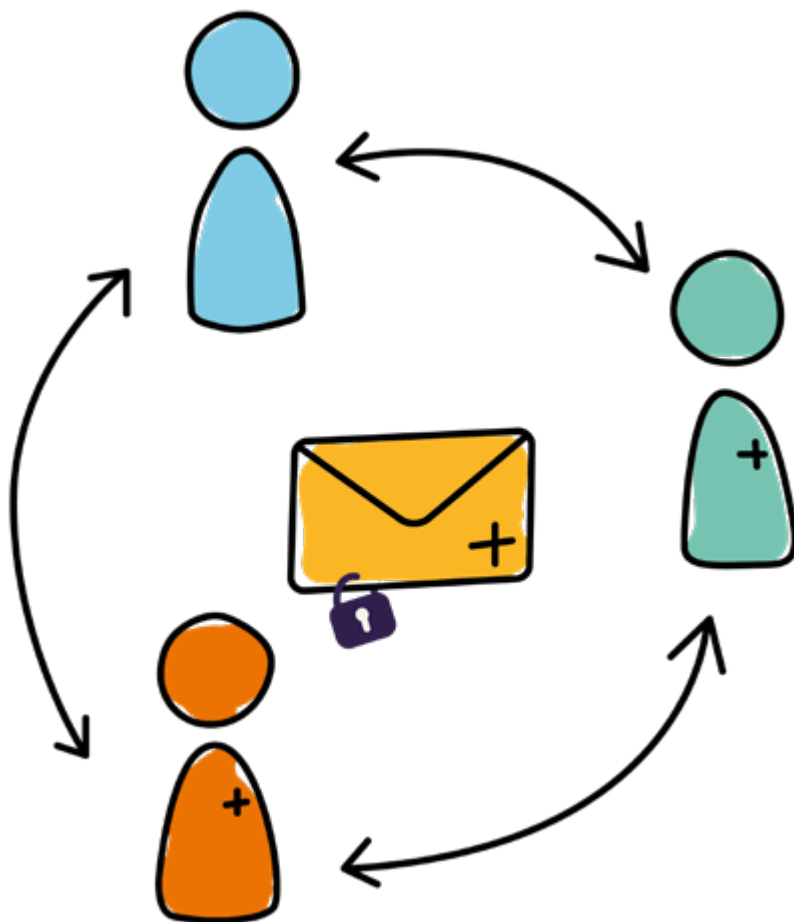


# VEILIG MAILEN, HOE REGELEN WE DAT?!

Implementatiehandboek voor de kleine zorgpraktijk





Er zijn diverse manieren om in de zorg informatie digitaal uit te wisselen. Bijvoorbeeld tussen informatiesystemen, zodat informatie direct op de juiste plek terecht komt. Of waar dat niet kan, met andere oplossingen. Mailen is er daar een van. Zorgverleners moeten afdoende maatregelen nemen om de veiligheid van de informatie te kunnen garanderen. De norm NTA 7516 beschrijft de eisen die worden gesteld aan veilige e-mail. Als je niet voldoet aan deze norm dan ben je als zorgverlener aansprakelijk. Dus, aan de slag! Dit handboek helpt je daarbij.

### Deel 3. Praktijkscenario's

Met aansprekende voorbeelden beschrijven we situaties die in jouw praktijk voor kunnen komen. We lichten toe waarom iets wel of niet mag en geven tips hoe je hier mee om kunt gaan. Zo kun je als zorgverlener veilig mailen met patiënten, collega's en anderen.

Dit handboek is geschreven voor tandartsen, fysiotherapeuten, huisartsen, apothekers en iedereen die werkt binnen een kleine zorgpraktijk.

Het handboek bestaat uit drie delen:

