



Informatieveilig
gedrag **in de zorg**

Aan de slag met informatieveilig gedrag!

Unieke aanpak voor meer informatieveiligheid in de zorg

Welkom bij onze eerste deel- en leerbijeenkomst!

28 november 2023 | Sietske Rozie en Manon van der Woude



Platform voor de
InformatieSamenleving



Informatieveilig
gedrag **in de zorg**

De impact van ChatGPT op de informatieveiligheid binnen jouw organisatie

Welk gedrag zie jij nu al?

28 november 2023 | Sietske Rozie en Manon van der Woude



Platform voor de
InformatieSamenleving



Wij zijn:

- Manon van der Woude



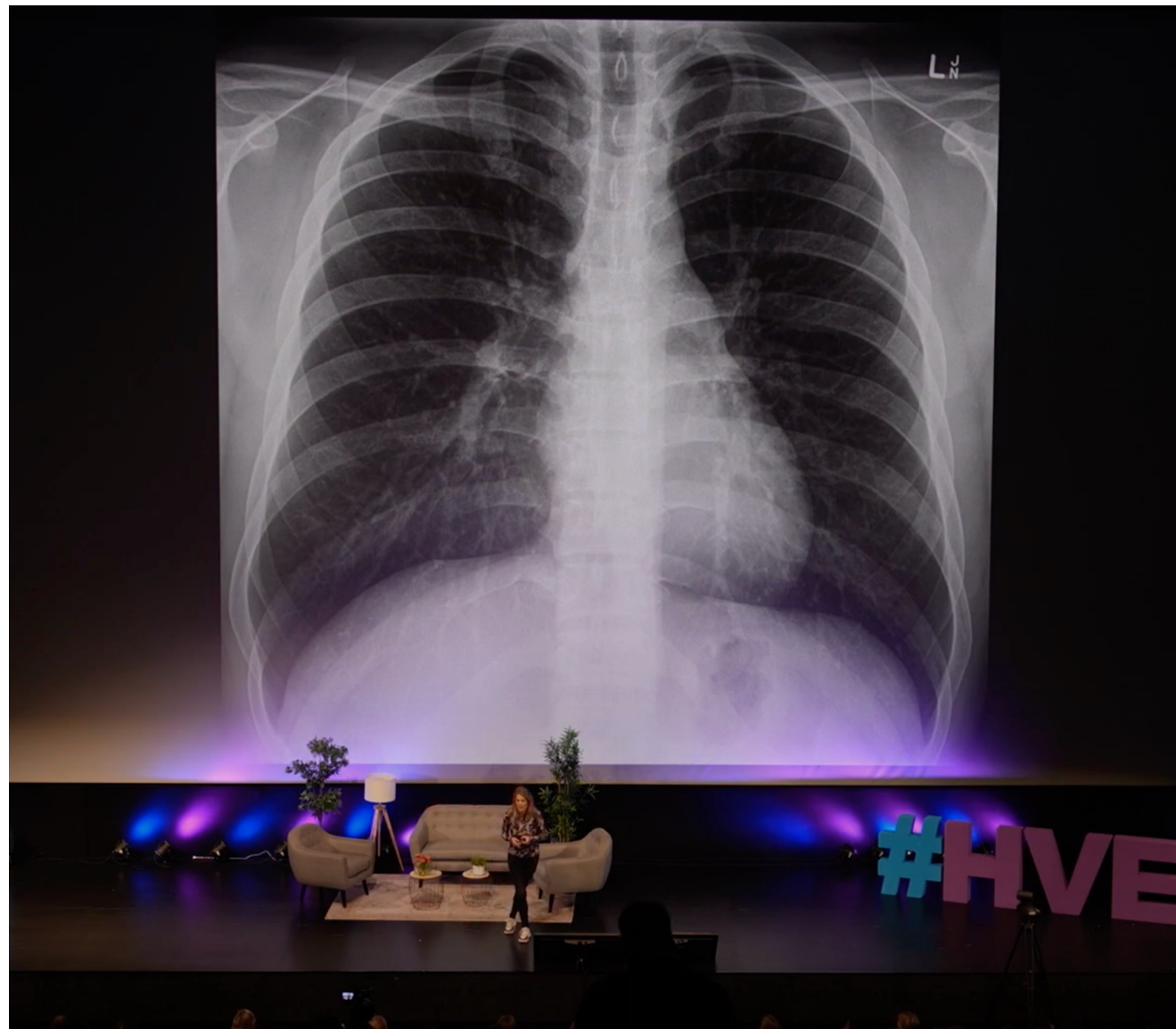
Manon van der Woude

Communicatieadviseur



Wij zijn

- Sietske Rozie





Jullie zijn:

- ggz, jeugdzorg, ziekenhuis, verpleeghuis, gehandicaptenzorg, thuiszorg, huisartsenpraktijk,
- SO, ISO, CISO, privacy officer, IVP, functionaris gegevensbescherming, medewerker kwaliteit divers,



Wat gaan we het komende uur doen?

- Intro LLM's algemeen en mbt informatieveiligheid
- Wat zien jullie nu al mbt gedrag en LLM's? + terugkoppeling
- Wat betekent dat voor het doelgedrag en huisregels? Suggesties verzamelen

- Inventarisatie behoeften toekomstige deel- en leerbijeenkomsten
- Break-out: welke thema's? Welke structuur?

Vraag 1. wie heeft zich afgelopen jaar verdiept in AI?

- Nee
- Ik lees / kijk / luister wat ik tegenkom
- Ik ga op zoek naar specifieke informatie
- Ik gebruik chatgpt / andere LLM

Wie heeft zich afgelopen jaar verdiept in AI?

nee	Uw antwoord	15%
ik lees / luister/ bekijk wat ik tegenkom		47%
ik ga op zoek naar specifieke informatie		9%
ik gebruik chatGPT / ander LLM		29%



Vraag 2. wie had zich daarvoor al verdiept in AI?

- Ja
- Nee

Had je je eerder dan een jaar geleden ook al verdiept in AI?



29 antwoorden



Vraag 3.

