raakt aan de kern van het systeem en de bruikbaarheid ervan, omdat dit proces volstrekt veilig maar ook flexibel en praktisch hanteerbaar moet zijn.

De Whitebox heeft een *decentraal* vertrouwensmodel (Appendix C). Daarbij gaat de Whitebox uit van decentrale verantwoordelijkheid voor het valideren van vertrouwenslinks. De huisarts bepaalt, soms zelfstandig en soms samen met de patiënt, welke partijen vertrouwd zijn en geautoriseerd kunnen worden binnen het zorgproces rondom een patiënt.

Om deze *trust* op te bouwen bestaan een aantal mogelijkheden:

1. De huisarts construeert in de Whitebox een harde, statische koppeling met een andere partij; dit kan een individuele arts zorgverlener zijn, bekend middels bijvoorbeeld dienst UZI nummer, maar is in de regel een koppeling met een (identity management systeem van een) specifieke zorgaanbieder. Het laatste gebeurt bij de koppeling met de HAP in de waarneempilot: de huisarts legt een vaste koppeling met een voor de HAP ingerichte Whitebox die bij de HAP staat en die eigendom is van de HAP (de “Hapbox”) via welke later (pre-bound) autorisaties/URLs kunnen worden aangemeld voor individuele patiënten.

18 Of eventueel expliciet en verifieerbaar door de dienstdoende huisartsen gemandateerde en geautoriseerde medewerkers, zoals triagisten

2. De huisarts construeert een *ongebonden* URL, die hij meegeeft aan de patiënt of verzendt via een bepaalde vertrouwde intermediair (dit kan bijvoorbeeld het veelgebruikte *ZorgDomein* systeem voor doorverwijzingen zijn) waarbij er vanuit gegaan wordt dat de URL niet op een verkeerde plek kan terechtkomen. Door de manier waarop binding werkt, is altijd helder *wie* de URL heeft opgepakt – [late] binden kan slechts eenmalig, wat het risico reduceert dat iemand ongemerkt misbruik kan maken van een verstuurde URL;
3. De laatste variant van *late binding,* aangevuld met een techniek om de *(late) binding* te valideren. Dit kan bijvoorbeeld door naast het versturen van de URL een *autorisatiecode* (vergelijkbaar met een PIN code) met de patiënt mee te geven, die nodig is vóórdat de URL gebruikt en gebonden kan worden.

Hoewel we inmiddels een aantal toepassingen hebben ontwikkeld die gebruik maken van dynamische koppelingen die gebruik maken van variant 3 (deze zijn momenteel in de testfase), ligt de nadruk voor het pilot onderzoek op de minder complexe variant 1.

In de pilot heeft de HAP een *HAPbox*. Elke arts met een Whitebox maakt eenmalig een vaste koppeling met de HAPbox van de HAP waarmee hij/zij een waarneemcontract heeft. Om deze koppeling te valideren is een procedure ontwikkeld waarbij de huisarts na registratie op een veilige manier een autorisatiecode krijgt toegestuurd; pas na invoeren van deze code is de koppeling geldig en bruikbaar. Tijdens de pilot bleek dat de autorisatiecode in de praktijk een aantal malen via het zorgmail e-mailsysteem van eNovation werd verstuurd; omdat de code alleen bruikbaar is om een reeds gelegde koppeling[19] te autoriseren, is ook deze procedure afdoende veilig.

Bij het aanmelden van de patiënt bij de target “Waarneming” wordt tevens een filter voor de *professionele samenvatting* geregistreerd, in het HIS en/of in de Whitebox. Dit filter wordt toegepast over de opgehaalde gegevens (die de Whitebox *live* kan ophalen uit het HIS) als een huisarts van de huisartsenpost de URL gebruikt om gegevens op te halen.

19 De registratie van de Whitebox bij de Hapbox, voorafgaand aan het sturen van een autorisiatiecode, houdt reeds een registratie van de sleutel van de betreffende Whitebox bij de Hapbox in; het is dus niet mogelijk met een eventueel gestolen autorisatiecode een willekeurig ander (Whitebox) systeem te koppelen.

Fig. 1 laat de procedure zien:

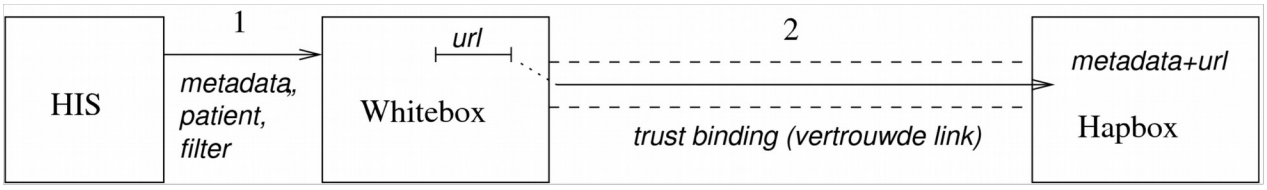


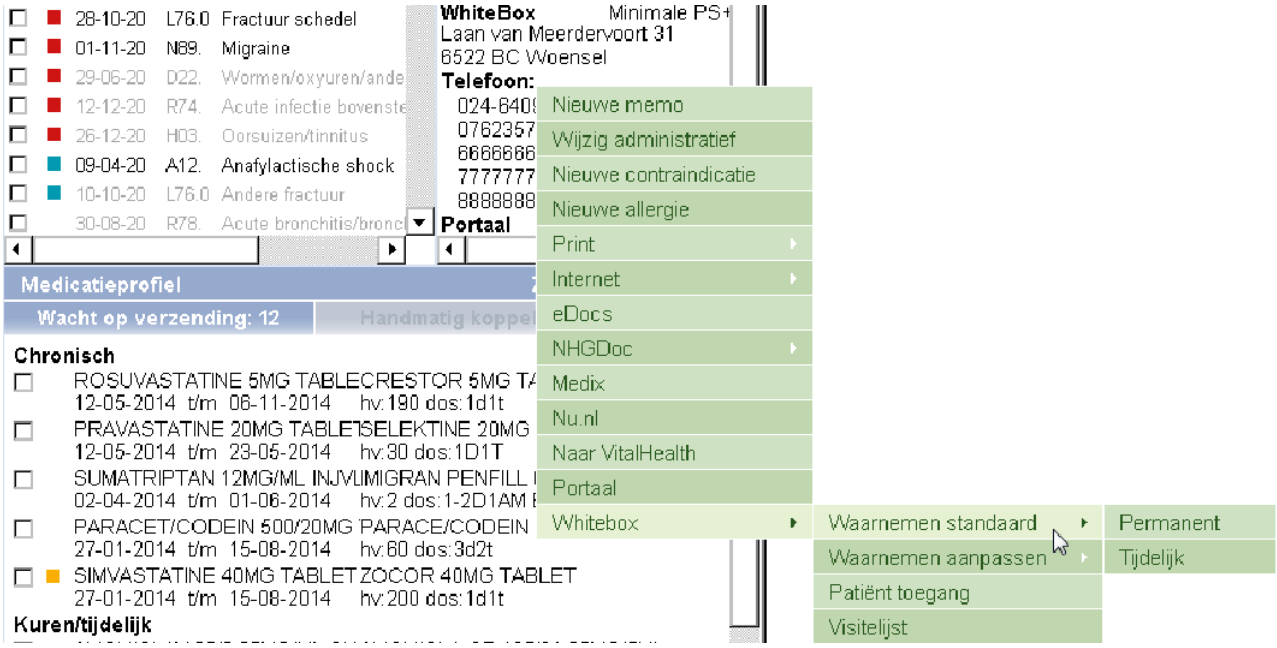
Fig. 1: Aanmelden patiënt bij de HAP. *Wanneer de huisarts een patiënt aanmeldt, specificeert deze de target "Waarneming" en een filter die aangeeft welke gegevens uit het dossier in de PS mogen komen. Het HIS stuurt NAW en andere gegevens van de patiënt (metadata) op naar de Whitebox, die een URL genereert en samen met de metadata aanmeldt bij de Hapbox, over de eerder opgezette vertrouwde link. Voor het opvragen van de gegevens van een patiënt wordt de metadata doorzocht en de URL geselecteerd in de Hapbox om – via een aantal stappen – de gespecificeerde PS op te kunnen vragen bij de Whitebox.*

Voor bruikbaarheid van het systeem is het essentieel om voor partijen met wie veel gecommuniceerd wordt – zoals de HAP en de eigen, vaste apotheek – een vaste vertrouwenslink te construeren. Dit proces is eenvoudig; voor de HAP koppeling initiëren we dit direct bij installatie van de Whitebox.

Wanneer er eenmaal een decentrale, één-op-één vertrouwenslink ligt, hoeft er bij volgende aanmeldingen niet langer te worden nagedacht over hoe een autorisatie (URL) veilig op de plek van bestemming te krijgen[20], dat kan over de dan reeds bestaande link.

De procedure om een geautoriseerde *trust link* tussen huisarts en huisartsenpost op te zetten is geëvalueerd in de pilot.

20 Uiteraard is dat laatste nog wel een punt voor dynamische "workflows" waarbij de ontvangende partij niet op voorhand al bekend is (bijvoorbeeld bij een open verwijzing). Hiervoor worden oplossingen uitgewerkt. Echter een groot deel van de dagelijkse situaties betreffen vaste partijen.



Figuur 2: "Rechtermuisknopmenu" voor het aanmelden van patiënten in het consultscherm in TetraHIS

2 Instelbare ontsluiting van gegevens: maatwerk samenvatting dossier

Autorisatie gaat in feite over de vraag *wie welke* gegevens mag inzien. Er is al aangegeven dat push autorisatie het mogelijk maakt om een specifieke zorgverlener of zorgaanbieder te autoriseren, zodat deze gegevens kan opvragen. Daarnaast echter is altijd relevant dat alleen de noodzakelijke gegevens opgevraagd (kunnen) worden. Welke gegevens in een bepaalde situatie *noodzakelijk* zijn voor een andere zorgverlener, hangt af van de situatie.

In de Whitebox is het *filter* dat bepaalt welke gegevens bij een specifieke push autorisatie, voor een specifiek soort ontvangende zorgverlener beschikbaar zijn, instelbaar per autorisatie. Mogelijkheden zijn een actueel medicatieoverzicht of AMO (welke feitelijk voor elke specialist en apotheker beschikbaar kan en moet worden gesteld – dit omvat alleen medicatie, allergieën, intoleranties en contra-indicaties), een minimale professionele samenvatting (AMO + een week of helemaal geen journaalregels, en een lijst van episodes met een attentiewaarde), een NHG professionele samenvatting (AMO + 4 maanden journaalregels en alle episodes), en een uitgebreide professionele samenvatting (zoals de NHG samenvatting, maar dan met journaalregels tot 2 jaar terug). Dit maakt maatwerk mogelijk.

De effectiviteit van de minimale PS als privacy-vriendelijk alternatief voor de NHG PS is onafhankelijk onderzocht door de Vrije Universiteit; het resultaat wordt later in dit verslag samengevat.

3 Innovaties: doorautoriseren en policies aan de bron

Whitebox URLs zijn gebonden aan een systeem of een gebruiker. Deze URL is vervolgens alleen nog bruikbaar voor de gebonden partij. Bij “workflows” waarin niet altijd voorhand voorspelbaar is welke gebruiker toegang nodig heeft tot gegevens, maakt de Whitebox mogelijk dat een (gebonden) gebruiker en/of de patiënt op een traceerbare wijze een nieuwe URL kan aanvragen[21], welke aan een zorgverlener (met een UZI pas) gegeven kan worden. Zo wordt het mogelijk voor een arts die bij de huisartsenpost werkt om een autorisatie ‘door te zetten’ naar bijvoorbeeld de dienstapotheker, of naar een arts van een spoedeisende hulp of een andere huisartsenpost in een andere regio. Deze functionaliteit is binnen de pilot nog niet getest, maar wel reeds ontwikkeld.

Een huisarts en/of de patiënt kan zelf een “policy” instellen in de Whitebox, die bepaalt of, en zo ja in welke situatie een geautoriseerde zorgverlener een autorisatie kan aanmaken en doorzetten.

Een belangrijke eigenschap is dat alle gebruik – inclusief *doorautorisaties* – van een URL altijd traceerbaar zijn naar de persoon die de URL heeft aangemaakt of gebruikt. Zo is aan de bron – voor huisarts en patiënt – altijd inzichtelijk wie op welk moment een autorisatie heeft aangemaakt, ontvangen, of gebruikt. Dit realiseert een balans tussen privacybescherming enerzijds, en inzetbaarheid/werkbaarheid in de praktijk anderzijds.

Rolgebaseerde toegangscontrole (RBAC)

De toegang tot gegevens wordt op het moment van bevraging bepaald door de functie/rol van de opvragende partij; vast te stellen, normaliter op basis van de *rolcode* die op de UZI pas van de opvragende zorgverlener vermeld staat. De meeste partijen zullen in de praktijk alleen een medicatieoverzicht en ICA informatie kunnen zien; andere informatie uit de PS wordt bij een doorautorisatie standaard weggefilterd behalve wanneer de opvragende partij een huisarts is.

Doorautoriseren

De mogelijkheid tot doorautoriseren maakt dat het Whitebox autorisatiesysteem flexibel bruikbaar is, ook in situaties die niet volledig te voorzien zijn. Tegelijkertijd zorgt het systeem ervoor dat er altijd een persoon – een arts – traceerbaar is als degene die de doorautorisatie realiseerde. Er zitten beperkingen

21 De voor de ontvangende partij zichtbare gegevens kunnen verschillen van de oorspronkelijke PS; meestal zal alleen een actueel medicatieoverzicht zichtbaar zijn (een apotheker zal minder informatie kunnen zien dan een huisarts).

aan de mogelijkheden tot doorautoriseren en aan de gegevens die hiermee beschikbaar worden gesteld. RBAC (role-based access control) met betrekking tot welke gegevens beschikbaar zijn is vermeld, maar RBAC wordt ook toegepast om te bepalen of een bepaalde zorgverlener een autorisatie mag uitgeven aan een andere partij.

Hoe vaak en in welke situatie een URL kopieerbaar is wordt bepaald door een *policy* die is ingesteld aan de bron, in de Whitebox. Er zijn vele policies denkbaar, waarbij de eigenschappen van de policy bepaald worden door (veel voorkomende) praktijkscenario's. Zo mag bijvoorbeeld een huisarts op de HAP een autorisatie doorzetten naar een SEH of naar een huisartsenpost in een andere regio, maar zal een dergelijke actie voor een openbare apotheker veel minder gebruikelijk zijn; die zal wellicht wel een autorisatie kunnen doorzetten naar een collega (dienst)apotheker die een herhaalrecept krijgt – waarbij die collega alleen een medicatieoverzicht kan zien – maar niet naar andere partijen. Een geautoriseerde dienstdoende huisarts of een SEH zal daarentegen wel een tijdelijke (door)autorisatie kunnen aanmaken om te zorgen dat een medicatieoverzicht inzichtelijk wordt gemaakt voor de (dienstdoende) apotheek wanneer deze een recept ontvangt[22]; ook kan deze een doorautorisatie maken voor de specialist wanneer de patiënt wordt opgenomen. Dit maakt dat het systeem de zorg rond de patiënt kan volgen. Daarbij wordt de patiënt elke keer geïnformeerd en is elke autorisatie traceerbaar aan de bron. Een aantal van deze scenario's is inmiddels uitgedacht voor de Whitebox, als basis voor het implementeren van een aantal standaard policies die passen bij het (Nederlandse) zorgveld.

Soorten berichten

Een belangrijke eigenschap die Whitebox URLs onderscheidt van bestaande systemen, is dat Whitebox URLs in principe onafhankelijk zijn van het precieze type medische informatie, of het precieze berichtenformaat dat via deze URL kan worden opgehaald of verstuurd. Het systeem is primair een autorisatiesysteem, en daarmee in staat verschillende documenten te transporteren. De Whitebox kan dan ook werken met verschillende berichtentypes, in Nederland "gestandaardiseerde" maar ook niet-gestandaardiseerde. Type aanduidingen in de URLs zorgen ervoor dat de cliënt kan zien welke gegevens beschikbaar zijn, zodat de cliënt desgewenst de meest geschikte kan selecteren: als alternatief kunnen meerdere URLs beschikbaar zijn voor één brondocument/dossier.

Ten slotte kunnen Whitebox URLs gebonden worden aan andere authenticatiemiddelen dan UZI passen. De mogelijkheden zijn instelbaar aan de bron. Zo is het bijvoorbeeld mogelijk om binnen een ziekenhuis, of op het niveau van een zorggroep, zelf (decentraal) authenticatiemiddelen uit te geven voor zorgverleners die lid zijn van die organisatie. Dit vereist dat er in deze organisatie een specifiek

22

identity management systeem wordt gebruikt en ingeregeld; ook mandateringen kunnen via een dergelijk systeem (onweerlegbaar) vastgelegd worden. Aan deze oplossingen wordt gewerkt.

4 Afbakening en doel pilot en verslag

Dit verslag beschrijft de *waarneempilot* met de Whitebox waarneemkoppeling die in de periode 2015-2017 is uitgevoerd in Amsterdam. In deze pilot is de Whitebox gebruikt om gegevens beschikbaar te stellen aan dienstdoende huisartsen op de huisartsenpost. Doordat dit een *geïntegreerde* koppeling betreft, die volledig onderdeel is gemaakt van het systeem van de huisarts en het systeem op de huisartsenpost, heeft de realisatie en uitvoering van de pilot enige tijd in beslag genomen.

De Whitebox is aan de huisartsen kant geïntegreerd in het huisartsensysteem TetraHIS, en in gebruik genomen door 20 van de ca. 30 huisartsen die in 2015 in Amsterdam TetraHIS gebruikten[23]. Via de Whitebox kunnen patiëntendossiers uit TetraHIS via de Whitebox opvraagbaar worden gemaakt voor huisartsen op de huisartsenpost. Naast 20 huisartsen met TetraHIS is medewerking verleend door de Huisartsenposten Amsterdam (HpA), en door Labelsoft, die een koppeling met de Whitebox in het systeem Call Manager gerealiseerd heeft.

Criteria voor de waarneemkoppeling in de pilot zijn:

- Betrouwbaarheid / robuustheid van de koppeling
- Eenvoud van gebruik in de praktijk (voor artsen)
- Begrijpelijkheid van het systeem (voor artsen én patiënten)
- Correctheid van de gegevens die overkomen / opgehaald worden

Later in dit verslag wordt de evaluatie van deze (en andere) aspecten beschreven.

23 Inmiddels zijn dit meer praktijken; we zijn in 2015 gestopt met vragen toen we het streefaantal van 20 bereikten. Huisartsen hebben ook voor de pilot reeds betaald voor het product. Inmiddels is ook een implementatie van de koppeling met MicroHIS gerealiseerd.

3 De Amsterdamse waarneempilot: opzet en implementatie

Aan de pilot in Amsterdam doen 20 huisartsen mee, die het HIS van Tetra (TetraHIS, heden Bricks Huisarts genoemd) gebruiken. Dit is ongeveer 70% van de TetraHISsers in Amsterdam op het moment dat met de pilot werd begonnen[24]. Aan de kant van de Huisartsenpost wordt de pilot ondersteund door het Call Manager systeem van Labelsoft. De Huisartsenposten Amsterdam (HpA) hebben meegewerkt aan het installeren van een zogeheten "Hapbox" op de HAP, en heeft zorggedragen voor de administratieve handelingen die met beheer van het systeem gemoeid zijn.