Deel 1.  
Stappenplan

Deel 2.  
Toolkit

Deel 3.  
Praktijkscenario's

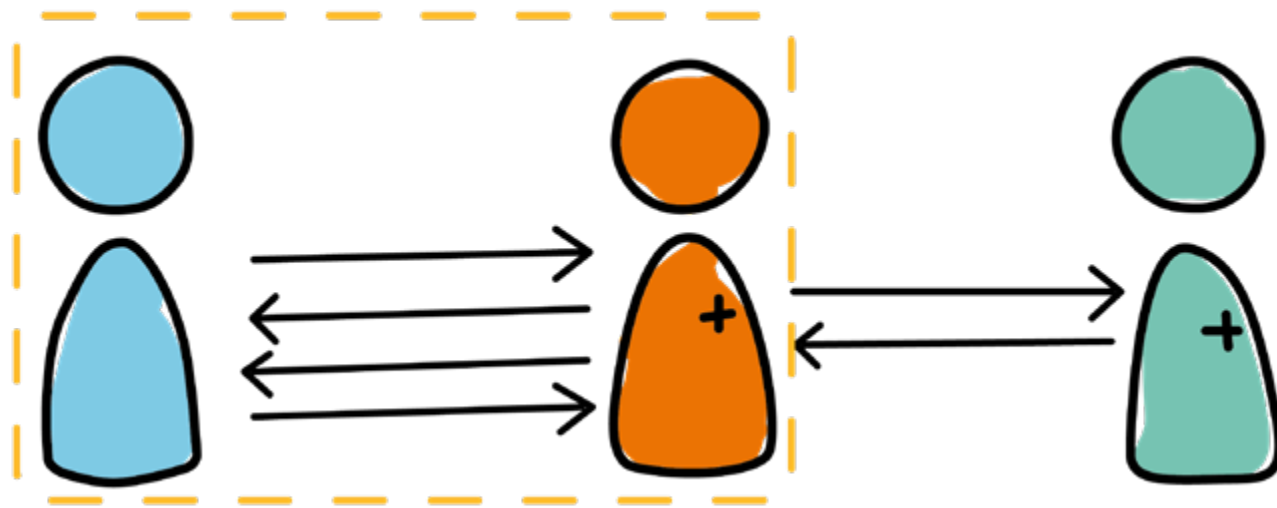
#### Tip

Start met de 'Praktijkscenario's' en lees daarna het 'Stappenplan'. Vanuit het 'Stappenplan' wordt verwezen naar de 'Toolkit'.

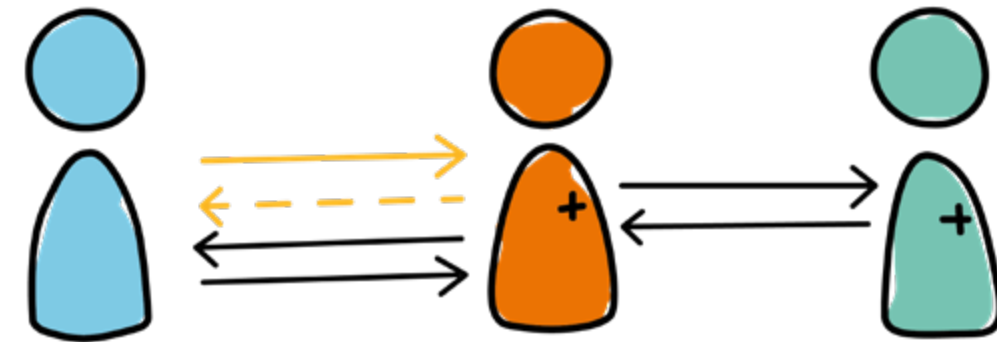
## Deel 3. Praktijkscenario's

<b>Communicatie met patiënten</b>	<b>6</b>
Scenario 1 – Patiënt zoekt contact met zorgverlener	7
Scenario 2 – Zorgverlener zoekt contact met patiënt	12
<b>Communicatie met collega zorgverlener</b>	<b>15</b>
Scenario 3 – Zorgverlener neemt contact op met collega	16
Scenario 4 – Collega neemt contact op met jou als zorgverlener	18
<b>Overige communicatie</b>	<b>19</b>
Scenario 5 – Patiënt mailt met mantelzorger/eigen netwerk	19
Scenario 6 – Communiceren met andere professional	21
Scenario 7 – Communiceren met je informatiesysteem	22

# Communicatie met patiënten



## Scenario 1 – Patiënt zoekt contact met zorgverlener



Piet mailt zijn tandartsenpraktijk, omdat hij wil weten wat de openingstijden zijn. Hij gebruikt hiervoor zijn eigen e-mailaccount zonder extra beveiliging.

Dat Piet voor deze vraag zijn eigen onbeveiligde e-mailaccount gebruikt, is geen probleem. Zijn vraag over openingstijden is niet medisch inhoudelijk en heeft daardoor geen extra beveiliging nodig.

Om verwarring in de praktijk te voorkomen is het aan te raden ook dit soort vragen per e-mail te beantwoorden via een veilige weg. Dit kun je opnemen in de praktijkafspraken. Denk bijvoorbeeld aan:

'We mailen vanuit de praktijk **altijd** via een veilig kanaal. Ook als een patiënt ons via een onveilige weg mailt, het prima vindt als we via diezelfde weg terugmailen en als het om niet medische informatie gaat.' Kijk voor meer voorbeelden van praktijkafspraken in de 'Toolkit'.

Als Piet gevraagd had wanneer en met wie hij een afspraak heeft, dan gaat het wel om persoonlijke medische informatie en moet de mail sowieso via een veilig kanaal beantwoord worden.

Je kunt niet afdwingen dat Piet via een veilige weg een vraag stelt. Wel kun je Piet ontmoedigen door hem beter te informeren door:

- het standaard e-mailadres van de website af te halen en een veilig alternatief aan te bieden. Bijvoorbeeld via een beveiligd e-consult.  
*Onze praktijk maakt enkel gebruik van veilige kanalen om informatie met u te delen. Vragen kunt u stellen via ...*
- duidelijk aan te geven dat het e-mailadres alleen voor vragen is over openingstijden etc. en dat medisch inhoudelijke vragen via een andere weg moeten en met welke reden.  
*Het e-mailadres praktijk@info.nl is alleen bedoeld voor vragen die niet medisch zijn. U kunt hier terecht voor vragen over bijvoorbeeld openingstijden. Voor medische vragen gebruiken wij – ook voor uw veiligheid – een beveiligde toepassing. U kunt ons bereiken via...*
- In een antwoordmail duidelijk aangeven dat het antwoord via een beveiligd kanaal wordt verstuurd. Het blijft de keuze van Piet of hij gebruik maakt van de voorgestelde veilige kanalen.  
*'Het antwoord op uw e-mail sturen we via een ander kanaal. Dit is een beveiligde verbinding om uw privacy zo goed mogelijk te waarborgen. Mocht u hier vragen over hebben dan kunt u ons telefonisch bereiken via 012 – 3456789'.*



Vaak zal een patiënt geen veilige e-maildienst hebben. De NTA 7516 stelt het bieden van een veilig alternatief aan personen door de zorgverlener verplicht.

