



***Ga samen in gesprek.
Dat voorkomt een datalek.***

Hulpmiddel voor een goed gesprek en meer bewustwording



Inleiding

Een datalek kan iedereen overkomen: wat je functie ook is en hoe goed je bedoelingen ook zijn. Daarom is het belangrijk om stil te staan bij hoe het mis kan gaan en wat hiervan de gevolgen kunnen zijn.

In dit document tref je waargebeurde praktijksituaties aan*. Misschien denk je bij het lezen van de verhalen: wat heftig! Dat klopt. Door de realiteit niet mooier te maken dan deze is, stimuleren we bewustwording en gedragsverandering. Hopelijk helpen de verhalen iedereen in de zorg om het belang van informatieveiligheid écht te voelen. Door vervolgens met de quiz en opdrachten aan de slag te gaan, zetten we dat gevoel om in actie en zorgen we uiteindelijk voor een positieve, leerzame ervaring.

Niet elk voorbeeld zal precies aansluiten bij jouw eigen werksituatie. Toch is de kans groot dat er altijd minstens één situatie bij zit die herkenbaar is of inzichten biedt voor jouw dagelijkse praktijk. Verschillende zorgsectoren komen aan bod, zodat het geheel een breed en realistisch beeld schetst van de kwetsbaarheden in onze zorg.

Dit document is bedoeld ter ondersteuning van gesprekken en om bewustwording te vergroten. We adviseren om de verhalen altijd te koppelen aan een gesprek. Voor tips over hoe je de verhalen kan gebruiken, zie de volgende pagina.

*De personen op de foto's zijn niet de persoon van het voorbeeld.



Waarom dit document?

In de zorg werken we dagelijks met gevoelige informatie van cliënten, collega's en samenwerkingspartners. Een kleine onoplettendheid kan al leiden tot een datalek, met grote gevolgen voor de betrokkenen en de organisatie. Niet iedereen is zich bewust van de risico's. Dit document helpt om het eerlijke gesprek over informatieveiligheid in de organisatie te voeren en bewustwording van medewerkers te vergroten.

Wat staat er in dit document?

Dit document bevat sprekende voorbeelden van datalekken, gebaseerd op waargebeurde incidenten. Je kunt deze voorbeelden gebruiken als gespreksstarter. Zo maak je collega's bewust van de risico's van een datalek. Daarnaast bevat dit document meerdere quizvragen zodat je collega's op een speelse manier kan informeren over informatieveilig gedrag.

Hoe gebruik ik dit document?

- Plan een overleg van 15 minuten in
- Kies 2-3 herkenbare voorbeelden die aansluiten bij jullie dagelijkse praktijk
- Toon de voorbeelden en bespreek gevoelens en herkenning.
- Moedig openheid aan, ook bij twijfel of lage risicobeleving.
- Stel een van de quizvraag en ga in gesprek
- Maak het interactief met Kahoot, Mentimeter, Slido of briefjes.
- Sluit af met de vraag: wat nemen we hiervan mee?



“Ik verstuurde per ongeluk een medisch rapport naar een groepsmailadres, waardoor meer dan 100 mensen onbedoeld de gegevens van de patiënt kregen.”



Even dubbelchecken helpt fouten voorkomen.



“Ik keek met goede bedoelingen,
maar zonder toestemming, in een
cliëntendossier en dreigde
daardoor mijn baan te verliezen.”

Toestemming vragen kost amper tijd.
Het niet doen kan je je baan kosten.



"Wij verzamelden medicijndoosjes in een open inleverbak bij de balie. De stickers met namen, geboortedata en medicatiegegevens waren nog goed leesbaar. Een bezoeker maakte er foto's van en deelde deze op sociale media om 'aan te tonen hoe slordig we met gegevens omgaan'."



Gebrek aan zorgvuldigheid kan het vertrouwen schaden.
Bescherm privacy, elke dag.



“Ik liet mijn werktelefoon even op tafel liggen in de huiskamer. Bij terugkomst was de telefoon verdwenen, waarschijnlijk meegenomen door een cliënt. Op de telefoon stonden onbeveiligde contactgegevens van cliënten en collega's. Het datalek moest gemeld worden en leidde tot zorgen bij familieleden.”

Gegevens beschermen is geen extra taak.
Het hoort bij goede zorg.



“Tijdens het begeleiden van een training in de oefenzaal werd ik even weggeroepen.

Mijn computer stond nog aan, met het dossier van een van de deelnemers op het scherm. Andere cliënten zagen persoonlijke informatie zoals diagnose en behandelplan.

Een van hen diende een klacht in bij de practiceigenaar.”



De reputatie van jouw organisatie staat op het spel.
Laat zien dat gegevens bij jullie veilig zijn.



“Ik zette afspraken uit ons administratiesysteem in mijn privé-agenda om overzicht te houden. Daardoor kwamen cliëntgegevens in een onbeveiligde omgeving terecht. Bij een controle werd dit ontdekt en moest melding worden gedaan van een datalek. Ik kreeg een waarschuwing.”

