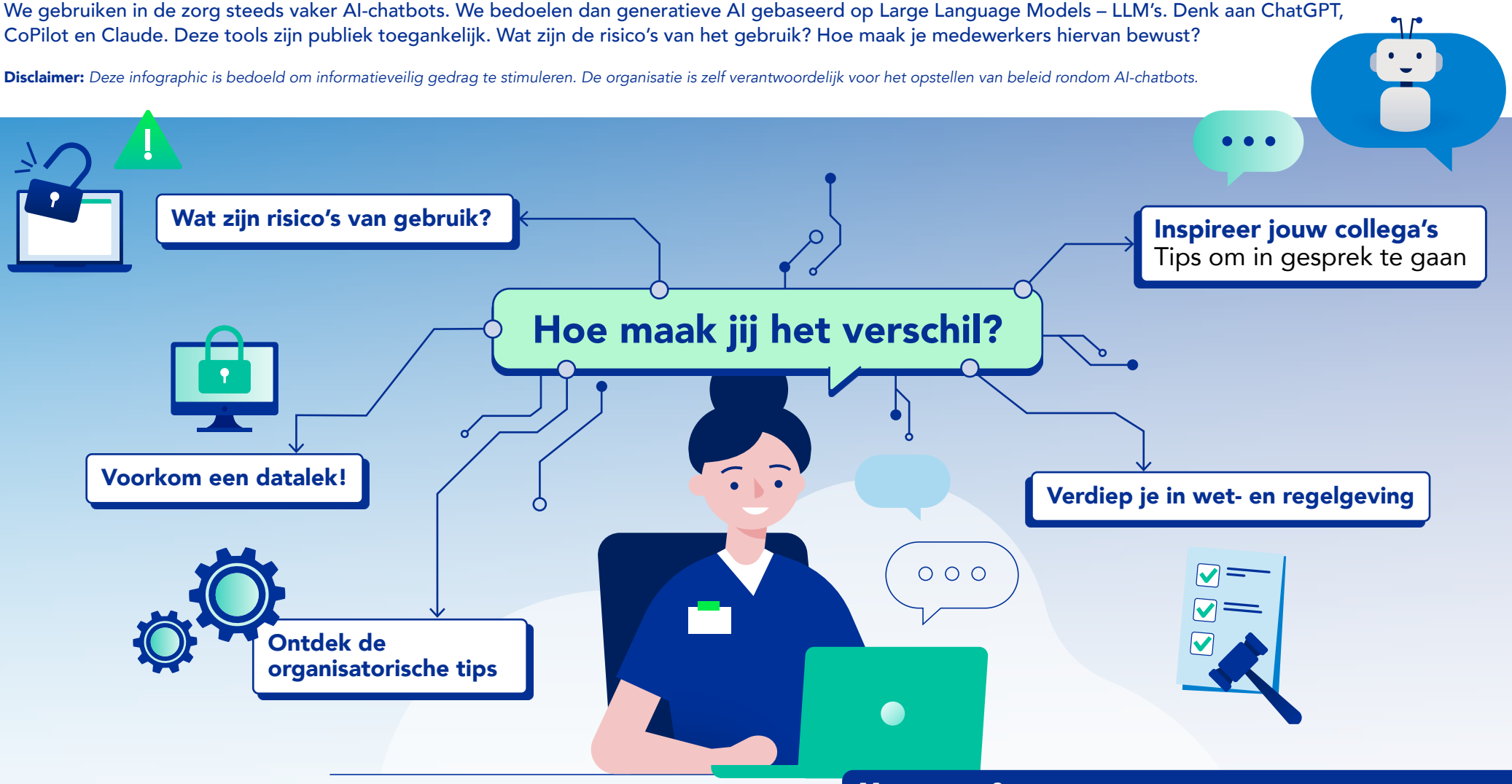
In gesprek over AI-chatbots Tips voor Informatieveiligheidsprofessionals*

We gebruiken in de zorg steeds vaker AI-chatbots. We bedoelen dan generatieve AI gebaseerd op Large Language Models – LLM's. Denk aan ChatGPT, CoPilot en Claude. Deze tools zijn publiek toegankelijk. Wat zijn de risico's van het gebruik? Hoe maak je medewerkers hiervan bewust?

Disclaimer: *Deze infographic is bedoeld om informatieveilig gedrag te stimuleren. De organisatie is zelf verantwoordelijk voor het opstellen van beleid rondom AI-chatbots.*



Meer weten?

De ontwikkelingen op het gebied van AI gaan snel. Zorg dat je hiervan op de hoogte blijft. Houd de website Aan de slag met informatieveilig gedrag in de zorg in de gaten en abonneer je op de nieuwsbrief.