Het systeem dat wordt gebruikt in de waarneempilot bestaat uit de volgende componenten:

1. Whiteboxen bij de huisartsen. De 20 TetraHIS huisartsen hebben elk een eigen Whitebox. Deze staat in het lokale netwerk van het TetraHIS systeem (TetraHIS staat lokaal in de praktijk), in veel gevallen letterlijk fysiek naast of op de TetraHIS server. Via een service die op de TetraHIS database server draait is het HIS opvraagbaar voor patiënten die zijn aangemeld door Tetra; deze service levert vervolgens een *professionele samenvatting* op. Het aanmelden vindt plaats via een protocol (API) dat de Whitebox aanbiedt. Hiermee geeft Tetra van elke aangemelde patiënt door wat diens lokale TetraHIS identifier, en diens BSN en andere *metadata* (naam, adres, geboortedatum, geslacht) zijn. De lokale ID is nodig voor het kunnen opvragen van een *PS*.

2. Een Hapbox bij de Huisartsenpost (HAP). De Hapbox is een systeem bij de HAP dat eigendom is van de HpA. Het is een server die er net zo uitziet als een Whitebox. De Hapbox wordt via het Internet benaderd door Whiteboxen van artsen die zich willen aanmelden bij de HAP, waarna de Hapbox beheerder de aanmelding moet goedkeuren. Vervolgens kunnen de aangesloten Whiteboxen de *metadata* en URLs registreren voor alle patiënten die de huisartsen aanmelden (zie hoofdstuk 6). Deze informatie belandt in een *index* in de Hapbox. De index kan te allen tijde geüpdatet worden door de HISsen/Whiteboxen (bijv. bij afmelden patiënt of veranderen van het woonadres van een patiënt). Via deze index kan het HAPIS zoeken of een patiént via een Whitebox gegevens beschikbaar heeft gesteld.

Een tweede functie naast de *index* functie is dat de Hapbox een register bevat van (de UZI passen van) alle artsen en medewerkers op de HAP. Dit is *identity management* functionaliteit. De Hapbox beheerder (een medewerker van de HAP) is verantwoordelijk voor het beheren/actualiseren van de lijst met UZI passen van geautoriseerde medewerkers van de HAP. Daarnaast kan de Hapbox beheerder

24 We zijn gestopt met huisartsartsen bellen of zij mee wilden doen toen het aantal van 20 deelnemers bereikt was, omdat dit het voor de pilot afgesproken maximum aantal was.

de *logging* inzien betreffende alle relevante operaties zoals het zoeken en opvragen van gegevens.

De Hapbox heeft dus als functie:

- Het managen (aanmelden/afmelden) van Whiteboxen van aangesloten huisartsen
- Het managen van een index met door de verschillende Whiteboxen aangemelde patiënten en hun metadata, die doorzoekbaar is voor het HAPIS;
- Identity management: het bijhouden van een lijst van UZI passen/credentials van alle artsen en medewerkers die werkzaam zijn op de HAP en die toegang tot Whitebox gegevens mogen hebben.

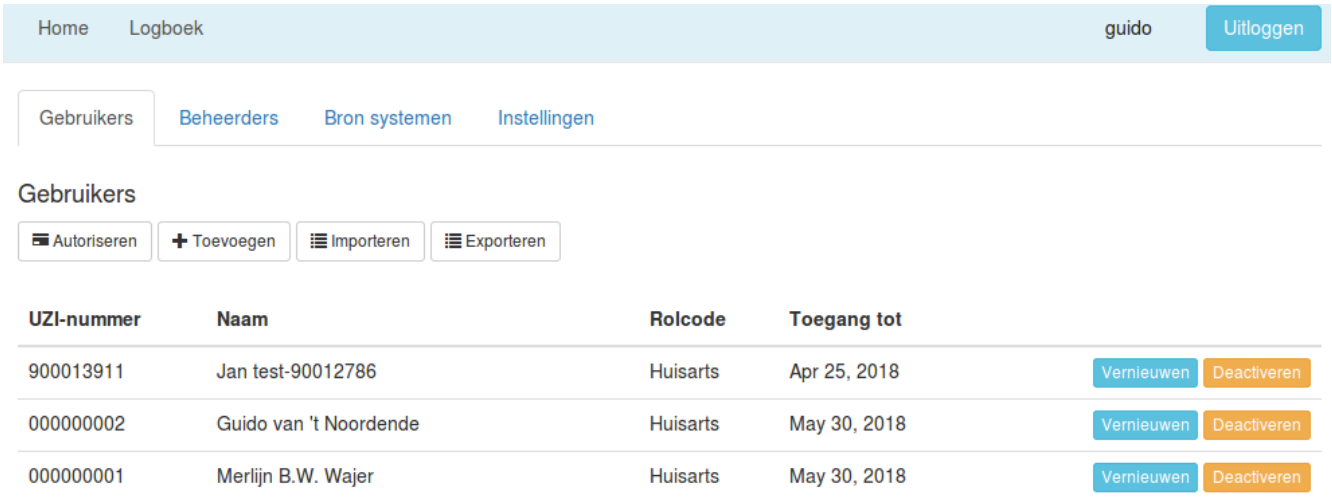


Fig. 2: Beheersinterface van de Hapbox; hier getoond de interface voor gebruikersautorisaties.

Van belang is dat ook de Hapbox een decentraal systeem is, dat eigendom van de huisartsenpost is. Immers, dáár is het dat de patiënt wordt aangemeld: de HAP is als organisatie de zorgaanbieder de (contractueel) de verantwoordelijkheid voor de dienstwaarneming voor huisartsen in de avonden, nachten en weekenden op zich neemt.

NB: De ontwikkeling van het systeem is niet met de Hapbox begonnen, maar met de ontwikkeling van push autorisatie vanuit de Whitebox (huisarts). De ontwikkeling van de Hapbox is ontstaan ten behoeve van en in het kader van de pilot, met als doel om autorisaties bij de huisartsenpost te kunnen registreren (en daarmee, impliciet, autorisaties te kunnen koppelen (binden) aan de huisartsenpost) zodat alleen huisartsen die aan de huisartsenpost verbonden zijn, de gegevens van een patiënt waarvoor de HAP geautoriseerd is kunnen opvragen.

Concreet betekent dit dat op het moment dat een patiënt daadwerkelijk bevraagd wordt via een

(gebonden) URL die oorspronkelijk door de Whitebox is uitgegeven, de Whitebox eerst bij de betreffende Hapbox nagaat of de arts (UZI pas) in de (vertrouwde) gebruikersadministratie als geautoriseerd is opgenomen. Daarnaast geeft de Hapbox voordat het dossier wordt opgevraagd,

1 Integratie Whitebox in TetraHIS

De Whitebox is volledig geïntegreerd in TetraHIS. De Whitebox kan gezien worden als een communicatiemodule van het HIS; welke gegevens ontsloten worden, voor welke partijen, wordt door de arts vanuit TetraHIS bepaalt. Het primaire doel van uitvoeren van de Whitebox als “hardware communicatie module” is dat dit de implementatie van de beveiligingsprotocollen gescheiden blijft van de HIS implementatie, en zo het HIS ontzorgt maar tevens zorgt dat de Whitebox communicatieprotocollen kunnen worden doorontwikkeld (en de beveiliging van het systeem gewaarborgd kan blijven) zonder dat daarbij een te grote afhankelijkheid van het HIS ontstaat. Voor een beveiligingssysteem is bijvoorbeeld relevant dat het direct geüpdatet kan worden zonder daarvoor de volgende release van het HIS af te hoeven wachten.

In een praktijkscherm in het HIS kan onder meer de *default PS* voor de waarneemkoppeling worden ingesteld. Tevens kan in het praktijkscherm:

- De koppeling tussen HIS en Whitebox worden ingesteld of verbroken;
- Het aantal aangemelde patiënten bekeken worden
- batch (her)aanmeldingen, afmeldingen of correcties voor lijsten patiënten, via een wizard.

Voor de huisarts is de Whitebox op vier manieren zichtbaar:

1. De huisarts kan rechtstreeks op zijn/haar Whitebox inloggen, onder meer om vertrouwenslinks met derde partijen op te zetten. Tevens kan de huisarts zo de gedetailleerde logging bekijken, en accounts uitgeven voor zichzelf en collega’s (bijv. visite-app) en voor patiënten.
2. De huisarts ontvangt een mail van de Whitebox als er iets relevants te zien is op de Whitebox (bijv. Loggegevens na opvragen van gegevens); dan kan de huisarts op de Whitebox inloggen voor meer informatie;
3. Het HIS kent één of meer “aanmeldknoppen” in het patiëntscherm / consultscherm van de patiënt waarmee de huisarts de patiënt kan aanmelden bij specifieke *lijsten* van de Whitebox. Bijvoorbeeld de waarneemlijst (voor de pilot) of de visitelijst (maakt patiënt zichtbaar op de visite-app). Via deze knoppen kan de huisarts ook het PS filter voor de patiënt aanpassen (zie figuur).
4. Op de Whitebox is van elke patiënt de PS te zien via een “preview” modus. Zo kan de arts precies zien wat er in de PS te zien is.

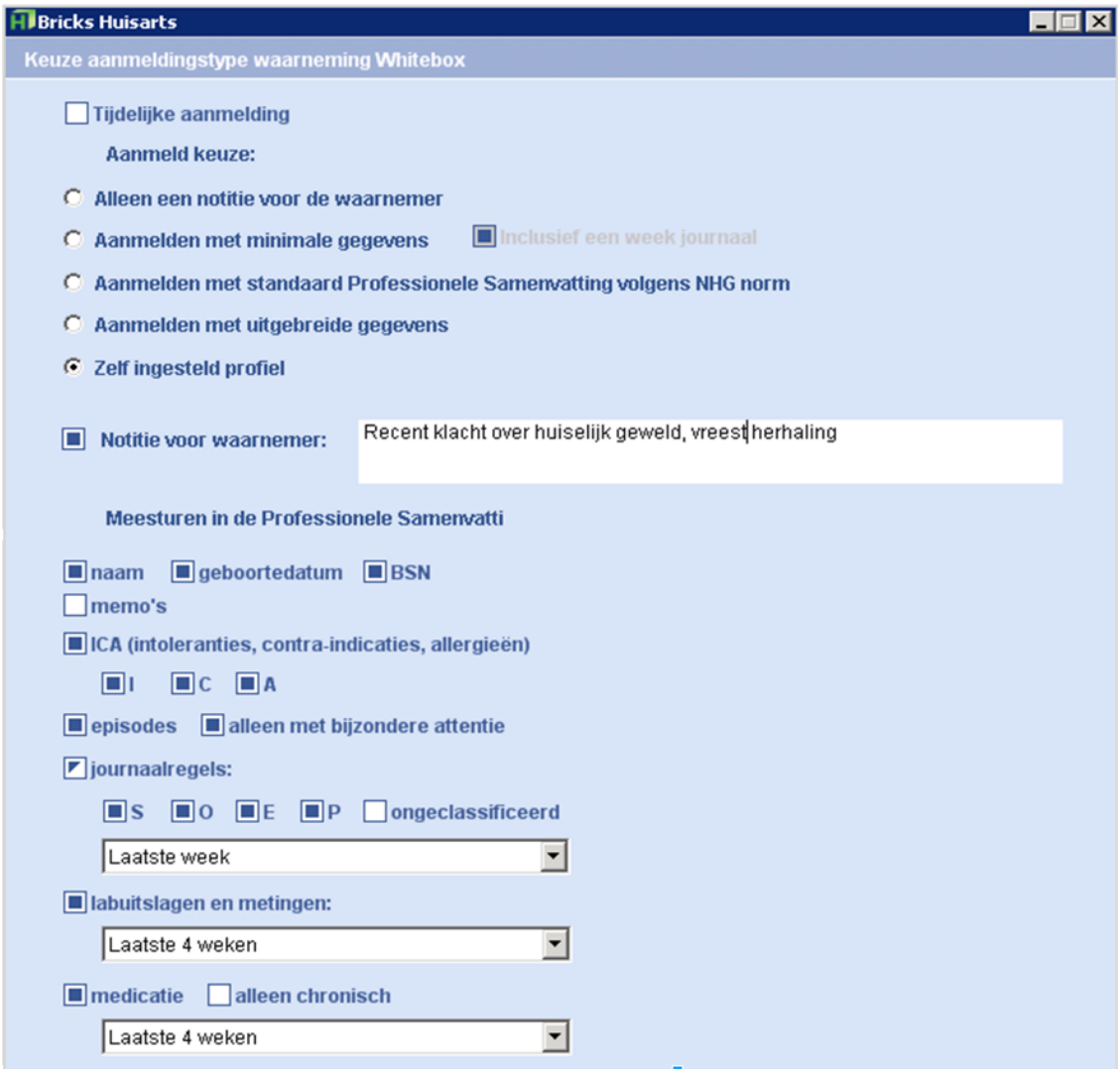


Fig. 3: scherm om (custom) aanpassingen aan de inhoud van een PS te kunnen invoeren, in TetraHIS. Dit scherm is zowel beschikbaar om praktijkbreed als per patiënt aanpassingen aan de (default) PS te kunnen instellen.

2 Integratie in het HAPIS (Call Manager)

Voor de pilot was het essentieel dat de HAP koppeling geïntegreerd zou worden in het HAPIS. Hoewel de Hapbox een eigenstandige web interface heeft waarop geautoriseerde huisartsen met een UZI pas kunnen inloggen om patiëntgegevens op te zoeken en op te vragen, is bij een huisartsenpost met ruim 400 huisartsen ondenkbaar dat huisartsen een ander systeem naast het HAPIS gebruiken voor inzage in patiëntendossiers, gegeven de drukte van diensten waarin elke extra stap niet alleen ingewikkeld, maar ook (te) tijdrovend is. Daarom is van het begin af aan ingezet op een geïntegreerde koppeling.

Het HAPIS – in geval van de HpA Call Manager van Labelsoft – moet geautomatiseerd kunnen vinden

of er via één van de Whiteboxen van aangesloten huisartsen gegevens van een bepaalde patiënt beschikbaar zijn, en deze vervolgens kunnen opvragen. Om dit te kunnen realiseren moet het Whitebox systeem – concreet de Hapbox die onderdeel uitmaakt van het Whitebox waarneemsysteem – de volgende functies bevatten:

1. Zoekfuncties voor het HAPIS om specifieke patiënten te kunnen zoeken / vinden op basis van metadata (naam, adres, geboortedatum, geslacht, BSN);
2. Een manier om een URL aan Call manager te geven waarmee een arts de PS kan opvragen bij de Whitebox van de arts van betreffende patiënt;
3. Een methode voor authenticatie van de opvragende arts, die werkt binnen Call manager; heden wordt *token authenticatie* gebruikt voor het authenticeren van de arts bij het opvragen van de PS bij de Whitebox van de arts van de patiënt. Dit vindt plaats over een beveiligde verbinding met de Whitebox die door Call manager is opgezet, en is onzichtbaar voor de opvragende arts.
4. Een manier om zeker te zijn dat alleen geautoriseerde zorgverleners gegevens kunnen opvragen middels genoemde UZI passen (identity management).

De interfaces voor deze interacties zijn beschikbaar als REST en als JSON-RPC interfaces. Weliswaar blijkt het implementeren van de cliënt software om de Hapbox / Whitebox interfaces vanuit Call manager te bevragen niet zo triviaal dat het in een dag gedaan is, het is wel in relatief korte tijd te doen. De belangrijkste reden dat de implementatie langer duurde dan verwacht, is dat de het Whitebox project als een pilot project voor alleen de HAP Amsterdam niet altijd de hoogste prioriteit kon krijgen.

3 Informatievoorziening patiënten

Voor de pilot is in 2014/2015 een patiëntenfolder ontworpen die de waarneemtoepassing beschrijft[25]. Hierin worden de eigenschappen van de Whitebox uiteengezet alsmede het doel (beschikbaarheid van gegevens op de huisartsenpost), en wordt de toestemmingsprocedure voor de koppeling met de huisartsenpost uitgelegd. Hierbij wordt uitgegaan van expliciete toestemming vooraf, op basis van de informatie die de arts verschaft, *tenzij* in geval van medische noodzaak waarbij de patiënt niet in staat is om toestemming te geven[26]. Dit is gebaseerd op de visie van de HKA dat toestemming vragen

25 Zie: https://hka-pilot.nl/static/bindocs/patientenfolder.pdf

26 Het wettelijk kader waarbinnen de pilot opereerde stond en staat dit toe, mits de gegevensuitwissleing geen verwerking van persoonsgegevens door een derde partij impliceert. Ook het huidige wettelijke kader (Wgbo en de Wet cliëntenrechten bij elektronische uitwisseling van gegevens in de zorg) staat dit toe; zie Appendix D.

belangrijk is. Whitebox Systems deelt deze visie: ook Whitebox Systems gelooft dat toestemming vragen essentieel is als basis van vertrouwen, doordat zo voor de patiënt volstrekt helder (transparant) is welke gegevens uitgewisseld worden met wie. Er is ruimte voor uitzonderingen en dat is belangrijk, maar de initiators van de Amsterdamse pilot vonden dat de norm moet zijn dat de patiënt – zeker als uitwisseling niet strikt noodzakelijk is – eerst om toestemming gevraagd wordt voordat zijn of haar gegevens worden uitgewisseld.

De folder is in 2015 voorgelegd aan patiëntenvereniging Cliëntenbelang Amsterdam (CBA). Zij hebben de folder ook gedeeld met een aantal patiënten uit hun achterban. Het CBA heeft geen aanvullend commentaar ter wijziging van de folder gegeven. Ook een (her)lezing door onder meer deelnemende artsen riep geen (negatieve) reacties of vragen op. Er was wel een verzoek om een Engelstalige versie van de folder, door een arts in Amsterdam Zuid-Oost. Deze is inmiddels gerealiseerd.

In de pilot is de folder aan de patiënt meegegeven bij de toestemmingsvraag. In een aantal gevallen namen patiënten de folder eerst naar huis om deze rustig te kunnen lezen alvorens te beslissen om wel of geen toestemming te geven. Tot nog toe zijn hier geen aanvullende vragen op gekomen, ook deze patiënten antwoordden uiteindelijk “is goed” aan hun arts.

De patiëntenfolder zal iets moeten worden aangepast om deze in de toekomst ook bruikbaar te maken als informatievoorziening bij het vragen van toestemming voor andere koppelingen dan met de huisartsenpost, door een aantal paragrafen die nu exclusief de koppeling met de huisartsenpost beschrijven aan te passen. Deze aanpassing is in voorbereiding maar beïnvloedt de huidig gegeven toestemmingen niet (omdat op basis van deze toestemmingen, de patiënt alleen is aangemeld bij de huisartsenpost).

4 Evaluatie

In dit hoofdstuk evalueren we de aannames, opzet en het gebruik van het Whitebox systeem, zowel de component bij de huisarts (Whitebox) als de component bij de huisartsenpost (Hapbox). De evaluatie omvat een onderzoek naar patiënt/artsperspectieven op de Whitebox en andere systemen, een onderzoek naar de opzet en effectiviteit van de voor en tijdens de Whitebox pilot ontwikkelde minimale PS, en een rapportage van de ervaringen van huisartsen en de huisartsenpost ten aanzien van het model en het gebruik van het systeem in de praktijk.

1 Onderzoek voorkeuren patiënten en huisartsen

In 2015 is in het kader van de pilot in opdracht van het Informatica Instituut van de Universiteit van Amsterdam (UvA) een onafhankelijk onderzoek gedaan naar de opvattingen van patiënten en zorgverleners aangaande de elektronische uitwisseling van medische gegevens.

Dit onderzoek richtte zich op de vraag hoe huisartsen en patiënten / burgers denken over de wijze waarop medische gegevens elektronisch uitgewisseld (zouden moeten) worden; het onderzoek wordt in geactualiseerde vorm publiek gemaakt in het kader van de pilot [Roelofsen 2017].