AI is in onze organisatie onderdeel van het beleid

- Ja
- nee

AI is in onze organisatie
onderdeel van het beleid / visie /
strategie

nee **Uw antwoord**

90%

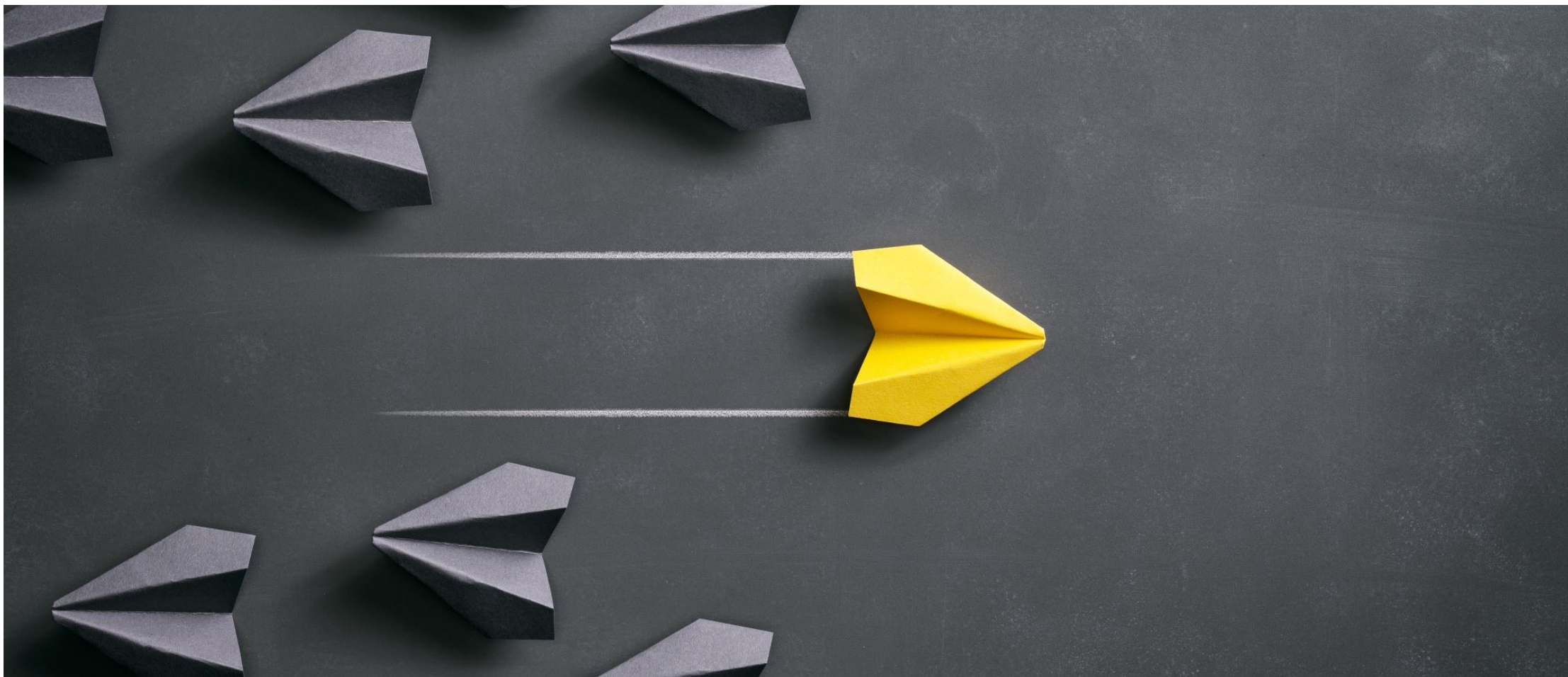
ja

10%

31 antwoorden

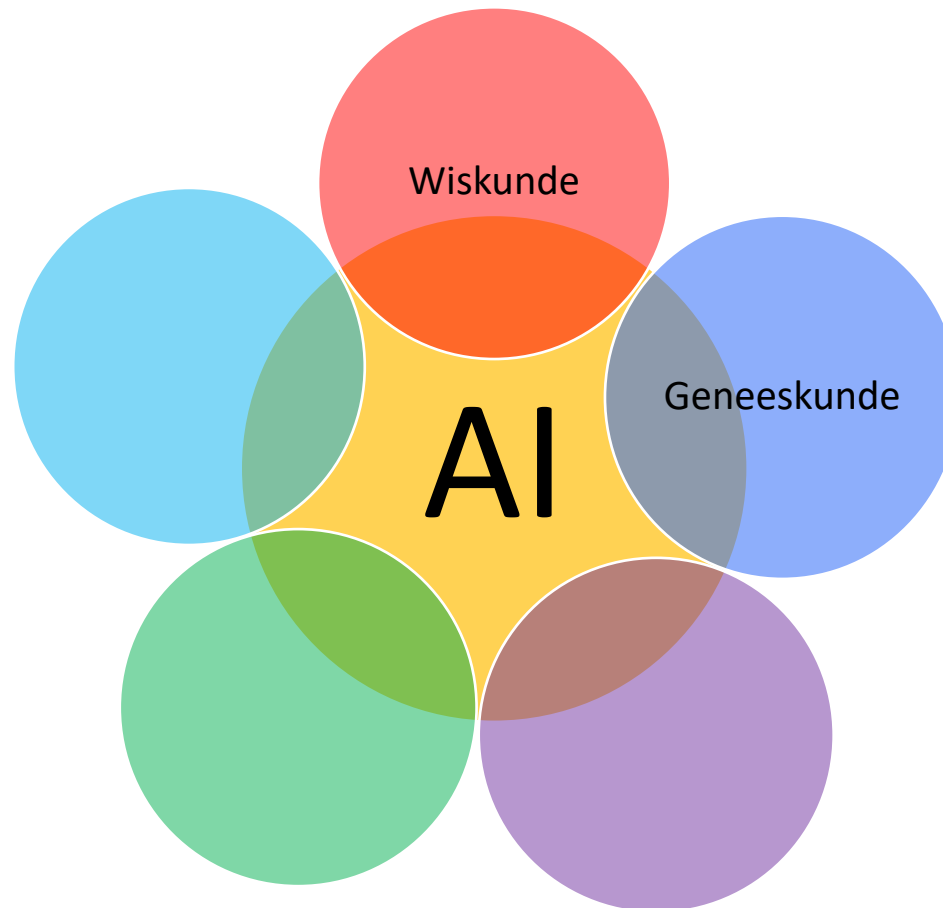


Korte AI intro: Beter worden met AI



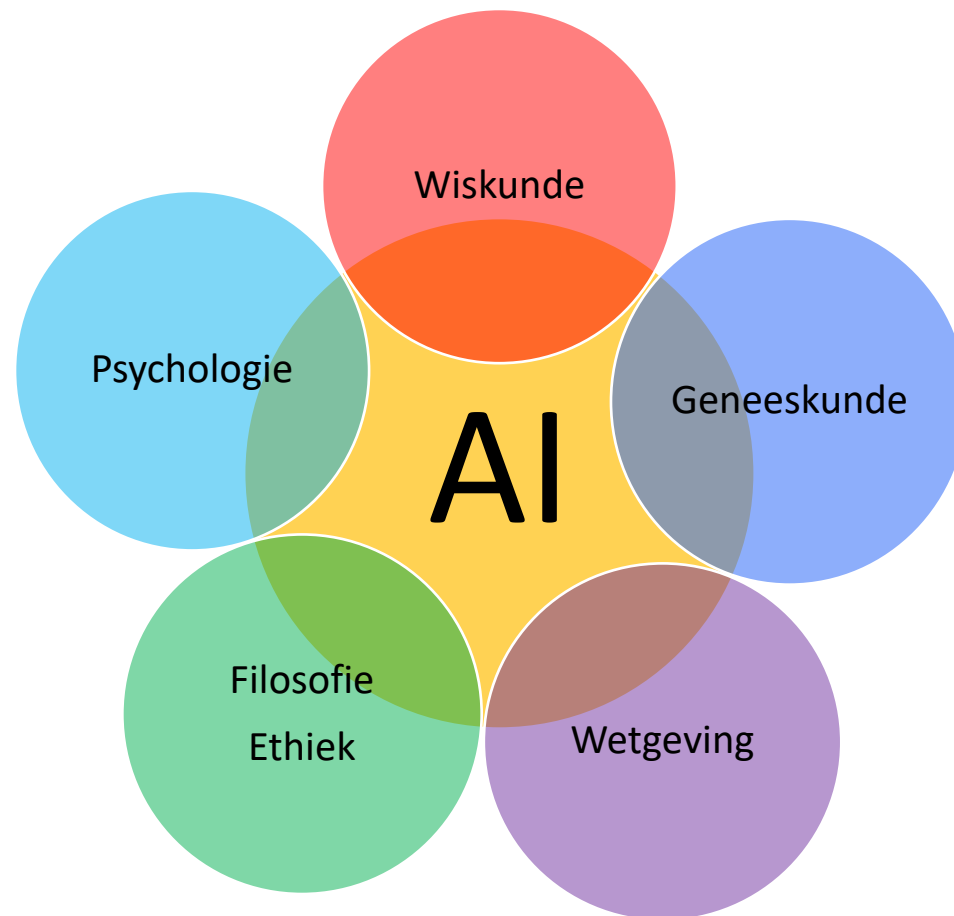


Welke kennisdomeinen spelen een rol bij AI?

