

AI-chatbots zijn handig, maar gebruik ze verstandig

Deze toolkit bevat uitleg, tips en hulpmiddelen
om direct mee te starten



Inleiding

AI-chatbots bieden zorgorganisaties volop kansen om beter en efficiënter te werken. Tegelijkertijd brengt AI ook risico's met zich mee voor de privacy en informatiebeveiliging. De kans bestaat dat vertrouwelijke informatie onbedoeld wordt gedeeld of dat medewerkers verkeerde beslissingen nemen door AI-gebruik. Daarom is het belangrijk om medewerkers te ondersteunen bij het maken van bewuste keuzes over het veilig inzetten van AI-chatbots.

Deze toolkit biedt praktische hulpmiddelen om organisaties en teams in de zorg te ondersteunen bij het slim, bewust, veilig en verantwoord gebruiken van AI-chatbots. Volg een eenvoudig stappenplan om het probleem gericht aan te pakken. Kies vervolgens de passende hulpmiddelen uit deze toolkit, zoals de explainervideo, en zet deze in waar ze het effect hebben. Zo maak je veilig gebruik van AI-toepassingen stap voor stap onderdeel van de dagelijkse praktijk.

De toolkit is ontwikkeld voor CISO's, FG's, privacy officers, informatieadviseurs, ICT en andere professionals die zich bezighouden met informatiebeveiliging en privacy in de zorg. Zij kunnen de hulpmiddelen inzetten om binnen hun organisatie het bewust en veilig gebruik van AI-chatbots onder de aandacht te brengen.

De hulpmiddelen in deze toolkit zijn ontwikkeld binnen het programma Informatieveilig gedrag in de zorg (IVGZ), in samenwerking met professionals uit het werkveld. Hun praktijkervaring, kennis en expertise zijn vertaald naar praktische hulpmiddelen die direct toepasbaar zijn binnen zorgorganisaties.

Alle hulpmiddelen uit deze toolkit zijn ook afzonderlijk te downloaden via [de website](#) van het programma Informatieveilig gedrag in de zorg.

Samen zorgen we voor goede, veilige en betrouwbare zorg.



Waarom aan de slag met bewust en veilig gebruik van AI-chatbots?

In de zorg gebruiken collega's steeds vaker AI-chatbots om bijvoorbeeld teksten te schrijven, informatie samen te vatten of mee te denken over een vraag. Daarbij kan één alledaagse handeling al genoeg zijn om gevoelige informatie te delen of onjuiste informatie te gebruiken. Het kan snel gebeuren, maar de gevolgen kunnen groot zijn.

Deze voorbeelden laten zien wat er kan gebeuren als AI-chatbots niet veilig en niet bewust worden gebruikt.

Hoe kan het misgaan?



Ik plakte informatie uit een patiëntdossier in een AI-chatbot om snel een brief te maken. Daar stonden persoonsgegevens in die ik niet mocht delen. We moesten dit als mogelijk datalek onderzoeken en de patiënt informeren.



Ik sprak na een patiëntgesprek mijn rapportage in met een handige AI-tool. Later hoorde ik dat deze tool niet was goedgekeurd. De opname bevatte patiëntgegevens en we konden niet meer achterhalen waar die gegevens terecht waren gekomen.

Zelf aan de slag met bewustwording?

Gebruik deze voorbeelden binnen je organisatie om het gesprek over bewust en veilig gebruik van AI-chatbots op gang te brengen. Bespreek met collega's welke AI-chatbots zij gebruiken, welke informatie zij invoeren en hoe zij controleren of de uitkomsten kloppen. Zo maak je risico's herkenbaar en bewust en veilig gebruik bespreekbaar.

Wat kunnen de gevolgen zijn?



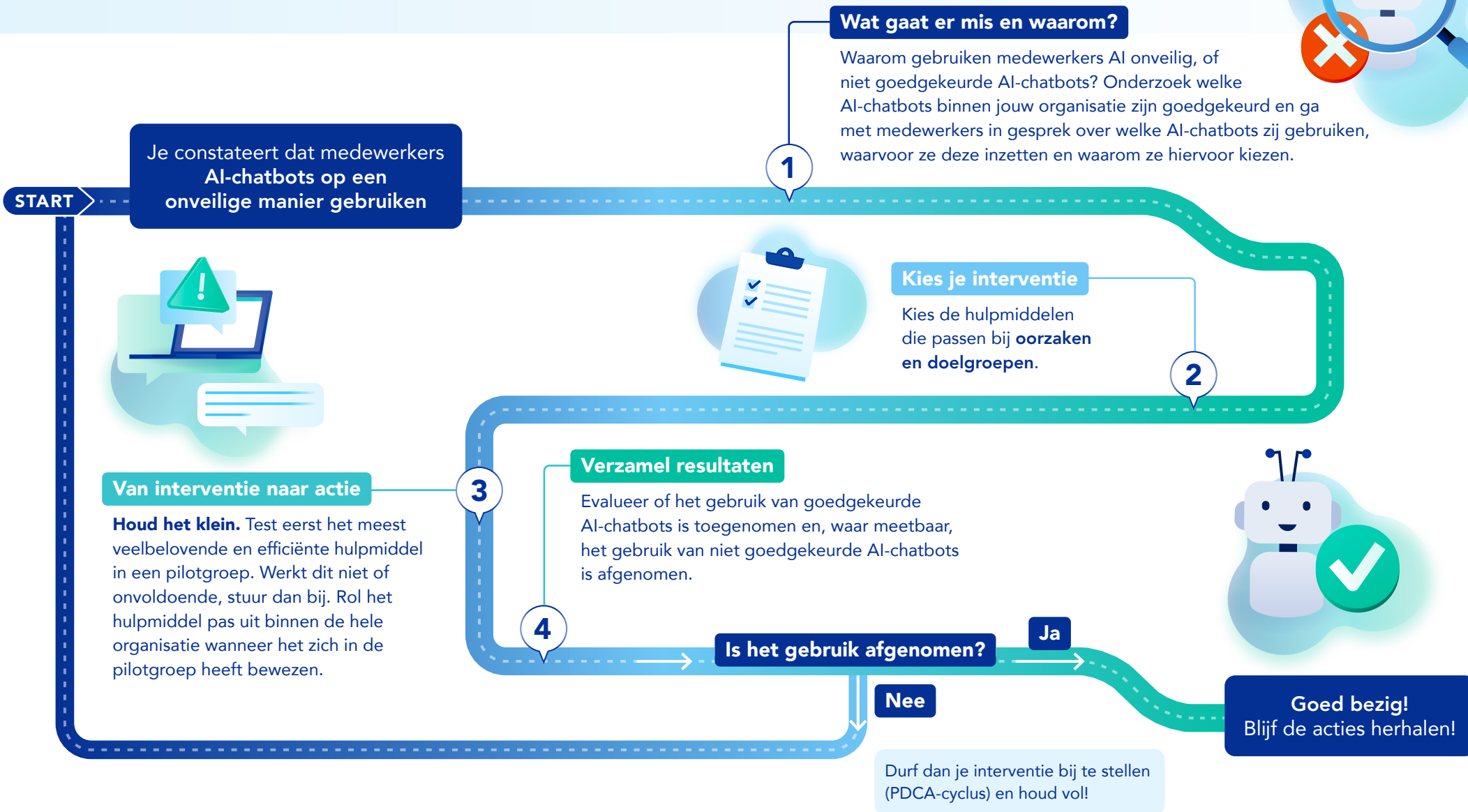
Ik nam informatie uit een AI-chatbot over zonder deze goed te controleren. De informatie bleek niet te kloppen en kwam terecht in een advies aan een patiënt. We moesten het advies achteraf corrigeren.



