

# Veilig communiceren is zorgen voor elkaar



De toolkit  
Veilig communiceren  
bevat uitleg, tips  
en middelen om  
direct te starten



Informatieveilig  
gedrag in de zorg

# Voorwoord

Het is steeds belangrijker dat medewerkers van zorgorganisaties veilig omgaan met informatie en zich bewust zijn van de risico's van bijvoorbeeld phishingmails of het delen van medische gezondheidsinformatie via een onbeveiligd communicatiekanaal. Toch is de informatieveiligheid op de werkvloer niet altijd vanzelfsprekend. Dat heeft verschillende oorzaken. Denk aan dat medewerkers die:

- Phishingmails niet herkennen.
- Niet weten wanneer en waar een datalek gemeld moet worden.
- Niet bekend zijn met wat wel en wat geen veilig communicatiekanaal is om medische gezondheidsinformatie te delen.

Deze problemen zijn niet uniek. Daarom zetten we collectieve denkkraft in voor gemeenschappelijke problemen.

Het programma Informatieveilig gedrag in de zorg reikt zorgorganisaties praktische tools aan om te werken aan het vergroten van informatieveilig gedrag. Met de eerste werkgroep Veilig communiceren focussen we op het probleem dat zorgprofessionals persoonsgegevens versturen via een niet beveiligd communicatiekanaal. Dit is namelijk een van de grootste uitdagingen bij het komen tot informatieveilig gedrag.

- Hoe zorgen we ervoor dat medewerkers weten wanneer ze veilig moeten communiceren?
- Hoe zorgen we ervoor dat de risico's bekend zijn?
- Hoe zorgen we ervoor dat een veilig communicatiekanaal ook wordt gebruikt?

*“We nemen deel aan de werkgroep Veilig communiceren omdat we graag een zinvolle bijdrage willen leveren aan het bevorderen van informatieveilig gedrag in de zorgsector. Veel zorginstellingen stuiten op dezelfde uitdagingen op het gebied van informatieveiligheid. In plaats van steeds zelf op zoek te gaan naar een werkbare oplossing, doen we dat nu met elkaar. Dit bespaart niet alleen tijd, maar leidt ook tot waardevolle relaties. Deze contacten zijn van essentieel belang om regelmatig in gesprek te gaan met gelijkgestemden, elkaars standpunten te begrijpen en uitwisseling van beleid, visies en procesplannen mogelijk te maken. Zo ontstaat er een win-win situatie.*

*Dankzij de coördinatie van ECP zijn we in staat specifieke problemen diepgaand te onderzoeken en werkbare producten te ontwikkelen. De werkgroep Veilig communiceren heeft een waardevolle toolkit opgeleverd die ook in jouw zorgpraktijk goed kan worden toegepast.*

***Veel succes!”***

**Gerry van Tol,**

Coördinator Informatie Beveiliging, Libra Revalidatie & Audiologie

**Marja Bakker,**

Projectleider ICT, Admiraal De Ruyter Ziekenhuis (ADRZ)