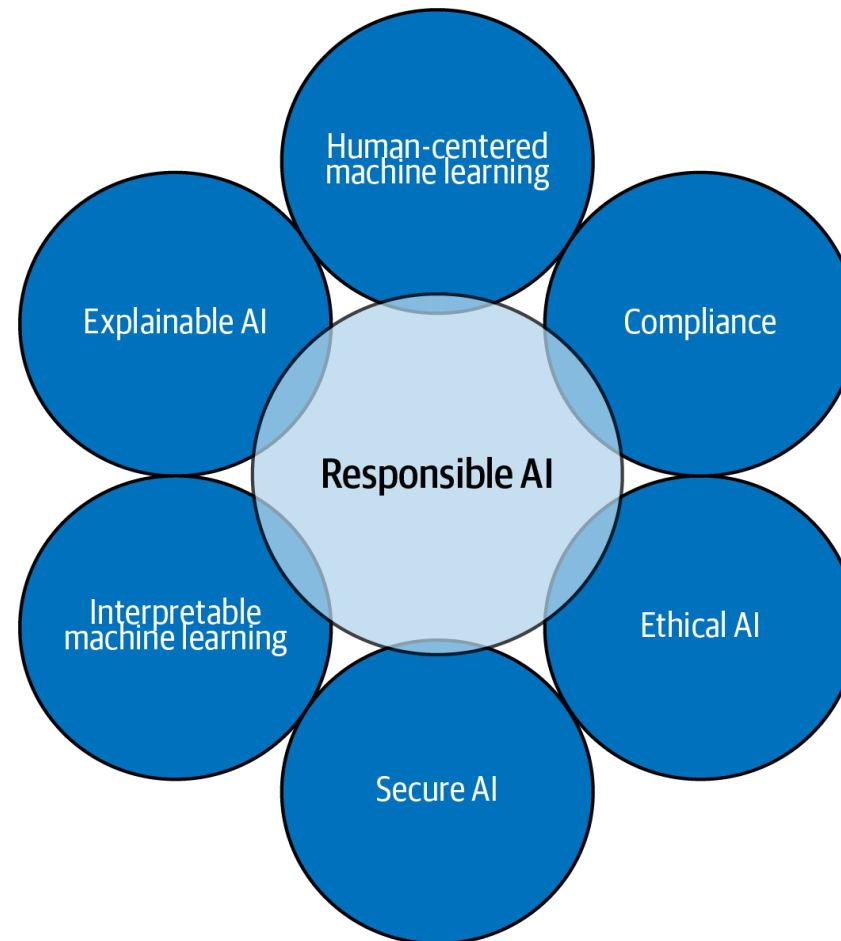




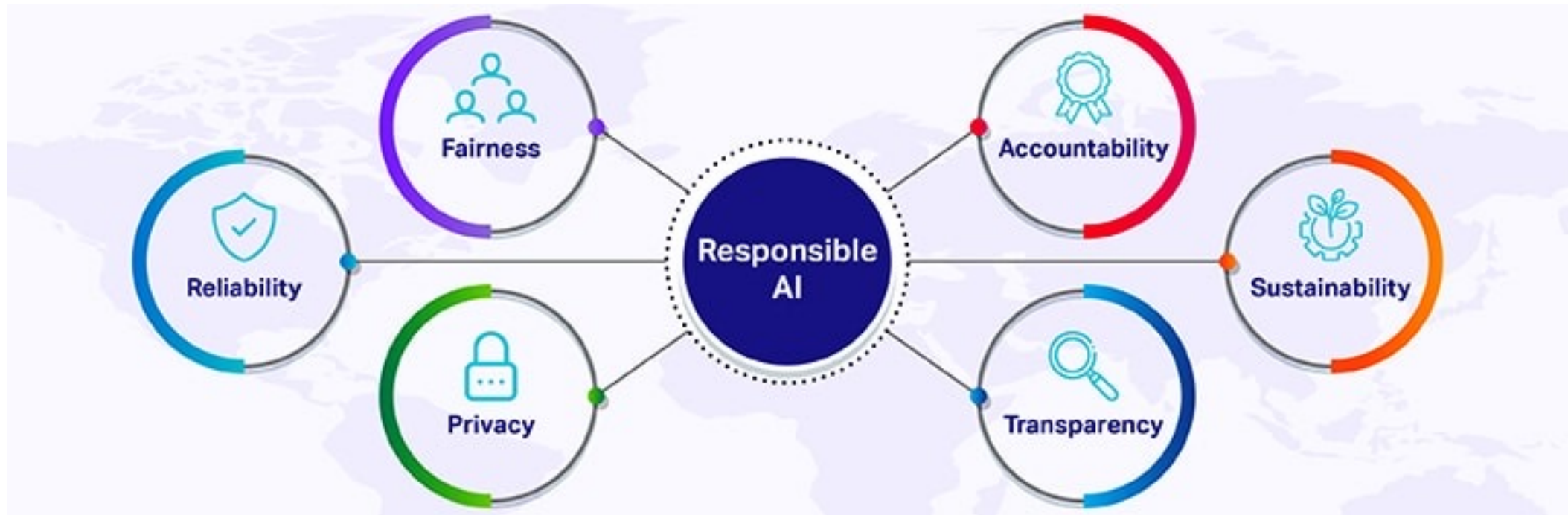
Inhoud en vorm: hoe gaan we om met AI?



Verantwoordelijkheid bij ontwikkeling en gebruik



Maar vergeet niet: sustainability hoort daar ook bij!



2020: tijdens de Algemene Beschouwingen

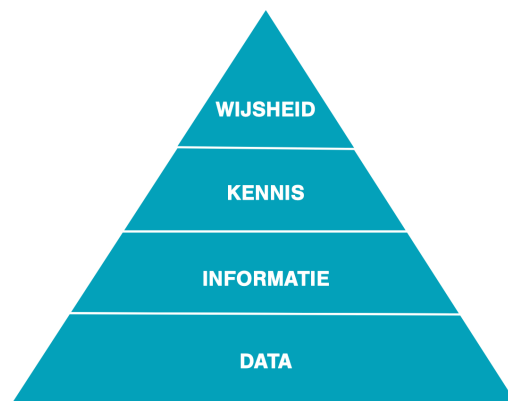


Filmfragment:
Wopke Hoekstra, toen nog minister
van Financiën, over AI en het werk
van diverse professionals: hij denkt
dat radiologen nu eigenlijk al
overbodig zijn

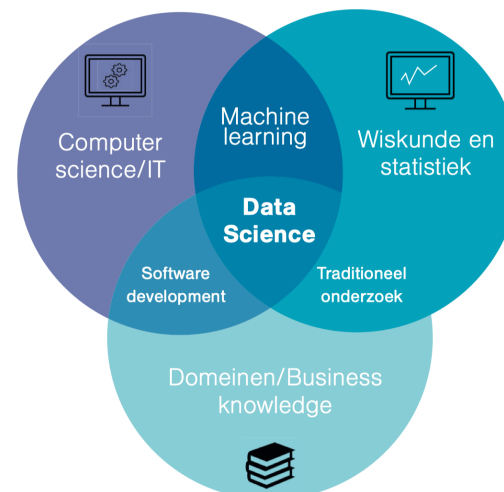
Korte en lange termijn

Roy Amara, president van the stitute for the future 1971-1990:

“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run”



Figuur 15.3 Visualisatie van het DIKW-model, de DIKW-hiërarchie waarin in vier stappen wordt gewerkt van ruwe data naar wijsheid



Figuur 15.1 Schematische weergave van subdisciplines van data science



Mei 2023



LLM Large Language Model: buzzzz words

- **GPT:** staat voor “generative pre-trained transformer”, wat een soort groot taalmodel is: een neurale netwerk dat is getraind op een zeer grote hoeveelheid tekst om overtuigende, mensachtige taaluitkomsten te produceren.
- **Prompts**
- **Generative AI**
- **Autofill**
- **Hallucinaties**
- **Chatbot**
- **Staking Hollywood**
- **“clickworkers” in Kenia**

chatGPT heeft inmiddels 1,5 miljoen gebruikers in Nederland
En 100 miljoen wereldwijd



Een bedreiging? Verdwijnen bepaalde banen?



Journalistieke keuzes 25-08-2023

Hoe een AI-gegenereerde foto in het NOS Journaal terecht kwam



Het is je misschien helemaal niet opgevallen, maar dat is precies het punt. In het NOS Journaal van 18.00 op donderdag 24 augustus zat een achtergrondfoto die niet echt was. De 'schermafbeelding' van koningspinguïns op Antarctica was geen echt archiefbeeld van die dieren, het was een door AI gegenereerde manipulatie.



Is de ontwikkeling van AI als een vrije val?



Break-out 1:

- Zien jullie al dat medewerkers LLM's zoals chatGPT gebruiken?
- Wat vinden jullie daarvan?
- Krijgen jullie daar vragen over?
- Wat was daarna jouw reactie?