Ik vroeg een AI-chatbot om mee te denken over een cliënt en dacht dat ik de gegevens voldoende anoniem had gemaakt. Door de combinatie van details was toch te achterhalen om wie het ging. Daarmee had ik onbedoeld herleidbare cliëntinformatie gedeeld.



Bewust en veilig gebruik AI-chatbots



1. Wat gaat er mis en waarom?

Je ziet dat collega's in je organisatie steeds vaker AI-chatbots gebruiken. Ze doen dit onveilig of kiezen chatbots die ze eigenlijk niet mogen gebruiken. Het is verleidelijk om meteen aan de slag te gaan, maar het is belangrijk om eerst te begrijpen waar dit gedrag vandaan komt. Breng daarom met een nulmeting de situatie in jouw organisatie in kaart. Wie gebruiken AI-chatbots? Waarom gebruiken ze die? Weten je collega's wat wel en niet veilig is? Gebruik de **Compacte Wegwijzer** om te bepalen welke onderwerpen je in de nulmeting onderzoekt.

Spreek minimaal vijf collega's of zet een korte vragenlijst uit. Zo leer je over wat er misgaat en waarom. Benut bij je mini-onderzoek het overzicht van de **Meest voorkomende gedragsoorzaken** op de volgende pagina ter inspiratie.

Heb je de belangrijkste oorzaken in beeld?

Ga dan verder met **stap 2**.

Zo ontdek je waar het misgaat



Kleine zorgorganisaties

- Bespreek tijdens een werkoverleg welke AI-chatbots collega's gebruiken, waarvoor en waarom.
- Vraag welke gegevens collega's invoeren in AI-chatbots en of zij weten wat wel en niet mag.
- Vraag collega's hoe zij controleren of antwoorden van een AI-chatbot kloppen.
- Bespreek situaties waarin collega's twijfelden over het bewust en veilig gebruik van een AI-chatbot.
- Kijk ook naar situaties waarin het wél goed gaat. Wat helpt collega's om veilig met AI-chatbots te werken?
- Doe eventueel een korte quiz om te onderzoeken wat collega's weten. Combineer dit met gesprekken om ook andere oorzaken te achterhalen.

Grotere zorgorganisaties

- Ga in gesprek met collega's. Maak hierbij gebruik van het overzicht van de **Meest voorkomende gedragsoorzaken**, herkennen de medewerkers de punten uit dit overzicht?
- Breng in kaart welke AI-chatbots op verschillende afdelingen of locaties worden gebruikt en waarvoor. Waar gaat het goed en waar kan het beter? Wat kunnen verschillende afdelingen van elkaar leren?
- Zet een korte vragenlijst uit en ga aanvullend in gesprek met collega's uit verschillende functies of afdelingen.
- Onderzoek welke afspraken en richtlijnen voor het gebruik van AI bestaan en hoe bekend en werkbaar deze zijn.
- Bespreek de risico's die uit de nulmeting naar voren komen ook in het Risk Comité. Zo creëer je draagvlak voor maatregelen, kan waar nodig budget worden vrijgemaakt en krijgt het onderzoek een concreet vervolg.
- Vergelijk afdelingen of locaties. Waar gaat bewust en veilig gebruik goed en wat is daar anders?
- Kijk niet alleen naar kennis, maar ook naar de werkomgeving. Zijn de juiste AI-chatbots bijvoorbeeld makkelijk beschikbaar en weten collega's waar zij informatie en hulp kunnen vinden?



Meest voorkomende gedragsoorzaken

Dit overzicht geeft voorbeelden van veelvoorkomende gedragsoorzaken van onveilig gebruik van AI-chatbots. Gebruik het om te verkennen welke oorzaken binnen jouw organisatie of team een rol kunnen spelen. De oorzaken zijn ingedeeld volgens het **COM-B model**. Rechtsboven vind je een schematische weergave van het model en een verwijzing naar meer informatie.

Gebruik het overzicht als inspiratie voor je eigen onderzoek. Herken je bepaalde oorzaken? Bespreek dan met collega's of deze inderdaad een rol spelen en onderzoek of er andere oorzaken zijn. Zo krijg je zicht op wat het gedrag veroorzaakt en kun je in de volgende stap een passende interventie kiezen.