# Inhoudsopgave

## Implementatieroute ————— 4

### Stap 1 - Onderzoek oorzaken ————— 5

Knelpuntenanalyse ————— 6

### Stap 2 - Bepaal actieplan ————— 7

### Stap 3 - Aan de slag! ————— 8

### Stap 4 - Verzamel resultaten ————— 9

Tips veilig communiceren ————— 10

## Toolkit Veilig communiceren ————— 12

### Toelichting ————— 13

### Animatievideo ————— 14

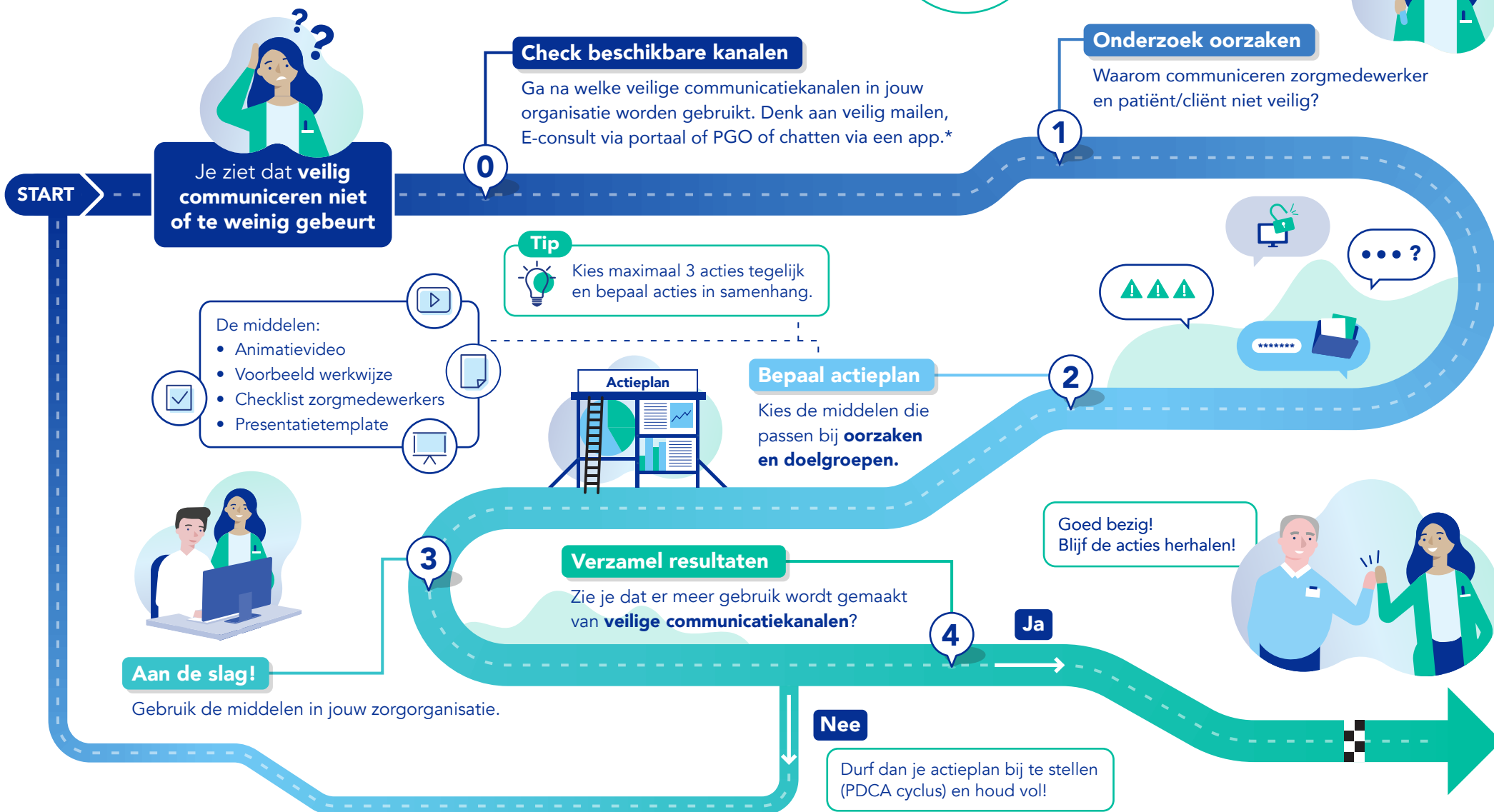
### Voorbeeld werkwijze veilig communiceren ————— 15

### Checklist voor zorgmedewerkers ————— 17

### Presentatietemplate ————— 18

# Implementatieroute

Veilig communiceren is zorgen voor elkaar



# Stap 1 – Onderzoek oorzaken

Je ziet dat mensen niet of te weinig veilig communiceren. Je hoort bijvoorbeeld via de Functionaris Gegevensbescherming dat een patiënt/cliënt zich heeft beklagd over het ontvangen van een niet beveiligde mail van een zorgmedewerker. Of je ziet dat de gebruikersaantallen van apps voor videobellen en veilig appen achterblijven.

Waarom blijft het doelgedrag achter? Om te bepalen hoe je met deze toolkit aan de slag kunt, is het handig om te weten wat de oorzaken van het niet veilig communiceren zijn. Wie communiceren onveilig en waarom? Betreft het bijvoorbeeld de communicatie tussen zorgmedewerkers onderling of tussen zorgmedewerkers en patiënten/cliënten? En waarom kiezen ze voor e-mail en niet voor de veilige communicatiekanalen die de organisatie heeft gekozen?

De knelpuntenanalyse laat de meest voorkomende oorzaken van onveilig communiceren zien. Je kunt deze gebruiken als startpunt voor jouw analyse of als praatplaat. Ga vooral in gesprek met medewerkers, observeer gedrag en kijk wat gebruikersaantallen je vertellen.

Bij het onderzoeken van de oorzaken kun je ook gebruik maken van het Voorbeeld werkwijze veilig communiceren. Deze laat vanuit het perspectief van de eindgebruiker zien op welke momenten in het zorgproces gebruikers keuzes maken over wel of niet veilig communiceren.

Heb je de belangrijkste oorzaken in kaart? Ga door naar stap 2.

