Factsheet 3

IV Wvggz

1 Inleiding en doel factsheet

De Wet verplichte geestelijke gezondheidszorg (Wvggz) treedt in werking op 1 januari 2020. Gemeenten bereiden zich voor op deze nieuwe wet. Ook in ketenverband wordt hard gewerkt om de wet vanaf de startdatum goed uit te kunnen voeren. De VNG maakt periodiek een factsheet over de informatievoorziening die nodig is om de uitvoering van de Wvggz te ondersteunen. De doelgroep van deze factsheet zijn degenen die vanuit gemeenten bezig zijn met de informatievoorziening (IV) van de Wvggz. Dit is de derde factsheet over de IV van de Wvggz. De eerste twee factsheets zijn – samen met veel andere informatie over de wet – te vinden op vng.nl onder Wvggz.

Deze derde IV factsheet kent de volgende opbouw:

- Testomgeving Khonraad: hoe ziet de nieuwe functionaliteit er uit?
- Ketenetiquette voor het gebruik van veilige mail
- Veilige mail: hoe te voldoen aan de NTA?
- Bijlage 1: Overzicht van de manier waarop met de verschillende ketenpartners gecommuniceerd wordt in het kader van de Wvggz
- Bijlage 2: Een communicatiebericht over de voortgang van de implementatie en in het bijzonder over veilige mail; opgesteld door het ketenprogramma
- Bijlage 3: Checklist voor de IV-implementatie van de Wvggz (opgesteld in samenwerking met VLOT)

De inhoud van deze factsheet is afgestemd met de gemeentelijke werkgroep IV-Wvggz, waarin momenteel deelgenomen wordt door onder andere de gemeenten Utrecht, Den Bosch, Ede, Deventer, Arnhem, Den Haag, Rotterdam, Amsterdam, Delft, Apeldoorn en BAR. Ook is afgestemd met de firma Khonraad en het ketenprogramma Wvggz.

Voor meer informatie over de Wvggz kunt u ook gebruik maken van de handreikingen voor de crisismaatregel, het verkennend onderzoek en de implementatie van de Wvggz. Meer informatie hierover vindt u op de website van de VNG: www.vng.nl/wvggz. Daarnaast is er informatie beschikbaar op de website www.dwangindezorg.nl .

2 Testomgeving Khonraad: hoe ziet de nieuwe functionaliteit er uit?

Wat vind ik op de testomgeving?

De testomgeving van het nieuwe Khonraad systeem is beschikbaar via de URL madurodam.khonraad.nl. Let op: er staat dus geen 'www' in deze URL. Als je deze URL intypt, kom je op een inlogscherm. Je typt je inlogcode en

pincode in, klikt op 'login' en ontvangt kort daarna per sms een extra code. Deze vul je ook in op de pagina die dan verschenen is en daarna ben je ingelogd in de testomgeving.

Je kunt in de testomgeving de stappen uit de werkprocessen doorlopen, zowel voor de crisismaatregel als voor de zorgmachtiging (i.e. verwerken meldingen en het verkennend onderzoek). In het menu aan de linkerkant van de pagina selecteer je daarvoor 'Oefenomgeving Wvggz'. Dan kom je op een pagina met een overzicht van alle te testen stappen in de werkprocessen. Je kunt nu de verschillende onderdelen van het werkproces selecteren en zelf doorlopen. Daarbij heb je ook de optie om voorbeeldgegevens in te laden, zodat je niet zelf alle velden hoeft te vullen.

Hoe kan ik een account voor de testomgeving krijgen?
Je kunt een mail sturen aan Rilana van Slooten van Khonraad (via 2020@khonraad.nl) met de vraag om een persoonlijk account voor de testomgeving. In de mail geef je ook je 06-nummer door; dat wordt gebruikt voor een 2-factor authenticatie om toegang te krijgen tot de testomgeving. Daarna wordt het account voor je aangemaakt en krijg je daarover per mail bericht met de gegevens die nodig zijn om in te loggen.

3 Ketenetiquette voor het gebruik van veilige mail

Dit hoofdstuk beschrijft de etiquette bij het gebruik van beveiligd mailen. De veilige e-mail wordt door verschillende organisaties voor verschillende doelen gebruikt. Zo kan het de primaire uitwisseling zijn daar waar een organisatie (nog) geen beschikking heeft over een systeemkoppeling met haar ketenpartner(s). Daarnaast kunnen partijen die wel beschikken over een systeemkoppeling gebruik maken van de veilige mail om ad-hoc vragen te stellen die niet langs de weg van de systeemkoppeling kunnen worden uitgewisseld. Ook kan veilige mail gebruikt worden in het geval een bestaande koppeling tijdelijk niet beschikbaar is.