2. medewerkers gebruiken LLM / chatGPT

ja	58%
weet ik niet Uw antwoord	19%
nee	23%

27 antwoorden



Voorbeelden van formeel LLM-gebruik binnen EPD:

Model achter ChatGPT

De proef is een initiatief van de Amerikaanse epd-leverancier Epic in samenwerking met de Epic vereniging Nederland, waar alle Nederlandse ziekenhuizen met dat epd deel van uitmaken. [Epic liet eerder al weten op dit vlak samen te werken met Microsoft](#), een van de partijen achter OpenAI. Die onderneming werd in korte tijd bekend door ChatGPT te lanceren. De toepassing van Epic maakt dan ook gebruik van hetzelfde onderliggende taalmodel: GPT4.

Europese primeur: Artificial Intelligence helpt artsen bij beantwoorden vragen van patiënten

♡ 0 | ➦



Het ETZ (Elisabeth-TweeSteden Ziekenhuis) stimuleert patiënten om gebruik te maken van patiëntenportaal MijnETZ. Patiënten kunnen



Informatieveilig
gedrag in de zorg

Huisartsenpraktijk zet chatbot 'Praat met de Dokter' in



Wat vinden jullie van de naam van deze chatbot?

Huisarts peter dekkers

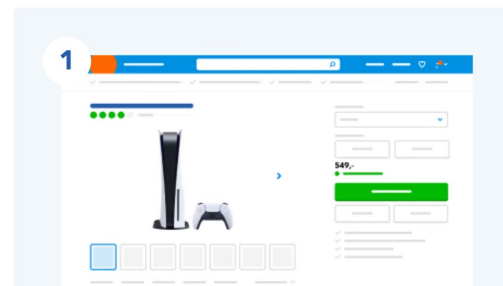


Informatieveilig
gedrag in de zorg

O, kom maar eens kijken!

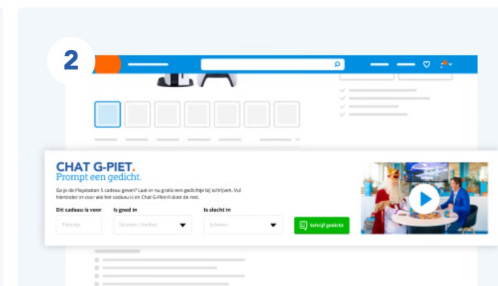


Zo werkt het



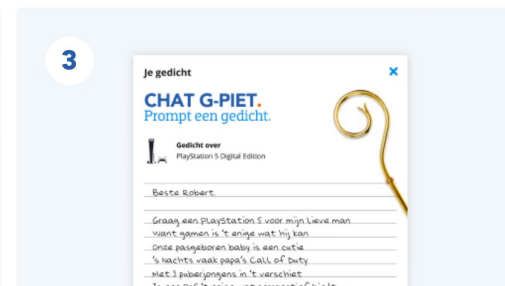
STAP 1.

Ga naar Coolblue.nl en kies een product dat jij cadeau wilt geven.



STAP 2.

Laat weten wie de gelukkige ontvanger is, inclusief karaktereigenschappen.



STAP 3.

Laat je verrassen met een gratis gepersonaliseerd gedichtje van Chat G-Piet.

Recente gedichten

Beste Brian.

Wat ben jij toch een ster in mooie dingen shoppen
Maar qua autorijden moet jij 't nog ver schoppen
Want voordat je jouw shoppingbudget kan besteden
Ben je al 3 keer de verkeerde kant op gereden

En na een dagje je auto te hebben volgeladen
Kan je de terugreis ook al raden
Met dit cadeau ben je nooit meer de weg kwijt
En heb je voor winkelen nog meer tijd

Sint en Chat G-Piet

Gedicht voor Brian

Brian wil graag een navigatiesysteem. Hij is slecht in navigeren, maar kan wel goed shoppen.

Beste Jackie.

Welke muziek er draait boeit jou niet
Want je weet te bewegen op elke beat
Maar zet je 't dan ook op een zingen
Zijn 't tranen die in onze ogen springen

Niet van ontroering, als je dat dacht
Want wat een lawaai komt er uit jouw schacht
Houd het daarom maar bij dansen
Daar liggen voor jou de beste kansen

Sint en Chat G-Piet

Gedicht voor Jackie

Jackie wil graag Just Dance. Hij is namelijk goed in dansen, maar is slecht in zingen.

Beste Sander.

In de keuken staan terwijl je je uitslooft?
Geen denken aan, geen haar op je hoofd
Want zelfs al zou je een poging wagen
Is het maar de vraag of 't zou slagen

Maar opruimen daarin ben je een held
Door jouw skills verdwijnt elke vuilnisbelt
En met deze elektrische mop
Is 't zo weer schoon, zonder geschrob

Sint en Chat G-Piet

Gedicht voor Sander

Sander wil graag een elektrische dwel. Hij is slecht in koken, maar is goed in schoonmaken.

Generative: naast taal ook audio en beeld

[Featured insights](#)[Capabilities](#)[Industries](#)[Technology](#)[About us](#)[Careers](#)

Light

[Sign in](#) | [Register](#)[Home](#) > [Tech Effect](#) > Managing the risks of generative AI

Managing the risks of generative AI

A playbook for risk executives — beginning with
governance

[Cybersecurity](#)[Generative AI](#)