## Nuttige documenten



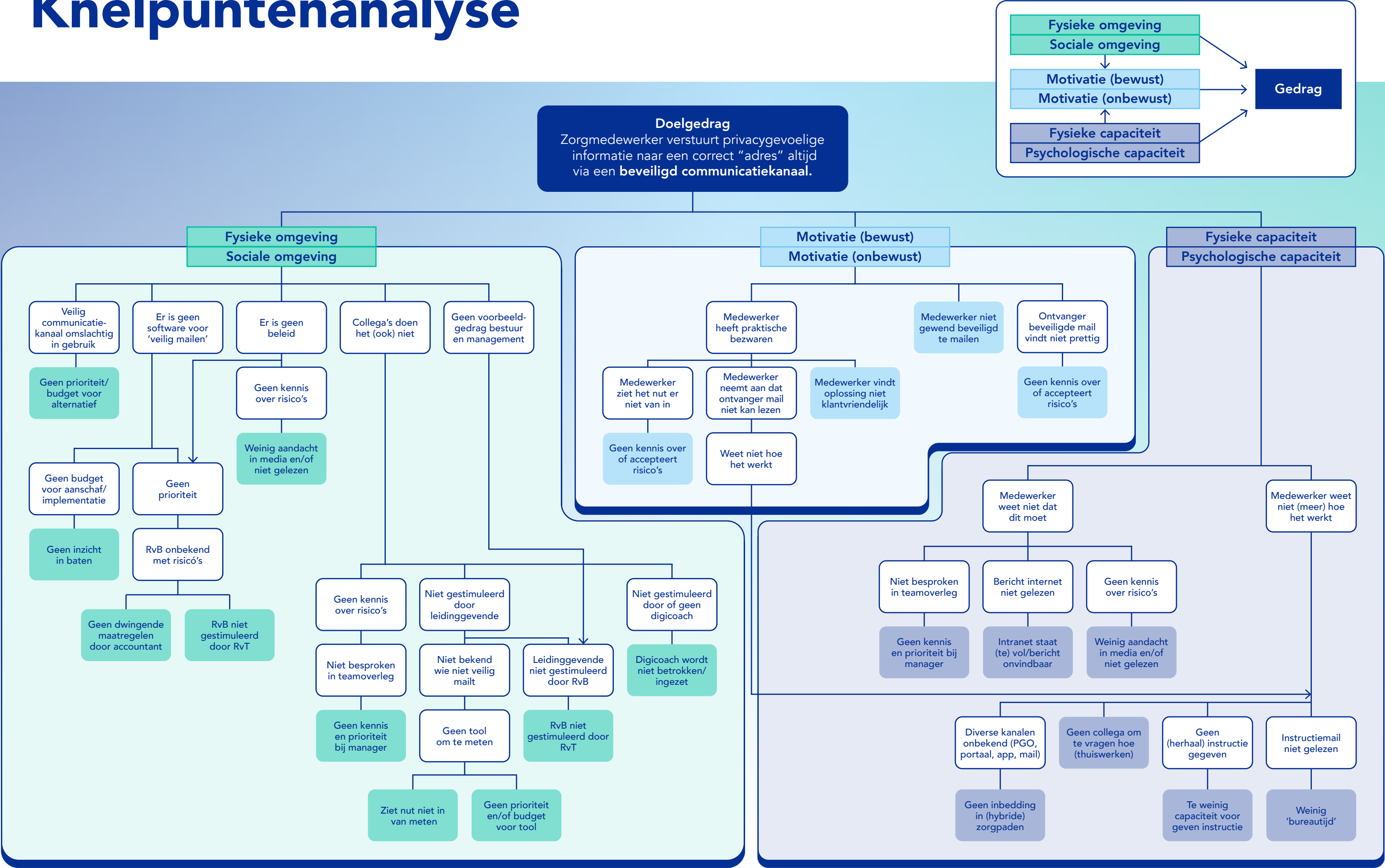
- De knelpuntenanalyse.
- Gedragsfactoren onderzoeken uit de Wegwijzer Informatieveilig gedrag in de zorg.
- Voorbeeldopbouw van een gespreksleidraad aan de slag met Informatieveilig gedrag in de zorg.

## Tip



- Voer korte gesprekjes bij de koffieautomaat.
- Betrek digicoaches en vraag wat zij hierover weten.
- Benut gebruikersdata, zodat je weet waar in de organisatie de grootste uitdagingen liggen.
- Bespreek met de data analisten of ze een maandelijks dashboard kunnen aanleveren.

# Knelpuntenanalyse



# Stap 2 – Bepaal actieplan

Dan is het nu tijd om een actieplan te maken. Dat doe je natuurlijk niet alleen, maar met de belangrijkste betrokkenen. Denk aan digicoach, Functionaris Gegevensbescherming, security officer, communicatieadviseur, projectleider veilig communiceren, (innovatie)manager(s) én patiënten/cliënten (ervaringsdeskundige). Samen bedenken jullie welke middelen uit deze toolkit je bij welke doelgroepen kunt gaan inzetten.

Twijfel je over de juiste mix en prioritering? Laat iedereen stemmen en ga in gesprek over de uitkomsten. Denk ook goed na over hoe je een besluit neemt: op basis van consensus of consent? Vergeet tot slot niet dat je plan niet in beton gegoten is. Je kunt permanent monitoren en bijstellen.

Heb je het actieplan opgesteld?

Ga door naar **stap 3**.



## Nuttige documenten



- Verdieping over het kiezen van interventies vind je op de **website** van Informatieveilig gedrag in de zorg.
- De hulpmiddelen uit deze toolkit.
- Explainer video's per stap van de wegwijzer: **video stap 4; interventies kiezen**.
- Informatie en handreikingen zoals:
  - **Veilig mail informatieberaad in de zorg**.
  - **Handboek veilig mailen** van Informatieberaad in de zorg.
  - **Kennisbank - Z-CERT**.