Probleem (risico)

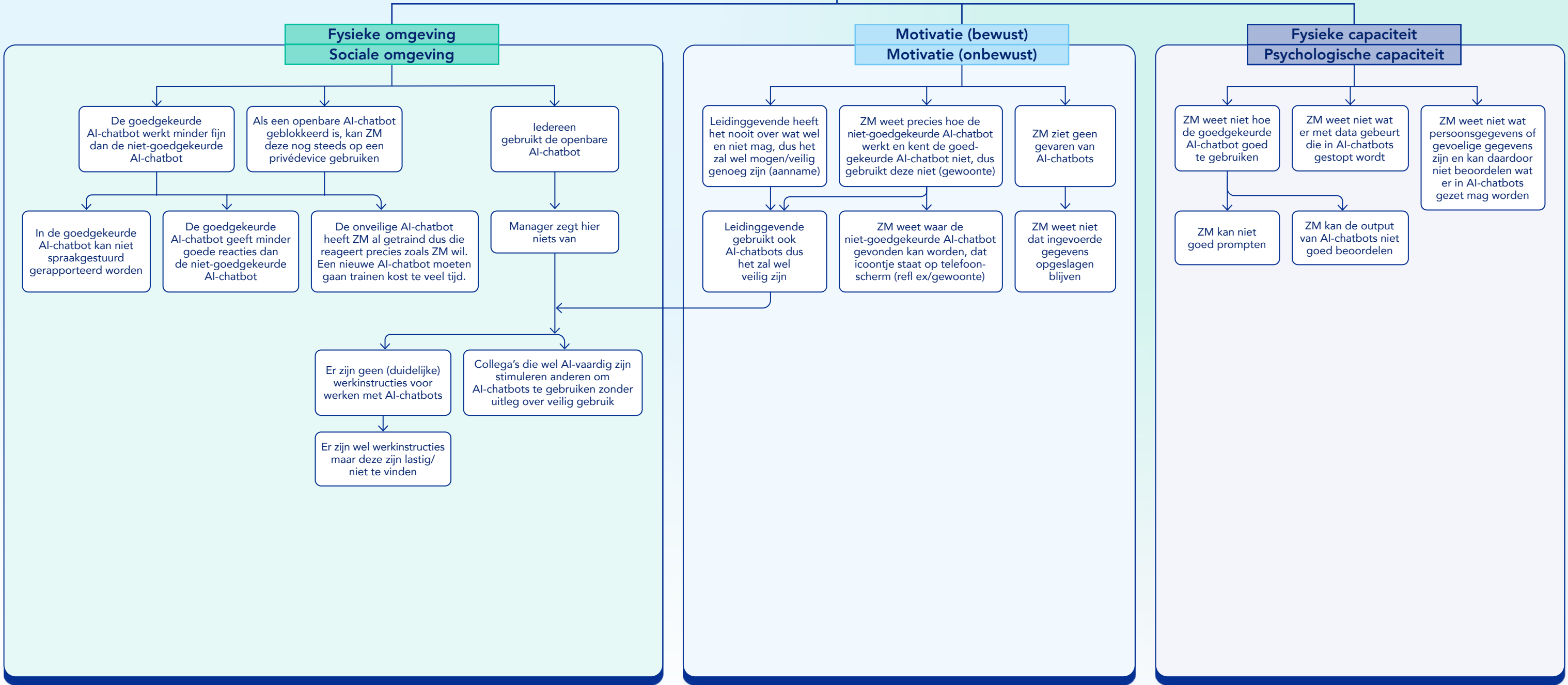
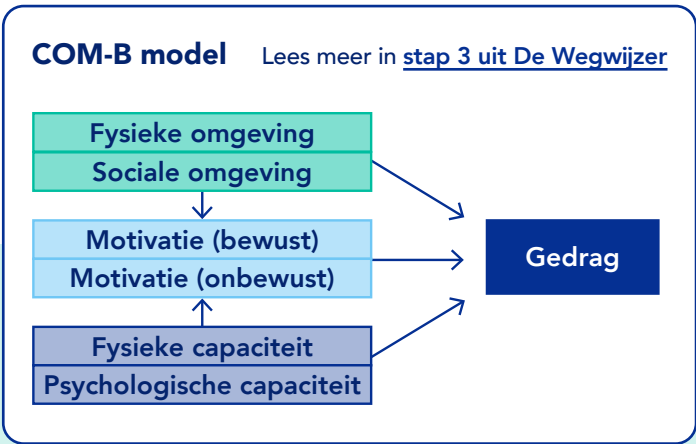
Zorgmedewerker veroorzaakt een datalek door onveilig gebruik van een AI-chatbot of neemt een onjuiste beslissing met AI.

Doelgroep

Zorgmedewerkers (ZM): zorgprofessionals en andere werknemers binnen een zorgorganisatie.

Doelgedrag

Zorgmedewerkers gebruiken alléén de **door de organisatie goedgekeurde AI-chatbot** voor hun werkzaamheden en gebruiken deze chatbot bewust en veilig.



2. Kies je interventies

Je weet nu wat de belangrijkste oorzaken zijn voor het onveilig gebruik van AI-chatbots. Bepaal welke acties nodig zijn om te zorgen dat mensen de juiste AI-chatbots gebruiken en dat ze deze bewust en veilig gebruiken.

Kies vervolgens welke middelen uit de toolkit passen bij jouw doelgroep en situatie. Op de [overzichtspagina](#) vind je alle hulpmiddelen uit de toolkit, met per hulpmiddel het doel en een voorbeeld van hoe je het kunt inzetten.

[Bekijk hier](#) de tips voor het kiezen van een passend hulpmiddel.

Twijfel je over de aanpak?

Bespreek de mogelijkheden met elkaar en maak samen een keuze. Blijf de voortgang volgen en stel het actieplan bij als dat nodig is. Is het actieplan klaar? Ga dan verder met [stap 3](#).