In het kort
Veilig e-mailen is niet enkel een technische aangelegenheid, maar is juist gericht op het veilig uitwisselen van persoonlijke gezondheidsgegevens. Voor het beveiligd mailen maken partijen vanaf 1 januari 2020 gebruik van veilige mail producten die interoperabel kunnen werken. Daarmee verzendt en ontvangt een ieder veilige mails vanuit het eigen product en ben je niet meer afhankelijk van de producten van de wederpartij.

Interoperabiliteit is onderdeel van een nieuwe Nederlandse Technische Afspraak (NTA 7516) die vanaf mei 2020 van kracht gaat. Een aantal leveranciers van veilige mail producten heeft toegezegd om ter ondersteuning van de uitvoering van de Wvggz per 1 januari 2020 hun producten al interoperabel te maken. Voor meer informatie over welke leveranciers dit betreft zie www.informatieberaadzorg.nl

Adressering
De wet geeft voor de praktijk van de ketenpartners op een aantal punten een tijdslijn aan die gehanteerd moet worden. Zo moet er bijvoorbeeld binnen 18 uur een beslissing over een crisismaatregel genomen worden en heeft de gemeente 14 dagen de tijd voor het uitvoeren van een verkennend onderzoek. Voor de uitvoerbaarheid van de wet is het dus noodzakelijk dat e-mailberichten met zekerheid tijdig worden afgehandeld.

Daarvoor is tijdigheid van verwerking van veilige mails en bereikbaarheid van organisaties en personen van belang. Iedere organisatie heeft daarbij een eigen verantwoordelijkheid om e-mailadres(sen) waarop deze bereikbaar is kenbaar te maken aan zijn/haar regionale samenwerkingspartners. Een geëigende manier om bereikbaarheid te bewerkstelligen kan het gebruik van functionele e-mailadressen zijn. Hierover dienen regionale afspraken te worden gemaakt zodat helder is wie op welk (functioneel) adres bereikbaar is voor welke vragen en acties. Goede inrichting, beheer en gebruik van de (functionele) mailadressen hoort daar ook bij.

Opbouw bericht
Het kan ook handig zijn om afspraken te maken over de opbouw van veilige mailberichten, bijvoorbeeld om deze snel te kunnen afhandelen en doorzoeken. In ketenverband zijn daarom de volgende uitgangspunten geformuleerd:

- **Onderwerp**
  Bij het gebruik van veilige mail wordt voorgesteld om een zaak- of dossiernummer in het onderwerp op te

nemen, gevolgd door de processtap waar het bericht betrekking op heeft, bijvoorbeeld "123456789 – Verkennend onderzoek". Dit maakt het mogelijk om goed te zoeken in binnenkomende mails en deze waar nodig handig te routeren. In het onderwerp wordt dan een limitatief lijstje aangehouden om aan te geven op welke processtap het bericht betrekking heeft. Er is landelijk (nog) geen limitatieve lijst opgesteld, waarmee het raadzaam is dit op regionaal niveau te bespreken.

- **Inhoud**
  Als er informatieproducten worden uitgewisseld, dan is het advies om in die mail slechts gegevens op te nemen die nodig zijn om de processtap uit te voeren waar de meegestuurde bijlagen betrekking op hebben.

  Verder is het aan te raden je contactgegevens als verzendende partij op te nemen zodat er ook buiten de veilige mail om (bijvoorbeeld telefonisch) contact kan worden gelegd indien nodig.

- **In één mail één casus**
  Als er over meerdere casussen gegevens worden uitgewisseld, dan wordt aangeraden om dat in verschillende mails te verzenden. Dit verminderd de kans op het bovenmatig gebruik en buitenproportioneel uitwisselen van gegevens.