## Tip



- Zorg dat je actieplan ook een communicatieplan bevat.
- Denk na over hoe je een besluit over het actieplan neemt: via consent of consensus?
- Consulteer een collega informatieveiligheidsprofessional uit een andere instelling en benut elkaars ervaringen.

# Stap 3 – Aan de slag!

Het is tijd om aan de slag te gaan met jouw acties. De betrokken collega's gaan aan de slag met de uitvoering van het actieplan.

Start met het op maat maken van de middelen uit deze toolkit. Je kunt er eigen logo's aan toevoegen, maar ook de 'tone of voice' en taal aanpassen aan jouw organisatie en doelgroep. Overweeg om hierbij de beoogde eindgebruikers te betrekken. Zij kunnen je waardevolle feedback geven.

Zijn de middelen op maat gemaakt? Dan kun je ze gaan delen en gebruiken. Nu is het zaak om niet achterover te leunen maar de betrokken collega's te ondersteunen en volgen. Zij gaan ontdekken of de middelen die jullie gebruiken aansluiten bij de behoeften. Hebben zij tips of adviezen nodig? Zorg dat je voor hen klaar staat.

Ben je inmiddels een aantal weken onderweg? Tijd om een reflectiemoment te organiseren, bekijk de ervaringen en voorlopige effecten. Vervolgens ga je door naar **stap 4**.

## Nuttige documenten



- Verdieping over het uitvoeren van interventies vind je op de [website](#) van Informatieveilig gedrag in de zorg.
- Explainer video's per stap van de wegwijzer: [video stap 5 – interventies uitvoeren](#).
- [Home – Helpdesk Digitale Zorg](#) biedt hulp aan patiënten/cliënten en zorgmedewerkers bij digitale zorg.
- [Informatiepunt Digitale Overheid](#).
- Digitale vaardigheden verbeteren [Verbeter je digitale vaardigheden met deze 19 tips - Vliegwielfcoalitie](#).

## Tip



- Gebruik niet te veel middelen naast elkaar en tegelijkertijd.
- Denk na over op welk veilig communicatiekanaal je de acties wilt inzetten.
- Zijn er meer veilige communicatiekanalen? Pak ze dan één voor één aan.
- Benut mogelijkheden van het veilig communicatiekanaal die het gebruiksgemak verhogen. Bijvoorbeeld default instellingen in de software.

# Stap 4 – Verzamel resultaten

Zie je een positieve ontwikkeling in het gebruik van veilig mailen, Persoonlijke Gezondheidsomgevingen, e-consulten of communicatie-apps? Dat is mooi! Je bent begonnen met het oogsten van jullie inspanningen. Het is wel belangrijk om door te pakken. De kracht van jouw aanpak zit in de herhaling.

Het is slim om te kijken wat, na deze inspanningen, alsnog de meest hardnekkige oorzaken voor het niet veilig communiceren blijven. En aan de hand van deze inzichten scherpen jullie het actieplan aan. Misschien vraagt het gerichte inzet van de middelen bij achterblijvende doelgroepen. Of moet je toch voor andere middelen gaan kiezen.

Ben je tevreden met jullie inzet en lijkt veilig communiceren de nieuwe standaard? Dan is de tijd van verankeren aangebroken.

## Nuttige documenten



- Verdieping over het verankeren van je acties vind je op de [website](#) van Informatieveilig gedrag in de zorg.
- Explainer video's per stap van de wegwijzer: [video stap 6 – verankeren en rapporteren](#).

## Tip



- Gebruik data uit systemen om te meten of er meer veilig wordt gecommuniceerd.
- Maak heldere afspraken over wanneer welk communicatiekanaal te gebruiken en leg dit vast in zorgpaden.
- Communiceer welk veilig communicatiekanaal de standaard is en waarom. Leg dit ook uit aan de patiënten/cliënten. Bijvoorbeeld met een (digitale) flyer.

# Tips veilig communiceren

## Tip



Informeer zorgmedewerkers dat ze patiënten/cliënten kunnen adviseren gebruik te maken van een bestaande helpdesk die ondersteuning biedt bij bijvoorbeeld hoe je een veilige mail kan openen. Maak inzichtelijk welke mogelijkheden er zijn, regionaal en/of landelijk zoals:

- [Home – Helpdesk Digitale Zorg Home](#) biedt ondersteuning om digitale zorg voor iedereen toegankelijk te maken, voor zowel zorgprofessionals als patiënten/cliënten.
- Maak afspraken met een regionale/lokale bibliotheek, waar patiënten/cliënten terecht kunnen met vragen over inloggen DigiD, patiënten portaal etc.
- [Informatiepunt digitale overheid | Hulp en informatie | Bibliotheek.nl](#)
- [Verbeter je digitale vaardigheden met deze 19 tips](#) - Vliegwielercoalitie