**Chantal is vergeten wanneer en bij welke fysiotherapeut ze een afspraak heeft. Ze mailt hiervoor de praktijk via onbeveiligde weg.**

Het lijkt erop dat Chantal eenzelfde soort 'organisatorische vraag' stelt als Piet. Toch is dit niet zo. Doordat Chantal vraagt wanneer ze bij welke zorgverlener moet zijn, is het een persoonlijke medisch inhoudelijke vraag geworden. Als zorgverlener ben je dus verplicht via een veilig kanaal te antwoorden.

Patiënten weten vaak niet dat een vraag over een afspraak persoonlijke medische informatie bevat. In de standaardmail om aan te geven dat je via een ander kanaal antwoordt, is het goed om dit te vermelden. Dit vergroot de kans dat Chantal een volgende keer het veilige kanaal zal gebruiken.

Uitdaging is dat het voor Chantal – en alle andere patiënten die mailen - wel toegankelijk en gebruiksvriendelijk moet zijn om een veilige e-maildienst te gebruiken. Ze moet:

- geen aanpassing hoeven te doen;
- veilig en eenvoudig op een bericht kunnen reageren;
- altijd de e-mail kunnen lezen zonder dat ze er een account bij de leverancier voor aan moeten maken;
- de afzender van het bericht duidelijk herkennen.



Wil Chantal het antwoord op haar e-mail toch gewoon via haar eigen e-mailbox ontvangen, dan is dit – ondanks haar toestemming - niet toegestaan. Het antwoord moet via een veilig kanaal verstuurd worden.

**Bob doet via het contactformulier op de website van zijn zorgverlener het verzoek zijn dossier te mailen.**

Het is Bob's recht om zijn eigen medisch dossier in te zien en hij mag het altijd opvragen. Als zorgverlener moet je hierin kunnen voorzien. Delen via het portaal vanuit HIS/ECD/EPD is vaak de meest gebruiksvriendelijke en veilige manier. Een alternatief is het delen via een persoonlijke gezondheidsomgeving (PGO) of eventueel veilig mailen via een beveiligd kanaal. Gebruik in ieder geval geen generieke websites voor bestanddeling, zoals WeTransfer of Dropbox.

Het is wettelijk verplicht om inzage in het dossier te geven. Tot 1 juli 2020 is het prima om een papieren versie te delen. Na 1 juli 2020 ben je wettelijk verplicht Bob gratis digitaal inzage in zijn dossier te geven (vanuit de wet op cliëntenrechten bij elektronische verwerking van gegevens in de zorg, <https://www.rijksoverheid.nl/documenten/brochures/2017/06/01/elektronische-gegevensuitwisseling-in-de-zorg>). Digitaal is hierin een breed begrip. Iemand's dossier op een USB-stick – mét extra beveiliging – geeft ook digitale inzage.

Voor communicatie met patiënten worden patiëntportalen steeds populairder. In een patiëntportaal kan een patiënt de eigen gezondheidsgegevens in zien. Vanaf 1 juli 2020 moeten patiënten namelijk overal digitaal hun medische gegevens in kunnen zien. Een nieuwe manier om gegevens in te zien, is via een persoonlijke gezondheidsomgeving (PGO). Een PGO is grotendeels vergelijkbaar met een portaal. Het grote verschil is dat een portaal vaak zorgaanbieder specifiek is en een PGO van de patiënt is. Een PGO bundelt informatie van meerdere zorgaanbieders en kan zo een totaaloverzicht bieden. Via patiëntportalen en PGO's is het vaak mogelijk om laboratoriumuitslagen te downloaden. Je hoeft de uitslagen dan niet via mail toe te sturen, enkel een melding dat het in het portaal/PGO te vinden is. Kijk op MedMij.nl om alles te weten te komen over PGO's en de ontwikkelingen.

Grote bestanden versturen via de e-mail is vaak niet mogelijk. Maar er zijn wel leveranciers die een veilige e-maildienst aanbieden die ook grotere bestanden veilig kan oversturen. Op de website over veilige email van het informatieberaad staat een lijst met leveranciers die (willen) voldoen aan NTA 7516. Informeer hier eventueel naar de mogelijkheden.

**Rani gebruikt een veilige e-maildienst om zijn huisarts te vragen naar zijn laboratoriumuitslagen. Hij stuurt de e-mail naar [info@praktijk.nl](mailto:info@praktijk.nl).**

Dit is een veilige manier van mailen van medisch inhoudelijke vragen. Rani heeft alles goed op orde.