Voorbeeld:
midjourney

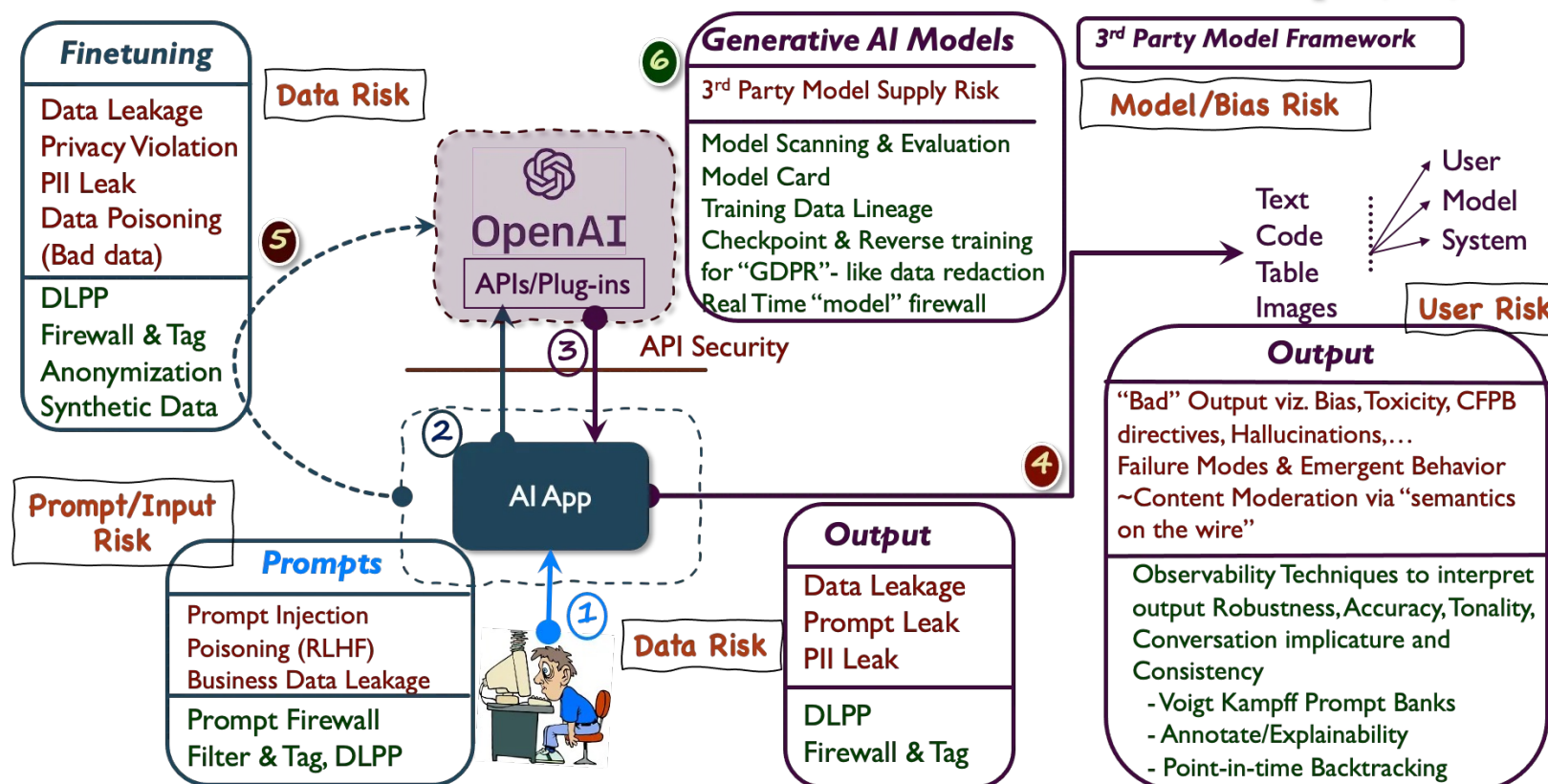
Risico: bias





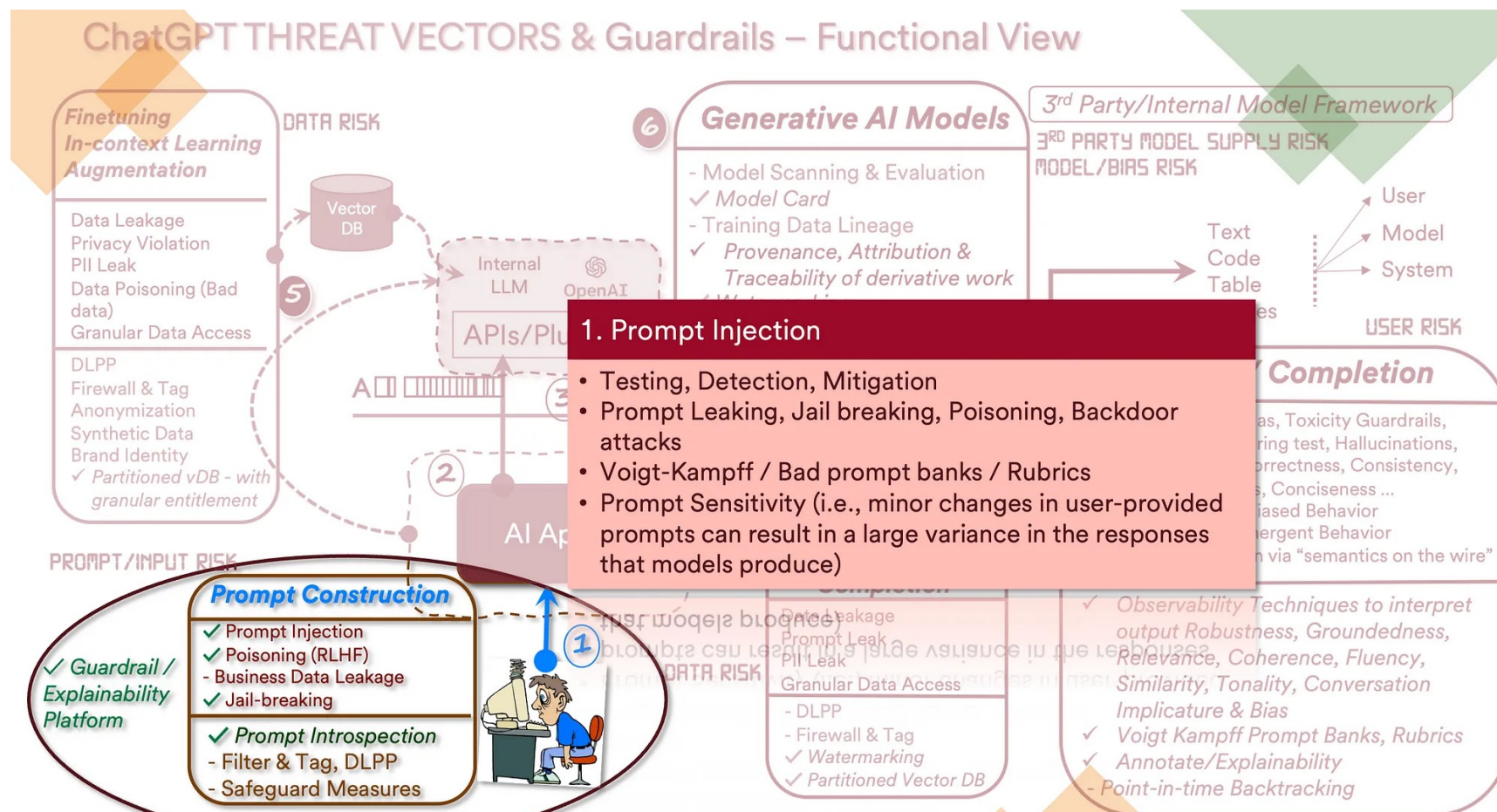
Geïnspireerd op het PWC rapport mei 2023

ChatGPT THREAT VECTORS & GUARDRAILS FOR LLMOps (5/5)





Focus: prompt construction





Wat kan er mis gaan? 2 bekende voorbeelden:

INGRESS

[4.4.2023] Samsung workers accidentally leaked trade secrets via ChatGPT

3 instances in a month and ChatGPT doesn't keep secrets !

1. In one instance, an employee pasted confidential source code into the chat to check for errors – exposed source code itself for a new program, internal meeting notes data relating to their hardware..
2. Another employee shared code with ChatGPT and "requested code optimization."
3. A third, shared a recording of a meeting to convert into notes for a presentation

That information is now out in the wild for ChatGPT to feed on

Other (potential) scenarios include sharing confidential legal documents or medical information for the purpose of summarizing or analyzing lengthy text



- *Consider this a cautionary tale to be remembered, the next time you turn to ChatGPT for help.*
- *Samsung certainly will*



Jurisprudentie opzoeken...cfr medische diagnose?

ChatGPT IN THE COURT

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING

ARTIFICIAL INTELLIGENCE + HUMAN LAZINESS —

Lawyer cited 6 fake cases made up by ChatGPT; judge calls it “unprecedented”

Judge weighs punishment for lawyer who didn't bother to verify ChatGPT output.

JON BRODKIN - 5/30/2023, 11:52 AM

Lawyer: ChatGPT said the cases were real !!

... provided an excerpt from ChatGPT queries in which he asked the AI tool whether it is a real case.

ChatGPT answered that it "*is a real case*" and "*can be found on legal research databases such as Westlaw and LexisNexis*"

- The judge wrote that they may be sanctioned "for the use of a false and fraudulent notarization in his affidavit filed on April 25, 2023"
- The law firm could be sanctioned for "*the citation of non-existent cases to the Court,*" "*the submission to the Court of copies of non-existent judicial opinions annexed to the Affidavit filed on April 25, 2023,*" and "the use of a false and fraudulent notarization in the affidavit filed on April 25, 2023"