## Tip



- Betrek digicoaches. Zij weten vaak wat oorzaken zijn van het niet veilig communiceren. En kunnen met je meedenken bij de stappen uit de implementatieroute
- Betrek een communicatieadviseur en zorg dat je actieplan ook een communicatieplan bevat.
- Denk na over hoe je een besluit over het actieplan neemt: via consent of consensus?
- Consulteer collega-IVP'ers uit andere instellingen en benut elkaars ervaringen.
- De meeste 'veilig mail software' maakt inzichtelijk welke medewerkers structureel niet veilig mailen. Het is daardoor mogelijk en zinvol om met betreffende medewerkers in gesprek te gaan over *waarom* ze dit niet doen.
- Gebruik 'veilig mail software' waar default instelling 'veilig mailen' mogelijk is. 'Veilig mailen' is dus geen extra handeling en geen extra tijd.
- De mogelijkheid dat een gebruiker 'veilig mail' versturen kan deactiveren is doorgaans een instelling in de software. Deze mogelijkheid is uit te schakelen, zodat een gebruiker het zelf niet kan veranderen.

1

2

3

4

## Tip



- Patiënten/cliënten willen of moeten de mogelijkheid hebben om op een veilige manier te mailen. Ook als de zorgverlener daar niet voor kiest. Het is onvoldoende duidelijk bij wie een patiënt/cliënt dit bespreekbaar kan maken of kan melden als zijn/haar zorgverlener niet 'veilig mailt'. Op de website van de zorginstelling kan worden vermeld waar en hoe een patiënt/cliënt een klacht kan melden (bijvoorbeeld Functionaris Gegevensbescherming, Klachtenfunctionaris of een Vertrouwenspersoon).
- Doe geen aannames dat een patiënt/cliënt niet veilig zou willen of kunnen communiceren. Bespreek dit tijdens een consult en maak hierover afspraken.
- Maak in de organisatie duidelijke afspraken over wanneer welk communicatiekanaal te gebruiken. Leg dit zoveel mogelijk vast in zorgpaden.
- Maak als organisatie een keuze en beleid op welke wijze er 'veilig' wordt gecommuniceerd. Met welk middel en waarom. Communiceer dit in je organisatie. En ook met je patiënten/cliënten met bijvoorbeeld (digitale) flyers.

## Tip



- Bij het meten van ongewenst en gewenst gedrag is data systemen te halen. Benut gebruikersdata, zodat je weet waar in de organisatie de grootste uitdagingen liggen. Bespreek met BI of ze een maandelijks dashboard.
- Als je organisatie eerdere veilige communicatiekanalen gebruikt, is het advies om deze één voor één te implementeren. Iedere implementatie heeft aandacht nodig.
- Als er al verschillende veilige communicatiekanalen beschikbaar zijn, maar deze worden nog niet (optimaal) gebruikt, dan kun je de implementatieroute integraal op alle beschikbare middelen toepassen.
- Gebruik niet (te) veel communicatiekanalen naast elkaar.



# Toolkit

## Veilig communiceren



# Toelichting

De toolkit Veilig communiceren bevat diverse hulpmiddelen die je kunt inzetten in jouw organisatie. De middelen zijn ontwikkeld in samenwerking met de werkgroep Veilig communiceren bestaande uit meerdere zorgprofessionals uit de verschillende sectoren. Met als doel dat deze hulpmiddelen je ontzorgen en helpen bij het stimuleren van het doelgedrag: veilig communiceren.

## Een aantal tips:

### Tip



#### Durf te kiezen

Niet alle middelen hoeven geschikt te zijn voor jouw organisatie. Bepaal welke middelen het meest gaan helpen in het oplossen van de knelpunten die bij jullie spelen in het komen tot veilig communiceren.

### Tip



#### Kies een mix van middelen

Ieder mens is anders. De een bekijkt het liefst een filmpje, de ander leest liever een checklist en weer een ander heeft behoefte aan een goed gesprek. Dus: mix middelen.