Zo kies je wat je gaat doen



Kleine zorgorganisaties

- Houd het klein. Begin met één of enkele acties die passen bij de belangrijkste oorzaak uit stap 1.
- Vraag jezelf bij iedere actie af: welk probleem lossen we hiermee op en waarom verwachten we dat dit werkt?
- Vraag een paar collega's uit de doelgroep of de gekozen actie hen helpt en of deze past bij hun dagelijkse werk.
- Kies acties die niet alleen kansrijk zijn, maar ook uitvoerbaar met de beschikbare tijd, mensen en middelen.
- Vraag andere zorgorganisaties uit de regio om ervaringen of voorbeelden als de toolkit onvoldoende aansluit op jouw situatie.

Grotere zorgorganisaties

- Stel een kernteam samen met bijvoorbeeld privacy, informatiebeveiliging, ICT, kwaliteit, juridische zaken, communicatie, een DT-lid dat AI in portefeuille heeft en collega's uit de dagelijkse praktijk. De [Uitgebreide Wegwijzer](#) adviseert om verschillende rollen bij het kiezen van interventies te betrekken.
- Koppel iedere interventie aan een oorzaak uit stap 1. Houd daarbij rekening met de doelgroep en de context.
- Combineer waar nodig verschillende soorten acties. Kies bijvoorbeeld niet automatisch alleen voor communicatie of voorlichting.
- Overweeg een andere mix van acties voor verschillende doelgroepen, afdelingen of locaties.
- Vergelijk mogelijke acties op verwacht effect en haalbaarheid. Kijk bijvoorbeeld naar uitvoerbaarheid, kosten, acceptatie en mogelijke nadelige effecten.
- Bepaal vooraf hoe je gaat meten of het gewenste gedrag verandert. Benut daarbij waar mogelijk gegevens die al in de organisatie beschikbaar zijn.

Tips bij het kiezen van hulpmiddelen

Kies wat past bij het knelpunt

Sluit aan bij de oorzaken uit stap 1. Weten collega's onvoldoende over de kansen en risico's van AI-chatbots? Gebruik dan bijvoorbeeld de [explainervideo](#) of (maak) een eigen video. Weten zij vooral niet hoe ze AI-chatbots bewust en veilig gebruiken? Kies dan de [Infographic Bewust en veilig gebruik AI-chatbots](#) met praktische tips voor het dagelijks gebruik.

Sluit aan bij wat collega's nodig hebben

Kijk wat collega's al weten en waar zij nog over twijfelen. Gebruik de [explainervideo](#) om het onderwerp op een toegankelijke manier te introduceren en de [Infographic Veilig gebruik AI-chatbots](#) als praktisch hulpmiddel. Stem de inzet af op de kennis en dagelijkse praktijk van je doelgroep.

Zorg ook voor duidelijke afspraken en ondersteuning

Bewust en veilig gebruik vraagt niet alleen iets van collega's. Gebruik de [Infographic Tips voor professionals](#) om binnen de organisatie het gesprek te voeren over risico's, beleid en bewust en veilig gebruik. Zorg dat collega's weten welke AI-chatbots zij mogen gebruiken en welke afspraken gelden.



3. Van interventie naar actie

Je hebt gekozen welke acties en middelen passen bij de oorzaken van het onveilig gebruik van AI-chatbots. Bepaal nu hoe je deze in de praktijk gaat uitvoeren. Maak een eenvoudig actieplan: wat ga je doen, voor wie, wanneer en wie is daarbij betrokken?

Denk ook na over hoe je collega's bereikt. Welk communicatiekanaal past bij de doelgroep? Is een combinatie van kanalen nodig? Welke toon past bij de boodschap en wat is een goed moment?

Voer de acties uit en houd in de gaten hoe ze in de praktijk werken. Vraag collega's naar hun ervaringen en kijk of zij vaker de juiste AI-chatbots kiezen en deze bewust en veilig gebruiken.

Werkt een actie niet zoals verwacht?

Onderzoek waar dit aan ligt en stel je aanpak bij. Ga daarna door naar [stap 4](#).

Zo breng je acties in de praktijk



Kleine zorgorganisaties

- ➔ Gebruik communicatiekanalen die collega's al kennen en gebruiken. Vraag bij twijfel aan collega's hoe je hen het beste kunt bereiken.
- ➔ Sluit waar mogelijk aan bij bestaande momenten, zoals een werkoverleg of teamoverleg.
- ➔ Spreek per actie af wie deze uitvoert en wanneer.
- ➔ Vraag collega's tijdens de uitvoering of de acties en afspraken duidelijk en werkbaar zijn.
- ➔ Zoek één of meer enthousiaste collega's die kunnen helpen om veilig gebruik van AI-chatbots onder de aandacht te houden.

Grotere zorgorganisaties

- ➔ Bepaal per doelgroep welke communicatiekanalen daadwerkelijk worden gebruikt. Ga er niet automatisch vanuit dat bijvoorbeeld intranet iedereen bereikt. Dit aandachtspunt komt expliciet terug in de [Uitgebreide Wegwijzer](#).
- ➔ Denk na over de toon en afzender. Van wie neemt de doelgroep de boodschap het makkelijkst aan: een leidinggevende, bestuurder, expert of collega? Vraag de afdeling communicatie om mee te denken!
- ➔ Leg per actie vast wat er moet gebeuren, wie verantwoordelijk is en wanneer de actie wordt uitgevoerd.
- ➔ Ga tijdens de uitvoering langs bij afdelingen of locaties om te horen en zien hoe de aanpak in de praktijk werkt.
- ➔ Vind ambassadeurs die helpen om de acties binnen verschillende afdelingen of locaties onder de aandacht te brengen.
- ➔ Zie je afdelingen of locaties waar de aanpak goed werkt? Deel hun ervaringen en voorbeelden met de rest van de organisatie.