In het onderzoek zijn de afwegingen en voorkeuren van huisartsen en patiënten onderzocht door middel van diepte-interviews onder een aantal huisartsen en patiënten. In de gesprekken kregen de deelnemers verschillende aspecten voorgelegd waarin huidige systemen (LSP en Whitebox) van elkaar verschilden, en werd hun gevraagd om hun afwegingen en voorkeuren rondom deze situaties te delen. De verschillen werden als eigenschappen van systemen voor uitwisseling van medische gegevens gepresenteerd zonder dat helder was of het eigenschappen van het LSP of de Whitebox betrof. Dit was het beginpunt van een open gesprek waarin respondenten werden uitgenodigd hun eigen ideeën over de uitwisseling van gegevens te formuleren.

Uit het onderzoek werd duidelijk dat er zowel onder huisartsen als onder patiënten subgroepen onderscheiden kunnen worden die verschillende afwegingen maken en verschillende wensen uiten aangaande het wel of niet uitwisselen van gegevens.

Onder patiënten worden drie subgroepen geïdentificeerd:

1. patiënten die zich medisch kwetsbaar voelen;
2. patiënten die zich sociaal kwetsbaar voelen;
3. gezonde patiënten c.q. niet speciaal kwetsbare patiënten.

Op basis van hun medische gezondheid en achtergrond, maken patiënten uit verschillende subgroepen verschillende afwegingen ten aanzien van hun bereidheid tot het elektronisch uitwisselen van medische gegevens en ten aanzien van de wijze waarop dit gebeurt.

- Patiënten die zich medisch kwetsbaar voelen, achten het belang van het elektronisch uitwisselen van gegevens groot. Zij stellen in eerste instantie minder eisen aan de wijze waarop het uitwisselen plaatsvindt.

- Patiënten die zich sociaal kwetsbaar voelen door hun medische situatie of achtergrond, zijn kritisch over het uitwisselen van medische gegevens en over de wijze waarop dit gebeurt. Zij willen graag controle houden over wie welke gegevens leest.

- Gezonde patiënten verwachten niet altijd winst uit het delen van gegevens, maar hebben vaak ook weinig te verbergen. Zij vinden het niet altijd nodig om kritisch te kijken naar het uitwisselen van gegevens.

Het vertrouwen in de eigen huisarts is over het algemeen groot, en men is daarom geneigd eenvoudig het advies te volgen van de huisarts. Een deel van de gezonde patiënten is kritischer en betwijfelt de noodzaak van het op voorhand beschikbaar stellen van medische gegevens.

Uit de gesprekken werd duidelijk dat vrijwel **alle** patiënten (in alle drie subgroepen, dus óók de medisch kwetsbare patiënt) liever meer controle hebben over hun medische gegevens dan nu mogelijk is (in het LSP). Slechts een deel van de patiënten laat deze wens tot meer controle meespelen in de uiteindelijke beslissing om wel of geen toestemming te geven. Als patiënten inschatten dat hun risico op gezondheidsschade groot is, prevaleert aanwezigheid van een uitwisselingssysteem uiteindelijk voor op de wijze waarop deze uitwisseling plaatsvindt.

Ook onder huisartsen werden twee subgroepen onderscheiden, namelijk zelfstandig cq individualistisch ingestelde huisartsen, en collectivistisch ingestelde huisartsen.

- De ‘Individualistisch ingestelde huisarts’ betwijfelt of de laagdrempelige beschikbaarheid van medische gegevens tot verbeteringen in de kwaliteit van zorg of patiëntveiligheid leidt. Zij vindt de potentiële gezondheidswinst van een enkele patiënt niet opwegen tegen het risico op privacy-schade voor een grote groep patiënten. Zij wil graag dat alleen die gegevens in te zien zijn die relevant zijn voor een specifieke zorgverlener in een specifieke situatie.

- De ‘collectivistisch ingestelde huisarts’ benadrukt het belang van de aanwezigheid van medische gegevens voor de continuïteit van de zorg, en gaat ervan uit dat dit de kwaliteit van zorg en patiëntveiligheid zal vergroten, zelfs al is het maar voor een enkele patiënt. Zij achten het risico op privacy-schade niet zo groot en stellen de potentiële gezondheidswinst van een enkele patiënt voorop in hun afweging. Zij hebben in eerste instantie minder duidelijke voorkeuren voor de wijze waarop het uitwisselen geregeld wordt.

De afwegingen en voorkeuren van de collectivistisch ingestelde huisartsen komen overeen met de afwegingen en voorkeuren van de medisch kwetsbare patiënten en veel gezonde patiënten die in ieder geval verzekerd willen zijn van toegang tot hun gegevens in noodsituaties. De individualistisch ingestelde huisartsen sluiten in hun afwegingen en voorkeuren meer aan bij de wens van de meeste patiënten om meer controle te hebben over de gegevens in bepaalde situaties. Het lijkt erop dat de individualistisch ingestelde huisarts zich meer identificeert met patiënten die zich sociaal kwetsbaar voelen of gezonde patiënten/burgers c.q. niet speciaal kwetsbare patiënten; en dat de collectivistisch ingestelde huisarts zich meer identificeert met de medisch kwetsbare patiënt. In elk geval komen de meningen van deze huisartsen overeen met de genoemde patiëntengroepen.

Alle patiënten en huisartsen zijn het erover eens dat de patiënt uiteindelijk bepaalt welke informatie ingezien kan worden en door wie. De meeste patiënten en een deel van de huisartsen willen controle over welke gegevens door welke personen ingezien kunnen worden.

De meeste patiënten en huisartsen vinden het belangrijk dat (bepaalde) gegevens direct toegankelijk zijn in noodsituaties. De mening over de benodigde omvang van de gegevens, zowel in nood als in alle andere situaties, verschilt onder patiënten en onder huisartsen.

Een aantal patiënten stelt voor dat er onderscheid gemaakt wordt tussen een systeem voor noodsituaties en een systeem voor alle andere (dat wil zeggen niet-nood) situaties. In het laatste systeem worden dan meer gegevens beschikbaar gesteld, maar op een gecontroleerde manier en alleen voor die zorgverleners die direct betrokken zijn bij de behandeling.

Concluderend omvatten het LSP en de Whitebox ieder een ander deel van de wensen en (ontwerp)eisen van patiënten en huisartsen. Het LSP lijkt meer aan te sluiten bij de opvattingen van collectivistisch ingestelde huisartsen en bij medisch kwetsbare patiënten, hoewel van de laatste groep een deel zegt ook meer controle te willen over de uitwisseling van medische gegevens. Als voorbeeld wordt het gebruik van een PIN code genoemd. De Whitebox lijkt meer aan te sluiten bij de individualistisch ingestelde huisarts, en de sociaal kwetsbare en tenminste een deel van de gezonde patiënten.

Het onderzoek stelt dat het vanuit het patiëntenbelang gerechtvaardigd is om te concluderen dat (eigenschappen van) beide systemen – Whitebox én LSP – nodig zijn om aan de wensen van de verschillende patiëntengroepen te voldoen[27].

2 Onderzoek naar een minimale professionele samenvatting voor dienstwaarneming

In 2015-2016 is in het kader van de pilot een onderzoek uitgevoerd naar een *minimale professionele samenvatting (minimale PS)*, in vergelijking met de *NHG PS* welke wordt gebruikt in het LSP, en die daarvoor reeds werd gebruikt in de voorganger van het LSP, OZIS. Deze NHG PS is ontwikkeld door het Nederlandse Huisarts Genootschap (NHG).

De standaard NHG PS ontsluit de volgende gegevens [NHG]:

- Alle actieve episodes
- Contra-indicaties, intoleranties, en allergieën
- Journaalregels (SOEP) van de laatste 4 maanden, met een minimum van 5 (eventueel meer dan 4 maanden geleden[28]).
- Alle actieve medicatie (hetgeen automatisch actieve chronische medicatie includeert).
- Meetwaarden tot 4 maanden terug

De NHG PS bevat vrij veel medische informatie waarvan niet op voorhand vaststaat dat deze noodzakelijk is voor dienstsituaties. De begrenzing van 4 maanden lijkt bijvoorbeeld vrij arbitrair. Deelcontactverslagen (SOEP regels) kunnen veel informatie bevatten die privacygevoelig is, zoals subjectieve observaties of familiaire of psychische informatie. Er kunnen wel gegevens worden afgeschermd [NHG], maar hier zijn in het HIS handelingen voor nodig die in de praktijk vaak zullen worden nagelaten - standaard worden gegevens niet afgeschermd.

---

27 Noemenswaardig is dat met een keuze voor Whitebox én LSP (zowel binnen het zorgsysteem als geheel als, desgewenst, binnen individuele praktijken) de cumulatieve dekkingsgraad in van het systeem in de zin van gegevens die beschikbaar zijn op bijvoorbeeld de huisartsenpost, maar in de toekomst ook voor apothekers en in spoedsituaties, omhoog gaat.

28 Dit is recentelijk (in 2017) aangepast voor het LSP; het maximum van 4 maanden is nu ook bij het LSP absoluut, ook als de PS hierdoor minder dan 5 consulten bevat. [NB: de NHG PS van de Whitebox paste deze begrenzing altijd reeds toe, en was in die zin initieel niet volledig conform de NHG specificatie; heden is het dit dus wel].

Er is tijdens de pilot een kwalitatief onderzoek gedaan om te komen tot een minimale PS voor dienstwaarneming, en er is een kwantitatieve evaluatie van deze PS uitgevoerd.

Ontwerp en inhoud van de minimale PS

In het kader van de pilot is besloten om een werkgroep van artsen samen te stellen die zich zou buigen over de vraag wat een *minimale PS* zou kunnen inhouden, welke kan voldoen als minimale gegevensoverdracht naar de dienstdoende huisarts(enpost). Daarbij werd uitgegaan van de minimaal noodzakelijke gegevens voor snelle effectieve beoordeling van de belangrijkste zaken uit het huisartsdossier. Het idee was tevens dat een minimale PS tevens “information overload” zou kunnen voorkomen, waarbij een huisarts door het dossier moet spitten om de juiste informatie te kunnen vinden, in plaats van direct duidelijk de belangrijkste informatie gepresenteerd te krijgen.

Deze werkgroep van vier huisartsen (waarvan één professionele waarnemer) is in een viertal sessies bijeengekomen, om eerst de gedachten te inventariseren en vervolgens tot consensus te komen over wat de minimale PS zou inhouden. Deze minimale PS is vervolgens (in TetraHIS) geïmplementeerd als PS die via het Whitebox systeem beschikbaar is en gekoppeld kan worden als filter over de informatie van een gegeven patiënt. Naast de NHG PS en een uitgebreide PS (waarin informatie tot 2 jaar terug opvraagbaar is) was de minimale PS praktijkbreed of per patiënt als *PS-filter* instelbaar in de pilot.

De weerslag van de bevindingen van de werkgroep is te vinden in [Bakker et al., 2015] . Op basis van de motivaties die in [Bakker et al., 2015] te vinden zijn, is de minimale PS door de werkgroep vastgesteld als:

- Alleen actieve episodes met attentiewaarde (episode+)
- Alle contra-indicaties, intoleranties, en allergieën
- Journaalregels (SOEP) tot maximaal 1 week terug of helemaal niet
- Alle chronische medicatie, en actieve niet als chronisch gemarkeerde medicatie met een uitloop van 1 maand na de stopdatum.
- meetwaarden/labuitslagen tot 2 weken terug.

De werkgroep kon geen volledige consensus bereiken over het wel of niet includeren van SOEP regels tot één week terug. 1 week werd als maximum geaccepteerd, omdat eventuele relevante recente informatie die (als een vorm van overdracht) leesbaar zou zijn voor de waarnemer, na een week in een episode zou moeten zijn terug te vinden als het belangrijk genoeg was; echter, een aantal artsen

vonden ook deze ene week te risicovol en onnodig, en besloten dat het belangrijker was om zeker te zijn dat eventuele privé informatie die in een dergelijke SOEP regel zou staan niet beschikbaar zou komen voor de waarnemer. Ook in de pilot praktijk, zagen we dat artsen soms om deze reden de minimale PS zonder journaalregels kozen.

Beide samenvattingen hebben we in de pilot “MinimalePS” genoemd, maar door een extra “+” symbool erbij werd aangegeven dat de “MiniPS+” ook een week journaalregel bevatte. Welke variant standaard in de praktijk gebruikt wordt, is eenvoudig in het HIS in te stellen door de arts (zie hoofdstuk 9).

In de pilot ontstond verder soms discussie over de periode van meetwaarden; wellicht is beter deze op te hogen naar 1 maand[29].

Onderzoek effectiviteit van de minimale PS

Naast de kwalitatieve argumentatie om te komen tot een MinimalePS (+) is besloten om de minimalePS ook (kwantitatief) te onderzoeken. Er is door de Vrije Universiteit een onderzoek uitgevoerd naar de waardering van de minimale PS, in vergelijking met de NHG PS, door in een lab setting een aantal casussen voor te leggen aan artsen, ondersteund door respectievelijk géén, een minimale, of een NHG PS. Uit het onderzoek blijkt dat artsen de PS vooral als ondersteunend gebruikten door te scannen naar aspecten die hun (werk)diagnose bevestigden of ontkrachten.

Uit het onderzoek kwam naar voren dat bij gebruik van de minimale PS géén essentiële informatie gemist werd, maar dat deze PS wel beter werd gewaardeerd (doordat er minder informatie gepresenteerd werd). De minimale PS bevatte voldoende aanvullende informatie om een beleid te kunnen voorstellen en er werd nauwelijks informatie gemist[30].

---

29 Twee “aangepaste PS-en” in de pilot (zie “pilot in cijfers”) bevatten precies deze aanpassing (verder waren dit minimale PS-en). Een objectief argument om meer meetwaardes te includeren, is dat sommige metingen (bijvoorbeeld, nierfunctiemetingen) bij bijvoorbeeld diabetespatiënten slechts eens in de drie maanden worden opgenomen. Gegeven relevantie voor medicatiebeleid/voorschrijven en – vermoedelijk – de lage privacy-impact van het delen van deze meetwaarde, is te beargumenteren dat deze waarde op 3 of 4 maaanden ingesteld zou moeten worden. Het is ook denkbaar om specifiek de nierfunctie langer te ontsluiten en andere lab/meetwaardes niet.

30 Wel werd informatie van specialisten gemist (specialistenbrieven), die niet standaard in de NHG of minimalePS is opgenomen. We overwegen om correspondentie met specialisten selectief includeerbaar te maken in de PS, indien een arts dat wenst. In de visitelijst correspondentie al geïncludeerd (in principe omvat dit het volledige dossier), na aanmelding van een patiënt.

Het volledige onderzoek van de VU is te vinden via de link in de referentielijst [Vrije Universiteit, 2017].

Overigens lijkt, ondanks de positieve uitkomst van de evaluatie van de minimale PS, een eenduidige uitspraak over welke gegevens noodzakelijk zijn voor een specifieke patiënt niet realistisch. Bij de ene patiënt kan het nuttig zijn om informatie van meer dan een jaar beschikbaar te hebben (bijvoorbeeld, de pijnbestrijdingshistorie van een terminale patiënt), terwijl voor een andere patiënt – bijvoorbeeld vanuit privacy perspectief – prettig is als bepaalde informatie juist niet beschikbaar is. Zo varieert de informatiebehoefte van arts tot arts en van patiënt tot patiënt. Het is duidelijk dat je het nooit voor álle artsen en patiënten en scenario's goed doet wanneer je een standaardformule hanteert – óók niet als dit de minimale PS is.
In de implementatie van de Whitebox is er daarom voor gekozen om meerdere typen PS aan te bieden aan huisartsen en patiënten, zodat maatwerk mogelijk is. Eén daarvan is de minimale PS.

3 Evaluatie gebruik Whitebox - ervaringen van huisartsen

De ervaringen met de Whitebox zijn goed. Artsen geven aan dat ze het systeem goed te begrijpen vinden (een belangrijk criterium voor de test), en dat het systeem eenvoudig in gebruik is. De Whitebox schermen zijn duidelijk en overzichtelijk.

Een specifieke positieve bevinding is dat artsen de 'preview' modus van de Whitebox, waarmee artsen direct kunnen zien wat de inhoud van de PS van een specifieke bij de Whitebox aangemelde PS is, erg overzichtelijk en prettig vinden.

Bij installatie van de Whitebox blijkt dat artsen snel hun weg weten te vinden in de instellingen voor de PS (in TetraHIS). Veelal wordt snel een selectie gemaakt voor een PS; een enkele keer experimenteert een arts direct met de mogelijkheid om een aangepast praktijkfilter te maken. In de regel vallen artsen na enig experimenteren terug op de NHG PS of op de minimale PS+. Een aantal artsen selecteren de minimale PS zonder week journaal (zie "de pilot in cijfers").

Huisartsen vinden het erg prettig dat zij ook een *Uitgebreide PS* kunnen selecteren, die alle episodes en twee jaar consulthistorie bevat. Artsen geven aan dat dit bij terminale patiënten erg nuttig kan zijn voor de dienstdoende art//s (denk aan uitzoeken historie pijnbestrijding). Het hoofdstuk over ervaringen van artsen gaat hier dieper op in.

Enkele deelnemers vragen uit zichzelf of in te zien is dat gegevens ingezien zijn, en door wie. De wetenschap dat dit kan via de logbestanden op de Whitebox en via de "snuffelverslagen" per mail, neemt bij hen een laatste drempel weg om de Whitebox te gaan gebruiken.

De algemene opvatting over de Whitebox is positief. Eén arts verwoordt het als volgt: *“dit is een veel beter idee dan LSP, de Whitebox is veel prettiger want je hebt zelf controle en alleen de HAP krijgt toegang.”* Deze arts geeft ook aan dat patiënten haar expliciet vragen om niet in het LSP te komen. *“Patiënten willen echt pertinent niet op het LSP’”.* Een andere arts die wel een LSP aansluiting heeft maar deze nauwelijks gebruikt, geeft iets soortgelijks aan: *“het is niet zo dat patiënten vragen om gegevensuitwisseling via het LSP, integendeel zelfs. Ze vragen juist ‘je zet me er toch niet in hé, je zet me er toch niet in?’”*

Installatieprocedure

Het configureren van de verbinding met de Hap(box) via de Whitebox is erg eenvoudig. Wel kwam het voor dat vergeten werd om de *autorisatie code* die de HAP beheerder opstuurde (zie navolgende sectie) in te voeren. Dit kon ertoe leiden dat de verbinding pas na langere tijd geactiveerd werd. We monitoren hier inmiddels actiever op en verzenden actief reminders om te zorgen dat dit niet aan de aandacht ontsnapt.

Installeren en het opzetten van een account op de praktijk gaat snel en is niet problematisch.

Omdat de Whitebox een eigenstandige inlogfunctie heeft, waar artsen mee in aanraking komen tijdens de set-up/configuratie bij de levering en installatie van de Whitebox (deze inlogfunctie is nodig voor onder meer het uitgeven van accounts) voelen artsen soms initieel een drempel om het systeem te gebruiken. Hoewel bij de installatie een demonstratie wordt gegeven hoe patiënten vanuit het HIS aan te melden zijn, blijkt dit toch snel weg te zakken als artsen niet direct met het systeem aan de slag gaan[31]. Zo blijft bij een aantal artsen de indruk hangen dat het nodig is om in de Whitebox in te loggen om het systeem te gebruiken. Een aantal keer hebben we daarom een vervolgafspraak gemaakt om nogmaals de werking uit te leggen. Het is meerdere keren voorgekomen dat artsen vervolgens alsnog verbaasd waren dat het gebruik zo gemakkelijk gaat, rechtstreeks vanuit het HIS.

De les hiervan is dat we sneller opvolging doen wanneer we zien dat het systeem niet gebruikt wordt, en dat we direct (HIS specifieke) documentatie bijleveren waarin het gebruik in de praktijk wordt uitgelegd aan de hand van schermopnames van de belangrijkste functies in het HIS.