### Tip



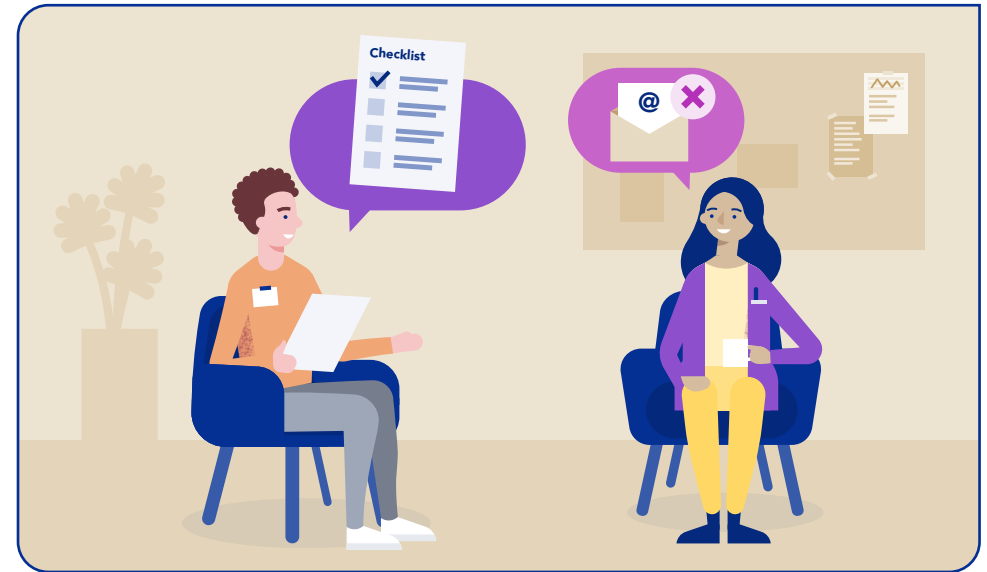
#### Maak de middelen op maat

Je kunt de middelen op maat maken o.a. door je logo toe te voegen. Voor sommigen middelen geldt dat je ook de teksten kunt aanpassen zodat de taal en boodschap passen bij je organisatie.

# Animatievideo

Komt er uit jouw analyse bij [stap 1](#) dat mensen niet overtuigd zijn van het belang van veilig communiceren? Doe dan je voordeel met [deze animatievideo](#). In de animatievideo wordt kort en helder uitgelegd dat veilig communiceren belangrijk is. De nadruk ligt op hoe je in jouw organisatie kunt nagaan hoe je veilig kunt communiceren. En hoe je daarover met de patiënt in gesprek kunt gaan. Veilig communiceren is een kwestie van zorgen voor elkaar. Je kunt deze animatie gebruiken in jouw communicatie aanpak.

Bekijk ook eens de [animatievideo](#) over informatieveilig gedrag; over het belang van informatieveiligheid. Laat je communicatieadviseur weten dat ook deze video gebruikt kan worden.



# Voorbeeld werkwijze veilig communiceren

Het Voorbeeld werkwijze veilig communiceren, laat zien welke stappen een zorgmedewerker doorloopt bij het digitaal communiceren. Het werkproces start bij de actie om te communiceren met de patiënt/ cliënt of met een zorgmedewerker binnen of buiten de eigen organisatie. Het eindigt met het vaststellen dat het bericht is aangekomen.