4. Van resultaat naar blijvend gedrag

Bekijk wat de acties hebben opgeleverd. Herhaal de nulmeting die je in stap 1 hebt gedaan. Vergelijk waar mogelijk de resultaten met de situatie vóór de acties. Kijk ook naar de ervaringen van collega's om te begrijpen wat wel en niet werkt.

Gebruik deze inzichten om je aanpak bij te stellen. Misschien zijn aanvullende acties of afspraken nodig voor bepaalde doelgroepen of toepassingen. Of blijkt dat collega's meer ondersteuning nodig hebben bij het bewust en veilig gebruiken van AI-chatbots of het beoordelen van de uitkomsten.

Zorg er tot slot voor dat bewust en veilig gebruik van AI-chatbots onderdeel wordt van de dagelijkse praktijk. Leg afspraken vast, maak duidelijk welke AI-chatbots gebruikt mogen worden en blijf aandacht besteden aan bewust en veilig gebruik. Kijk ook wie binnen de organisatie verantwoordelijk is om dit onderwerp actueel te houden.

Wil je uitgebreider aan de slag met het veranderen en verankeren van informatieveilig gedrag?

De Compacte Wegwijzer helpt je gedrag te onderzoeken, passende interventies te kiezen en uit te voeren. Wil je meer verdieping? Gebruik dan de Uitgebreide Wegwijzer. Je kunt ook onze Masterclass volgen. Daarin ondersteunen we je stap voor stap bij het toepassen van de aanpak.

Zo breng je acties in de praktijk



Kleine zorgorganisaties

- Bespreek na een afgesproken periode hoe collega's AI-chatbots gebruiken. Wat gaat beter en waar ontstaan nog vragen of risico's?
- Herhaal je eerdere meting en vergelijk de resultaten. Kijk vooral of het gewenste gedrag vaker voorkomt.
- Bespreek voorbeelden waarin het gebruik van een AI-chatbot goed ging of juist tot twijfel leidde.
- Werkt een actie niet zoals verwacht? Kijk opnieuw naar de oorzaken uit stap 1 en bepaal wat je moet aanpassen.
- Spreek af wie verantwoordelijk blijft voor de controle van de afspraken over AI-chatbots en wie deze actueel houdt.

Grotere zorgorganisaties

- Herhaal waar mogelijk de eerdere meting en vergelijk de resultaten. Kijk of collega's vaker de juiste AI-chatbots kiezen en deze bewust en veilig gebruiken. De Uitgebreide Wegwijzer adviseert een voor en nameting om daadwerkelijk verandering in het doelgedrag te beoordelen.
- Kijk naast het effect ook naar de ervaringen van collega's. Welke interventies helpen hen en waar lopen zij nog tegenaan?
- Vergelijk afdelingen, locaties of doelgroepen. Waar werkt de aanpak goed en waar is bijsturing nodig?
- Gebruik incidenten, vragen en ervaringen van collega's om de aanpak verder te verbeteren.
- Beleg het beheer van afspraken, hulpmiddelen en communicatie bij een vaste functie of afdeling.
- Neem bewust en veilig gebruik van AI-chatbots op in bestaande processen, zoals onboarding, scholing, werkoverleggen of periodieke communicatie.
- Onderzoek regelmatig of nieuwe AI-toepassingen en gebruikssituaties vragen om andere afspraken, ondersteuning of interventies.



Hulpmiddelen in deze toolkit

Hieronder vind je een overzicht van de hulpmiddelen in deze toolkit, met het doel van ieder hulpmiddel en een praktisch voorbeeld van hoe je het kunt inzetten. Welk hulpmiddel je kiest, hangt af van het probleem dat je in stap 1 binnen jouw organisatie hebt vastgesteld. Weten medewerkers bijvoorbeeld niet waarom bewust en veilig gebruik van AI-chatbots belangrijk is? Zet dan de explainervideo in.

In gesprek over AI-chatbots

Pagina 12 ➔

Doel

Experts informatieveiligheid helpen om risico's van AI-chatbots te herkennen en veilig gebruik binnen de organisatie te ondersteunen.

Voorbeeld

Gebruik het hulpmiddel als leidraad om risico's, wet en regelgeving en beleid met collega's te bespreken en samen het bewustzijn rond veilig en verantwoord gebruik te vergroten.

Veilig en bewust gebruik AI-chatbots

Pagina 18 ➔

Doel

Collega's praktische richtlijnen geven om AI-chatbots veilig en verantwoord te gebruiken in hun dagelijkse werk.

Voorbeeld

Deel de infographic met collega's en gebruik deze als geheugensteun bij het gebruik van AI-chatbots. Bespreek de tips bijvoorbeeld tijdens een teamoverleg.

Explainervideo

Bekijk de video ➔

Doel

Collega's bewust maken van de mogelijkheden en risico's van AI-chatbots en uitleggen waarom veilig gebruik belangrijk is.

Voorbeeld

Laat de video zien tijdens een werkoverleg of op intranet en bespreek daarna welke AI-chatbots collega's gebruiken en welke risico's zij daarbij herkennen.



In gesprek over AI-chatbots

Tips voor de expert informatieveiligheid*

Disclaimer Dit hulpmiddel is bedoeld om informatieveilig gedrag te stimuleren. De organisatie is zelf verantwoordelijk voor het opstellen van beleid rondom AI-chatbots.

We gebruiken in de zorg steeds vaker AI-chatbots. Denk aan ChatGPT, CoPilot en Gemini. Deze toepassingen zijn publiek toegankelijk. Wat zijn de risico's van het gebruik? Hoe maak je medewerkers hiervan bewust?



* Met de expert informatieveiligheid bedoelen we functionarissen die informatieveiligheid in portefeuille hebben.

Inspireer jouw collega's!

