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?

Hoe maak jij het verschil?

Wat zijn risico's van gebruik?

Inspireer jouw collega's
Tips om in gesprek te gaan

Voorkom een datalek!

Verdiep je in wet- en regelgeving

Ontdek de organisatorische tips



Meer weten?

Wil je op de hoogte blijven van de nieuwste inzichten en praktijkvoorbeelden? Houd de website **Aan de slag met informatieveilig gedrag in de zorg** in de gaten en abonneer je op de nieuwsbrief.

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

Plaats hier het logo van uw organisatie

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.



Plaats hier het logo van uw organisatie

Risico's

Maatregelen



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

- 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.

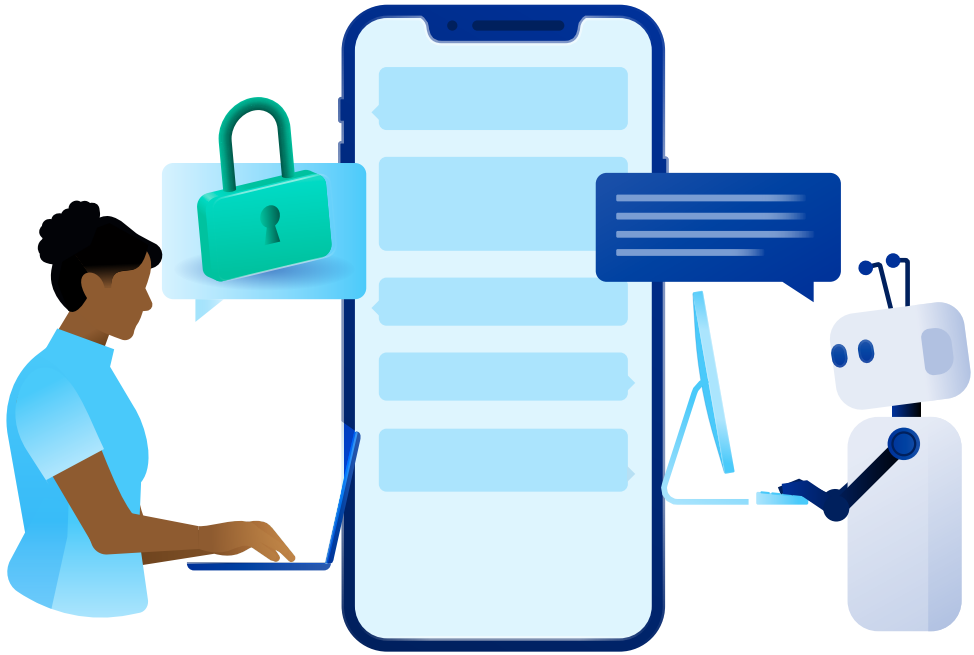
Raadpleeg jouw brancheorganisatie voor (landelijk) beleid.

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 leidinggevenden, 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.



Plaats hier het logo van uw organisatie

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.



Plaats hier het logo van uw organisatie