Functionaliteit en bediening Whitebox

De Whitebox schermen zijn duidelijk en overzichtelijk. Bij installatie blijkt dat huisartsen direct, en heel

31 Het feit dat heden ook direct een visitelijst wordt bijgeleverd, helpt doordat artsen dan sneller geneigd zijn om met het systeem te experimenteren, omdat de arts die op eigen houtje kan proberen zonder toestemming van de patiënt nodig te hebben.

intuïtief, aan het werk gaan om met de mogelijkheden om een eigen PS te selecteren (in Tetra, zie voorbeeld scherm in hoofdstuk 9). Huisartsen maken duidelijk (en snel) hun eigen keuze in welke PS standaard gedeeld moet worden, en kunnen dit ook onderbouwen. De keuze lijkt afhankelijk van hoe zij tegen de noodzaak van gegevensuitwisseling aankijken, maar ook van hun inschatting van de privacygevoeligheid van gegevens die zij in met name de journaalregels noteren - in relatie tot het nut van deze informatie voor waarnemers. Veelal wordt snel een selectie gemaakt voor een variant van de minimale PS, met geen of één week journaalregels. Slechts in vijf gevallen werd initieel een NHG PS gekozen, met als reden dat dit de landelijke standaard is. Drie van deze artsen betrof een huisarts die reeds het LSP gebruikte. In alle gevallen is dit later bijgesteld en alsnog een minimale PS gekozen, óók door de drie artsen die ook een LSP aansluiting gebruiken.

Huisartsen geven aan dat zij het prettig vinden dat de minimale PS geen of weinig consultregels bevat. Eén huisarts wilde eerst de minimalePS+ kiezen, maar besloot vervolgens om de consultregels uit te zetten, met als redenatie *"een abortus, of problemen met relatie wil je niet dat zichtbaar zijn op de post. Een episodelijst is genoeg, met de medicatielijst."*

Een enkele keer experimenteert een arts direct met de mogelijkheid om een aangepast (eigen) praktijkfilter te maken. In de regel vielen artsen na enig experimenteren terug op de standaard NHG PS of op de minimale PS+, of een kleine variatie daarop (bijv. minimalePS+ met 1 maand meetwaarden i.p.v. de 2 weken die standaard is in de minimalePS). Een aantal artsen selecteren de minimale PS zonder week journaal. In de meeste gevallen kiezen huisartsen voor de minimale PS met een week journaalregels (zie ook resultaten in "de pilot in cijfers").

De keuze om in de minimale PS alleen actieve episodes met een attentiewaarde te tonen heeft niet tot discussie geleid. Vrijwel alle artsen reageren positief op de mogelijkheid alleen episodes met attentiewaardes te selecteren. Daarbij realiseren zij zich dat zij dan wel door de episodelijst moeten heenlopen om te zorgen dat privacygevoelige en niet-relevante informatie geen attentiewaarde moet krijgen, en dat episodes die wel belangrijk zijn wel een attentiewaarde krijgen. Artsen geven zelfs aan het een prettig idee te vinden om ten tijde van het vragen van toestemming aan de patiënt even de episodelijst door te lopen om te zien of hier wel juiste informatie in staat die relevant is voor de waarnemer. *"Het is belangrijk deze even na te lopen voordat je gegevens ontsluit."* We hebben bij de installatie ook zelf kunnen waarnemen dat artsen direct en snel aan de slag gaan met de episodelijst van een patiënt die zij kiezen als voorbeeld om te zorgen dat de episodelijst goed staat.

Het aanpassen van attentiewaardes in de episodelijst blijkt voor een arts een klusje van 10-20 seconden en is iets waar zij heel intuïtief en snel mee werken; artsen geven aan dat dit voor hen meteen een goed moment is om te kijken of de episodelijst nog wel klopt en de juiste (en voor

waarnemers relevante) informatie bevat.

Huisartsen geven ook aan dat zij het erg prettig vinden dat zij desgewenst voor een specifieke patiënt ook een *Uitgebreide PS* kunnen selecteren, die alle episodes en twee jaar consulthistorie bevat die bijvoorbeeld bij terminale patiënten erg prettig kan zijn voor de dienstdoende arts.

Toestemming vragen

In de pilot hebben alle artsen toestemming aan patiënten gevraagd voor het delen van gegevens met de huisartsenpost. Er is een informatiebrochure die de werking van de Whitebox beschrijft, en voordat gegevens van een patiënt worden aangemeld bij de post wordt de patiënt eerst om toestemming gevraagd.

In beginsel kiest de huisarts voor de PS die hij/zij wil gebruiken; voor individuele patiënten is eenvoudig van de standaard (praktijk)instelling af te wijken.

Artsen in de Whitebox pilot geven aan dat de werking van de Whitebox goed en vrij eenvoudig is uit te leggen aan patiënten. De strekking van de vraag is *"het lijkt mij zinvol dat uw gegevens opvraagbaar zijn voor de dienstdoende huisarts op de huisartsenpost. Dit gaat via een rechtstreekse verbinding, hier zit niets tussen. Vindt u dat goed?"* Een arts geeft aan dat een patiënt een enkele keer de informatiefolder even thuis wil doorlezen voordat hij toestemming geeft, waarna het antwoord tot nog toe steeds bevestigend is.

Een huisarts geeft aan dat de manier waarop de dokter toestemming vraagt waarschijnlijk bepalend is voor of de patiënt toestemming geeft. Dit gaat ook op voor de toestemming voor het LSP. "*Je kunt patiënten makkelijk sturen door hoe je het zegt, door hoe je toestemming vraagt. Je zegt gewoon 'het is goed voor u'. En dan zegt de patiënt 'dat is goed dokter, als u dat denkt '* Maar tegelijkertijd geeft deze arts, die zelf standaard de minimale PS (zonder consultregels) heeft gekozen, aan: "*dat er geen consultinformatie wordt gestuurd/gedeeld wordt vinden patiënten heel prettig. Dat betekent dat wat in consult gezegd wordt, tussen de patiënt en mij blijft."* Blijkbaar is dit een geruststellende gedachte. Kennelijk is de wetenschap dat gegevens slechts beperkt gedeeld worden toch belangrijk voor het vertrouwen tussen patiënt en arts.

Artsen zijn op verschillende manieren terughoudend bij het vragen van toestemming. Een arts die weinig patiënten heeft aangemeld via de Whitebox: *"ik ben iemand die minimaal aanmeldt maar alleen die patiënten aanmeldt waarvan ik verwacht dat er problemen komen in weekend of avond, en dat goede overdracht belangrijk is, met name de zieke mensen."*

Dezelfde arts vindt het ook belangrijk dat er eerst een contact is, dat hij er als moment tussen zit. *"Het LSP vind ik te groot, te breed. Van jullie [systeem] vind ik het mooi dat ik het selectief kan doen, dat ik zelf beslis, in overleg met patiënt, dan kan ik ook zeggen 'ik zorg ervoor dat die koppeling er komt, dus mocht er in het weekend wat zijn dan zijn ze op de hoogte, dan kunnen ze het inzien'".*

De meeste artsen in de pilot geven aan dat zij een voorstander zijn van het opt-in toestemmingsmodel – alleen voor tijdelijke aanmeldingen als een vorm van overdracht bij spoed maken zij een uitzondering – omdat zij hechten aan een duidelijke en transparante vorm van voorlichting aan patiënten. Tegelijkertijd geven meeste artsen desgevraagd wel aan dat zij eigenlijk vinden dat patiënten waarvoor een medische noodzaak bestaat, gewoon zouden moeten kunnen overdragen naar de HAP; dit kan ook, via een tijdelijke aanmelding (van op dit moment twee weken). Een aantal artsen geven aan dat zij dit als de belangrijkste reden voor gebruik van de Whitebox zien, d.w.z. zij gebruiken de Whitebox eigenlijk als een soort overdrachtssysteem zien voor patiënten die – op dat moment – ziek zijn.

Pro-actief patiënten benaderen gebeurt maar in een aantal gevallen; twee artsen (met alleen een Whitebox) hebben de griepprik campagne gebruikt (die uitgaat naar patiënten van 60+ jaar oud en chronisch zieken, ca. 20% van de populatie) om mensen actief aan te schrijven met de vraag of zij akkoord gingen met aanmelding; de respons hierop was dat ongeveer 60% "ja" invulde op de vraag of hun gegevens (een "mini samenvatting") alleen met de huisartsenpost Amsterdam mochten worden uitgewisseld via een directe beveiligde verbinding. Aanvullende informatie werd gegeven via informatie op de website en aan de balie (folder).

Eén arts (ook met alleen een Whitebox) besloot om alle patiënten door de assistente te laten bellen met de vraag of hun gegevens mochten worden aangemeld. De gedachte was (optimistisch) dat binnen een aantal maanden alle patiënten zouden kunnen zijn gebeld, echter door onder meer personeelswisselingen is dit hier niet van gekomen. Na twee maanden waarin ongeveer 75 patiënten per maand zijn aangemeld, vlakte het aantal aanmeldingen af. Deze methode van toestemming vragen lijkt tijdsintensief, en daarmee wellicht niet de meest efficiënte vorm van toestemming vragen.

De meeste artsen in de pilot hebben besloten om patiënten toestemming te vragen in de spreekkamer, als het nodig is. Het aanmelden van patiënten (en het toestemming vragen) zit echter niet altijd 'in hun systeem' en een consult is kort en het gaat daar over de zorgvraag. Dit blijkt tot gevolg te hebben dat dit relatief weinig gebeurt: een aantal artsen in de pilot meldt in de praktijk weinig of geen patiënten aan, hoewel er ook artsen zijn die steevast en constant patiënten blijven aanmelden.

Enkele artsen kwamen met het idee om de toestemmingsvraag via een andere route te regelen. Een aantal huisartsen in de pilot kennen een hoge mate van automatisering, en gebruiken met regelmaat

een App om met hun patiënten te communiceren. Gegeven een afdoende strak protocol voor *face-to-face uitgifte* van een App-account, zou een dergelijke App gebruikt worden om de toestemmingsvraag te stellen, of om gericht een groep patiënten te informeren over een voorgenomen uitwisseling van gegevens met de huisartsenpost.

4 Gebruik UZI passen op de HAP – lessons learned

In de eigen praktijk hoeft een huisarts geen UZI pas te gebruiken om de Whitebox te benaderen. Het systeem wordt bediend vanuit het HIS, en wanneer nodig kan de huisarts op de Whitebox inloggen via een eigen (2-factor) inlogsysteem. Hierbij is gebruik van een UZI pas mogelijk, maar niet verplicht. Op de huisartsenpost is gebruik van UZI passen echter noodzakelijk, als gegevens van patiënten via de Whitebox opgehaald moeten worden, zodat de eigen huisarts (en de patiënt) kunnen zien wie gegevens opgehaald heeft, en zodat de Whitebox kan checken dat de opvragende partij inderdaad een huisarts is (deze informatie staat op de UZI pas van de arts). Het gebruik van UZI passen op de HAP blijkt niet zonder problemen.

Zowel de eerste bevraging van de Hapbox (opzoeken patiënt) als het opvragen van het dossier moet met een UZI pas plaatsvinden. De eerste UZI pas is een medewerkerspas op naam; voor het daadwerkelijke opvragen van het dossier is een huisartsen UZI pas nodig. De reden is in beide gevallen dat alle acties traceerbaar zijn. De UZI passen moeten opgenomen zijn in de lijst met UZI passen die in de Hapbox wordt bijgehouden. In de praktijk leidt dit tot problemen wanneer medewerkers en/of artsen:

(a) geen UZI pas bij zich hebben, omdat zij er geen hebben of omdat deze verlopen is, of gewoon als (inloggen met) de UZI pas vergeten wordt

(b) de UZI pas (nog) niet geregistreerd is in de Hapbox.

In de praktijk blijkt met name (a) vaak voor te komen in Amsterdam. Hier is kennelijk veel weerstand tegen het gebruik van UZI passen, omdat dit geassocieerd wordt met (het verplichten van) het LSP. Bovendien zijn er kosten aan de aanschaf van de UZI pas verbonden en, is bestellen traag. Bij het LSP in Amsterdam werkt men hieromheen door assistentes (met een UZI pas) *onder mandaat* te laten inloggen op het LSP.

De mandaten zoals die heden in Call Manager geïmplementeerd zijn, op basis van de formele LSP specificatie, zijn niet cryptografisch controleerbaar aan de bron [Noordende, 2010]. Daarom is de

keuze om op eenzelfde wijze onder mandaat te werken voor de Whitebox niet gemaakt.

De technische limitaties van de huidige mandaatstructuur (waardoor mandaten niet door de Whitebox controleerbaar zijn) zijn in de context van de Hapbox oplosbaar. Whitebox werkt heden aan een oplossing voor genoemd mandaatprobleem, door aan de Hapbox een systeem te koppelen voor het cryptografisch vastleggen van mandaten, zodat in de toekomst beperkt geldige, cryptografisch valideerbare mandateringen gebruikt kunnen worden. Dit systeem is in ontwikkeling en zal komend jaar getest worden. Heden is dit systeem nog niet beschikbaar.

Wellicht is het belangrijkste dat het inloggen met een UZI pas is in Call Manager beduidend trager is dan inloggen met gebruikersnaam/wachtwoord. Dit probleem is een algemeen probleem; hier wordt ook in de context van het LSP aan gewerkt.

Probleem (b) is oplosbaar: er zijn inmiddels meerdere huisartsenposten in Nederland die gebruik van de UZI pas eenvoudigweg verplichten, vanuit de overweging dat dit een veiliger authenticatiemiddel is dan gebruikersnaam/wachtwoord. De HpA heeft ook besloten om gebruik van de UZI pas tijdens diensten te gaan verplichten.

Het belang van UZI passen is dat toegangscontrole op een veilige manier controleerbaar, traceerbaar en uitvoerbaar wordt. Gebruikersnaam/wachtwoord is een veel minder veilige methode dan het gebruik van een op smartcards (zoals de UZI pas) gebaseerde methode, waarbij een digitale sleutel voor het inloggen (authenticatie) en ondertekenen van berichten en verzoeken, veilig is opgeslagen op de smartcard en deze alleen gebruikt kan worden na het invoeren van een persoonlijke PIN code. Hoe onhandig het gebruik van UZI passen soms ook is, het zorgt ervoor dat de Whitebox alle binnenkomende verzoeken om informatie *zelf* kan authenticeren en ervoor kan zorgen dat alleen geautoriseerde artsen persoonlijke gegevens van patiënten kunnen inzien. Bovendien is hiermee voor zowel de eigen huisarts als eventueel de patiënt direct zichtbaar wélke huisarts op de huisartsenpost gegevens heeft ingezien – dit zit dus (in contrast met het LSP) niet ‘verstopt’ in het HAPIS of achter de assistent(e) die onder mandaat gegevens heeft opgehaald namens alle huisartsen op de huisartsenpost.

Hoewel het eenvoudiger is om medewerkers van een huisartsenpost (assistenten/triagisten) te verplichten tot gebruik van een UZI pas dan artsen, is ook hier een procedure nodig voor de situatie waarin een UZI pas vergeten wordt. Verder is het zo dat tijdelijke of nieuwe medewerkers niet zomaar een persoonsgebonden UZI pas krijgen; ten eerste vanwege kosten, maar met name ook omdat de aanvraagprocedure voor nieuwe UZI passen traag is.

Het probleem dat medewerkers geen geautoriseerde UZI pas gebruiken is in zoverre ernstig dat als voor een patiënt in Call manager geen “call” is aangemaakt door een medewerker met een geldige UZI pas, er ook geen URL te vinden zal zijn in de call en de arts dan dus ook geen dossier kan opvragen.

Het tweede probleem is dat de autorisaties van medewerkers in de Hapbox niet altijd up-to-date zijn. Als oplossing hiervoor hebben we besloten de beheerder direct te informeren over mislukte zoekacties en mislukte opvragingen van gegevens. De Hapbox beheerder wordt dagelijks geïnformeerd over gelukte en mislukte bevragingen; door bij een autorisatie failure in de logfiles te kijken, kan de Hapbox beheerder snel zien welke UZI pas dit betreft, bekijken of de betreffende UZI pas wel geautoriseerd had moeten zijn. Zo kan de autorisatielijst snel geactualiseerd worden. In de toekomst is de wijze van informeren aanpasbaar door de beheerder.

Naarmate we sterker doordrongen raakten van het feit dat huisartsen zelden met een UZI pas inlogden, hebben we besloten om de beschikbaarheid van Whitebox dossiers duidelijker te tonen in Call manager. Huisartsen die zonder UZI pas inlogden terwijl er wel een Whitebox URL in de call geregistreerd was, kregen per december 2016 een pop-up te zien die aangaf dat er een Whitebox dossier beschikbaar was mits de arts opnieuw in zou loggen met zijn/haar UZI pas.
Dit najaar, in het kader van de afronding van de pilot en ingebruikname van de Whitebox, is verder ingezet op voorlichting van huisartsen met nadruk op noodzaak om met de UZI pas in te loggen, onder meer tijdens een aantal bijeenkomsten die door de regionale organisatie Sigra/EZDA georganiseerd werden. Eind 2017 is besloten de UZI pas in de loop van 2018 te verplichten.

5 Evaluatie gebruik Hapbox – ervaringen vanuit de huisartsenpost

De huidige setup- en installatieprocedure voor de Hapbox is relatief eenvoudig. Tijdens de setup procedure wordt een eerste lokale beheerdersaccount op de Hapbox aangemaakt. Vanaf dit moment is de beheerder van de Hapbox in staat om UZI passen te registreren, via een eenvoudige web interface. Er kunnen ook andere adminstrator accounts worden aangemaakt, die de beheerstaken eventueel kunnen overnemen.

De belangrijkste functies van de Hapbox zijn het administreren van geautoriseerde Whiteboxen die patiënten mogen aanmelden bij de Hapbox, het opzoekbaar maken van aangemelde patiënten, en het administreren van geautoriseerde artsen op de HAP, en ten slotte logging.

Het systeem autoriseert op dit moment verzoeken op basis van een lijst met geautoriseerde UZI passen in de Hapbox. Call manager zorgt ervoor dat de Hapbox bevraagd kan worden om een patiënt op te zoeken. Hiertoe wordt in Call manager de URL van de Hapbox geconfigureerd. De bevraging van

de Hapbox om patiënten op te zoeken gebeurt heden met de (geautoriseerde) UZI pas van een assistent(e), vanuit Call manager. Het dossier zelf wordt beveiligingstechnisch door de huisarts (met een UZI pas) rechtstreeks bij de Whitebox opgevraagd. Dit gebeurt vanuit Call manager, dus niet via de Hapbox, middels een URL die de Call manager van de Hapbox ontvangt, met behulp van de UZI pas van de huisarts[32].

Het beheer van de Hapbox omvat de volgende aspecten:

- Management van UZI passen van medewerkers en artsen die verbonden zijn aan de HAP;
- Het managen/autoriseren van koppelingen van aangesloten Whiteboxen;
- Inzien van logging van events, waaronder zoekacties en opvraging van gegevens .

De beheersfunctionaliteit blijkt eenvoudig te bedienen.

Methode

Om de ervaringen met de Hapbox – het systeem waar de Whiteboxen van aangesloten huisartsen meekoppelen op de Huisartsenposten Amsterdam (HpA) – te evalueren, is de gebruiker van de Hapbox, Cees Dekker, geïnterviewd. Dekker is vanaf het begin af aan bij het project betrokken en heeft de pilot vanuit de kant van de HpA mede begeleid.