Tips om in gesprek te gaan

Maak medewerkers bewust van gedragsrisico's bij het gebruik van AI-chatbots

- 1 Sluit aan bij reguliere werkoverleggen in je organisatie en ga in gesprek over de kansen, maatregelen en tips uit dit hulpmiddel.
- 2 Start bij de koffieautomaat eens een gesprek met collega's over AI-toepassingen en vraag ook of zij onderling met andere collega's erover praten en waar collega's behoefte aan hebben/wat ze willen weten over AI.
- 3 Leg het beleid en de gedragsregels niet alleen vast, maar bespreek ze regelmatig en maak ze praktisch. Bijvoorbeeld in teamoverleggen aan de hand van casussen.
- 4 Organiseer een workshop of een debat met medewerkers en/of leidinggevenden. Gebruik daarbij stellingen of een prikkelend artikel. Leestip: [Informatieveilig gedrag steeds belangrijker door AI in de zorg.](#)
- 5 Zorg dat je mag spreken of deelnemen aan het onboarding-programma voor nieuwe medewerkers en heb een pitch of film over bewust en veilig AI gebruik.
- 6 Bespreek met de afdeling communicatie welke ideeën zij hebben voor bewustwording, scholing en voor de verspreiding van dit hulpmiddel voor medewerkers.
- 7 Zorg dat je de infographic voor zorgmedewerkers opneemt in de opleidingsmaterialen voor (nieuwe) medewerkers.
- 8 Maak je eigen communicatiemiddelen met de info uit deze toolkit. Alle inhoud is vrij te gebruiken onder de Creative Commons licentie.



Risico's



Er ontstaan datalekken doordat medewerkers gevoelige gegevens in niet goedgekeurde/gecontroleerde AI-toepassingen invoeren.

Maatregelen



- Informeer medewerkers dat ze geen persoonsgevoelige gegevens mogen invoeren in een AI-chatbot. Let ook altijd op met medische- en bedrijfsgevoelige gegevens. **En leg uit waarom dit niet mag.**
- Gebeurt het toch? Zorg ervoor dat medewerkers dit als datalek melden. Neem dit type datalek **als voorbeeld** op in het meldformulier Datalekken.



De **Toolkit melden datalek** kan je hierbij helpen.



Medewerkers nemen de antwoorden van de AI-chatbot over en handelen daarnaar, zonder na te gaan of de inhoud klopt of betrouwbaar is.

Maak medewerkers bewust van gedragsrisico's bij het gebruik van AI-chatbots:

Leg uit hoe een AI-chatbot aan zijn antwoorden komt. Zelfs bij exact dezelfde prompts kan je de volgende keer een ander antwoord krijgen. Dat is riskant voor zowel de zorg als voor bedrijfsprocessen.



De **Toolkit Datalekken voorkomen** kan je hierbij helpen.



Met het gebruik van (bepaalde) AI-chatbots kun je in strijd handelen met wet- en regelgeving. Het invoeren van patiëntgegevens kan bijvoorbeeld in strijd zijn met de AVG en je geheimhoudingsplicht.

Verdiep je in de relevante **wetgeving en richtlijnen**, zoals AVG, MDR/IVDR, AI Act, WGBO door bijvoorbeeld het volgen van een training. Zorg dat jouw organisatie hieraan voldoet of bespreek dit met de verantwoordelijke mensen in jouw organisatie. We hebben de belangrijkste wet- en regelgeving op een rijtje gezet op pagina 17 van deze toolkit.



Raadpleeg jouw brancheorganisatie voor (landelijk) beleid.



Voorkom een datalek!

Zet geen persoons-, medische of bedrijfsgegevens in de AI-chatbot

- ① Een AI-chatbot slaat de gegevens die je invoert op, zoals gegevens over een patiënt/cliënt, project of sollicitant. Je hebt dan geen controle meer over deze gegevens. Gegevens die jij invoert, kunnen gebruikt worden voor antwoorden die de AI-chatbot aan andere mensen geeft. Ook kunnen de gegevens voor andere doelen worden gebruikt. Bijvoorbeeld dat de AI-chatbot wordt getraind op basis van data die gebruikers zelf invoeren.
- ② Zorg dat alles wat je invoert, in de EU blijft. Het maakt uit in welk land de gegevens zijn opgeslagen. Landen hebben verschillende regels over privacy en bescherming van gegevens. Dit bepaalt hoe gegevens mogen worden verzameld, opgeslagen, verwerkt en gedeeld. De EU heeft met de AVG de strengste en dus meest veilige privacyregels ter wereld. Lees [hier](#) meer over de AVG.
- ③ Stel een instructie op voor zorgmedewerkers zodat ze de AI-chatbot goed instellen. Bescherm je input. Vink alle mogelijkheden aan ter bescherming van de invoer (bijvoorbeeld: geen inspectie van de chatgeschiedenis door derden, geen verwerking van chatgeschiedenis in het verder trainen van het model). Bedenk wel dat er in de kleine lettertjes vaak wordt omschreven dat de input toch (tijdelijk) wordt opgeslagen.



Hoe kun jij het verschil maken?

Ontdek onze organisatorische tips!