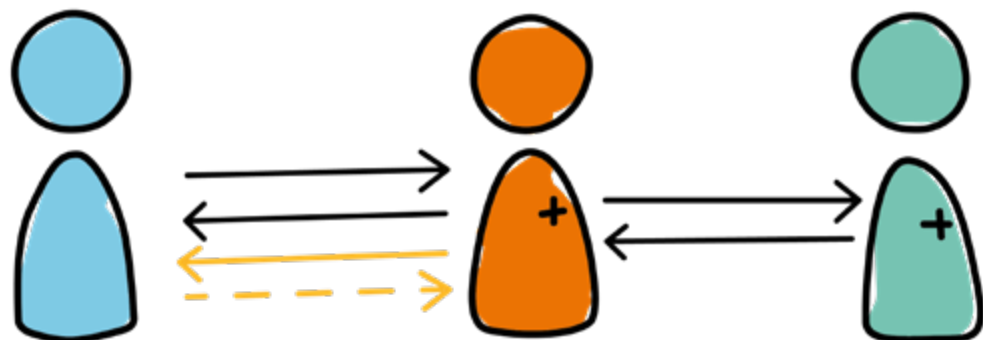
Als [info@praktijk.nl](mailto:info@praktijk.nl) ook werkt op een veilige e-maildienst is de e-mail van Rani direct leesbaar. Als [info@praktijk.nl](mailto:info@praktijk.nl) (nog) geen extra beveiliging heeft, moet je een aantal handelingen verrichten om de e-mail te openen en te lezen.

De communicatie blijft alleen veilig als je ook weer via een veilig kanaal het antwoord stuurt. Vaak betekent dat dat het antwoord niet uit de info-mailbox kan worden gestuurd, maar vanuit een persoonlijke mailbox van de zorgverlener. Tenzij de praktijk specifiek praktijkafspraken heeft vastgelegd over het gebruik van een groepsmailbox zoals [info@praktijk.nl](mailto:info@praktijk.nl). Raadpleeg de 'Toolkit' voor meer voorbeelden van praktijkafspraken.

Idealiter kunnen Rani en de zorgverlener hun eigen gekozen veilige e-maildienst gebruiken. De praktijk is vaak anders, omdat de meeste consumentendiensten (nog) niet voldoen aan de eisen van NTA 7516.

Je kunt zien dat een e-mail veilig is verstuurd, omdat dit zichtbaar in het ontvangen bericht staat. Staat dit er niet, dan moet je ervan uitgaan dat het bericht via gangbare (onveilige) e-mail is verstuurd.

## Scenario 2 – Zorgverlener zoekt contact met patiënt



**Sophie belt de doktersassistente omdat ze wil weten wat de uitslagen zijn van het bloedonderzoek dat ze uit heeft laten voeren. Ze krijgt het telefonisch te horen. Omdat Sophie de uitslagen ook in wil zien, vraagt ze of dat kan. De doktersassistente geeft aan dat ze deze in haar portaal kan inzien.**

De praktijk heeft een patiëntportaal waar de laboratoriumuitslagen in te zien te zijn. Dit is een beveiligd portaal en daardoor een veilig medium om medische informatie te delen. Sophie ontvangt een e-mail zodra er een bericht voor haar in het portaal klaar staat (denk aan mijnoverheid.nl). Sophie logt in en kan haar laboratoriumuitslagen inzien. Deze praktijk is goed voorbereid.

Het inscannen van de resultaten om ze als PDF-bijlage via een onveilige e-maildienst te versturen, is niet toegestaan. Ook op een andere manier via onveilige e-mail communiceren is niet toegestaan volgens de NTA 7516.

Als de praktijk geen portaal heeft, kan het bericht via een veilige e-maildienst worden verstuurd. Sophie krijgt dat een e-mail in haar eigen mailbox. Ze moet zich authenticeren - met 2-factor authenticatie - om de e-mail te kunnen openen. Als je een veilige e-mail stuurt aan een patiënt moet het retourbericht ook altijd veilig zijn.

Naast het inzien van laboratoriumwaarden kan het patiëntportaal meer functionaliteiten aanbieden. Denk bijvoorbeeld aan het e-consult. Via het e-consult kunnen patiënten op een veilige manier een vraag stellen. Een andere functionaliteit is het inzien van het medisch dossier. Vanaf 1 juli 2020 ben je verplicht om het medisch dossier digitaal aan te bieden aan patiënten.

Als Sophie telefonisch aangeeft dat het prima is om het naar haar mailbox te sturen, dan is dit alsnog niet toegestaan en moet je een andere manier vinden.

Ook mantelzorgers en andere gemachtigden kunnen gegevens van een patiënt voor wie ze gemachtigd zijn opvragen en inzien.

De praktijk kan verzoeken dat Sophie langskomt om de uitslag van haar bloedonderzoek op papier op te halen.