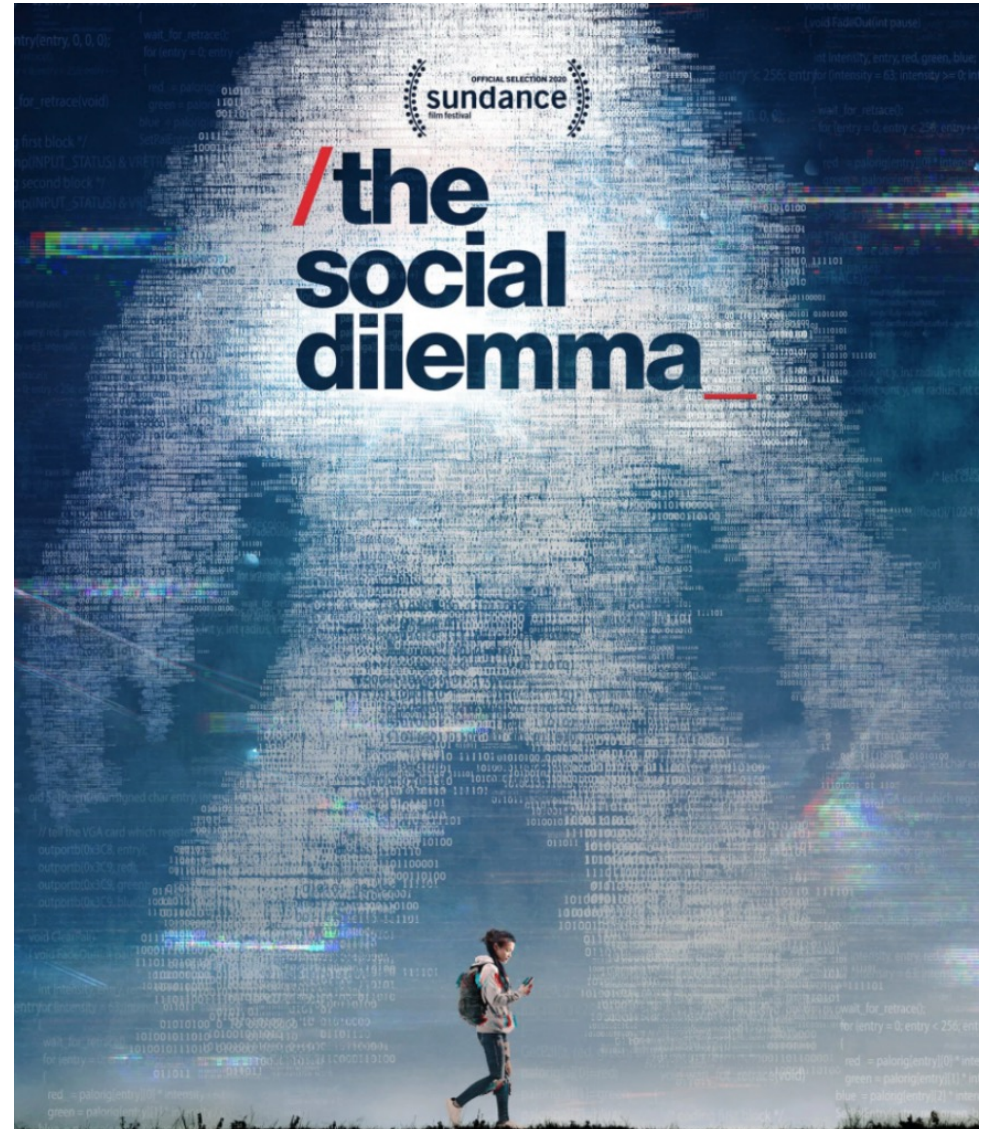


Informatieveilig
gedrag in de zorg

Nieuwe technologie komt met een nieuwe verantwoordelijkheid

Bij social media is het mis gegaan

Nu bij AI: wel reguleren: bijv EU AI Act



Ondertussen: hoe stabiel is Open AI?



• NIEUWE PODCASTAFLEVERING

Microsoft CEO Satya Nadella on the OpenAI Debacle
On with Kara Swisher

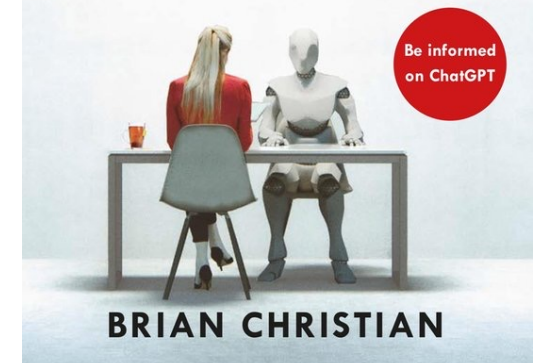
21 nov. · 30 min. 14 sec



'Vital reading. This is the book on artificial intelligence that we need right now' **Mike Krieger**, co-founder of Instagram

THE ALIGNMENT PROBLEM

How Can Artificial Intelligence
Learn Human Values?





AI And Machine Learning

Managing the Risks of Generative AI

by Kathy Baxter and Yoav Schlesinger

June 06, 2023



serggn/Getty Images



Wat doet chatGPT “zelf” aan informatieveiligheid?

ChatGPT

Tips for getting started

Ask away

ChatGPT can answer questions, help you learn, write code, brainstorm together, and much more.

Don't share sensitive info

Chat history may be reviewed or used to improve our services. Learn more about your choices in our [Help Center](#).

Check your facts

While we have safeguards, ChatGPT may give you inaccurate information. It's not intended to give advice.

Okay, let's go



www.informatieveiliggedragzorg.nl



De Wegwijzer ▾ Inspiratie Activiteiten Downloads Hulp en contact ▾ Over



Contact →



Het waarom

1

Vorbereiden



2

Doelgedrag bepalen



Probleem nader analyseren



Keuzelijst doelgedrag
opstellen



Doelgedrag kiezen



Doelgroep bepalen



Vorbereiden van de
meting

3

Gedragsfactoren
onderzoeken



0-meting doelgedrag

4

Interventies kiezen



5

Interventies uitvoeren



[Home](#) > Doelgedrag bepalen



Stap 2

Doelgedrag bepalen

Waarom

Doelgedrag (het gewenste gedrag dat je bij medewerkers zou willen zien) formuleren, schept duidelijkheid en eenduidigheid over wat de organisatie precies van medewerkers verwacht. Door het doelgedrag nauwkeurig te bepalen, weet je welk gedrag je wilt zien en maak je de beoogde verandering meetbaar. Het geformuleerde doelgedrag is de basis voor een scherpe gedragsanalyse en het ontwikkelen van een effectieve interventie.



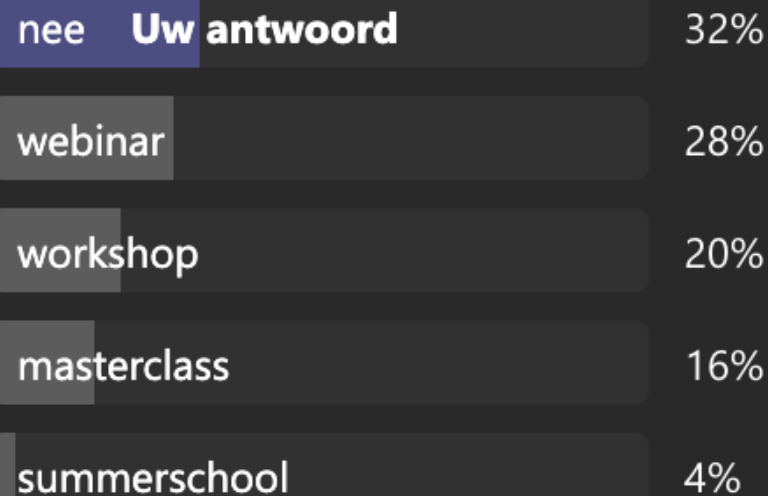
Met wie?



Vraag 4. Heb je al eerder deelgenomen aan een activiteit van IVGZ?

- Nee
- Webinar
- Workshop
- Masterclass
- Summerschool

Heb je al eerder deelgenomen aan een activiteit van IVGZ?





Zie onze methode: de wegwijzer: Wat is doelgedrag?

Gewenst gedrag dat je graag bij medewerkers zou willen zien om het probleem op te lossen of te verkleinen.



Waarom doelgedrag formuleren?

- Voor jezelf duidelijk maken wat je verwacht van medewerkers
- Basis voor ontwikkelen van effectieve interventies



Checklist doelgedrag

- ☐ Is het doelgedrag concreet geformuleerd? Wie moet wat precies doen?
- ☐ Is het geformuleerde doelgedrag te observeren?
- ☐ Kun je er één foto van maken?
- ☐ Zou je het doelgedrag kunnen voordoen, zodat anderen het kunnen nadoen?
- ☐ Is het doelgedrag positief geformuleerd?



Break-out 2 : Doelgedrag mbt LLM gebruik

- Wat betekent dat voor het doelgedrag?
- Zou je en huisregels willen opstellen?
Suggesties verzamelen

Suggestie van Sietske:
medewerkers melden het als ze een
LLM gaan gebruiken of willen gaan
gebruiken of al gebruiken

(ook omdat daar nu geen zicht op is)



Laten we het eens vragen aan... chatGPT!