- ① Stel een AI-beleid en AI-visie op. Wijs een portefeuillehouder aan voor AI in het directieteam. Voer samen met relevante stakeholders een risicoanalyse uit om kansen, risico's en verantwoordelijkheden in kaart te brengen.
- ② Investeer in opleidingen voor medewerkers. Dit zorgt voor hogere adoptie van AI-mogelijkheden en zorgvuldiger gebruik. Doe dit door het opstellen van leerlijnen op meerdere niveaus en functies. Heb aandacht voor verschillende leerstijlen. De een leert door te doen, de ander door de kunst af te kijken of over AI te lezen.
- ③ Investeer in AI-kennis en vaardigheden bij leidinggevendenden, zodat zij voorbeeldgedrag laten zien en medewerkers kunnen faciliteren in het optimaal benutten van van AI mogelijkheden.
- ④ Stel een leesbare richtlijn op over verantwoord gedrag bij het gebruik van AI. Zet hierin een lijst van door de organisatie goedgekeurde AI-chatbots en benoem de voorwaarden en risico's voor gebruik. Maak daarbij concreet wat wel en niet is toegestaan en communiceer dit met medewerkers.
- ⑤ Bespreek hoe elke procesverantwoordelijke AI-toepassingen meeneemt in het (IT) proces. Benut daarbij de kansen van AI en kijk naar wat slim is om op te pakken. Doe dit door te kijken naar wat collega-instellingen doen op AI: deel DPIA's, risico-analyses, ga op werkbezoek en informeer bij de brancheorganisaties.
- ⑥ Koppel je beleid op AI-chatbots aan je duurzaamheidsbeleid. Realiseer je dat AI-chatbots veel energie verbruiken. Moedig het gebruik van een gewone zoekmachine aan en ontmoedig het onnodig genereren van afbeeldingen door AI.
- ⑦ Voor grote organisaties: Overweeg om een multidisciplinaire AI groep of een AI board op te richten. Deze groep beoordeelt de geschiktheid van AI-toepassingen, zoals chatbots, en houdt toezicht op ethische aspecten, kwaliteit en veiligheid. Daarnaast evalueert de groep periodiek of de gebruikte AI-toepassingen nog aansluiten bij de behoeften van de organisatie en of er inmiddels betere of veiligere alternatieven beschikbaar zijn. Lees [hier](#) hoe andere organisaties dit doen in de Levende case study naar het gebruik van AI in de zorg.



Verdiep je in wet- en regelgeving

- ① De **Wet op de geneeskundige behandelingsovereenkomst (WGBO)** verplicht zorgverleners om verantwoordelijkheid te nemen voor hun medisch handelen, ook wanneer zij daarbij AI gebruiken. Patiënten/cliënten moeten volledig geïnformeerd worden en instemmen met behandelingen, inclusief die waarbij AI betrokken is.
- ② Volgens de **Algemene Verordening Gegevensbescherming (AVG)** moet een organisatie controle hebben over persoonsgegevens en toestemming voor gebruik. Voor het gebruik van AI-chatbots voor verwerking van persoonsgegevens is vaak geen toestemming. Jouw AVG-rechten als gebruiker zijn vaak niet gegarandeerd. Je kunt bijvoorbeeld de gegevens die AI-toepassingen over jou hebben niet verwijderen of aanpassen. Zelfs als je een chat wist, is het onbekend of deze echt verwijderd is.
- ③ Als er vragen of problemen komen door AI-chatbots, is het onduidelijk wie verantwoordelijk is. Dit kan problemen geven voor jou of je werkgever.
- ④ Elke AI-chatbot werkt volgens andere instellingen en gebruikt jouw gegevens anders.
- ⑤ AI is een medisch hulpmiddel als het een medisch doel heeft. Medische hulpmiddelen moeten voldoen aan de (kwaliteits)eisen uit de **Medical Device Regulation (MDR)**. [Meer informatie over MDR en IVDR | Medische hulpmiddelen en technologie | Rijksoverheid.nl](#)
- ⑥ De Europese **AI Act** is een wet waaraan elke relevante AI-toepassing moet voldoen. Dit betekent dat AI moet voldoen aan eisen zoals transparantie, menselijke controle en voortdurende monitoring om te voorkomen dat ze schadelijke beslissingen nemen. Daarnaast moeten deze systemen nauwkeurig zijn en mogen ze geen discriminerende resultaten opleveren. De AI Act stelt niet alleen regels aan AI-toepassingen, maar ook aan de organisaties die ze gebruiken. Organisaties moeten ervoor zorgen dat medewerkers die met AI werken voldoende kennis en vaardigheden hebben, bijvoorbeeld door hen op te leiden of te trainen. Lees hierover meer: [Verordening artificiële intelligentie: Raad geeft definitief groen licht - Consilium \(europa.eu\)](#).
- ⑦ Vraag altijd toestemming als je een gesprek met iemand wilt opnemen, dus ook als je hier een AI-chatbot voor gebruikt.



Veilig en bewust gebruik van AI-chatbots

voor medewerkers

We gebruiken in de zorg steeds vaker AI-chatbots, zoals ChatGPT, CoPilot en Claude. Ze bieden kansen, maar brengen ook risico's met zich mee. Zorg dat je er veilig en bewust mee omgaat. Ontdek de tips!



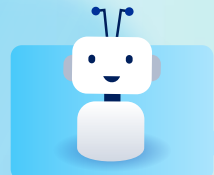
Je kunt (mogelijke) datalekken of andere incidenten creëren.

Als je in een AI-chatbot gegevens invoert over bijvoorbeeld een patiënt/cliënt project of sollicitant, worden deze opgeslagen.

Je hebt dan geen controle meer over deze gegevens en ze kunnen voor training van de chatbot en zelfs als input voor antwoord op toekomstige vragen van anderen worden gebruikt.

Waarom moet je voorzichtig zijn met AI-chatbots?

Denk goed na over welke informatie je aan een AI-chatbot geeft en of het antwoord klopt en nuttig is.



Je kunt verkeerde beslissingen nemen door verkeerde antwoorden van de AI-chatbot.

AI-chatbots spreken niet altijd de waarheid. Het antwoord van een AI-chatbot hangt af van de gegevens waarop hij is getraind, jouw prompt en zelfs van het moment; ook bij exact dezelfde prompt kan het antwoord verschillen.

Dit komt doordat een LLM steeds opnieuw het meest waarschijnlijke volgende woord voorspelt. Omdat er meerdere goede antwoorden zijn, verschilt het antwoord elke keer.

Een AI-chatbot kan onzin gebruiken als bron en onzinnige uitkomsten geven. Ook als het op een geselecteerde dataset is getraind. Door verkeerde informatie of adviezen van de AI-chatbot, kunnen nare situaties ontstaan.

Je kunt handelen in strijd met wet- en regelgeving.