# Communicatie met collega zorgverlener

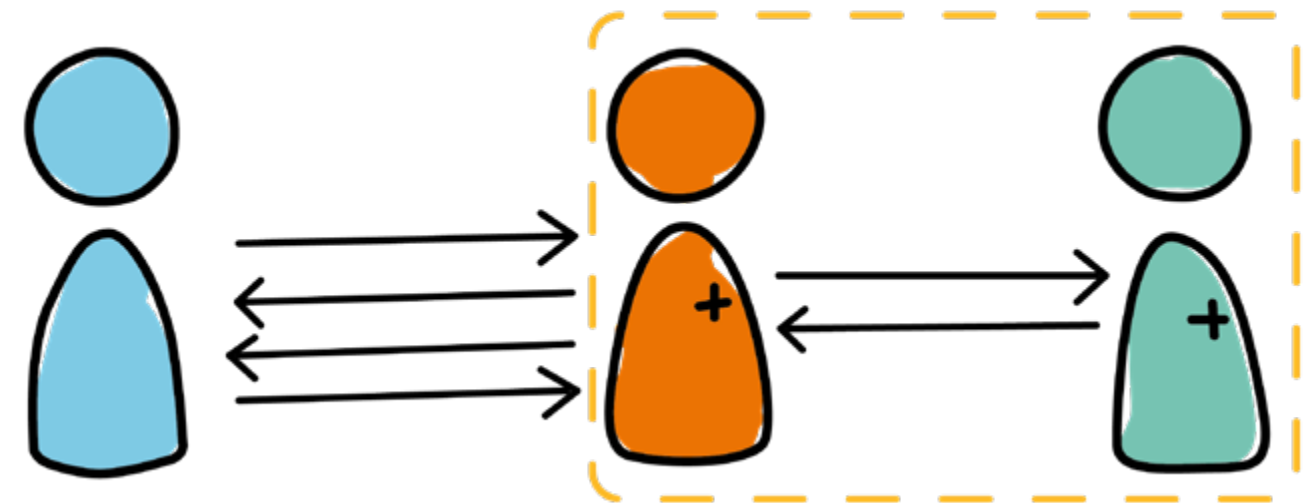
Martijn ontvangt van zijn huisartsenpraktijk een nieuwsbrief in zijn mailbox, een automatisch gegenereerd bericht. De praktijk introduceert een nieuwe huisarts en laat Martijn weten dat er een nieuwe vestiging geopend is.

Dat Martijn dit bericht in zijn eigen mailbox krijgt vanaf zijn huisarts zonder beveiliging is in dit geval geen probleem. Iedereen heeft immers een huisarts. En het gaat hier om praktische en logistieke informatie. Zolang de praktijk geen medisch inhoudelijke informatie in de e-mail meestuur, mag dit.

Het is wel aan te raden ook dit soort berichten te versturen met een veilige e-maildienst. Zo voorkom je dat je fouten maakt.

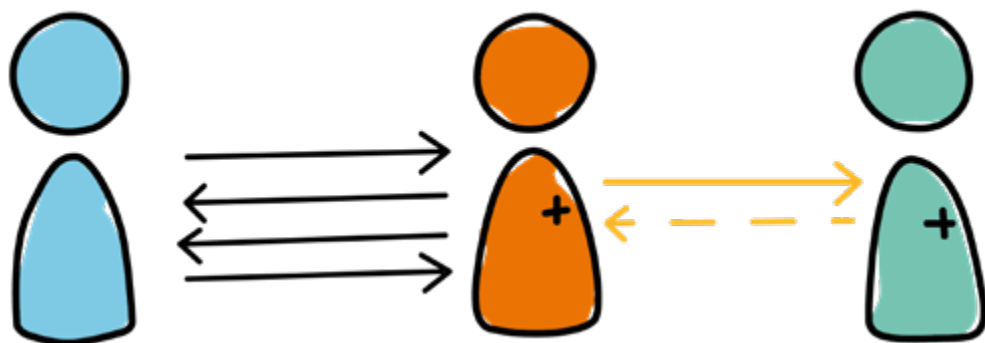
Voorbeelden van automatisch gegenereerde e-mails die naar meerdere personen tegelijk worden verstuurd zijn: afspraakherinneringen, nieuwsbrieven, evaluatiemails en logistieke informatie.

Het ziekenhuis kan Martijn een afspraakherinnering via de e-mail sturen: 'Martijn, u wordt morgen tussen 12.00 en 16.00 in het ziekenhuis verwacht'. Omdat het al snel over persoonlijke medische informatie gaat, kan je als ziekenhuis niet de exacte afspraak mailen. Lees meer over 'het grijze gebied' in de 'Toolkit'.





### Scenario 3 – Zorgverlener neemt contact op met collega



David is onder behandeling bij een psycholoog. De psycholoog besluit – in gezamenlijk overleg – David door te verwijzen naar een psychiater. De psycholoog blijft in contact met de psychiater om betrokken te blijven bij het welzijn van David. Voor dit contact gebruiken ze beide een andere veilige e-maildienst.

Communicatie tussen zorgverleners onderling valt binnen de scope van NTA 7516 en moet dus op een veilige manier gebeuren. De psycholoog en psychiater van David gebruiken beide een veilige e-maildienst en voldoen hiermee aan de NTA 7516.

Als beiden een e-maildienst gebruiken die voldoet aan de NTA 7516, kunnen de veilige e-maildiensten goed met elkaar communiceren, ongeacht of zij dezelfde dienst gebruiken of niet. Lees meer tips in de 'Toolkit'.