Een aantal onderwerpen zijn hierbij specifiek geëvalueerd:

- Wat is de beheerslast
- Wat zijn aandachtspunten of verbeterpunten in de werking van de Hapbox en/of de beheersfunctionaliteit?
- Wat zijn gedachten over het model, met name het decentrale model van de Whitebox en wat dit – qua verantwoordelijkheden en mogelijkheden voor de huisartsenpost – impliceert?
- Hoe verhoudt het model en het systeem zich tot het LSP, en biedt de Whitebox een meerwaarde – in Amsterdam en eventueel daarbuiten?
- Reflectie/visie op Whitebox Systems als leverancier

Het interview nam ca. 1.5 uur in beslag, en bestond uit een semi-gestructureerd interview op basis van de vragen die in de Appendix zijn opgenomen.

32 Heden wordt in Call manager ingesteld welke artsen een Whitebox hebben, zodat Call manager de Hapbox alleen bevraagt voor patiënten van huisartsen met een Whitebox. Zo wordt gerealiseerd dat alléén van patiënten met een huisarts die een Whitebox hebben, het dossier wordt opgevraagd. Na de pilot wordt deze beperking opgeheven.

De resultaten worden hieronder gegroepeerd samengevat.

Beheerslast

Het beheer van de Hapbox is niet veel werk. De belangrijkste taken zijn:

- Het accepteren/autoriseren van Whiteboxen die worden aangemeld. Dit is per aangemelde Whitebox een eenmalig proces, waarbij de beheerder een signaaltje van de Whitebox krijgt (per mail) dat er een aanmelding is, en vervolgens via de Hapbox een brief kan printen die hij/zij naar de huisarts die een Whitebox aanmeldt moet sturen, met daarin een autorisatiecode. Heel soms is een herhaling nodig als de arts de autorisatiecode niet tijdig invoert[33].
- Het invoeren van autorisaties van huisartsen en medewerkerspassen in de autorisatielijst in de Hapbox. De hoeveelheid werk hangt af van de hoeveelheid mutaties; met name bij een veel wisselend personeelsbestand kan regelmatige aanpassing nodig zijn. Vervanging van UZI passen vereist geen nieuwe invoer: de ingevoerde code is het unieke UZI nummer, niet het specifieke pasnummer van de arts of assistent. De Whitebox biedt een mogelijkheid om UZI lijsten te importeren als een csv bestand (deze kunnen beheerd worden middels Excel), om batchgewijs artsen en assistenten te autoriseren voor een bepaalde periode, naar keuze van de beheerder. Incidenteel nieuwe passen aanmelden en verwijderen kan ook. Een ondersteuning hiervoor wordt geboden door de logbestanden: als er een autorisatie error is doordat een UZI pas niet geautoriseerd is, krijgt de beheerder een signaal per mail en kan hij opzoeken in de Hapbox welke pas tot een autorisatie-error leidde; deze kan vervolgens (na check of deze arts wel bij de post werkt) geautoriseerd worden.
- Het nakijken van de logging, om te zien of er onregelmatigheden hebben voorgevallen, of dat er andere aandachtspunten zijn (bijvoorbeeld, autorisatie errors [zie boven] of problemen in de bereikbaarheid van een Whitebox).

Een ruwe schatting is dat het beheer van de Whitebox in vol ornaat, als er zo'n 200 huisartsen zouden zijn aangesloten, in totaal ca. 2 à 4 uur per week zou kosten voor logging, handleidingen maken, problemen opvangen.

33 We overwegen het proces iets aan te passen zodat een autorisatiecode reeds op voorhand verstuurd kan worden naar een gegeven zorgverlener; dit impliceert dat een Whitebox direct gekoppeld kan worden, op het moment dat deze bij een arts geïnstalleerd wordt.

Aandachtspunten en verbeterpunten gebruik Hapbox

De beheersinterface is overzichtelijk en eenvoudig. Tijdens de pilot zijn wat verbeteringen aangebracht, zoals het eenvoudig kunnen exporteren van logbestanden. Over het algemeen wees het gebruik redelijk voor zich. Er zijn enkele kleine opmerkingen: “Ik vind de interface eenvoudig, maar er zijn verbeteringen mogelijk. Dan denk ik aan standaardfuncties als het on-the-fly kunnen sorteren van een lijstje (door op de kolom te klikken), etc. Dit zijn functies die je (inmiddels) intuïtief verwacht.” Hier wordt aan gewerkt.

De manier van rapporteren richting de beheerder – bijvoorbeeld, de mailberichten waarin de beheerder wordt geïnformeerd over de status van de Hapbox of belangrijke gebeurtenissen, zoals het aantal opvragingen in een nacht of (mislukte) pogingen om gegevens op te vragen door niet geautoriseerde huisartsen – kunnen wat meer op de persoon afgestemd worden. Met name ook de huidige algemene “snuffelverslagen”, zodat een beheerder alleen specifieke events ziet waar hij in geïnteresseerd is. Deze aanpassingen zijn haalbaar en zullen op korte termijn in samenspraak met de HAP opgepakt worden.

Daarbij wordt de HAP wel geholpen door het beheersinstrument wat meer te ontwikkelen, bijv. meer inzicht in de index van de Hapbox. Hoe ga je om met die cijfers (alerting, reporting)? Whitebox Systems en de HpA gaan werken aan een stappenplan voor de ontwikkeling van de beheersinterface.

Een mogelijk idee is verder nog om de logging van de Hapbox te integreren met een beheerstool die ook logging informatie van het LSP en Call Manager bevat; zo kan informatie uit diverse bronnen gecombineerd worden in één overzicht.

Voor- en nadelen van het decentrale model, perspectief van de HAP

De Whitebox presenteert zich nadrukkelijk als een *decentraal* alternatief voor het LSP of andere centraal geïmplementeerde of georganiseerde systemen. Dit is niet alleen een kwestie van techniek, maar ook van organisatie en zeggenschap. Ook hierover is Cees Dekker bevraagd. Wat vindt hij van het model?

“De Whitebox is een decentraal concept. Dat impliceert verantwoordelijkheid. Dat ervaar ik wel als een extra taak, maar daarmee komt ook meer controle. We hebben meer inzicht in bij welke systemen we gegevens op kunnen vragen, en wie daar achter zit.”

Een voordeel kan zijn dat de Whitebox kan faciliteren bij het monitoren van een aantal voor de regio belangrijke zaken. Bijvoorbeeld, wat is de bereikbaarheid van een bepaalde huisarts (netwerk, Whitebox, HIS), over een gegeven periode? Dit kan inzichtelijk worden gemaakt via de beheersinterface, bijvoorbeeld met grafieken[34], zodat de beheerder – indien hij hiertoe het mandaat heeft gekregen van de organisatie en de aangesloten huisartsen – een huisarts wiens systeem minder presteert kan aanspreken.

Soortgelijk kan een huisarts worden aangesproken op bepaalde zaken zoals de kwaliteit van de opgeleverde dossiers *"dit zou bij voorkeur iets moeten zijn wat artsen zelf doen*."

Uit een praktijktest WDH (LSP) uit 2010/2011 kwam een wens naar voren dat artsen naar hun collegae konden terugkoppelen wat zij van de informatie vonden die zij zagen, bijvoorbeeld als de episodelijst onoverzichtelijk was (uit die toets kwam dat waarnemend artsen met name problemen hadden met een te groot aantal episodes, [Dekker 2011]). Technisch biedt de Whitebox ook de mogelijkheid om waarnemers bepaalde informatie te laten terugkoppelen naar de eigen huisarts, via hetzelfde communicatiekanaal als via welke gegevens worden opgevraagd. Het voordeel van de decentrale aanpak van de Whitebox is dat huisartsen en hún post samen afspraken kunnen maken wat de rol van de huisartsenpost is; er is geen externe partij die dit bepaalt of oplegt. Het kan belangrijk zijn richting artsen om bijvoorbeeld als huisartsenpost met de artsen af te spreken dat de informatie waar de huisartsenpost inzicht in heeft via de Hapbox en monitoring, niet naar derden gaat.

Hoe verhoudt het model zich tot het LSP, en heeft het meerwaarde?

Dekker vindt de Whitebox een waardevolle aanvulling op het LSP. *"Het uitgangspunt is: hoe zorg je ervoor dat patiënt die zich op de post meldt, optimaal behandeld wordt? Dan wil ik dat er informatie over die patiënt die belangrijk is opvraagbaar is en dat patiënt daar zelf iets over kan zeggen. En dat de dokter die waarneemt daar zelf een beslissing over kan nemen of hij de informatie wel/niet gebruikt. Dan is er aan de voorwaarden voldaan. Hoe je dat technisch uitwerkt, maakt niet uit."*

Voor de huisartsenpost staat de beschikbaarheid van informatie centraal. En daarbij gaat het niet zozeer om welke gegevens.

34 De Hapbox is in staat om in de belangrijkste parameters inzicht te bieden. De Hapbox heeft een directe koppeling met de aangesloten Whiteboxen; via deze koppeling kan de Hapbox niet zelf gegevens opvragen (daarvoor is een UZI pas nodig), maar wel een aantal diagnostische 'calls' uitvoeren, onder meer om netwerk performance te testen en om te kijken welke Whitebox en HIS versie bij een huisarts is en of Whitebox en HIS responsive zijn. Hier is een speciale 'ping' call op de Whitebox ontwikkeld, die alléén door de Hap(box) is aan te roepen.

“Er zijn genoeg dokters die zeggen ‘de inrichting van het LSP is voor mij ruim voldoende’; er zijn ook artsen die denken ‘nee, ik wil meer controle,' en dan is de Whitebox een goede oplossing. […] Voor mij is het vooral ingegeven door: de zorg voor de patiënt is het grootste belang. Daar heeft patiënt iets over te zeggen, maar de huisarts heeft daar ook een rol in, als die zegt “ik zorg voor mijn patiënt, dat is mijn verantwoordelijkheid; ik adviseer hem, ik licht hem voor, en ik kies vanuit mijn beroepscode ook voor een bepaalde aanpak, ook welke gegevens ik deel en welke niet. Er zijn huisartsen die zeggen ‘het LSP is goed genoeg’ en andere die zeggen ‘ik wil er meer controle over’. En voor die dokters is de Whitebox een mooie aanvulling.”

In zekere zin past de manier waarop het systeem invulling geeft aan diversiteit goed bij Amsterdam.

Er zijn geen (negatieve) opmerkingen over de techniek of de beveiliging van de Whitebox. *“We staan achter het technische concept, we vertrouwen de techniek”.* “*Samenvattend: technisch zit het goed in elkaar; je hebt als huisartsenpost en als dokters meer controle over met wie je gegevens uitwisselt, dat kun je patiënten ook aanbieden en dat vinden we in Amsterdam ook belangrijk, en het bestaat ook naast die andere oplossing het LSP – dan heb je een mooie oplossing. “*

Oganisatie Whitebox Systems

Dekker ziet dat de organisatie gegroeid is in haar rol en op professionaliteit. Inmiddels is een teststraat ingericht, bijvoorbeeld. En de organisatie is meer pragmatisch geworden. *“Als leverancier spelen jullie heel flexibel in op wat de gebruiker wenst, binnen de randvoorwaarden die er technisch zijn, of die er vanuit het concept zijn.”* Daarnaast ziet hij voordelen in de kleinschaligheid van de organisatie. “*Het is natuurlijk wel een voordeel dat we één-op-één kunnen overleggen over hoe de beheersapplicatie eruit moet zien*.” Dat zal ongetwijfeld wat formeler worden. *“Er zal een gebruikersorganisatie komen, we zullen jaarplannen moeten gaan maken, wensenlijsten indienen, etc. Dat zijn normale ontwikkelingen.”*

Een paar vragen liggen nog wel op tafel en moeten uiteindelijk in afspraken met Whitebox Systems worden vastgelegd. Zoals, wie is verantwoordelijk voor welk deel van de keten? “*Bij het LSP is dit een meertrapsraket met verschillende schakels; nadat ik een call in het incidentmanagement systeem registreer wordt hier uiteindelijk op teruggekoppeld. Maar of alle schakels in deze “ketenregie” goed functioneren gebeurt beetje buiten mijn blikveld. Ik heb hier weinig zicht op. Het voordeel van de Whitebox is dat ik hier meer zicht op heb. Maar we moeten dan wel zelf actie ondernemen.”*

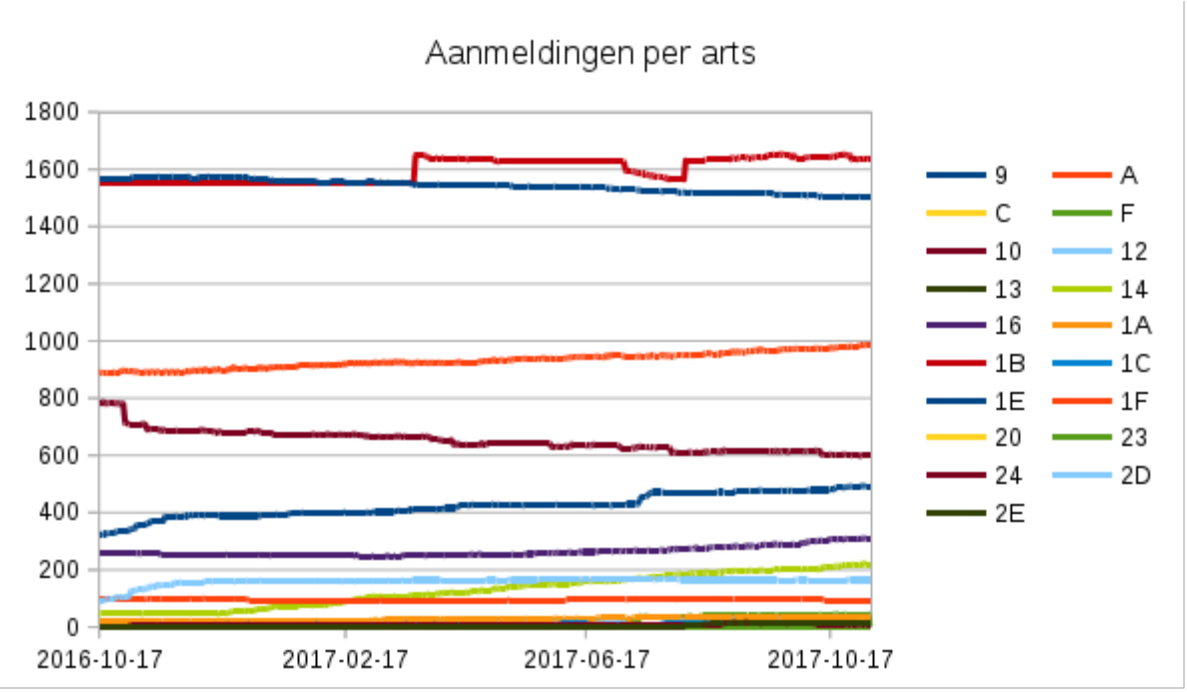
Bij escalatie van problemen zijn minder partijen betrokken. Een eerste aanspreekpunt bij problemen is

de hosting partij van de HAP, die kan vaststellen waar de problemen liggen: bij de leveranciers van het HAP systeem, bij een component van Whitebox Systems (hardware of software) of was er een probleem met een verbinding met een huisarts? Afhankelijk van waar het probleem ligt, kan Whitebox gebeld worden, die desgewenst weer met de hostingpartij van de huisarts contact kan opnemen.

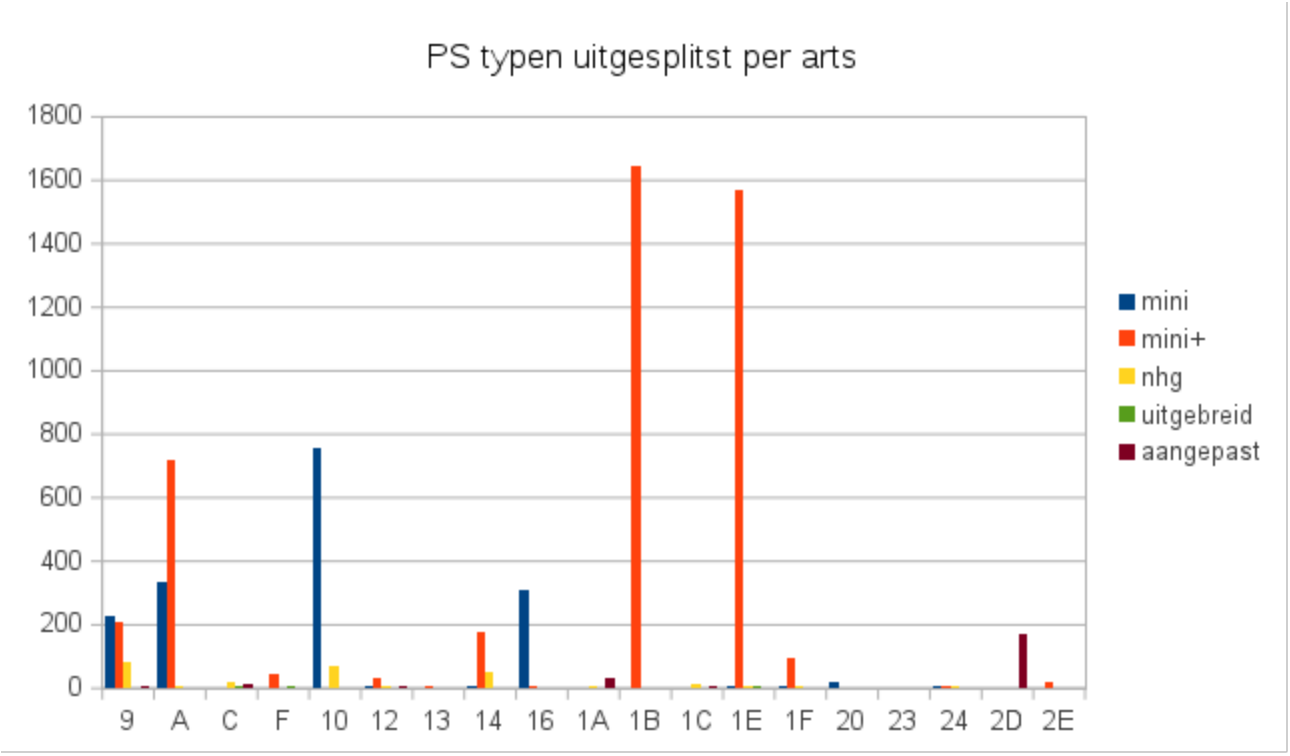
Verder stelt Dekker nog wat vragen over aansluiting bij vragen uit de markt, zoals het in het HIS kunnen plaatsen van overdrachtsinformatie. De Whitebox loopt hier reeds op vooruit door in TetraHIS ervoor te hebben gezorgd dat een (permanente) notitie geplaatst kan worden bij de patiënt, los van de journaalregels, en wil verder vanuit de visitelijst ook tijdelijke overdrachtsnotities kunnen ‘inschieten’ bij de HAP. Hiervoor is een verzoek ingediend bij Call Manager. Zodra het HIS specifiek velden voor overdrachtsinformatie gaat bevatten, zal Whitebox deze ontwikkelingen volgen.

6 De Pilot in cijfers

Over de pilot periode zijn een aantal aspecten getalsmatig bijgehouden. Per device is dagelijks het aantal aangemelde dossiers geregistreerd. Op 17 oktober 2016 zijn we begonnen deze aantallen uitgesplitst te registreren, zodat zichtbaar werd hoeveel van elk type professionele samenvatting (miniPS, miniPS+, NHG, uitgebreid, aangepast) aangemeld werd. Veelal werd dit bepaald door de praktijk (default) instelling, maar uiteraard was het mogelijk om hiervan af te wijken per patiënt. Om deze reden tonen we hieronder de getalsmatige resultaten van de pilot sinds 17 oktober 2016 (peildatum heden 7 november 2017).