4 Veilige mail: tussenstappen naar de NTA 7516

Dit hoofdstuk beschrijft de tussenstappen die nodig zijn om de interoperabiliteit zoals vastgesteld in de NTA 7516 Technische Handreiking te bereiken in het kader van de Wvggz. Deze tussenstappen zijn nodig om per 1 januari 2020 veilig te kunnen mailen zonder dat de leveranciers van veilige mail al volledig voldoen aan de NTA 7516. Vanuit de NTA 7516 is een uiteindelijke implementatie van de gehele technische handreiking per mei 2020 vereist.

Hieronder beschrijven we 5 tussenstappen op weg naar het voldoen aan de NTA 7516. Deze stappen worden gezet door de leveranciers van de veilige mail producten. Dit hoofdstuk is wat 'technischer' van aard dan de andere hoofdstukken van deze IV factsheet, om precies te kunnen aangeven waar de tussenstappen over gaan.

Stap 1: Veilig transport

De technische handreiking van de NTA 7516 gaat grotendeels uit van de 'pas-toe-of-leg-uit'-lijst voor open standaarden van Forum Standaardisatie op het gebied van veilig transport van e-mail. Deze lijst vormt de basis van het onderdeel interoperabiliteit. De technische handreiking vereist voor de uitgaande e-mails het gebruik van DANE-beveiliging, met als fall-back (voor ontvangende mailservers die geen DANE ondersteunen, zoals office365 en Gmail) transportbeveiliging op basis van root certificate name validatie. Dit wordt beschreven in bijlage C van de technische handreiking van de NTA 7516.

Beide inrichtingen vereisen dat de ontvangende organisatie zijn of haar domein heeft beveiligd met DNSSEC. Sommige stakeholders maken zich zorgen dat een groot deel van de zorgverleners die betrokken zijn in de Wvggz voor 1 januari geen DNSSEC op hun domein kunnen aanzetten of te laten overstappen naar een registrar die dit wel ondersteunt. Indien dit een probleem blijkt te zijn, kunnen leveranciers een aanvullend fall-back scenario implementeren op basis van certificate pinning op de veilige maildienst. Hierbij is het voorstel om dit te beperken tot de certificaten van de belangrijkste inkomende e-mailproviders, waaronder Office365 en Google. Dit laatste fall-back scenario is een stap die niet in de technische handreiking is beschreven en daardoor voor meerwerk voor leveranciers zal zorgen.

Leveranciers moeten wel onderling minimaal (bij certificate pinning) de garantie afgeven en technisch valideren dat veilig transport is gegarandeerd, ingevuld met STARTTLS. Daarnaast moet het werkveld altijd bij een veilige maildienst een SPF record implementeren en gestimuleerd worden gebruik te maken van DKIM en DMARC.

Stap 2: Garantie op 2FA bij ontvanger door NTA-compliancy verklaring in DNS controleren

Een essentieel onderdeel van de NTA 7516 is de garantie dat de ontvanger met 2-factor authenticatie (eIDAS substantieel) wordt geauthentiseerd. Om als verzender te valideren dat de ontvanger dit heeft ingericht, wordt gebruik gemaakt van controle op de aanwezigheid van een specifiek DNS-veld in het domein van de ontvanger,

waarmee, door aanwezigheid en geldige inhoud van dit veld, de ontvanger verklaart volledig aan de NTA 7516 te voldoen.

De controle op aanwezigheid van dit DNS-record zou een los onderdeel kunnen zijn in de stappen op weg naar het voldoen aan de NTA 7516. Controle op geldigheid en actie op de inhoud van de record, zoals het niet afleveren van een ongeldig DNS record of e-mails sturen naar een andere MX dan de primaire MX, volgt dan op een later tijdstip.

Stap 3: Valideren geldigheid van DNS-record
Controleren op de geldigheid van het DNS-record, inclusief het niet afleveren in geval van onjuiste content en informeren van beheerder van het domein hierover, kan als los onderdeel worden geïmplementeerd.

Stap 4: Andere SMTP voor inkomende e-mail dan primaire MX in DNS gebruiken
De handreiking van de NTA 7516 beschrijft de mogelijkheid om een andere mailserver dan de normale mailserver te gebruiken voor de afhandeling van inkomende veilige berichten. Hiervoor bestaat de mogelijkheid om in het NTA-DNS-veld een alternatieve MX-server op te nemen.