SI You

huisregels voor medewerkers van een ziekenhuis voor het gebruik van chatgpt

 ChatGPT

Huisregels voor medewerkers van een ziekenhuis bij het gebruik van ChatGPT kunnen helpen bij het bevorderen van professioneel en verantwoordelijk gedrag. Hier zijn enkele suggesties:

1. **Vertrouwelijkheid en Privacy:**

- Vermijd het delen van gevoelige of vertrouwelijke patiëntinformatie via ChatGPT.
- Zorg ervoor dat alle gesprekken in overeenstemming zijn met de geldende privacywetgeving en het ziekenhuisbeleid.

2. **Nauwkeurigheid en Betrouwbaarheid:**

- Gebruik ChatGPT als aanvullend hulpmiddel en niet als enige bron van informatie.
- Corrigeer onjuiste informatie die door ChatGPT wordt verstrekt en raadpleeg altijd de officiële protocollen en procedures.

3. **Professioneel Taalgebruik:**

- Houd de communicatie professioneel en respectvol.
- Vermijd taalgebruik dat als beledigend, discriminerend of ongepast kan worden beschouwd.

Laten we het eens vragen aan... chatGPT !

beschouwd.

4. **Informed Consent:**
 - Zorg ervoor dat patiënten geïnformeerd zijn over het gebruik van ChatGPT in hun zorgproces.
 - Informeer patiënten over de beperkingen van kunstmatige intelligentie en benadruk het belang van menselijke validatie.
5. **Beheer van Gevoelige Onderwerpen:**
 - Wees voorzichtig bij het bespreken van gevoelige onderwerpen en zorg ervoor dat de informatie die wordt verstrekt, geschikt is voor de situatie.
6. **Toegang en Verantwoordelijkheid:**
 - Beperk de toegang tot ChatGPT tot geautoriseerd personeel.
 - Wijs verantwoordelijkheden toe voor het monitoren en beoordelen van de interacties met ChatGPT.
7. **Rapportage van Problemen:**
 - Meld eventuele technische of ethische problemen onmiddellijk aan de bevoegde autoriteiten binnen het ziekenhuis.
8. **Opleiding en Ondersteuning:**
 - Zorg voor voldoende training en ondersteuning voor medewerkers die ChatGPT gebruiken.
 - Blijf op de hoogte van updates en ontwikkelingen op het gebied van AI in de gezondheidszorg.
9. **Bewustwording van Beperkingen:**
 - Erken de beperkingen van ChatGPT en zoek menselijke expertise wanneer nodig, vooral in noodgevallen of kritieke situaties.
10. **Continue Evaluatie:**
 - Evalueer regelmatig het gebruik van ChatGPT in de klinische praktijk en pas de huisregels aan op basis van de ervaringen en feedback van medewerkers.



Huisregels omgang met LLMs in het MUMC+

Documentgegevens

Titel	Huisregels omgang met Large Language Models (LLMs) in het MUMC+
Werkgebied	<i>Kunstmatige intelligentie en gegevensbescherming</i>
Trefwoorden	<i>Kunstmatige Intelligentie KI Artificial Intelligence AI Large Language Model LLM ChatGPT Bard Gegevensbescherming AI-chatbot</i>



Samenvatting / Doel

Alleen invullen als dit een toegevoegde waarde heeft.

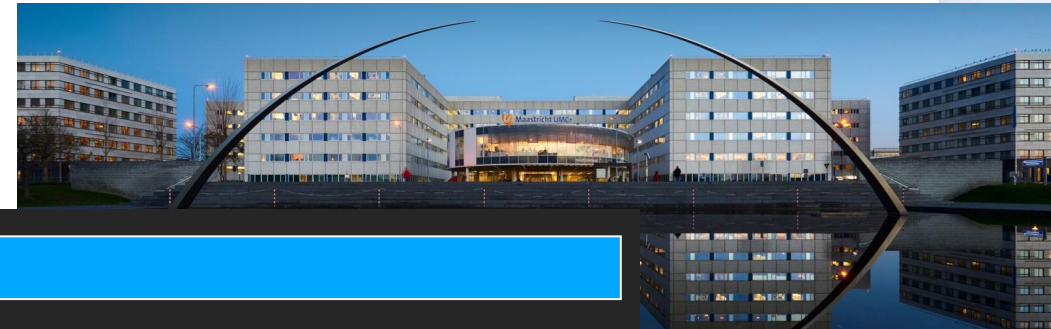
Doel huisregels:

- Ethisch en verantwoordelijk gebruik van LLMs, zoals ChatGPT.
- Duidelijk bepalen welk gedrag acceptabel is
- Duidelijkheid over de behandeling en bescherming van informatie bij het gebruik van LLMs.



Huisregels omgang met LLMs in het MUMC+

Opgesteld ter overbrugging naar landelijke richtlijnen



Aandachtspunten

Aandachtspunten kunnen o.a. zijn op het gebied van veiligheid, privacy, gegevensbescherming etc.

Bescherming van gegevens bij input

Controle op juistheid en interpretatie van de output

Voldoen aan geldende wet- en regelgeving

LLMs moeten altijd beschouwd worden als taalmodel, niet als kennismodel. Dit betekent bijvoorbeeld dat je ze niet kan inzetten voor het stellen van een diagnose, maar wel voor het herschrijven van jouw input.



Huisregels omgang met LLMs in het MUMC+

- Bescherming van privacy
- Bescherming bedrijfsgegevens
- Bescherming van je input: Settings -> Data controls -> Chat history & training
- Professionele controle op correctheid
- Compliance met nationale en internationale wet- en regelgeving



Huisregels omgang met LLMs in het MUMC+

Gezien er nog geen landelijke richtlijnen zijn is dit document opgesteld door een intern expert-panel.

Documentcoördinator:

Maïke Imkamp – projectleider AI voor Digitale Zorg (ZorgInnovatieLab / programma Digitale Zorg)

Auteur:

Maïke Imkamp – projectleider AI voor Digitale Zorg (ZorgInnovatieLab / programma Digitale Zorg)

Beoordelaars:

Guido Penders - stafadviseur, KIO Kwaliteit en Veiligheid

Astrid Brouwers - stafadviseur, KIO Kwaliteit en Veiligheid

Raimond Creusen - Kwaliteits Coördinator, MIT Kwaliteit Risicomanagement & Processen

Willem Hagenbeek - CISO, MIT Informatiebeveiliging

Catelijne Buursink - Functionaris Gegevensbescherming, KIO Kwaliteit en Veiligheid

Autorisator:

Karin Faber - Directeur, Kwaliteit Innovatie en Onderzoek



Communicatie van de huisregels LLM MUMC

- Lay-out en vormgeving huisregels optimaliseren: volgt
- Delen met geïnteresseerde ziekenhuizen:
- Posters ophangen: volgt
- Quizz: nu al: 1 quizzvraag per keer als pop-up