Gegevens delen in een onbeveiligde omgeving is als een het roepen van een geheim in een volle zaal. Denk na waar en hoe je informatie deelt.



“Tijdens de zorgverlening aan een cliënt liet ik per ongeluk mijn werktabelt open op bed liggen, waarop het zorgplan van een andere cliënt zichtbaar was. Een familielid dat op bezoek was, las onbedoeld deze vertrouwelijke gegevens en sprak mij hierop aan. Dit leidde tot wantrouwen bij de familie.”

Een scherm vergrendelen kost een seconde.
Een scherm open laten kan wekenlange gevolgen hebben.



"Ik gaf per ongeluk een kennis toegang tot de WhatsAppgroep van werk. Pas na een week werd dit opgemerkt en de persoon verwijderd. In die periode zijn er foto's van een cliënt gedeeld en is een andere cliënt in de app besproken. Dit leidde tot een ernstig datalek."

Wat je deelt, zie je niet altijd meteen.
Wees kritisch op wie meekijkt en meeleest



"Ik vulde mijn gegevens in op een online tool die achteraf een phishingwebsite bleek te zijn. Hierdoor werd schadelijke software geïnstalleerd, wat ons volledige netwerk platlegde. Als gevolg daarvan konden mijn collega's dagenlang niet werken."

Gebruik alleen veilige software, apps en tools.
Zo bescherm je jezelf én je collega's.



“Ik opende een phishingmail en vulde mijn gegevens in. Hierdoor namen hackers mijn account over. Ze versleutelden gegevens en eisten losgeld. Ik moest afspraken afzeggen en behandelingen liepen vertraging op.”



Heb je twijfels over een mail?
Overleg met je collega, leidinggevende of ICT.



“Na een slecht-nieuwsgesprek liet ik mijn tas bij een cliënt liggen. Daarin zaten vertrouwelijke gegevens van andere cliënten. Hij maakte foto’s en dreigde ze online te zetten als we hem niet verder hielpen. Ik besepte niet dat zo’n kleine fout zulke grote gevolgen kon hebben.”

Let altijd op je spullen.
Een kleine misstap kan grote consequenties hebben.



“Ik gaf per ongeluk een kopie van het dossier van een kind mee aan andere ouders. Nu hebben de ouders van dat kind een rechtszaak tegen me aangespannen.”



Een kleine check voorkomt ellende.
Controleer altijd de ontvanger.



"Ik deelde per ongeluk het adres van een pleeggezin met de biologische ouders van een kind. Daardoor moest het pleeggezin verhuizen."



Controleer met wie je gegevens deelt.
Gevoelige info verdient extra zorg.



"Ik word bedreigd, omdat ik per ongeluk een dossier met de verkeerde persoon deelde."



Jouw veiligheid staat op het spel.
Check altijd naar wie je gegevens verstuurt.



"Ik gebruikte een openbaar Strava-profiel om mijn sportprestaties te delen met vrienden. Nu weet een forensische cliënt waar ik woon en stalkt hij me."



Kies je software en apps zorgvuldig.
Check de privacyinstellingen.

Vraag 1



Wat is het grootste risico van het opslaan van cliëntgegevens op een onbeveiligde privételefoon of in een persoonlijke app zoals een online agenda?

- A. De gegevens gaan verloren bij een update
- B. De gegevens zijn toegankelijk voor onbevoegden
- C. De medewerker raakt zelf het overzicht kwijt
- D. Er is geen risico zolang het om zorgafspraken gaat

Toelichting vraag 1



Correct antwoord: B.

De gegevens kunnen toegankelijk zijn voor onbevoegden

Volgens de Autoriteit Persoonsgegevens zijn onbeveiligde apps en cloudopslag belangrijke oorzaken van datalekken. In 2023 ging 34% van alle gemelde datalekken over onbedoelde verstrekking van gegevens aan derden. (Rapportage Datalekken Autoriteit Persoonsgegevens, 2023.)

Wil je meer weten over hoe je veilig om kan gaan met patiënt- en cliëntgegevens? Gebruik het hulpmiddel 'Veilig omgaan met patiëntgegevens' van het programma Informatieveilig Gedrag in de Zorg.

Vraag 2



Je laat per ongeluk een patiëntendossier openstaan op een computerscherm in een ruimte waar anderen hebben meegelezen. Wat zou je moeten doen?

- A. Niets doen, zolang niemand het lijkt te hebben gezien
- B. Direct afsluiten en hopen dat het niet nog eens gebeurt
- C. Het melden bij je leidinggevende en/of FG (functionaris gegevensbescherming)
- D. De cliënt zelf inlichten en verder niks ondernemen

Toelichting vraag 2



Correct antwoord: C.
Het melden bij je leidinggevende en/of FG

Zorginstellingen zijn wettelijk verplicht om mogelijke datalekken te beoordelen en zonodig te melden bij de Autoriteit Persoonsgegevens binnen 72 uur. Ook kleine fouten kunnen grote gevolgen hebben.