Hoe je AI-chatbots gebruikt, kan in strijd zijn met wetten en regels zoals MDR/IVDR, AVG, de AI Act en de WGBO. Overtredingen kunnen leiden tot sancties voor de organisatie en, afhankelijk van de situatie, ook tot andere gevolgen voor betrokken professionals.





Voer nooit **privacygevoelige gegevens** in, **in niet goedgekeurde** AI-chatbots zoals persoons- of herleidbare gezondheidsgegevens en bedrijfsgevoelige gegevens. Lees [hier](#) meer.



Gebruik alleen AI-chatbots die door **jouw organisatie zijn goedgekeurd**.



Heb je toch privacygevoelige gegevens gedeeld met de AI-chatbot? **Meld dit datalek** bij de juiste persoon binnen jouw organisatie.



Bekijk de animatie [melden datalek](#).



Vraag na of er binnen jouw organisatie **beleid- en gedragsregels** zijn over het gebruik van AI-chatbots.



Schrijf goede prompts.

Prompts zijn de opdrachten die je aan een AI-chatbot geeft.

- Wees duidelijk over het onderwerp, de doelgroep en de toon.
- Lees [hier](#) meer over wat een goede prompt is.

Gebruik een AI-chatbot vooral voor inspiratie of als **digitale assistent**. Nooit als vervanger van een professional. Medische beslissingen, diagnoses en zorg blijven altijd de verantwoordelijkheid van de professional.

- Controleer altijd of het antwoord klopt bijvoorbeeld door het checken van de bron en blijf zelf nadenken.
- Blijf je eigen kennis en gezond verstand gebruiken. Zie het antwoord van de AI-chatbot als inspiratie en niet als leidend.
- Meer weten? Bekijk [deze video](#).

Tips

Waar kan je AI-chatbots wél bij gebruiken?



Blijf zelf nadenken en controleren.



Voer nooit persoons- of bedrijfsgevoelige gegevens in.

Hulp bij het maken van samenvattingen, bijvoorbeeld van bestaande wetenschappelijke artikelen. Doe dit niet met vertrouwelijke informatie zoals patiëntendossiers en bedrijfsrapportages, zoals een jaarplan of kwaliteitsplan.

Rapportages en overdrachten schrijven in een goedgekeurde AI-tool zonder persoonsgegevens.

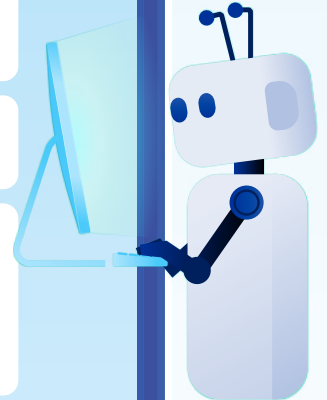
Notulen van een overleg samenvatten of omzetten in een verslag.

Verslaglegging automatiseren in de door jouw organisatie goedgekeurde AI-tool.

Uitleg van bijvoorbeeld (concept) mails, patiënt- of cliëntcommunicatie en brieven in heldere taal (B1-niveau), feedback vragen op geanonimiseerde plannen, ideeën, teksten of analyses.

Samenvatten van complexe dossiers/richtlijnen in een goedgekeurde AI-tool. Let op! Blijf altijd zelf checken. De eerste keer dat je een dossier/richtlijn leest, lees zelf! Als geheugensteuntje kan je daarna de samenvatting gebruiken.

Ideeën en kwaliteitsverbetering.



In samenwerking met de werkgroep AI-chatbots

Alex Beckers	Adviseur informatiebeveiliging en privacy in de zorg, Beckers Consult
Danique Arendonk-de Ruijter	Beleidsadviseur kwaliteit en veiligheid, Dé Provinciale Kraamzorg, Lunavi Kraamzorg
Jacqueline Pronk-van der Noort	Stafadviseur kwaliteit & veiligheid Digitale zorg, UMC Utrecht
Renée van der Sluis	Beleidsmedewerker informatiebeveiliging, Alerimus
Ildikó Vajda	Senior adviseur patiëntbelang, Patiëntenfederatie Nederland

Meelezers

Pieter van Kuilenburg	Coördinator werkgroep Gezondheid en Zorg, NL AI Coalitie
Saskia Haitjema	Universitair hoofddocent, UMC Utrecht
Dirk Lukkien	Senior onderzoeker Digitale zorg, Vilans
Nathan van der Lei	Machine Learning Engineer, Expertisecentrum zorgalgoritmen
Marc Jacobs	Datawetenschapper en statistisch adviseur, eigenaar van MSJ Advies
Ande Swinkels	Jurist/privacyfunctionaris, Vilans
Chris van Zwolle	Product Owner Kennisproducten, Z-CERT
Linda de Lange	Business consultant, Z-CERT

Meelezers revisie 2026

Anton Vos, Information Security Officer, Pro Persona — Boris van Moorsel, Informatieadviseur, Mesdag — Claudia Benning, Beleidsmedewerker kwaliteit & Functionaris Gegevensbescherming, DrieGasthuizenGroep — Eric Consten, Senior Privacy Officer, Ipse de Bruggen — Janneke Brandwijk, Informatieadviseur Cybersecurity, Pieter van Foreest

Colofon

De toolkit AI-chatbots zijn handig, maar gebruik ze verstandig is een uitgave van het programma Informatieveilig gedrag in de zorg (IVGZ).

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, NHG (mede namens LHV en INEEN), NVZ, UMCNL en VGN zijn bij het programma betrokken.

Versie 2, september 2026 © Informatieveilig gedrag in de zorg

Auteurs

Bettine Pluut, Informatieveilig gedrag in de zorg
Mariët de Waal, Informatieveilig gedrag in de zorg
Maud Madsen, Informatieveilig gedrag in de zorg
Sebastiaan Stam, Informatieveilig gedrag in de zorg
Sophie Jellema, Informatieveilig gedrag in de zorg

Communicatie

Demi van Spronssen, ECP | Platform voor de Informatiesamenleving