Dit implementeren vraagt voor veilige mailproviders die al inkomende mail afhandelen, maar alleen in een gesloten netwerk, mogelijk meerwerk omdat dit vereist dat NTA-providers ook gebruik maken van een publiek netwerk zoals het internet waarop het kunnen ontvangen en dat zaken als SPAM en BOUNCE handling hierop zijn ingericht.
Dit kan als los onderdeel worden gerealiseerd. In de tussentijd kan de primaire MX de gevoelige e-mails ontvangen.

Stap 5: Digitaal ondertekenen van mails met CADES
De technische handreiking beschrijft het ondertekenen van e-mails met CaDES als maatregel om de integriteit (dus onderweg aanpassen) van e-mails te waarborgen. Ook dit kan als los onderdeel worden geïmplementeerd.

Resume
Met de tussenstappen zoals hierboven beschreven kan worden toegewerkt naar het voldoen aan de eis rondom interoperabiliteit vanuit de NTA 7516 voor de Wvggz en biedt dit de mogelijkheid om in ieder geval veilig te kunnen e-mailen over publieke netwerken per 1 januari 2020.

Bijlage 1: Overzicht manieren van communiceren

Onderstaand overzicht is een momentopname. Na verloop van tijd zullen naar verwachting meer informatieproducten via systeemkoppelingen worden uitgewisseld. Zo is het streven om in de communicatie met het OM ook de berichten over de zorgmachtiging via de systeemkoppeling te laten lopen.

Gemeenten ontvangen gegevens van cq verzenden gegevens aan:
- de GGZ aanbieders t.b.v. crisismaatregelen via het Khonraad systeem;
- de GGZ aanbieders t.b.v. zorgmachtigingen via de veilige mail;
- het OM t.b.v. de crisismaatregelen via de koppeling met het Khonraad systeem;
- het OM t.b.v. de zorgmachtigingen via de veilige mail / BerichtenBox;
- de IGJ via de koppeling met het Khonraad systeem;
- Stichting PVP via de koppeling met het Khonraad systeem;
- de Raad voor Rechtsbijstand via de koppeling met het Khonraad systeem;
- de advocatuur via de berichtenbox van het Khonraad systeem;
- de gezinsvoogdijmedewerker via de veilige mail of per post;
- de Rechtbank op papier;
- de wijkagent/politie via de veilige mail en/of Seeburger;
- de VHH/ZVH via de veilige mail;
- de huisarts via de veilige mail;
- de woningcorporatie via de veilige mail;
- de schuldhulpsanering via de veilige mail;
- de burgers via de veilige mail, per post, telefonisch of via het portaal van de gemeente.

Bijlage 2 – Noodzakelijke tussenstappen naar veilige gegevensuitwisseling

In deze bijlage nemen we een communicatiebericht zoals aangeleverd door het ketenprogramma integraal over:

De afgelopen periode is er hard gewerkt om de invoering van de Wvggz per 1 januari 2020 mogelijk te maken. Tegelijkertijd zien we ook dat er nog een aantal stappen gezet moet worden en dat veel details pas recent uitgewerkt konden worden. Dit heeft consequenties voor het tijdpad van de komende maanden.

Stand van zaken

Er zijn regionale oefensessie en drie landelijke ketenconferenties gehouden om partijen breed te informeren. Meerdere handreikingen over de uitvoering van de wet zijn vastgesteld, ook zijn vragen over de uitleg van de wet beantwoord. En het overgangsrecht is met zes maanden verlengd. De informatieproducten zijn in een 0.9 versie vastgesteld. De aankomende weken leveren de ketenpartijen hun definitieve informatieproduct op. Ook de vaststelling van de NTA 7516 is in een vergevorderd stadium, zodat veilige e-mail per mei 2020 interoperabel moet zijn.

Tussenstappen in technische handreiking

Omdat in de Wvggz persoonlijke gegevens worden uitgewisseld, zoals gezondheids-, politie- en justitiegegevens kan de uitwisseling van die gegevens niet plaats vinden met gewone mail. In de keten is afgesproken daarom te werken met de technische norm NTA 7516. Hoewel deze norm pas in mei 2020 verplicht kan worden afgedwongen, is een aantal leveranciers van beveiligde mail nu al bezig met het aanpassen van hun aanbod aan deze norm.