* Met Informatieveiligheidsprofessionals (IVP's) bedoelen we functionarissen die informatieveiligheid in portefeuille hebben, zoals (C)ISO, FG, (beleids)adviseur kwaliteit en veiligheid, CIO, CMIO en CNIO.

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 deze infographic.
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.
3. Leg het beleid en de gedragsregels van jouw organisatie uit.
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.
6. Bespreek met de afdeling communicatie welke ideeën zij hebben voor bewustwording, scholing en voor de verspreiding van de infographic voor medewerkers.
7. Zorg dat je de infograhic voor zorgmedewerkers opneemt in de opleidingsmaterialen voor (nieuwe) medewerkers.

Risico's	Maatregelen
 Er ontstaan datalekken doordat medewerkers gevoelige gegevens in AI-chatbots invoeren.	• Informeer medewerkers dat ze geen persoons-, medische of bedrijfsgevoelige gegevens mogen invoeren in een AI-chatbot. **En leg uit waarom dit niet mag**. • Gebeurt het toch? Zorg ervoor dat medewerkers dit als datalek melden. Neem dit type datalek 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. Inbreuk op intellectueel eigendom is hiermee ook een risico.	**Maak medewerkers bewust van gedragsrisico's bij het gebruik van AI-chatbots:** Leg uit hoe een AI-chatbot aan zijn antwoorden komt. Dit hangt sterk af van hoe de AI-chatbot wordt getraind en welke prompts je gebruikt. Dat is riskant voor zowel de zorg als voor bedrijfsprocessen. Informeer bij collega's van andere zorgorganisaties en deel kennis en ervaringen
 Met het gebruik van (bepaalde) AI-chatbots kun je in strijd handelen met wet- en regelgeving.	Verdiep je in de relevante **wetgeving en richtlijnen**, zoals AVG, MDR/IVDR, AI Act, WGBO en tuchtrecht. Zorg dat jouw organisatie hieraan voldoet of bespreek dit met de verantwoordelijke mensen in jouw organisatie. 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, project of sollicitant. Je hebt dan geen controle meer over deze gegevens. 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.

2. 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. Dit komt doordat een AI-chatbot wordt getraind op basis van data die gebruikers zelf invoeren.

3. 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 verder trainen model). Stel een instructie op voor zorgmedewerkers zodat ze de AI-chatbot goed instellen. Hiermee zet je een stap in de goede richting maar bedenk dat er in de kleine letterjes vaak wordt omschreven dat de input toch (tijdelijk) wordt opgeslagen.

Hoe kun jij het verschil maken?
Ontdek onze organisatorische tips!

1. Bedenk hoe je AI-chatbots wilt aanbieden. Is een publieke AI-chatbot geschikt? Of is het beter voor de organisatie om een eigen LLM omgeving in te kopen of te ontwikkelen?

2. Overweeg om een multidisciplinaire AI-groep of commissie op te richten. Hiermee bespreek je bijvoorbeeld de geschiktheid van een AI-chatbot of andere AI-toepassingen, ethische en kwaliteitsaspecten.

3. Volg het gebruik van AI-chatbots door medewerkers, zonder daarbij hun privacy te schenden. Dit kan anoniem. Bijvoorbeeld door te kijken hoe vaak bepaalde AI-chatbots worden benaderd met een organisatie-account en hoeveel unieke gebruikers er zijn. Dit helpt bij het nemen van beslissingen over het gebruik van AI en acties in te zetten gericht op het bevorderen van veilig gedrag.

4. Maak een lijst van door de organisatie goedgekeurde AI-chatbots en benoem de voorwaarden en risico's voor gebruik.

5. Bespreek hoe elke procesverantwoordelijke AI-toepassingen meeneemt in het (IT) proces.

6. Koppel je beleid op AI-chatbots aan je duurzaamheidsbeleid. Realiseer je dat AI-chatbots veel energie verbruiken. Een standaard zoekmachine is zuiniger.

Verdiep je in wet- en regelgeving

1. 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.

2. Jouw AVG-rechten als gebruiker zijn vaak niet zeker. Je kunt bijvoorbeeld de gegevens die AI-toepassingen over jou hebben niet verwijderen of aanpassen.

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 heeft andere regels 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. Lees hierover meer
   Verordening artificiële intelligentie: Raad geeft definitief groen licht - Consilium (europa.eu)

7. De **Wet Geneeskundige Behandelovereenkomst (WGBO)** vereist dat zorgverleners verantwoordelijkheid nemen voor de medische beslissingen die zij, eventueel met hulp van AI, nemen. Patiënten moeten volledig geïnformeerd worden en instemmen met behandelingen, inclusief die waarbij AI betrokken is.

8. Vraag altijd toestemming als je een gesprek met iemand wilt opnemen, dus ook als je hier een AI-chatbot voor gebruikt.