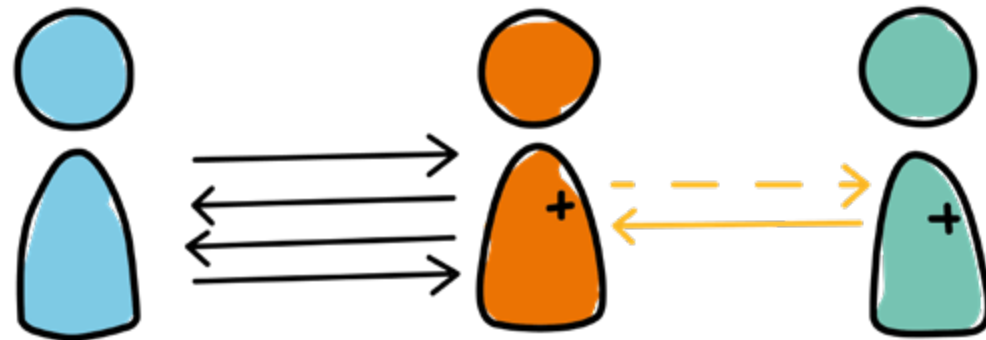
Je collega zorgverlener levert informatie die je in een patiëntdossier wilt verwerken. Vaak moet dit handmatig. Maar er zijn ook ICT-leveranciers die het mogelijk maken een e-mail van je collega zorgverlener direct in je eigen informatiesysteem te verwerken. Dit is geen vereiste van de NTA 7516. Als je het wel wenselijk vindt, kun je het opnemen in het programma van eisen (PvE). Een voorbeeld van een PvE vind je in de 'Toolkit'.



Voor communicatie over een patiënt met een collega is het aan te raden te kijken welke mogelijkheden je informatiesysteem biedt. Neem hiervoor contact op met je ICT-leverancier.

# Overige communicatie

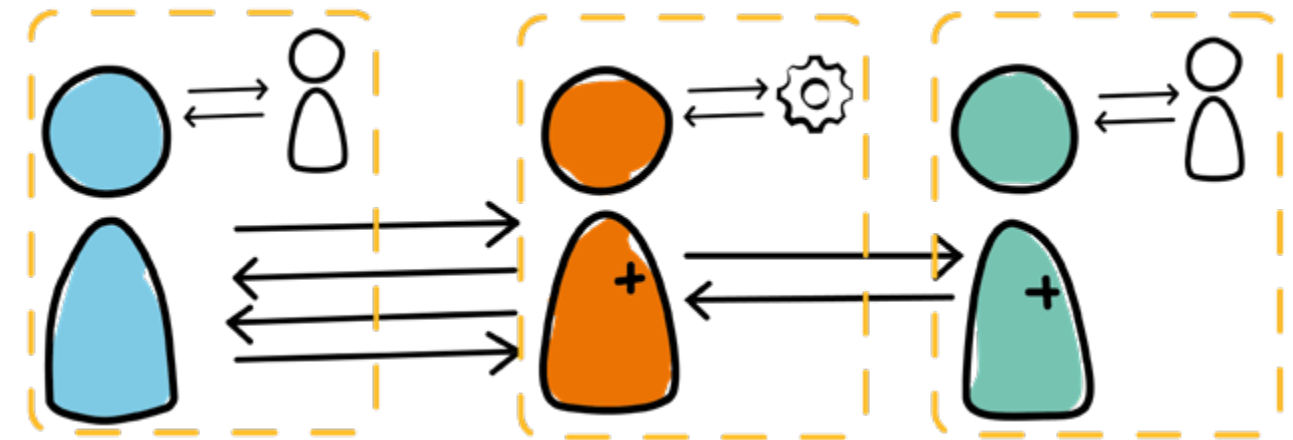
## Scenario 4 – Collega neemt contact op met jou als zorgverlener



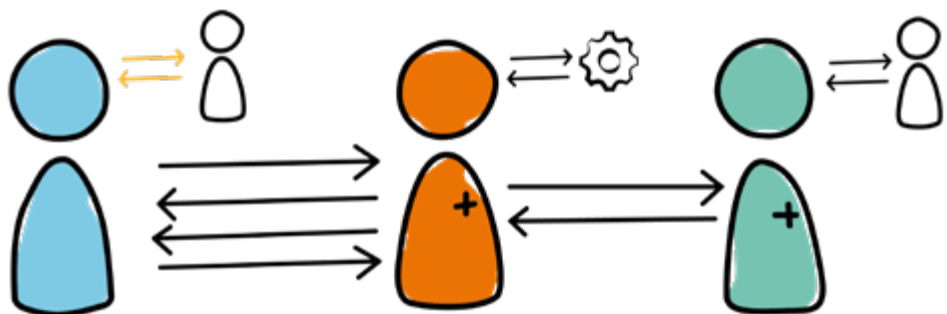
Tandarts en kaakchirurg mailen beiden met een veilige e-maildienst, die nog niet voldoet aan de NTA 7516.