Op 1 januari 2020 is interoperabiliteit in zijn volle omvang niet haalbaar. In samenspraak met enkele leveranciers en het Informatieberaad Zorg is een 'tussen oplossing' bedacht. Deze 'tussen oplossing' doet geen afbreuk aan de NTA-norm. Aan de hand van de voorgestelde tussenstappen kunnen de leveranciers samen met de stakeholders bepalen tot welke stap het voor hen mogelijk is een start te maken met NTA-interoperabiliteit en welke stappen zij nog niet kunnen doorvoeren. Vanuit de NTA 7516 norm is een uiteindelijke implementatie van de gehele technische handreiking per 1 mei 2020 vereist.

Proces naar behoren doorlopen

De ketenpartners moeten met hun leveranciers van veilige e-mail samen goed kijken naar de inrichting van veilige e-mail. Gezamenlijk moeten zij de risico's van het onveilig uitwisselen van informatie in het proces van de zorgmachtiging en de crisismaatregel minimaliseren. De inventarisatie van de tussenstappen bij diverse ketenpartners is cruciaal om te zorgen dat de dienstverlening inderdaad gereed zal zijn voor de ondersteuning van de Wvggz. Als dat niet het geval is, dan kan bijvoorbeeld het proces van de zorgmachtiging of de crisismaatregel niet naar behoren worden doorlopen. Ook kunnen ketenpartners juridische risico's lopen, wanneer zij niet in staat zijn tot het beveiligde mailverkeer.

Vragen?

Wil je meer weten over de voortgang over de technische handreiking? Kan dan eens op de volgende websites: https://www.informatieberaadzorg.nl/ en www.dwangindezorg.nl/uitvoering.

Of neem contact op met het Programmabureau Implementatie WVGGZ: WvggzWzdWfz@minvws.nl

Bijlage 3 – Checklist Implementatie IV Wvggz

Nr.	Vraag	Toelichting	Uitwerking voor de regio, planning, contactpersonen
Stap 1. Organisatie en werkprocessen De manier waarop de werkprocessen zijn ingericht bepalen ook hoe de informatievoorziening eruit komt te zien.			
1.1	**Keuze voor uitvoeringsorganisaties.** Waar/bij welke organisatie zijn de taken belegd?	Het gaat i.i.g. om de volgende taken: • Verkennend onderzoek • Crisis Maatregel (alleen bij de BM, of is er ambtelijke ondersteuning) • Doorzetten zorgmachtiging • Ontvangen van meldingen • Horen • Informeren van betrokkene, advocaat en PVP	
1.2	**Zijn er procesbeschrijvingen voor de verschillende taken?**	Zie de taken bij 1.1.	
1.3	**Welke ICT-systemen worden voor welke taken ingezet?**	Het kan gaan om de volgende systemen: Khonraad • GGD-systemen (melding, VO) • Systemen Veiligheidshuis (GCOS, bijv. voor VO) • Veilige Mail • Overige systemen	
1.4	**Zijn er werkafspraken gemaakt over gebruik van Veilige Mail ('mail-etiquette')**	Een in ketenverband opgestelde handreiking over de 'etiquette veilige mail' is in IV factsheet 3 beschreven, die kan allicht gevolgd worden, maar moet waarschijnlijk wel voor de lokale situatie aangepast worden.	
1.5	**Hoe wordt betrokkene geïnformeerd over zijn rechten / plichten?**	Gaat die communicatie volledig via papier (folder e.d.) of wordt in die communicatie ook ICT overwogen?	
1.6	**Hoe wordt de aansluiting met de WZD gerealiseerd?**	Is er een werkproces beschikbaar over: • Keuze voor WVGGZ / WZD traject • Afstemming tussen WVGGZ en WZD	
1.7	**Formatie en aantallen gebruikers**	Hoeveel gebruikers zijn voor de verschillende systemen (i.i.g. Khonraad en Veilige Mail) voorzien, hoeveel gebruikerslicenties zijn daarvoor nodig? Voor welke organisaties moeten de licenties worden verkregen?	
Stap 2. Juridische randvoorwaarden In juridische zin moeten een aantal dingen geregeld worden, om het correct gebruik van de IV mogelijk te maken. Het gaat dan om een contract tussen de gemeenten en Khonraad, maar ook om formele vereisten vanuit de AVG (bijv. een verwerkingsovereenkomst).			
2.1	**Contract met Khonraad**	Wie wordt de contractpartner(s)? Zijn er aanvullende voorwaarden? Kosten? Is het budget beschikbaar?	
2.2	**Contract Veilige Mail**	Welke voorziening(en) worden gekozen? Licenties, kosten. Wie is contractpartner?	
2.3	**Verwerkingsovereenkomsten**	Allicht moeten er vanuit de AVG verwerkingsovereenkomsten worden gesloten met: • Khonraad • Veilige Mail leverancier • Uitvoerende partijen (VO, horen e.d.)	
2.4	**DPIA en afspraken archivering / bewaartermijnen**	• De gemeente moet als verwerkingsverantwoordelijke een DPIA uitvoeren. Doet elke gemeente een eigen DPIA of komt er één voor de regio? • bewaartermijnen nagaan en afspreken N.B. de VNG heeft aangekondigd te komen met een referentie DPIA. Die kan allicht gevolgd worden.	