Wil je meer weten over wat een datalek is? En wanneer je een datalek moet melden? Gebruik het hulpmiddel 'Melden datalek' van het programma Informatieveilig Gedrag in de Zorg.

Vraag 3



Waarom is het risicovol om foto's van cliënten in een WhatsAppgroep te delen, zelfs als deze groep alleen voor collega's is?

- A. WhatsApp is niet populair onder zorgprofessionals
- B. Ook al versleutelt WhatsApp berichten, het is niet veilig
- C. Je hebt geen controle over wie screenshots of berichten doorstuurt
- D. Collega's mogen geen berichten buiten werktijd bekijken

Toelichting vraag 3



Correct antwoord: C.

Je hebt geen controle over wie screenshots of berichten doorstuurt

Hoewel WhatsApp end-to-end encryptie gebruikt, is het risico op hergebruik of onbedoeld delen groot. De AVG vereist dat gevoelige informatie alleen via goedgekeurde, beveiligde communicatiekanalen wordt gedeeld.

Wil jij meer weten over hoe je kan voorkomen dat je op de verkeerde manier gegevens deelt? Gebruik het hulpmiddel 'Veilig communiceren' van het programma Informatieveilig Gedrag in de Zorg.

Vraag 4



Hoe gaan hackers het meest te werk bij het binnendringen van systemen in de zorgsector?

- A. Door fysieke toegang tot zorginstellingen
- B. Via phishingmails waarin ze zich voordoen als collega of zorgpartner
- C. Door medische apparatuur te hacken
- D. Via de social media van cliënten

Toelichting vraag 4



Correct antwoord: B.

Via phishingmails waarin ze zich voordoen als collega of zorgpartner

Phishing is verantwoordelijk voor het merendeel van de cyberaanvallen in de zorg. Volgens Z-CERT wordt ruim 60% van incidenten veroorzaakt door phishing. Hackers gebruiken vaak urgente of vertrouwelijke onderwerpen om medewerkers tot klikken te verleiden. (Z-CERT, Incidentanalyse 2023)

Wil je meer weten over wat een datalek is? En wanneer je een datalek moet melden? Gebruik het hulpmiddel 'Melden datalek' van het programma Informatieveilig Gedrag in de Zorg.

Vraag 5



Wat heb je te doen als je vermoedt dat een cliënt vertrouwelijke informatie van een andere cliënt in handen heeft gekregen (bijv. door een vergeten tas of telefoon)?

- A. De cliënt direct aanspreken en vragen de gegevens te wissen
- B. Je leidinggevende informeren en het incident melden volgens protocol
- C. Niets, tenzij de cliënt iets dreigt te doen met de gegevens
- D. Een melding maken op intranet en het team informeren

Toelichting vraag 5



Correct antwoord: B.

De leidinggevende informeren en het incident melden volgens protocol

Volgens de AVG moet elk vermoeden van onrechtmatige toegang tot persoonsgegevens onderzocht en beoordeeld worden.

Wil jij meer weten over hoe je kan voorkomen dat je op de verkeerde manier gegevens deelt? Gebruik het hulpmiddel 'Melden datalek' van het programma Informatieveilig Gedrag in de Zorg.

Vraag 6



Je collega voert patiëntinformatie in een gratis AI-tekstassistent om sneller een behandelplan op te stellen. Wat is het risico hiervan?

- A. Geen risico, als de gegevens niet worden opgeslagen op de computer
- B. Een mogelijk datalek, omdat gevoelige informatie naar een externe partij wordt gestuurd
- C. Geen probleem, als de AI accurate adviezen geeft
- D. Alleen een risico als de patiënt expliciet bezwaar maakt

Toelichting vraag 6



Correct antwoord: B.

Een mogelijk datalek, omdat gevoelige informatie naar een externe partij wordt gestuurd

Wanneer persoonsgegevens, vooral privacygevoelige gegevens zoals medische gegevens, worden ingevoerd in publieke AI-tools zoals ChatGPT of Copilot, kunnen deze gegevens mogelijk worden opgeslagen of gebruikt voor trainingsdoeleinden. Dit vormt een risico op een datalek.

**Wil jij weten waar je aan moet denken bij het gebruik van AI-chatbots?
Gebruik het hulpmiddel 'Veilig gebruik van AI chatbots' van het programma
Informatieveilig Gedrag in de Zorg.**



Colofon

[Bekijk hier het hulpmiddel 'Veilig communiceren'](#)

[Bekijk hier het hulpmiddel 'Veilig omgaan met patiëntgegevens'](#)

[Bekijk hier het hulpmiddel 'Veilig gebruik van AI-chatbots'](#)

[Bekijk hier het hulpmiddel 'Melden datalek'](#)

Het hulpmiddel *Ga in gesprek. Dat voorkomt een datalek!* is een uitgave van het programma Informatieveilig gedrag in de zorg. Je mag het kosteloos gebruiken, fijn als je dan wel verwijst naar het programma.

Informatieveilig gedrag in de zorg is een programma van stichting ECP | Platform voor de Informatiesamenleving, in opdracht van het ministerie van Volksgezondheid, Welzijn en Sport (VWS).