

FACTSHEET: Veilig werken met ChatGPT

Waarom is veiligheid zo belangrijk?

Veiligheid in de zorg is net als het dubbel op slot draaien van je voordeur: het beschermt waardevolle bezittingen, in dit geval de persoonsgegevens van patiënten. Het onzorgvuldig omgaan met namen en andere persoonlijke informatie kan leiden tot privacyinbreuken. Stel je voor dat gevoelige details van een patiënt per ongeluk openbaar worden; dit kan leiden tot grote persoonlijke en professionele schade, zowel voor de patiënt als voor jou als zorgprofessional. Denk aan identiteitsdiefstal, verstoring van de persoonlijke veiligheid van de patiënt, of zelfs juridische gevolgen voor jou of je organisatie. Het anonimiseren van patiëntgegevens is daarom geen overbodige voorzichtigheid, maar een essentiële stap om de integriteit en vertrouwelijkheid van medische zorg te garanderen.



Wat moet je weten om veilig te kunnen werken met ChatGPT?

Hoe staat jouw organisatie erin?

Laten we beginnen bij de allereerste check die je moet doen. Mag jij ChatGPT gebruiken van jouw organisatie? Er zijn organisaties die het gebruik ervan verbieden of juist stimuleren. In sommige organisaties moet je eerst een workshop hebben gevolgd, voordat je het mag gebruiken. Check hoe dit zit bij jouw eigen organisatie.

Wat valt er onder 'vertrouwelijke' informatie?

In de introductie heb je gelezen dat je niet zomaar alle gegevens met ChatGPT mag delen. Bepaalde informatie is vertrouwelijk, je kunt denken aan:

1. Bedrijfsgevoelige informatie. Dat zijn bijvoorbeeld gegevens waarvan je niet wilt dat concurrenten het in handen krijgen, zoals bedrijfsstrategieën of financiële gegevens.
2. Persoonsgegevens. Denk aan alles wat te herleiden is naar een persoon: namen, adressen, gezondheidsgegevens, noem maar op.



Hoe werkt het anonimiseren van gegevens?

Als je ChatGPT een vraag wilt stellen over een bepaalde cliënt/patiënt, is het belangrijk dat je alle persoonsgegevens vervangt door fictieve details. Verzin bijvoorbeeld namen en situaties die niet echt bestaan, maar wel helpen je vraag te formuleren. Dit verandert niets aan de kern van je vraag, maar beschermt de privacy van de cliënt/patiënt.



Wist je dat... je in jouw instellingen kunt aangeven dat OpenAI (de ontwikkelaar van ChatGPT) jouw gesprekken niet mag gebruiken om het taalmodel verder te trainen? Ga naar *instellingen > gegevensbeheer > 'Het model verbeteren voor iedereen'* zet je UIT.

Is alles wat ChatGPT zegt waar?

Nee! Niet alles wat ChatGPT zegt is waar. Misschien klinkt het raar, maar ChatGPT is er met name op getraind om een samenhangend verhaal te vertellen, los van of dit verhaal 100% kloppend is. Dat betekent voor jou het volgende:

- Neem nooit medisch advies aan van ChatGPT, maar zoek informatie bij een betrouwbare bron als Thuisarts.nl.
- Gebruik je gezonde verstand en dubbel check altijd zelf het antwoord wat ChatGPT geeft.
- Vraag in je prompt of ChatGPT je bronnen kan geven bij hetgeen wat hij schrijft.
- Stel samen met collega's richtlijnen op waaraan je wilt dat de antwoorden van ChatGPT voldoen. Je kunt bepaalde criteria formuleren en die in de in de prompt verwerken. Denk aan het verifiëren van de feiten en het afstemmen op bestaande zorgprotocollen.

Hieronder vind je een handige checklist!

Volg deze checklist voordat je ChatGPT gebruikt!

CHECK 1. Staat jouw organisatie het gebruik van ChatGPT toe?

Ja? Ga door naar stap 2!

Nee? Dan kun je ChatGPT helaas niet voor jouw werk inzetten.

CHECK 2. Gaat je vraag over medisch advies?

Ja? Gebruik dan geen ChatGPT. Zoek informatie op Thuisarts.nl of vraag een professional.

Nee? Ga dan door naar de volgende stap!

CHECK 3. Bevat je vraag (prompt) persoonlijke of gevoelige informatie

Ja? Vervang éérst alle persoonlijke of gevoelige informatie door fictieve details, voordat je je vraag aan ChatGPT stelt!

Nee? Dan ben je klaar om je vraag aan ChatGPT te stellen!

Teamopdracht

Maak tijd in een teamoverleg om te discussiëren over veilig werken met ChatGPT. Nodig eventueel een stafmedewerker uit die veel weet over privacy, of een ambassadeur rondom AI. Bespreek met elkaar: waar moet een antwoord van ChatGPT aan voldoen? Wanneer vinden jullie het antwoord van ChatGPT goed genoeg?

Probeer samen tot een lijst criteria te komen waarlangs jullie de antwoorden van ChatGPT kunnen leggen. Vergeet deze criteria niet te noemen in de prompt, zodat de chat weet waar hij rekening mee moet houden.

Deze factsheet is geüpdatet door Jet Zantvoord in december 2024 voor Digivaardig in de Zorg. Heb je opmerkingen of vragen over dit lesmateriaal? Mail dan naar info@digivaardigindezorg.nl.

Bronnen en afbeeldingen:

- ChatGPT-4
- Veiliginternetten.nl
- autoriteitpersoonsgegevens.nl

AAN DE SLAG MET DIGITALE VAARDIGHEDEN
FACTSHEET: VEILIG WERKEN MET CHATGPT