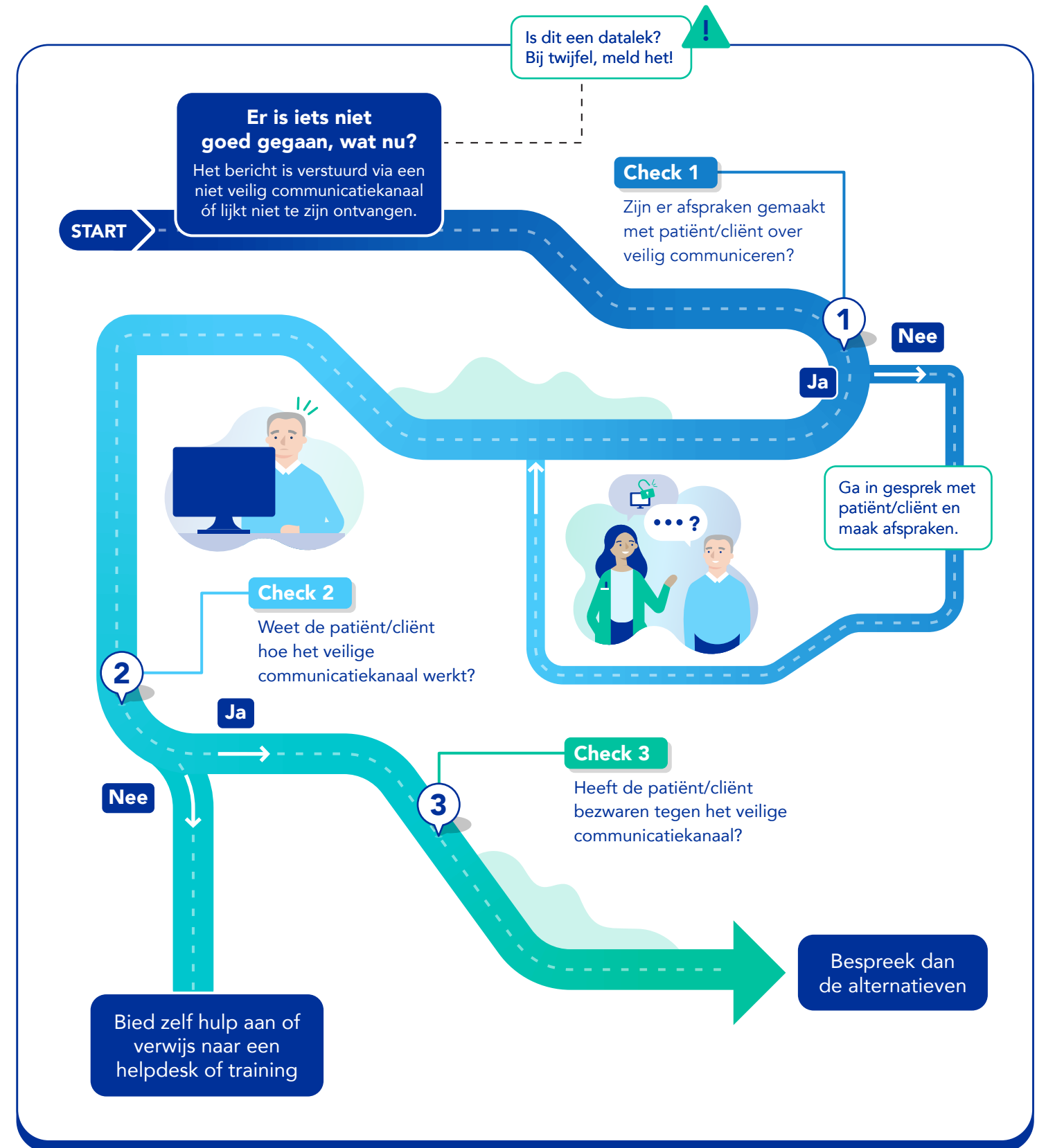
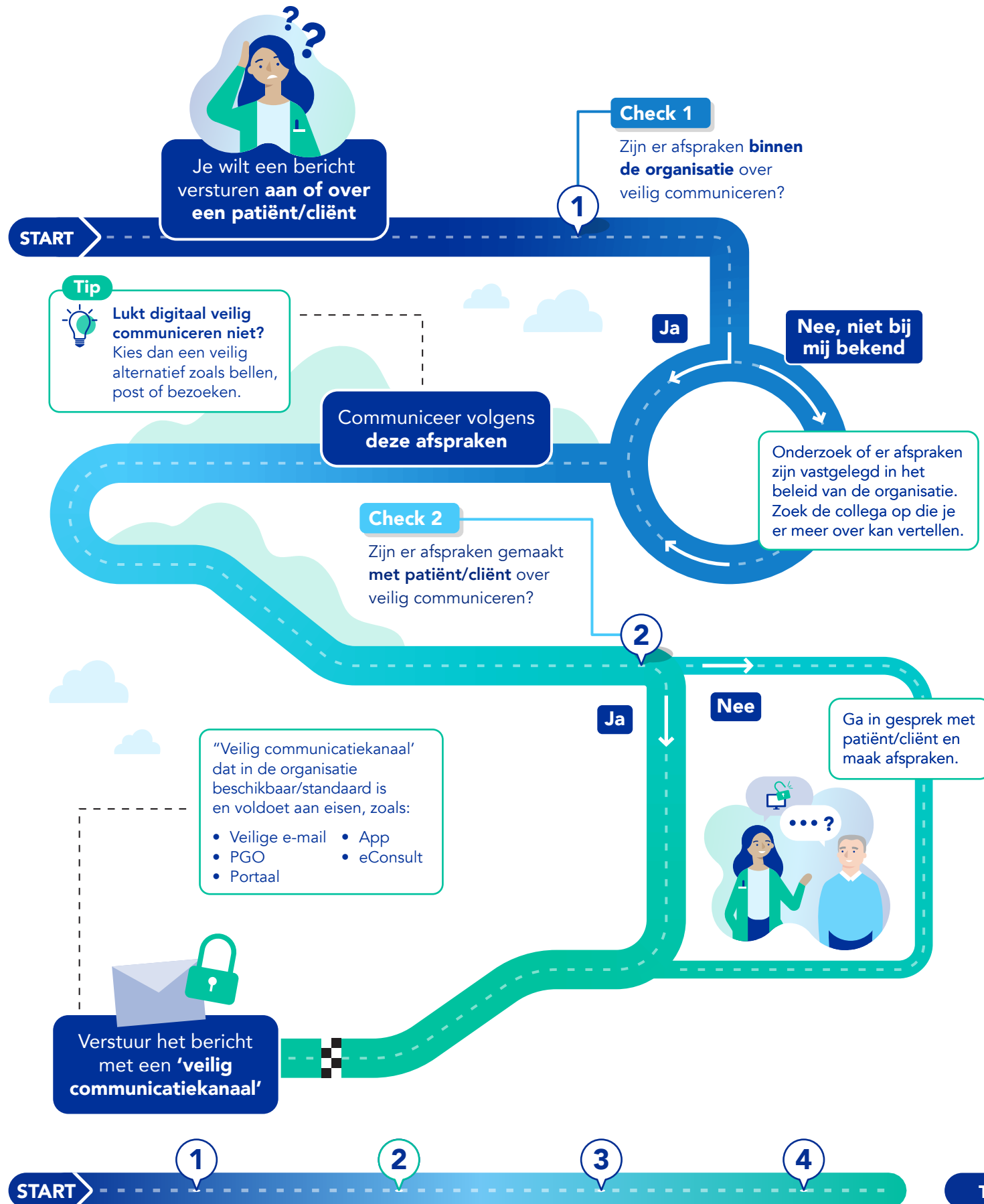
## Belangrijke onderdelen van het Voorbeeld werkwijze veilig communiceren

- Welke communicatiekanalen worden binnen de organisatie gebruikt? *Let op: niet elke zorgmedewerker weet wat er mogelijk is!*
- Is er keuze mogelijk uit offline (post, telefoon, bezoek) en/of online kanalen?
- Er bestaan verschillende online kanalen zoals videobellen, veilig mailen, chatten met een veilige app, of een e-consult via het patiënten portaal of de Persoonlijke Gezondheidsomgeving.  
*Let op: het is belangrijk dat de zorgmedewerker aandacht heeft voor de digitale mogelijkheden van de ontvanger. Bij twijfel is een gesprek met die ontvanger aan te raden.*
- Kom in actie als een reactie uitblijft!