Het contact en de uitwisseling van (medisch inhoudelijke) informatie gebeurt via veilige e-maildiensten. Maar, omdat deze diensten niet voldoen aan de NTA 7516, zal de ontvanger worden geconfronteerd met een veilige inlogmethode van de dienst van de verzender. De mail komt dus niet direct leesbaar in de inbox terecht, maar de ontvanger moet extra handelingen uitvoeren.

! Als een collega zorgverlener jou een bericht stuurt via onveilige e-mail, moet je dit beantwoorden via een veilige e-maildienst.



### Scenario 5 – Patiënt mailt met mantelzorger/eigen netwerk



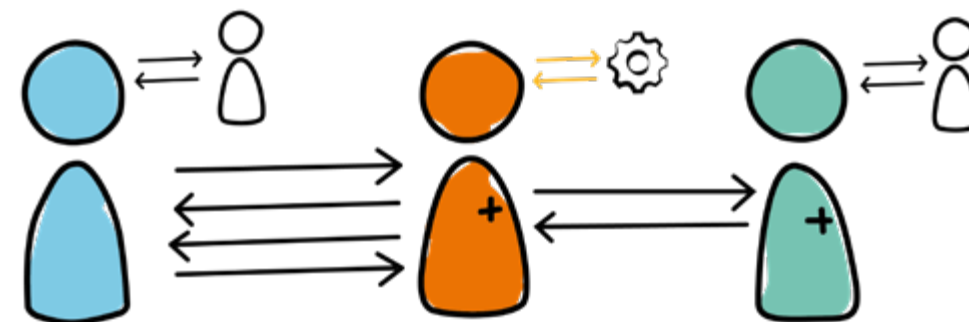
Tessa heeft via haar patiëntportaal de uitslagen van het bloedonderzoek bekeken. Ze wil de uitslagen graag delen met haar zus, die ook haar mantelzorger is.

Als officiële mantelzorger is de zus van Tessa waarschijnlijk gemandateerd om in te loggen in het patiëntportaal. Ze kan zo op een veilige manier de resultaten van het bloedonderzoek van Tessa bekijken.

Een andere optie om het bloedonderzoek op een veilige manier in te zien is door een veilige e-maildienst te gebruiken. Tessa moet de resultaten van haar bloedonderzoek downloaden, bijvoorbeeld als een PDF-versie. (Het is verplicht volgens de NTA 7516 dat je een bestand makkelijk moet kunnen downloaden.) De PDF kan Tessa via een veilige e-maildiensten naar haar zus sturen.

Voorbeeld van een slechte en onveilige oplossing: Omdat haar zus niet in het portaal mag, bedenkt Tessa een creatieve oplossing. Ze maakt een printscreen/foto van haar bloeuitslagen en stuurt deze via e-mail of WhatsApp naar haar zus. Een voor de hand liggende en gebruikelijke manier. De NTA 7516 verplicht niets over patiënt- en netwerkcommunicatie (familie, mantelzorgers, vrijwilligers, cliëntondersteuner, etc.). Wel ligt er voor jou als zorgverlener een taak om mensen attent te maken op de gevaren van onveilig mailen en wat wel veilige manieren zijn om persoonlijke medische informatie te delen.

### Scenario 6 – Communiceren met andere professional



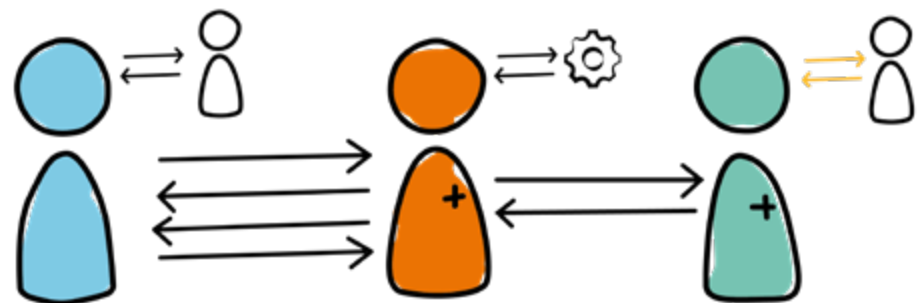
Een medewerker van de gemeente Delft neemt met spoed contact op met een GGZ-instelling.

Er wordt eerst telefonisch overlegd en besloten dat er meer (schriftelijke) gegevens nodig zijn voor een eventuele crisisopname.

De medewerker van de gemeente gebruikt hiervoor het landelijk beschikbare systeem waarin zowel de gemeente als de GGZ veilig gegevens kunnen delen.

Eventueel kan er gebruik gemaakt worden van veilig mailen via een NTA 7516 dienst. De NTA 7516 gaat over persoonlijke gezondheidsinformatie ongeacht in welke professionele keten deze gebruikt wordt.