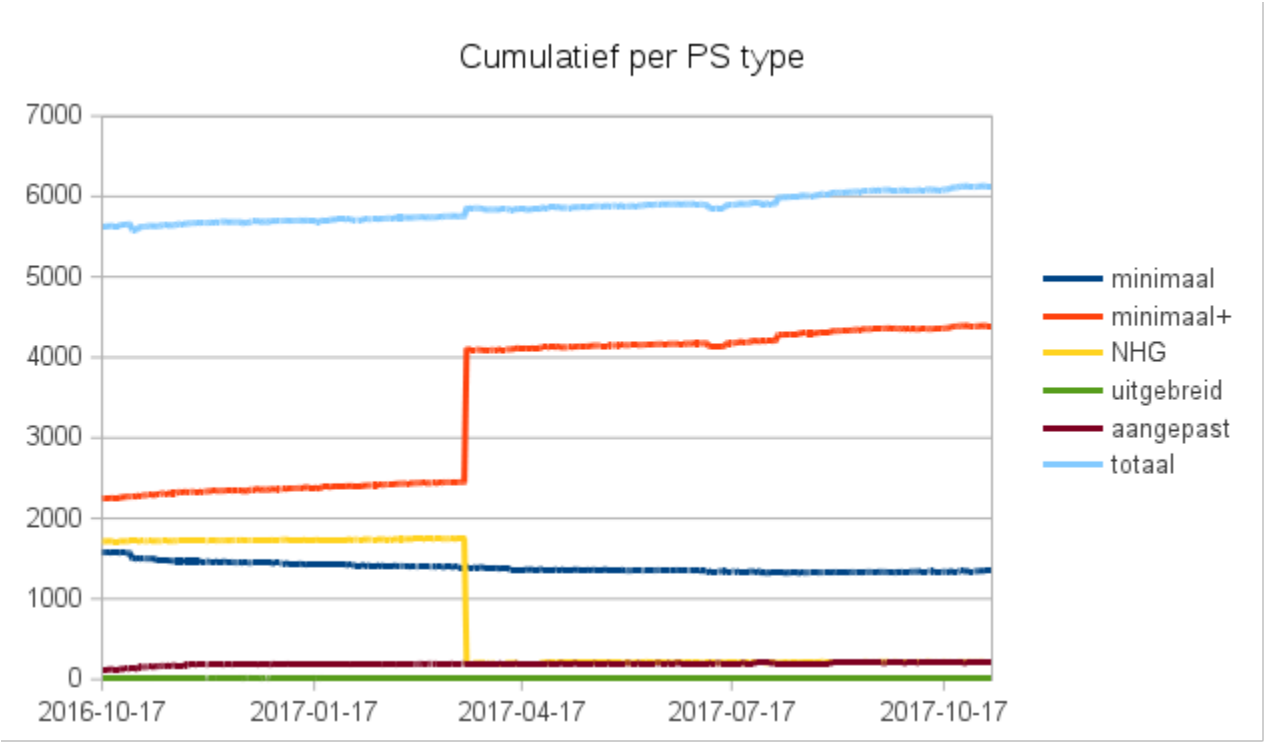


In figuur 1 wordt het aantal aanmeldingen per arts getoond. Een tweetal huisartsen heeft geen dossiers aangemeld. Verdere artsen variëren tussen enkele tientallen en (sinds begin van de pilot in 2015) ca. 1000 patiënten. Het verdient vermelding dat twee artsen (bovenaan de grafiek) initieel begonnen met een groot aantal aanmeldingen, door batchgewijs alle patiënten die reeds een LSP aanmelding hadden ook voor de Whitebox aan te melden. Merk op dat artsen in geval van de Whitebox geen prikkel hebben om meer patiënten dan nodig aan te melden.
Figuur 2 toont het aantal aanmeldingen per arts, uitgesplitst per type PS.



Getoond is de eindsituatie op 7 november 2017. Zichtbaar is dat veruit de meeste artsen gebruik maken van de minimalePS+ bij het aanmelden van patiënten. Veelal is dit ook de praktijk default. Er zijn enkele NHG PS-en zichtbaar, echter in alle gevallen omvat dit slechts een deel van de aanmeldingen; de verklaring ligt in dat initieel een aantal artsen de NHG PS als default PS kozen, maar op een later moment alsnog zijn overgestapt op de minimale PS+ als default PS voor nieuw aan te melden patiënten; de eerder aangemelde NHG PS-en blijft dan echter wel geldig, tenzij wanneer een arts al deze patiënten expliciet heraanmeldt met een andere PS. Behalve de minimalePS+, hebben ook enkele artsen gekozen voor de minimale PS; dit is de PS zónder consult/journaalregels (de minimale PS+ toont de laatste week journaalregels aan de dienstdoende arts). Dit correspondeert met de opvatting van een aantal artsen die ook in het hoofdstuk over de ervaringen/reflectie van huisartsen wordt genoemd. Twee artsen (1A en 2D) gebruiken een aangepaste PS die neerkomt op de minimale PS met een langere historie qua meetwaardes.

In de volgende figuur, wordt cumulatief getoond welke PS typen aangemeld zijn over de gehele periode 17 oktober 2016 – 7 november 2017:



Deze grafiek bevestigt dat de minimalePS+ het meest gekozen is en, over de tijd, het meest gebruikt wordt en blijft, ook voor nieuwe aanmeldingen; over de tijd loopt het aantal aanmeldingen met een minimalePS wat achteruit – navraag leert dat de twee betreffende artsen minder patiënten zijn gaan aanmelden, terwijl er wel patiënten zijn overleden (deze worden automatisch afgemeld). Betreffende artsen melden slechts patiënten aan als zij het strikt noodzakelijk achten.
Eén opvallend aspect is dat rond april 2017 het aantal aanmeldingen met een NHG PS daalt ten faveure van het aantal aanmeldingen met een minimale PS+. Dit is verklaarbaar doordat een arts, na een herinstallatie van de Whitebox na een storing, besloten heeft de NHG PS aan te passen voor de gehele lijst met eerder aangemelde patiënten, door deze batchgewijs opnieuw aan te melden met de minimalePS+.

De conclusie moet zijn dat de artsen in de pilot voor zover zij patiënten aanmeldden, een sterke voorkeur hebben voor het gebruik van de minimalePS+, gevolgd door de minimalePS. De NHG PS is een aantal malen initieel gekozen, maar later is men op deze keuze teruggekomen en heeft men nieuwe aanmeldingen met de minimalePS+ uitgevoerd.

Aantal zoekacties, gevonden patiënten, en aantal (geslaagde) opvragingen

Naast de hoeveelheid patiënten die worden aangemeld, is ook relevant hoeveel patiënten gevonden worden op de huisartsenpost. We nemen als beginpunt voor de peiling 10-7-1017. De reden hiervoor is dat op 10 juli een versie van Call Manager op de HAP is uitgerold, die een pop-up gaf waardoor artsen die zonder UZI pas ingelogd zijn, kunnen zien dat er een Whitebox dossier voor een gegeven patiënt is, en dat deze ingezien kan worden als zij met hun UZI pas ingelogd zijn. De periode van meten is 10-7-2017 t/m 10-10-2017. Dit zijn de cijfers:

- In totaal werden van de 19 pilot-huisartsen die 6112 patiënten hadden aangemeld[35], 1386 patiënten gezien op de post waarbij de Hapbox bevraagd werd. Dit impliceert niet alleen dat de patiënt bij de pilot huisarts geregistreerd was bij de intake tijdens triage, maar tevens dat de assistent(e) die de patiënt in de agenda zette met een geautoriseerde UZI pas was ingelogd (dit was niet altijd het geval). Als aan deze voorwaarden voldaan was, werd de Hapbox bevraagd.
- Van deze 1386 patiënten, werd in 171 gevallen (12.3%) daadwerkelijk een dossier gevonden.
- Van deze 171 ‘hits’ werden 16 dossiers opgehaald. Dit betekent concreet dat in minder dan 10% van de gevallen de arts op de huisartsenpost die een patiënt zag een UZI pas gebruikte om in Call Manager in te loggen.
- In 6 gevallen waarbij er een ‘hit’ was werd wel een opvraging geprobeerd, maar was de UZI pas van de opvragende arts niet geautoriseerd in de Hapbox. Dit was zichtbaar in de logfiles van de Hapbox en gerapporteerd in een “snuffelverslag” aan de beheerder.

35 Eén van de 20 pilot-huisarts is gestopt als deelnemer van de pilot wegens overname (stopzetting) van zijn praktijk. Uitgaande van een normpraktijk van 2300 patiënten, zouden ruwweg maximaal ca. 19*2300 = 49.400 patiënten aangemeld kunnen worden. Een aantal praktijken is aanzienlijk groter dan 1 normpraktiijk; ruwweg kan gesteld worden dat 10% van de patiënten van alle pratijken aangemeld is (gemiddeld).

5 Operationele ervaringen en ontwikkeling bedrijf van start-up naar groei

Dit hoofdstuk beschrijft de ontwikkeling van Whitebox Systems gedurende de pilot. Aandacht in dit hoofdstuk gaat uit naar de stappen die Whitebox Systems heeft gezet om van een development georiënteerde startup te komen tot een organisatie die (ook) de operationele aspecten van een bedrijf dat in de zorg – en in het algemeen – moet kunnen leveren. De lessons learned en de ontwikkeling die het bedrijf heeft doorgemaakt zijn vanuit organisatorisch oogpunt niet uniek of nieuw. Een bijzonder aspect is echter dat het systeem in hoge mate gedistribueerd is, en ook gedistribueerde verantwoordelijkheden kent. Bovendien produceert en levert het bedrijf niet alleen software, maar ook hardware. Wat dit impliceert voor de organisatie wordt in dit hoofdstuk behandeld. We nemen waar mogelijk een chronologische opbouw aan.

1 Organisatie: van development naar een operations

Whitebox is begonnen als een pure, (lean) development organisatie. Twee systeem programmeurs werkten aan het opzetten en functioneel maken en testen van het systeem. De directeur/oprichter nam alle andere, niet aan programmeren gerelateerde aspecten zoals publiciteit, relatiemanagement en het zoeken van financiering voor zijn rekening, naast het voorbereiden en uitvoeren van installaties bij en ondersteunen van huisartsen. Tevens was de directeur eindverantwoordelijk voor de technische beslissingen (dit is nog steeds het geval).

De stappen die gezet zijn omvatten in chronologische volgorde:

1. Keuze en opzet van een operating systeem en software distributie systeem, inclusief een framework voor het configureren en updaten van remote systemen (Whiteboxen);
2. Keuze van framework voor development (in Linux)
3. Een eerste *proof-of-concept (PoC)* -- een “verhuismap” – in feite een decentrale en veilige on-site variant van ‘WeTransfer’ ten behoeve van verhuizen / overdragen van medische dossiers; met deze PoC hebben we netwerk aspecten en user interface development en gebruik kunnen testen zonder dat een HIS koppeling noodzakelijk was;
4. Pre-setup configuratie management; management en uitlevering van backup keys en opslaan van versleutelde backups en monitoring bestanden van uitstaande devices;
5. De Whitebox en een Hapbox voor de waarneemkoppeling, waarbij de Whitebox gebaseerd was op de proof-of-concept code (3), welke gekoppeld moest worden met het HIS;

6. Opzet van een website, inclusief sales module (online/automatisch betalen);
7. Rond 2015, ontwikkeling van een aantal nieuwe Whitebox applicaties (proof of principle), waaronder de visitelijst en patiëntentoegang.
8. Doorgaand werk aan de (centrale) infrastructuur voor onder meer code distributie, TLS verkeer tunneling, en monitoring (van de status van devices, etc.)
9. Ontwikkeling van secure hardware voor het veilig booten van Whitebox systemen met nieuwe software of updates, inclusief een efficiënt software distributie systeem

Zoals aan bovenstaande te zien is, is het team opgezet als *DevOps* team – het team is niet alleen verantwoordelijk voor de ontwikkeling van de software, maar ook voor het testen en de deployment van de software.

De organisatie is langzaam maar zeker gegroeid. Initieel vond groei vooral op technisch vlak plaats, maar inmiddels heeft Whitebox ook personeel voor ondersteunende technische en meer commerciële functies, project management, klantencontact en contact met leveranciers. Zo bereidt de organisatie zich voor op het verstevigen van de uitrol en support-taken die horen bij de uitrol van het product.

Quality assurance (d.w.z. testen van eindgebruiker functionaliteit, onder meer via een test- en acceptatieomgeving) wordt uitgevoerd in een test omgeving. Ontwikkeling en testing ligt verspreid over alle leden van het technische team, de directeur, en de support engineer(s). Hierdoor houden alle personeelsleden voeling met het product zoals dit zich manifesteert aan eindgebruikers.

Development, release management en (keten)testing: de OTAP omgeving

De ontwikkeling en uitrol van Whitebox software is opgedeeld in zogeheten *stages* die overeenkomen met de Nederlandse OTAP terminologie: ontwikkeling, testing, acceptatie en productie. Elke nieuwe functionaliteit wordt in testing (eerste tests) en staging (vergelijkbaar met een beta release) eerst intern getest voordat de staging versie in beta naar een aantal artsen gaat, bijvoorbeeld artsen die om de specifieke functionaliteit gevraagd hebben. Een nieuwe release wordt nooit in één keer naar alle huisartsen tegelijkertijd doorgezet. Functionaliteit kan naar specifieke Whiteboxen, dan wel over kleine of grotere *device sets* (sets van Whiteboxes) worden uitgerold. In productie kunnen huisartsen een *staging* of een *stable* versie kiezen; staging komt overeen met een beta release.

Er zijn intern altijd een aantal devices die staging en stable software draaien. Zo hebben medewerkers altijd de beschikking over de huidige beta en productieversies van de software. Deze kunnen ook aan verschillende, door de samenwerkende leveranciers beschikbaar gestelde (test)omgevingen van verschillende versies van HIS en HAPIS systemen worden gekoppeld, ten behoeve van testing.

Dit maakt het mogelijk om ketentests uit te voeren met alle betrokken systemen, op basis van praktijkscenario's. Het uitvoeren van (beta) tests in de productieomgeving is onontbeerlijk, omdat interacties en bijvoorbeeld patiëntendossiers die in de praktijk voorkomen nooit helemaal te simuleren zijn in een testomgeving. Een Whitebox of Hapbox in *staging* kan in de regel snel worden omgezet naar een stable versie. Pas na de nodige tijd testen in staging, wordt de versie doorgezet naar productie en komt de nieuwe functionaliteit voor alle huisartsen beschikbaar.

Het technische team maakt gebruik van een project management en ticketing systeem waarin het plannen van (sub)taken en het vastleggen van tickets (waaronder ook bug reports en feature requests) plaatsvindt.. Dit systeem blijkt goed te kunnen schalen met de groei van het development team en het aantal developmenttaken en projecten.

Het monitoring systeem (welke de status van alle devices/Whiteboxen *real-time* bijhoudt – zie hieronder) kan kritieke events ook in het ticket management systeem inschieten, zodat de developers / system maintainers deze tijdig kunnen oppakken. Dit staat echter los van issues die alleen customer management raken, zoals wanneer een device offline is. Dergelijke issues worden pas naar het project en software management systeem doorgezet wanneer evident is dat het probleem acties van de developers (in hun rol van back-office support) vereist.

Customer support

De organisatie heeft via de pilot in Amsterdam (en kleine 'satelliet pilots' in onder meer Maastricht) voldoende ervaring om efficiënt en met een goede service Whiteboxen uit te rollen bij een (potentieel aanzienlijk) aantal klanten. Zo is er een customer relation management (CRM) systeem ingericht waarin klantrelaties, verslagen van gesprekken en afspraken in kunnen worden vastgelegd. Ook de inventarisatie van relevante gegevens van een klant voor de levering van een systeem vindt plaats in dit systeem, alsmede vastlegging van alle voor onderhoud relevante aspecten zoals de opstelling van het systeem en de installatie. Dit is relevant voor (on-site) support medewerkers.

Voor de installatie van een systeem zijn onder meer van belang:

- Wie is in de praktijk het algemene aanspreekpunt voor technische zaken
- Wie is de beheerder van het systeem (o.a., uitgeven accounts, nalopen logfiles, ontvangen van "snuffelverslagen");
- Wie is verantwoordelijk voor het netwerkbeheer
- Wie is verantwoordelijk voor het applicatiebeheer (HIS beheer: updates, etc.)

Deze informatie wordt vastgelegd in het CRM; hier worden ook zaken die opvolging behoeven in vastgelegd. Het CRM draait on-site op een eigen server van Whitebox Systems die alleen toegankelijk is voor geautoriseerde medewerkers.

Monitoring en alerting

Voor een decentraal communicatiesysteem dat permanent bereikbaar moet zijn, is een goed monitoring systeem essentieel en onontbeerlijk. De monitoring software (die door Whitebox Systems zelf ontwikkeld is) heeft gedurende de pilot een grote ontwikkeling doorgemaakt. Inmiddels monitoren we op:

- Up-time (bereikbaarheid netwerk);
- Versie nummers van de Whiteboxen en de daarachter liggende HIS server software (indien voorhanden);
- Latency (vertraging bij bevraging van een Whitebox – een maat voor de kwaliteit en de snelheid van de netwerkverbinding);
- Tijd sinds laatste keer her/opstarten (uptime)
- Geheugen en disk gebruik en -beschikbaarheid
- Indien voorhanden, kwaliteit van de disk en andere relevante hardware status informatie

Hiermee kunnen we pro-actief huisartsen informeren wanneer bepaalde zaken die de bereikbaarheid van de Whitebox beïnvloeden, aandacht behoeven. Tevens kunnen we met deze informatie pro-actief eventueel hardware onderhoud tijdig inplannen.

Verder worden als onderdeel van de pilot de volgende zaken centraal gemonitord:

- Het aantal aanmeldingen per Whitebox lijst (uiteraard zien we niet *wie* aangemeld zijn, alleen maar aantallen);
- Error reports: traden er fouten op bij bevragingen, bijvoorbeeld beschikbaarheids-issues, autorisatie errors?
- Status van de verbinding met de Hapbox
- Aantallen uitgegeven credentials voor lokale toegang (2 factor authenticatie)
- Het aantal gelukte en mislukte inlogpogingen (ter detectie potentieel misbruik);

Onze monitoring software is zo ingericht dat klanten alleen samenvattingen van relevante informatie ontvangen, tenzij het een urgent issue betreft. Wanneer we wel parameters monitoren uit de tweede lijst, doen we dat wanneer de huisarts ons hier expliciet opdracht en toestemming voor geeft. Kritieke

aspecten zoals bereikbaarheid en functioneren van de Whitebox in algemene zin monitoren we uiteraard wel.

Het monitoring systeem is inmiddels voor een deel geautomatiseerd en zeer geavanceerd, en dit wordt actief doorontwikkeld. Het systeem bestaat uit decentrale logging componenten (in de devices zelf), die onder meer e-mails naar de beheerder van het device kunnen triggeren, maar ook uit centrale logging/monitoring die Whitebox Systems in staat stellen om tijdig actie te ondernemen wanneer een bepaalde parameter van een systeem in de gevarenzone komt (bijv. disk space/health).

Belangrijk is dat nu veel monitoring-events (zoals dat een device niet bereikbaar is over het netwerk) geautomatiseerd verwerkt worden. We hebben een systeem ontwikkeld dat patronen in de monitoring events analyseert om klanten actief te informeren over relevante aspecten van hun systemen, zoals regelmatige korte onbereikbaarheid via het netwerk, wat enige aandacht behoeft als het regelmatig gebeurt. Op basis hiervan gaan we binnenkort geautomatiseerd mails uitsturen om klanten te wijzen op bepaalde belangrijke of minder belangrijke maar aanhoudende problemen. Deze functionaliteit wordt nu getest, met aandacht voor detail om te zorgen dat artsen alleen als het echt nodig is mail ontvangen. Uiteraard geldt dit ook voor support medewerkers die, als dit relevant is, via mail en via het CRM geïnformeerd worden om eventuele problemen te kunnen onderzoeken en eventueel actie te ondernemen of contact op te nemen met de betreffende klant.