# Voorbeeld werkwijze veilig communiceren

Veilig communiceren is zorgen voor elkaar



# Checklist voor zorgmedewerkers

Deze checklist wijst zorgverleners op wat er nodig is om veilig te communiceren.  
Je kan de checklist als voorbeeld gebruiken en de tekst overnemen.

| Checklist voor zorgmedewerkers                                                                                                                                                         |                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Ben je bekend met het waarom van veilig communiceren?                                                                                                         | <input type="checkbox"/> Weet je hoe je komt tot een keuze voor wel of geen digitale communicatie?                                                |
| <input type="checkbox"/> Weet je welke veilige digitale communicatiekanalen er in jouw organisatie worden gebruikt?                                                                    | <input type="checkbox"/> Check je na verzenden van jouw veilig verstuurd bericht of deze is aangekomen?                                           |
| <input type="checkbox"/> Ben je bekend met videobellen, veilig mailen, chatten via een veilige app, of een e-consult via het patiënten portaal of de Persoonlijke Gezondheidsomgeving? | <input type="checkbox"/> Weet je hoe je het gesprek kunt voeren met de patiënt/cliënt als deze niet weet hoe een veilig communicatiekanaal werkt? |
| <input type="checkbox"/> Weet je wanneer veilige communicatie nodig is en reguliere e-mail niet volstaat?                                                                              | <input type="checkbox"/> En weet je welke veilige alternatieven je kunt bespreken met de patiënt/cliënt?                                          |

## Twijfels bij beantwoorden van deze vragen?

Neem dan contact op met je collega die meer over dit onderwerp weet (is dat binnen jouw organisatie de Functionaris Gegevensbescherming, Privacy Officer, Projectleider ICT, Helpdeskmedewerker of iemand anders?).

# Presentatietemplate

Het presentatietemplate is een voorbeeldpresentatie die je kan gebruiken wanneer je jouw collega's meer wilt vertellen over veilig communiceren. De presentatie kan je aanpassen naar eigen context en behoeften (doelgroep, inhoud etc.). In de notities vind je per slide een toelichting.



**Stelling**

Als de zorgverlener bekend was geweest met de risico's van niet veilig mailen, dan zou hij/zij voor een andere optie kiezen

eens      oneens

Informatieveilig gedrag in de zorg

## Colofon

De toolkit Veilig communiceren is een uitgave van het programma Informatieveilig gedrag in de zorg.

Het programma Informatieveilig gedrag in de zorg wordt uitgevoerd door stichting ECP | Platform voor de Informatiesamenleving in opdracht van het ministerie van VWS. De brancheorganisaties ActiZ, de Nederlandse ggz, NFU, NVZ en VGN zijn bij het programma betrokken.

Gebaseerd op werkgroep methodiek Vliegwielfcoalitie (digitale transformatie in de zorg).

Versie 1, oktober 2023 ©Informatieveilig gedrag zorg

### Auteurs

Mariët de Waal, ECP | Platform voor de Informatiesamenleving  
Bettine Pluut, ECP | Platform voor de Informatiesamenleving  
Meelezer: Daan Brinkhuis, Z-Cert

### Communicatie

Manon van der Woude, ECP | Platform voor de Informatiesamenleving

## In samenwerking met werkgroep Veilig communiceren

|                     |                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------|
| Marco Pouwen        | Beleidsmedewerker Kwaliteit bij ELEOS                                                              |
| Ivar van der Loos   | Adviseur Privacy in de zorg bij Privacy Specialist BV                                              |
| Gerry van Tol       | Coördinator Informatiebeveiliging bij Libranet                                                     |
| Eveline Meyer       | Beleidsadviseur Kwaliteit bij De Rooyse Wissel                                                     |
| Tinka Versteeg      | Adviseur Informatieveiligheid en privacy en<br>Functionaris Gegevensbescherming bij Santé Partners |
| Naomi Meier         | CISO bij Altrecht                                                                                  |
| Jelle Jonker        | Projectleider Kwaliteit bij SZMK                                                                   |
| Marja Bakker        | Projectleider ICT bij Adrz                                                                         |
| Petra Waelepoel     | Ervaringsdeskundige patiëntenzorg                                                                  |
| Monica Bassie       | Adviseur en Privacy Officer bij Jong JGZ                                                           |
| Renske Grootendorst | Concernmanager Informatisering bij Koninklijke Visio                                               |
| Mila de Vries       | ICT Adviseur bij Koninklijke Visio                                                                 |
| Renilde Rottiers    | DPO bij Korian                                                                                     |