## Scenario 7 – Communiceren met je informatiesysteem

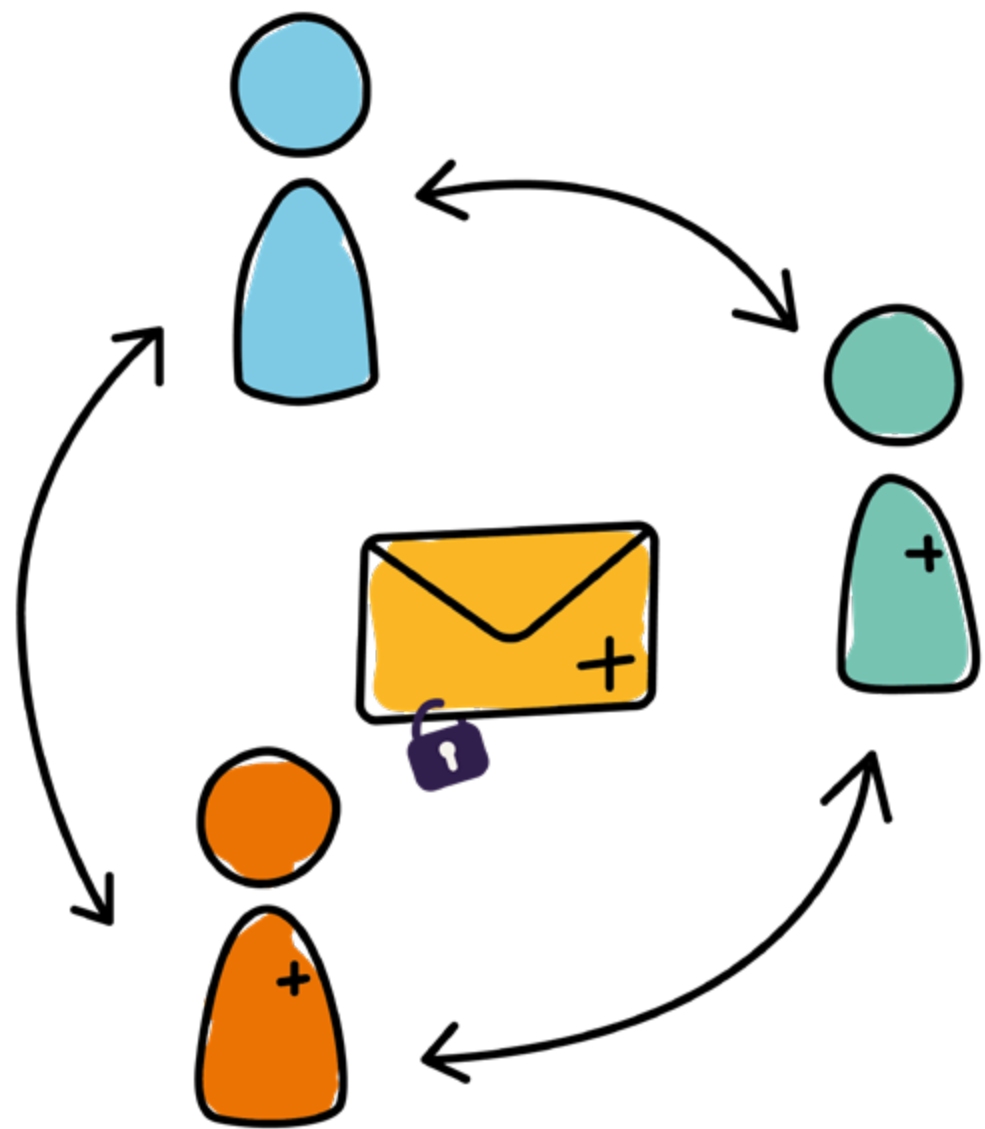


Chantal is onder behandeling bij de fysio voor pijnklachten in haar knie. Omdat de klachten niet afgenomen zijn, is ze geopereerd. Voor revalidatie gaat ze weer terug naar haar fysio. Ze mailt haar fysio hoe het met haar gaat.

Het gebruik van een veilige e-maildienst is hierbij verplicht. Chantal kan met een onveilige dienst mailen, als zorgverlener moet je antwoorden via een veilige e-maildienst.

De fysio wil de informatie die Chantal stuurt graag opnemen in zijn eigen informatiesysteem en toevoegen aan haar dossier. Vaak moet dit handmatig door tekst- of een bijlage uit een mail te knippen en te plakken in het dossier. Tegenwoordig zijn er ook ICT-leveranciers die het mogelijk maken een e-mail direct in je eigen informatiesysteem te verwerken. Belangrijkste aandachtspunt bij deze koppeling is dat je 100% zeker wilt zijn dat de juiste gegevens bij de juiste patiënt terechtkomen. Informeer bij veilige e-maildienstaanbieders en je ICT-leverancier naar de mogelijkheden. Dit is overigens geen vereiste van de NTA 7516. Vind je dit wel heel erg belangrijk? Neem het op in het programma van eisen (PvE).





# Colofon

Het handboek 'Veilig mailen, hoe regelen we dat?!' is een uitgave van Informatieberaad Zorg en Nictiz.

December 2019

©Informatieberaad Zorg

Het handboek bestaat uit drie delen:

1. Stappenplan
2. Toolkit
3. Praktijkscenario's

Bij 'Praktijkscenario's' horen het 'Stappenplan' en de 'Toolkit'.

## Auteurs

Charlotte Schreuder | Nictiz  
Ralph Wagter | Ministerie van Volksgezondheid, Welzijn en Sport