Op deze manier kant het support team focussen op relevante aandachtspunten, terwijl de (decentraal) verantwoordelijke partijen – huisartsen en HAPpen – snel geïnformeerd worden over relevante aandachtspunten die zij zelf kunnen oplossen. Zo blijft het systeem schaalbaar.

Naast geautomatiseerde monitoring blijft visuele (handmatige) inspectie van de status van alle devices relevant om zicht te kunnen houden op de status en (historische) performance van de apparaten in het veld; dit is belangrijk voor het actuele en historische overzicht. Een deel van van het monitoring dashboard wordt als voorbeeld in de volgende figuur getoond:

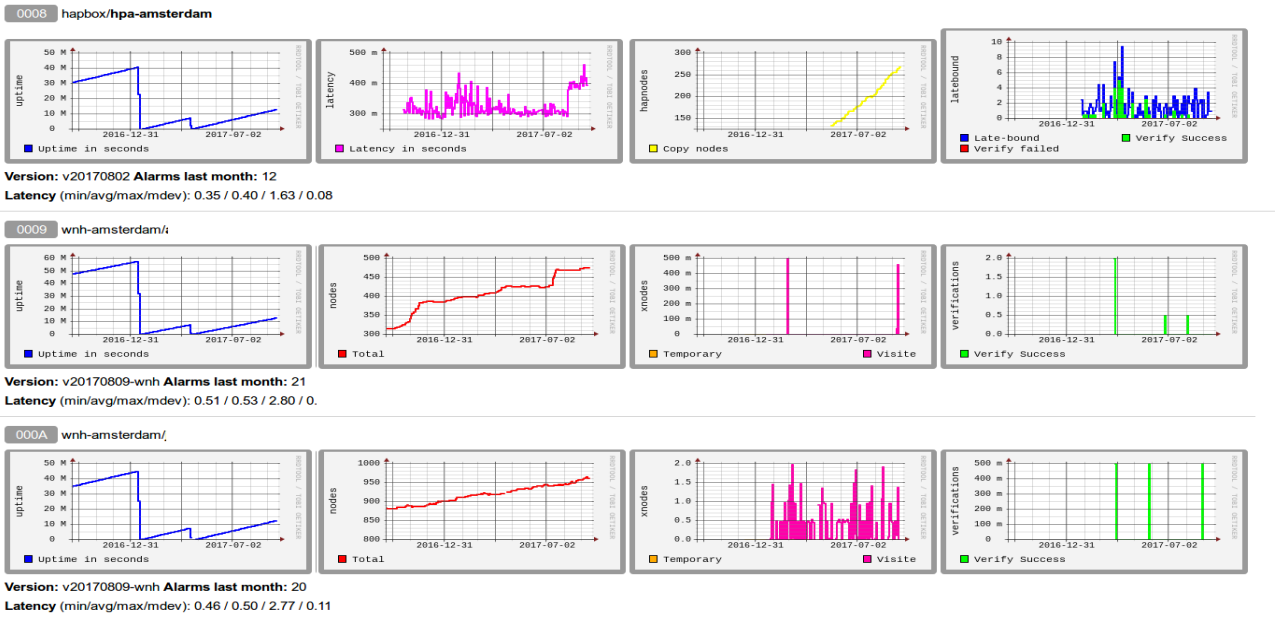


Fig. 3. *Screenshot van de statistics graphs van de Hapbox (bovenste regel) en twee Whiteboxen. Het hier getoonde dashboard laat een historisch overzicht over de laatste 12 maanden zien. Te zien zijn onder meer uptime (blauw, links; 2 resets door stroomstoring, verder continu up); netwerk latency; nodecounts, aanmeldingen op de visitelijst (paars) met één arts die de visitelijst niet, en een andere die de visitelijst regelmatig gebruikt, en het aantal "hits" bij een zoekactie (blauw) en aantal opgevraagde dossiers (groen).*

In geval van de Hapbox wordt ook gemonitord. Zo worden om het verloop van de pilot te monitoren voor elke dag het aantal (succesvolle) zoekacties geplot, alsmede het aantal succesvolle opvragingen ("hits") - heden zijn er gemiddeld tussen 3 en 5 zoekacties per dag "raak". Het aantal hits is uiteraard afhankelijk van de hoeveelheid aangemelde dossiers, inmiddels ruim 6.500. De Hapbox beheerder ontvangt status-updates met aantallen hits en bevragingen – deze worden dagelijks door de Hapbox verstuurd per mail, in aanvulling op de logbestanden die de beheerder via de Hapbox interface kan opvragen. Zo kan de Hapbox beheerder ook direct kijken wie gegevens heeft opgevraagd of wat de oorzaak was van falen van een opvraging (bijv. niet geautoriseerde UZI pas).

Uiteindelijk ligt voor de hand dat alleen de Hapbox beheerder deze statistieken krijgt, en niet Whitebox Systems. Het is de bedoeling dat de centrale logging van deze statistieken wordt uitgefaseerd na de pilot; de Hapbox houdt dit zelf bij. Overigens zijn via de Hapbox zeer uitgebreide rapportages beschikbaar. Op verzoek van de beheerder van de Hapbox van de HpA kunnen de logfiles in een Excel-compatible formaat geëxporteerd worden voor analyse doeleinden.

Bereikbaarheid tijdens de pilot en richting toekomst

De telefonische bereikbaarheid is tot dusverre voldoende gebleken. Wanneer huisartsen in het weekend of ‘s avonds een probleem met de Whitebox hadden (bijvoorbeeld, omdat deze offline ging), zagen we dit zelf of werden we de volgende werkdag gebeld; opvolging vond meestal direct op deze dag plaats.

Een enkele keer is ‘s avonds gebeld om vragen en opmerkingen door te geven. Op termijn zullen we een 24/7 noodlijn inrichten die bij toerbeurt door het team bemand wordt. Dit is vooral belang wanneer er problemen plaatsvinden bij de huisartsenpost.

Het offline gaan van Whiteboxen in het weekend zou wel een potentieel probleem kunnen zijn. Een buiten werktijden niet beschikbare Whitebox betekent immers dat in die (ANW dienst) tijden dossiers niet opvraagbaar zijn. Anderzijds, waar dit netwerkproblemen betreft, geldt dit ook voor de bereikbaarheid van het HIS – en dit zal dan ook impact hebben op beschikbaarheid van gegevens via bijvoorbeeld het LSP of een andere dienst die live gegevens opvraagt bij het HIS. De cumulatieve beschikbaarheid van gegevens blijft bij de Whitebox overigens relatief hoog: in geval dat één Whitebox uitvalt heeft dit immers alleen impact op de bereikbaarheid van die huisarts – niet op de bereikbaarheid van het gehele systeem. Dit is een inherente (positieve) eigenschap van een gedistribueerd systeem.

Voor de HAP zal een beschikbaarheidsprobleem grotere consequenties hebben. In tegenstelling tot een Whitebox zijn bij uitval van een Hapbox immers niet alleen de gegevens van patiënten van één huisarts niet beschikbaar maar de gegevens van alle patiënten in de regio die aan die Hapbox gekoppeld zijn. Voor de HAPpen zal een redundant (*primary-backup)* systeem ingericht worden, zodat een probleem met de Hapbox snel *on-site* te verhelpen is. Aanvullend zal Whitebox Systems een 24/7 storingslijn openstellen zodra Whitebox de productiefase in gaat. Over de hieraan gerelateerde response tijden en service aspecten zal met de HAP (HpA) een service-level agreement moeten overeenkomen.

2 Stabiliteit software en hardware, ervaringen met setup en installatie

De hardware en software van de Whitebox en de HisBox is tijdens de pilot zeer stabiel gebleken. De meeste storingen die we zagen hadden niets met de hardware of software te maken, maar bijvoorbeeld met het incidenteel lostrekken van een netwerk kabel of een adapter waardoor een Whitebox offline raakte. Dit kon meestal snel opgelost worden. Hoewel dergelijke issues snel via de monitoring opgemerkt worden, kunnen deze wel support tijd kosten en hebben daarmee invloed op de schaalbaarheid van het systeem in organisatorische zin. De geautomatiseerde logging systemen die

direct berichten naar artsen en beheerders sturen als een probleem zoals met de beschikbaarheid van hun Whitebox plaatsvindt, kan hierbij helpen. Verder proberen we een aantal problemen op voorhand te vermijden door zoveel mogelijk te kiezen voor een “plug and play” aanpak voor netwerk configuratie[36] – al kan de klant altijd kiezen voor eigen beheer / beheer door de eigen netwerk beheerder. Verder vereiste het vervangen van server certificaten (https certificaten) ook wat werk (op afstand); dit hebben we inmiddels ondervangen door het gebruik van Let’s Encrypt certificaten, waarbij de Whitebox zelf een nieuw certificaat kan aanvragen. Dit draait nu al enige tijd stabiel.

In de pilot werd een USB stick gebruikt om back-up sleutels op te slaan. Deze USB-stick werd door artsen niet altijd herkend als belangrijk om te bewaren. Op zich is opnieuw installeren van een Whitebox zonder een back-up restore geen probleem, maar het nadeel is dat (versleutelde) logfiles verloren kunnen gaan. In de productieversie van de Whitebox gaan we daarom twee smartcards meeleveren, die duidelijk gemarkeerd zijn als back-up sleutel, zodat meer evident is dat deze bewaard moeten blijven. Eén van deze twee sleutels mag wegraken[37]. We raden bij installatie aan één van de twee back-up sleutels op een veilige plek apart van de andere te bewaren, bij voorkeur buiten de praktijk. Dit om risico van verlies of diefstal van beide back-up sleutels te verminderen.

Wat hardware betreft, laten de Whitebox systemen, gebaseerd op een energiezuinige ARM processor, een uitstekende betrouwbaarheid en goede performance zien. Het enige probleem dat we zijn tegengekomen was gerelateerd aan de (proof-of-concept) oplossing voor opslag van data. Voor de pilot was als interne disk van de Whitebox gekozen voor een SD-kaart. We hebben de SD-kaarten in een zevental Whiteboxen moeten vervangen: de SD-kaarten van één specifieke leverancier gingen kapot na een plotselinge stroomstoring. Hierdoor hebben we wel de nodige ervaring opgedaan met betrekking tot opvolging en oplossen van een storing die meerdere praktijken tegelijkertijd raakt.

Voor de productiefase gaan we de disks in alle Whiteboxen vervangen door een (veel robuustere) SSD

36 Hiermee bedoelen we een aanpak die zaken zoals het instellen van port forwards zoveel mogelijk vermijdt. Waar mogelijk configureert de Whitebox zichzelf via DHCP om daarna een verbinding naar een centrale server van Whitebox Systems op te zetten via welke het verkeer wordt gerouteerd. Over deze server kunnen de client Whitebox en de server Whitebox via een *end-to-end* versleutelde en geauthenticeerde verbinding opzetten zodanig dat de centrale server op geen enkele manier de authenticatie kan beïnvloeden of de inhoud van de gegevensstroom kan inzien. Deze oplossing maakt het installeren en onderhouden van Whiteboxen een stuk eenvoudiger. Het werkt ook met ezorg netwerken.

37 Technisch gezien maken we gebruik van een *key sharing* systeem met drie sleutels, waarvan er minimaal twee nodig zijn voor het herstel van de backup. Whitebox Systems bewaart één van deze sleutels, de klant de andere twee, separaat.

en een on-board *boot medium* gebaseerd op SPI-flash, wat veel robuuster is dan SD kaarten (SPI-flash wordt ook voor BIOS gebruikt). Daarnaast hebben we geleerd dat dat enige diversiteit in de leveranciers/producenten van de interne hardware raadzaam is. Dit was echter al een uitgangspunt in het ontwerp: we willen dat de Whitebox bruikbaar is op een brede diversiteit van COTS (common off-the-shelf) componenten, waaronder het ARM-gebaseerde moederbord, smartcard reader, disk en adapter. Dit maakt ons zowel qua storingen als qua inkoop minder kwetsbaar voor leverings- of andere problemen, zowel in de productieketen als in specifieke devices. Uiteraard houden we bij welke specifieke hardware bij welke klant wordt gebruikt zodat we bij problemen met specifieke onderdelen gericht actie kunnen ondernemen.

Onderhoud

We rekenen erop dat de Whiteboxen elke drie tot vijf jaar (preventief) onderhoud nodig hebben, bijvoorbeeld het vervangen van een SSD, of incidenteel van een moederbord. Het apparaat is grotendeels herbruikbaar (onder meer via een modulaire behuizing en opbouw). Vervanging vereist bezoek door een monteur; ons monitoring systeem rapporteert de status van onder meer de disks en helpt ons bepalen wanneer we op bezoek moeten. De jaarlijkse licentiekosten dekken deze kosten.

Doorontwikkeling – ontwikkelde aanvullende diensten
Na aanvang van de pilot ontstond de vraag of de Whitebox ‘preview’ modus (die onderdeel is van de *administratieve interface* van de Whitebox die alleen de arts binnen de praktijk kan zien) niet geschikt te maken was voor gebruik tijdens visites. Als reactie hierop hebben we een *visitelijst* ontwikkeld, die het mogelijk maakt om een mobiiele visitetoepassing te gebruiken met minimaal risico. Patiënten kunnen vanuit het HIS bij de visitelijst worden aangemeld en zijn vervolgens een dag zichtbaar op een (uiteraard geautoriseerde) specifieke tablet of smartphone van de huisarts of POH-er. Op deze manier kunnen dossiers op eenvoudige wijze tijdens visites ingezien worden middels een visite-App. Alle artsen die de visistelijst App gebruiken vinden hem heel handig en zijn er erg tevreden mee. De app is inmiddels in productie genomen.

Ook is een vakantie/dagwaarneming App ontwikkeld, waarop de waarnemer gedurende een periode (bijv. Een weekend of een paar weken) inzage kan krijgen in dossiers van de huisarts. Deze app bevat ook een “terugkoppel” mogelijkheid waarin de waarnemend arts een samenvatting van bevindingen of acties kan terugsturen naar de eigen huisarts. Functionaliteit voor deze onderlinge waarneem-App wordt nog doorontwikkeld.

Over de duur van de pilot zijn een aantal verbeteringen aan de integratie in TetraHIS toegepast. Zo vond de aanmelding van patiënten initieel via een vrij uitgebreid “opt-in” scherm plaats. Dit is aangepast

zodat er in het consultscherm ook “snelmenu’s” te vinden zijn voor de meest voorkomende functies. Tevens zijn hiermee de verschillende “lijsten” (visitelijst, waarneemlijst tijdelijk/permanent, in de toekomst apotheek) snel toegankelijk. Zo zijn eenvoudig de verschillende aanmeldopties te vinden tijdens een consult. Via het patiënt selectiescherm en de agenda van het HIS zijn tevens ingangen voor aanmelden en afmelden van patiënten te vinden.

Ten slotte is een notitie voor de waarnemer toegevoegd, waarin specifieke notities kunnen worden aangemaakt die permanent zichtbaar blijven. Dit vult de SOEP regels aan, die bij een PS uit beeld verdwijnen na de ingestelde periode (1 week bij de minimale PS, tot 4 maanden bij de NHG PS), en kan ook handig zijn indien een arts überhaupt geen SOEP regels wil delen maar wel specifieke opmerkingen kwijt wil. [38]

De Whitebox heeft heden een (stabiele en functionele) feature set bereikt, bestaande uit:

- HAP koppeling
- Visite-App
- Dag/vakantie waarneming (via een account uitgegeven door de eigen huisarts, geldig gedurende een vooraf vastgestelde termijn)
- Patiëntentoegang

Met bovenstaande diensten kunnen we nu reeds een zinvolle bijdrage aan de praktijkvoering van de huisarts bieden. Deze functionaliteiten en het Whitebox platform waarop deze toepassingen draaien, zijn de afgelopen periode uitgebreid getest en zijn stabiel.

Realisatie van een koppeling met de eigen apotheker (relevant voor medicatiecontrole) alsmede een toepassing die eenvoudige (dynamische) koppelingen met onder meer ziekenhuizen en met patiëntenportalen mogelijk moet maken staan op de planning.

Koppeling met nieuwe HISsen

Afgelopen jaar is een nieuw koppelvlak voor MicroHIS gebouwd, die anders werkt dan de TetraHIS koppeling. De nieuwe koppeling maakt gebruik van een extra “tussenserver”, de *HisBox,* die zorgt voor een vertaling van de ‘HIS wereld´ naar de Whitebox wereld, cq “buitenwereld”.

38 Er wordt heden gewerkt aan een overdrachtsmodule die het mogelijk maakt overdrachten snel en efficiënt in te sturen. De idee is dat deze overdrachten tijdelijk inzichtelijk zijn, in tegenstelling tot een “notitie” die permanent beschikbaar is. Wij willen deze mogelijkheid om een overdrachtsnotitie “in te schieten” op korte termijn ook via de visitelijst toegankelijk maken.

De interface tussen MicroHIS en HisBox is eenvoudiger dan de koppeling tussen TetraHIS en de Whitebox. De HisBox neemt een aantal aspecten zoals lijst management van het HIS over, en voert bovendien dataconversie uit wanneer dit nodig is.

De HisBox draait al een tijd stabiel in een aantal MircosHis praktijken in Amsterdam.

De oplossing is modulair en bedoeld om relatief eenvoudig- zowel voorh het HIS als voor Whitebox Systems - meerdere HISsen te kunnen koppelen. Op het moment dat een nieuw HIS gekoppeld moet worden, verwachten we daarom dat deze koppeling heden relatief eenvoudig kan worden uitgevoerd.

3 Whitebox naast het LSP?

Er wordt vaak gesteld dat het gebruik van meerdere systemen voor het uitwisselen van gegevens geen goed idee is: te duur, te ingewikkeld. Eén systeem is toch veel beter? Hoewel te beargumenteren valt dat de Whitebox standaard voor een groot aantal toepassingen in de zorg toepasbaar is, lijkt de stelling dat één systeem beter is dan meerdere bij het gebruik van communicatiesystemen in de zorg, specifiek de Whitebox naast het LSP, misplaatst.

Ten eerste zorgt het gebruik van twee systemen met complementaire eigenschappen (functioneel en non-functioneel) tot een **hogere dekkingsgraad**, en daarmee tot een hogere beschikbaarheid van gegevens op het 'point of care' wanneer dat nodig is, simpelweg omdat mensen die "nee" zeggen tegen gebruik van één systeem wel geneigd kunnen zijn om ja te zeggen tegen het andere systeem (zie hoofdstuk 6).

Ten tweede vergroot het gebruik van meerdere systemen de **robuustheid** van het systeem als geheel, omdat bij onbereikbaarheid van één systeem het andere – mits dat werkt via een andere infrastructuur en ander netwerk - wel beschikbaar zal blijven. Een aantal huisartsen in de pilot geven aan dat zij het om deze reden fijn vinden dat er meer dan één systeem beschikbaar is voor het aanmelden van gegevens.

De systemen bedienen andere behoeftes en andere scenario's. In de pilot blijkt het gebruik van de Whitebox en het LSP tegelijkertijd eenvoudig, en dit functioneert zonder noemenswaardige problemen: de twee systemen werken probleemloos naast elkaar, zowel aan de kant van de huisarts als aan de kant van de HAP. Dit betekent dat er geen drempels zijn voor het gebruik van deze twee systemen naast elkaar.