Nr.	Vraag	Toelichting	Uitwerking voor de regio, planning, contactpersonen
2.5	**Mandatering/delagatie**	Welke taken moeten opgedragen worden aan derde partijen? Voor de mogelijke taken: zie 1.1 Wie maakt het mandateringsbesluit? Vast te stellen door B&W?	
Stap 3. Technische implementatie De systemen moeten in technische zin worden geïmplementeerd, de autorisaties moeten aan gebruikers worden uitgegeven.			
3.1	**Keuze voor systemen**	Voor alle taken (zie 1.1) moet worden bepaald welk ICT-systeem daarvoor wordt gebruikt. Kan die keuze per gemeente verschillen, of is de keuze regionaal?	
3.2	**Proces-keuzes doorgeven aan Khonraad**	Op basis van de lokale inrichting van de werkprocessen (zie stap 1.) maakt Khonraad een inrichting van het systeem die daarbij past. Khonraad maakt een vragenlijst, die de regio moet invullen. Termijnen n.t.b.	
3.3	**Autorisaties en toegang Khonraad**	Aanvragen van autorisaties bij Khonraad. Nagaan wie het beheer van de gebruikers doet: Khonraad of de eigen organisatie. Bij elke partij in de regio een functioneel beheerder / aanspreekpunt voor het Khonraad-systeem aanwijzen	
3.4	**Inrichting Veilige Mail-boxen**	• Aanvragen autorisaties • Inrichten mailboxen • Testen interoperabiliteit tussen gemeenten en ketenpartners • Worden er functionele mailboxen gebruikt, of persoonlijk?	
3.5	**Koppeling Khonraad – Veilige Mail**	Khonraad komt waarschijnlijk met een handreiking / uitleg over koppeling Veilige Mail. De keuze voor Veilige Mail systemen moet aan Khonraad doorgegeven worden, zij leggen dan de technische koppeling met het Khonraad systeem Vanuit VWS wordt gewerkt aan een uitleg over de NTA-norm (gele, blauwe, groene boekje)	
3.6	**Inrichting overige systemen**	Bijvoorbeeld bij GGD of Veiligheidshuis, systemen voor VO of horen. N.t.b.	
Stap 4. Training en opleiding van medewerkers en ketentesten Proefsessies draaien met de ketenpartijen of de systemen werken en medewerkers trainen in het gebruik van de systemen en de toepassing van de gemaakte werkafspraken			
4.1	**Training achtergrond Wvggz, werkafspraken / werkprocessen**	Zoals uitgewerkt in Stap 1. Er komt een generiek trainingsaanbod vanuit VNG – Academie, op basis van een uitvraag naar opleidingswensen gedaan in de ambtelijke werkgroep. Contactpersoon is Karen Kool van VNG Academie.	
4.2	**Training Knoppencursus Khonraad**	• Khonraad stelt een testomgeving beschikbaar (Madurodam) • Bijzondere aandacht voor de instructie van de burgemeesters In de trainingen van de VNG Academie zal ook aandacht zijn voor de werking van de IV	
4.3	**Testversie Khonraad (Madurodam)**	Gebruikers informeren over de testversie, en hen daar toegang toe geven	

Nr.	Vraag	Toelichting	Uitwerking voor de regio, planning, contactpersonen
4.4	**Training Veilige Mail**	• Knoppencursus • Hoe Veilige Mail te gebruiken naast je eigen mail • Uitleg etiquette Veilige Mail (zie stap 1.4)	
4.5.	**Testsessies met de regio**	'droogzwemmen' met de regio om te testen of de systemen voldoende werken en op elkaar aansluiten, en of de systemen voldoende aansluiten op de gekozen werkprocessen	