Workshop chatGPT voor medewerkers MUMC

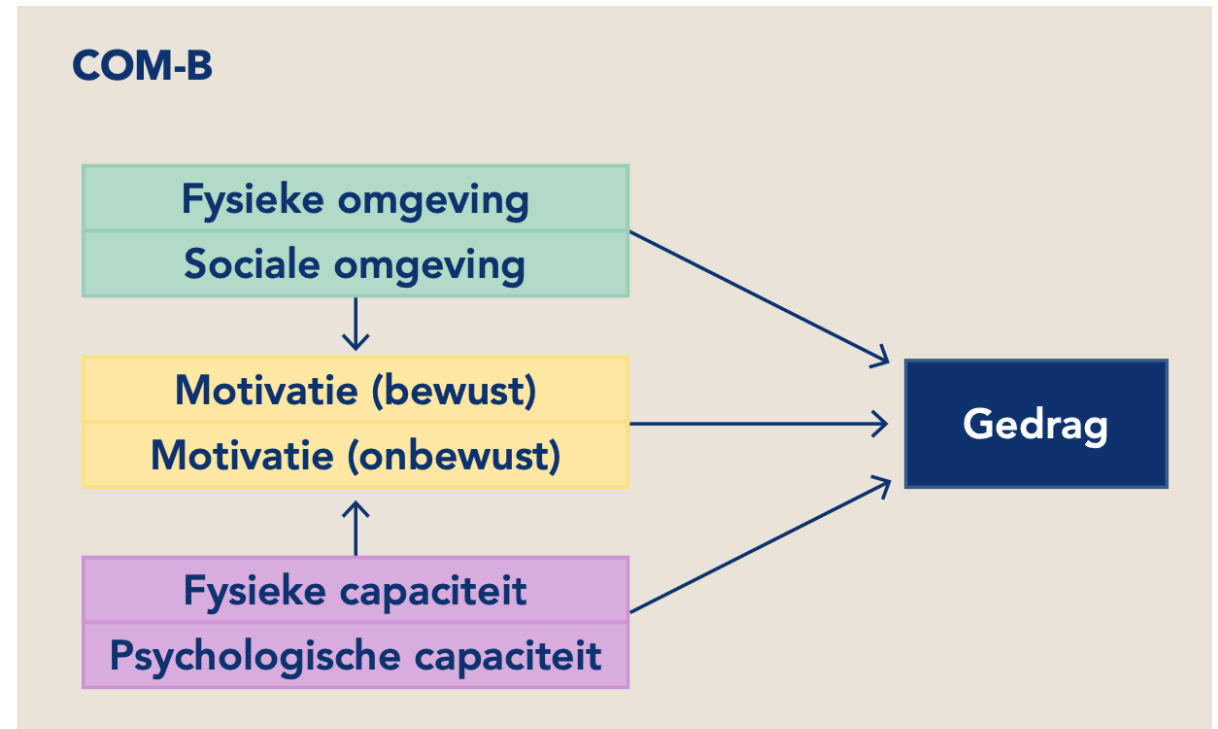
- Doel is om hen zelf te laten ervaren, zo zelf leren na te denken over de veiligheid van het gebruik
- Door meer kennis ook veiliger gebruik





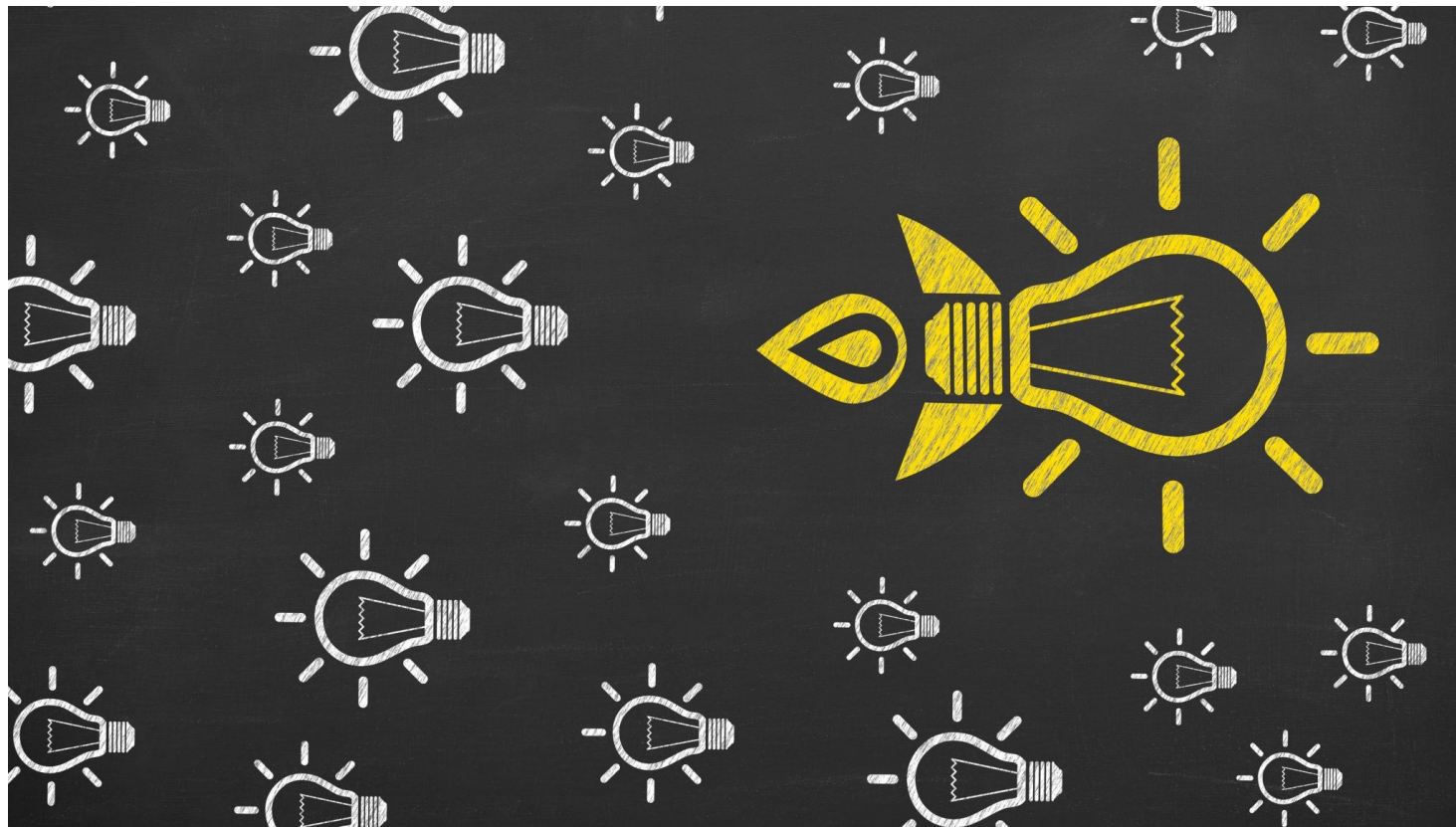
Workshop chatGPT voor medewerkers MUMC

- Doel is om hen zelf te laten ervaren, zo zelf leren na te denken over de veiligheid van het gebruik
- Door meer kennis ook veiliger gebruik





Aanvullende suggesties, vragen of opmerkingen





Break-out 3:

- Welke behoefte hebben jullie wat betreft toekomstige bijeenkomsten?
- Welke thema's of vraagstukken zouden jullie dan willen bespreken?
- In welke vorm?
- Andere ideeën / reflecties of suggesties?





Wat vond je van deze bijeenkomst?

- Vrije tekst



Zou je een collega aanraden mee te doen?

Zou je een collega aanraden
volgende keer deel te nemen?

ja **Uw antwoord** 100%

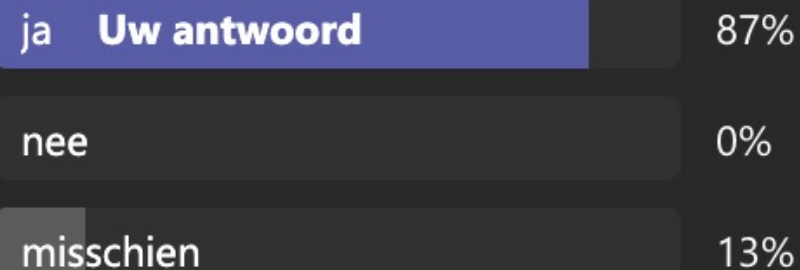
nee 0%

18 antwoorden



Zou je nu deel willen nemen aan een andere of volgende activiteit van IVGZ?

Zou je nu deel willen nemen aan een andere of volgende activiteit van IVGZ?



15 antwoorden



Wat doen we vanuit IVGZ tot nu toe en in 2024?

- Nieuw: toolkit veilig communiceren: zie website
- Nieuw: 2 x masterclass in 2024
- Nieuw: winterschool op 8 februari 2024: inschrijven is nu al mogelijk
- Nieuw: onze trainers zijn beschikbaar als sprekers op congressen/bijeenkomsten
- Nieuw: in gesprek met de bestuurders om zo meer draagvalk te creëren
- Nieuw: nieuwe doelgroep: huisartsen