Appendix A: vragenlijst huisartsen

Om de waarneemkoppeling te realiseren, moest het Whitebox systeem zowel in het HIS als in het HAPIS geïntegreerd worden. Vervolgens moest dit – in het lab en in de praktijk – getest worden, waarbij belangrijke criteria waren en zijn:

- Betrouwbaarheid / robuustheid van de koppeling
- Eenvoud van gebruik in de praktijk
- Begrijpelijkheid van het systeem
- Correctheid van de gegevens die overkomen / opgehaald worden

Vragenlijst

Onderstaande vragen worden/zijn als checklist achter de hand gehouden bij semi-gestructureerde interviews van huisartsen. Voor een deel van de vragen zijn (representatieve) antwoorden van een deel van de huisartsen die aan de pilot deelnemen al bekend. Explicitering en completering van deze vragenlijst is nuttig om te zien of er nog aanvullende vragen gesteld moeten worden.

Techniek:

- Wat vindt u van idee van een fysiek kastje in de praktijk?
- Wat vindt u van het concept in het algemeen?
- Hoe vond u aansluitings/installatieprocedure?
- Weet u nog hoe u moet inloggen etc.;
- Weet u nog waar de USB stick met backup key is?

Toestemming:

- Vindt u het bezwaarlijk om uw patiënten om toestemming te vragen? Waarom? (bijv. onderbreekt het gesprek, gêne, .)

- Denkt u dat het regelen van toegang eigenlijk wel nodig zou zijn, maar vraagt u toch geen toestemming? Is het te moeilijk uit te leggen, of zijn er andere drempels?

- Is er onzekerheid omdat het niet zeker is of de Whitebox na de pilot wel blijft bestaan? Zo ja: Vindt u onzekerheid hierover onprettig voor uzelf (dubbel werk) of voor uw patiënten (niet/lastig uit te leggen)? Zou zekerheid hierover voor u uitmaken?

- Is het verschil met het LSP duidelijk?

- Welke toestemmingsprocedure hanteert u? Bijv. Schriftelijk (griepprik) of mondeling in de praktijk, bellen, of laat u uw assistent(e) toestemming vragen? Wanneer / bij wie? Heeft u in strategie gewisseld? Wat bevalt het beste, waarom?

- Als u een formulier gebruikt: apart formulier? Bij griepprik, of anderszins? Intake formulier?

- Hoe zou u denken over een elektronische werving: opt-out of opt-in?

- Hoe staat u tegenover opt-out of juist opt-in?

- Welke PS gebruikt u? Waarom? Heeft u van PS instelling gewisseld? Waarom?

- Wat vindt u in het algemeen van de Whitebox, van het concept? Prijs/kwaliteit?

- Als u het systeem wel/niet wilt houden, wat zijn overwegingen? Is de “landelijke lijn” relevant? Overweegt u ook het LSP? Overweegt u beide systemen te nemen? Waarom wel/niet?

Service:

- Hoe vond u de support bij vragen e.d.?
- Hoe vond u de mailing(s); informatievoorziening, etc.? Wat kan hieraan verbeterd worden?
- Snuffelverslagen, zijn die nuttig? Ziet u graag nog andere informatie?
- Heeft u logboek ooit bekeken, bijv. Na een opvraging? [j/n/nvt]. Begrijpelijk?

Appendix B: vragen huisartsenpost

Vragen over het beheer:

- Is het systeem eenvoudig in gebruik? Of juist ingewikkeld?
- Mis je dingen of vind je dingen ingewikkeld? Bijv. qua administratieve handelingen?

Vragen over het model:

- Hoe vind / ervaar je het concept (bijv. procedure van goedkeuren koppelingen Whiteboxen), en het (decentrale) model?
- Wat zijn implicaties van het (decentrale) model vanuit het perspectief van de huisartsenpost? Positieve/negatieve punten?

Ander commentaar of opmerkingen op hoger niveau en vanuit het perspectief van de HAP?

Appendix C: Functionele en non-functionele eisen aan het systeem (requirements)

Het belangrijkste uitgangspunt van de Whitebox is dat de huisarts, met patiënt, zelf de controle heeft om te bepalen wie toegang krijgt tot welke gegevens.

De requirements (uitgangspunten) bij het ontwerp van de Whitebox zijn als volgt:

- Huisarts kan zelf heel precies de toegang tot gegevens regelen: welke gegevens, met wie, waardoor hij goed kan uitleggen wat hij deelt met wie.
- Patiënt kan gegeven toegang zien/traceren (logging), en zelf ook toegang tot gegevens kunnen geven middels push autorisatie, op een praktische manier.
- Er moet voor patiënten een mogelijkheid zijn om de eigen gegevens in te kunnen zien.
- Er moet een mogelijkheid zijn om gegevens van inzage te onderdrukken, in potentie zelfs zo dat de patiënt zelf de onderdrukte gegevens zelf niet meer kan zien. In dit geval, kan alleen de arts de gegevens weer zichtbaar maken. Dit biedt vergaande privacybescherming.
- in principe kunnen er ook “pull” systemen geconstrueerd worden middels de Whitebox technologie. Echter de keuze voor push autorisatie moet altijd zichtbaar en toegankelijk blijven voor arts en patiënt.
- Push autorisatie construeert een geauthentiseerd communicatiekanaal. Gegevenstransport terug naar de eigen arts (en patiënt) via de Whitebox moet mogelijk zijn.
- Whitebox communicatiekanalen zijn *end-to-end* beveiligd en geauthentiseerd; externe partijen in het communicatiepad kunnen niets met de getransporteerde (versleutelde/geauthentiseerde) informatie.
- Vertrouwenslinks met externe (geautoriseerde) partijen moeten decentraal kunnen worden opgezet, zonder tussenkomst van een derde: alle communicatiekanalen moeten bilateraal gevalideerd kunnen worden om te voorkomen ‘vertrouwde’ derden partijen nodig zijn de de beveiliging potentieel kunnen compromitteren.
- Whitebox moet minimaal gebruik kunnen maken van UZI passen voor identificatie/authenticatie. In de toekomst moeten ook andere authenticatiemiddelen ondersteund kunnen worden.
- Het moet mogelijk zijn of worden om in de Whitebox een (*decentraal)* systeem voor identity management toe te passen, waarin onder meer mandateringen op een cryptgrafisch valideerbare manier kunnen worden vastgelegd, zodat (alleen) valideerbaar bij een organisatie werkende artsen of (gemandateerde) medewerkers gegevens kunnen opvragen.
- De Whitebox moet alle verzoeken adequaat loggen, minimaal om aan de vigerende eisen van

de NEN7512 voldoen. In aanvulling op (en sterker dan) wat de NEN7512 vereist, zal de Whitebox altijd end-to-end authenticatie en versleuteling toepassen.

- Logging moet minimaal conform NEN7513 plaatsvinden. (Overigens: de eisen van NEN7512/13 zijn redelijk vanzelfsprekend vanuit beveiligingsperspectief; zie ook [Noordende2010a/b]).
- Waar mogelijk moet de Whitebox zoveel mogelijk gebruik maken of aansluiten op bestaande standaarden voor informatie representatie. Dit om te voorkomen dat adoptie en interoperabiliteit gehinderd wordt doordat leveranciers nieuwe/andere (informatie) standaarden moeten ondersteunen dan gebruikelijk.
- Whitebox Systems zal ijveren om de Whitebox standaard te laten adopteren door leveranciers, al dan niet als onderdeel of doorontwikkeling van een bestaande standaard.
- De Whitebox moet zelf ook op een (open) standaard gebaseerd zijn; dit kan een eigen standaard zijn, welke mogelijk aan te sluiten is op bestaande standaarden (bijv. IHE, FHIR) Whitebox wil géén “vendor lock-in” systeem bieden. Wel wil Whitebox Systems toonaangevend zijn in de ontwikkeling en de toepassing van de standaard. Beheer van de standaard moet volgens open standaard uitgangspunten plaatsvinden. Een aantal doelen zoals dat leveranciers altijd een privacy-vriendelijke optie (lees: push autorisatie) aan patiënten moeten aanbieden als ze de standaard gebruiken/licenseren, zullen mogelijk in beheers/stichtingstatuten vastgelegd worden.
- De Whitebox moet eigen regie van de patiënt mogelijk maken, *zonder* de patiënt voor alle uitwisseling van gegevens of de geheimhouding daarvan verantwoordelijk te maken.
- De huisarts moet het eigen Whitebox systeem kunnen (laten) controleren.
- Whitebox Systems moet, controleerbaar, niet zelf bij medische gegevens kunnen komen; dit zal technisch worden afgedekt in de architectuur en de architectuur (d.w.z., geen centrale diensten waar gegevens of autorisatielogica in staan die toegankelijk zijn voor de leverancier of andere partijen).
- De implementatie moet controleerbaar zijn, met betrekking tot bovenstaande eigenschappen.
- De Whitebox moet in lijn zijn met wettelijke verplichtingen, specifiek Wgbo/Wbp.
- Naast stringente privacy-eisen moet de Whitebox simpel en handig in gebruik zijn. Verder geldt dat gegevensuitwisseling altijd het zorgproces volgt.

Appendix D: Juridische aspecten gebruik Whitebox

Whitebox kiest bewust voor een aanpak volgens privacy-by-design principes. De aanpak van alleen gegevens delen als noodzakelijk, met alleen die partijen die bij de behandeling betrokken zijn, heeft een aantal voordelen. Naast het terugdringen van het aanvalsvlak (door het aantal systemen van waaruit gegevens opvraagbaar zijn te reduceren tot ee n minimum), zorgt het systeem ervoor dat altijd de meest actuele gegevens rechtstreeks bij de bron opvraagbaar zijn. De gekozen aanpak van zeer gerichte autorisatie maakt de juridische randvoorwaarden voor het gebruik van het systeem in specifieke situaties anders dan bij systemen die gegevens op voorhand voor meerdere partijen beschikbaar stellen.

In de literatuur worden systemen traditioneel in twee categorieën onderverdeeld: “push” en “pull”:

- **Push communicatie** is waar een zorgverlener een bericht *gericht* naar een *specifieke* andere zorgverlener/zorgaanbieder stuurt, waarbij op voorhand aan de verzendende zorgverlener bekend is dat de ontvangende zorgverlener bij de behandeling betrokken is. Push communicatie mag in de regel zonder (uitdrukkelijke) toestemming plaatsvinden, omdat het in de meeste gevallen zal gaan om een rechtstreeks bij de behandeling betrokkene en/of met de patiënt besproken is welke informatie aan wie beschikbaar gesteld zal worden.;
- **Pull communicatie** is waar een zorgverlener gegevens beschikbaar stelt aan een groep zorgaanbieder(s) waarbij niet op voorhand duidelijk is of deze zorgaanbieders bij de behandeling van de patiënt betrokken zijn. Bovendien maken pull communicatiesystemen op dit moment veelal gebruik van een externe infrastructuur die persoonsgegevens verwerkt. Een dergelijke systeem mag niet zonder uitdrukkelijke toestemming van de patiënt gebruikt worden voor de ontsluiting van de gegevens. Tevens kent pull communicatie de eigenschap dat gegevens *live* uit het bronsysteem worden opgehaald.

De Whitebox implementeert **push autorisatie**. Push autorisatie is een middenweg tussen push en pull communicatie, die de goede eigenschappen van push (privacybescherming) en de goede eigenschappen van pull (actuele gegevens, controleerbare toegang[39]) combineert**.** Bij push autorisatie weet de verzendende arts precies welke zorgaanbieder hij/zij toegang geeft (autoriseert) – dit is niet een groep zorgaanbieders, maar een *specifieke* zorgaanbieder waarvan de verzendende zorgverlener

39 “Push” impliceert dat informatie van een bron naar een volgende partij wordt gekopieerd bij het opsturen van gegevens. Daarna is aan de bron niet meer inzichtelijk wie de gegevens inziet. Bij push autorisatie wordt informatie altijd ingezien door, en verspreid via URLs die toegang geven tot de brondata. Alle autorisaties en toegang worden aan de bron gelogd.

op voorhand weet dat deze een behandelrelatie met patiënt heeft – zodanig dat alléén die geautoriseerde partij een vooraf gespecificeerde set van gegevens (live, actueel) kan ophalen. Tevens kent de Whitebox geen externe infrastructuur die persoonsgegevens verwerkt en waarvoor op grond van wettelijke regels toestemming gevraagd moet worden. De autorisatiemethodiek (en technische inrichting) is daarom gelijksoortig aan push communicatie.

De push autorisatie systematiek komt op essentiële punten meer overeen met push communicatie dan met pull communicatie. Immers, bij push autorisatie is voor de ontsluitende (autoriserende) partij volstrekt helder met wie gegevens worden uitgewisseld (wie een autorisatie krijgt) en dat/of deze partij een behandelrelatie heeft met de patiënt. Bovendien worden bij de Whitebox géén persoonsgegevens verwerkt of zichtbaar gemaakt anders dan bij de ontsluitende en de ontvangende (geautoriseerde) partij. Zolang de Whitebox gebruikt wordt voor het *bilateraal (één-op-één, via end-to-end versleuteling) uitwisselen van gegevens tussen direct bij de behandeling betrokken zorgaanbieders,* is toestemming vragen daarom in principe niet noodzakelijk.

Ook onder nieuwe wetgeving (de Wet cliëntenrechten bij elektronische uitwisseling van gegevens in de zorg) die in 2016 is aangenomen blijft het onderscheid tussen push en pull communicatie gehandhaafd, en geldt dat voor push communicatie geen toestemming hoeft te worden gevraagd mits deze communicatie plaatsvindt tussen direct bij de behandeling betrokken zorgaanbieders.

De wetgevingshistorie (bestaande uit Kamerbrieven en discussies tussen minister en Tweede en Eerste Kamer) benoemt expliciet een aantal voorbeelden van situaties waarin toestemming óók onder de nieuwe wet niet vereist is. Voorbeelden zijn communicatie tussen huisarts en apotheker, of een link waarmee een huisarts – die een permanente behandelrelatie heeft met de patiënt – inzage kan krijgen in dossiergegevens die een ziekenhuis via een eigen ziekenhuisportaal specifiek (alleen) aan de eigen huisarts beschikbaar stelt. Dergelijke situaties verschillen niet significant van traditionele “push” communicatie met de huisarts of de eigen apotheek, stelt de minister. De geschetste voorbeelden komen overeen met de manier waarop de Whitebox werkt in vergelijkbare situaties.

Een juridische toets die is uitgevoerd in het kader van de pilot analyseert in welke situaties wel en in welke situaties geen toestemming moet worden gevraagd voor het delen van gegevens via een Whitebox autorisatie [de Die, 2017]. Het rapport concludeert dat de Whitebox niet kwalificeert als een “pull” systeem zoals de Wet Cliëntenrechten bij elektronische uitwisseling van gegevens in de zorg en de gedragscode Elektronische Gegevensuitwisseling in de Zorg (EgiZ) bedoelen. Dat is relevant, omdat daarmee regels over toestemming voor het gebruik van (grootschalige) pull-systemen niet van toepassing zijn.

Het rapport concludeert tevens dat in het kader van huisartswaarneming door de huisartsenpost – het voor dit rapport meest relevante scenario – strikt genomen géén toestemming vereist is voor het delen van gegevens, *mits* er een medische noodzaak is voor het beschikbaar stellen van de gegevens (PS) aan de huisartsenpost voor deze patiënt.

De arts moet dus, net als bij push communicatie, bewust nadenken over welke gegevens de ontvangende partij kan inzien, en of het voor die partij noodzakelijk is om deze gegevens in te zien[40].

Het is dus bij push autorisatie, net als bij push communicatie, vereist dat op voorhand duidelijk is dat:
– er een (medische) noodzaak is voor de gegevensuitwisseling;
– helder is wie de (specifieke) ontvangende partij is;
– de ontvangende partij rechtstreeks betrokken is bij de behandeling, of een vervanger van diegene is;.
– alleen noodzakelijke gegevens worden uitgewisseld[41];

Wanneer aan deze randvoorwaarden is voldaan, is feitelijk geen toestemming nodig. In de praktijk kan impliciet toestemming worden gevraagd, zoals bij bijvoorbeeld verwijzingen normaal gebruik is.

Wanneer een arts wel expliciet toestemming vraagt is deze vraag, gegeven de gerichtheid van de autorisatie, zeer duidelijk en eenvoudig (mondeling) te stellen, en deze sluit aan op het zorgproces en daarmee op de beleving en de verwachtingen van de patiënt. In geval van een autorisatie met de waarneempost is dit bijvoorbeeld: *"Ik wil de belangrijkste gegevens uit uw medische historie ontsluiten voor de dienstdoende dokter op de huisartsenpost. Dit gaat via een directe, beveiligde verbinding, en hier zit verder niets tussen. Vindt u dit goed?"*.

In de Amsterdamse pilot hebben alle artsen ervoor gekozen om expliciet om toestemming te vragen. Deze aanpak zorgt er ook voor dat de patiënt samen met arts kan beslissen wie gegevens kan inzien, wat wenselijk is. Daarbij is het vragen van toestemming laagdrempelig, eenvoudig, en logisch in het zorgproces, zoals dat ook het geval is bij push communicatie – en zo wordt dat door deelnemers aan de pilot ook ervaren.

---

40 Daarbij moet de patiënt ook geïnformeerd worden. Normaal gesproken gebeurt dit mondeling, in de praktijk, maar de patiënt kan ook geïnformeerd worden via de post. Uiteraard kan een (geïnformeerde) patiënt altijd aangeven dat hij/zij de gegevensuitwisseling niet wil.

41 Hierbij moet bedacht worden dat bij een permanente autorisatie van de huisartsenpost mogelijk op voorhand niet altijd vaststaat of de ontsloten informatie op het moment waarop de informatie daadwerkelijk wordt opgevraagd nog steeds noodzakelijk is. Dit kan anders zijn wanneer het een zeer minimale gegevensset betreft (bijvoorbeeld, alleen actuele medicatie).

Referenties

[Bakker et al, 2015] H. Bakker, M.F. Huygen, A. Leloup, J.H. Thiel, G.J. van 't Noordende, “Verkenning van een minimale Professionele Samenvatting voor huisartswaarneming”, rapport HKA/UvA, 2015. (Vindbaar via https://whiteboxsystems.nl/pilot-resultaten)

[Dekker, 2011] Cees Dekker, *“Eindrapportage WDH praktijktest”,* Huisartsenposten Amsterdam 2011

[de Die, 2017] Mieke de Die, “Rapport juridische aspecten Whitebox”, Velink & de Die advocaten, 2017

[van Duivenbode, 2017]. J. van Duivenbode, *“Onderzoek zorg-infrastructuren”,* rapportage Nictiz, 2017

[vd Geest, 2014] D. van der Geest, *“De invloed van dossierinzage tijdens ANW-diensten op de huisartsenpost – een vergelijkende verkenning tussen Almere en Amsterdam”*, Scriptie co-assistentschap Vumc, Vrije Universiteit Amsterdam.

[Noordende 2010]. G.J. van ‘t Noordende “A security analysis of the Dutch Electronic Patient Record system”, System and Network Engineering Group Technical Report UVA-SNE-2010-01, University of Amsterdam, 2010

[Noordende 2011] G. van ‘t Noordende, *“Controlled Dissemination of Electronic Medical Records”* Proc. 2Nd USENIX conference on health security and privacy (HealthSec), San Francisco, CA, 2011

[Roelofsen 2017]: Eline Roelofsen, “Elektronisch uitwisselen van medische gegevens vanuit de huisartsenpraktijk – opvattingen van huisartsen en patiënten”, Universiteit van Amsterdam, 2017. (Vindbaar via https://whiteboxsystems.nl/pilot-resultaten)

[Thiel et al., 2015] H.Thiel, S.Zonneveld, G. van ‘t Noordende “Whitebox alternatief LSP”, Medisch Contact 9 sept 2015.

[Vrije Universiteit, 2017] *“De professionele samenvatting: verschillen in verwerking?”* een rapport uitgevoerd door Esmée S. Schregardus en Margot B.M. Oosterwechel, begeleid door L. Lagerwerf, Vrije Universiteit, 2017. (Vindbaar via https://whiteboxsystems.nl/pilot-resultaten)