Datalek gemeld? Leren is wat telt!

De toolkit Melden datalek bevat uitleg, tips en middelen om direct te starten

Informatieveilig gedrag in de zorg

Voorwoord

Als medewerkers van zorgorganisaties meteen in actie komen bij een datalek, blijft de schade beperkt. Ook leren we dan van datalekken en voorkomen we dat het nog een keer gebeurt. Zo werken we in de zorg continu aan informatie-veiligheid. Patiënten en cliënten moeten er immers op kunnen vertrouwen dat hun gegevens veilig zijn. Ook medewerkers willen dat organisaties zorgvuldig met hun persoonsgegevens omgaan.

Het is niet vanzelfsprekend dat een datalek wordt gemeld. Dat heeft verschillende oorzaken. Medewerkers...
- herkennen een datalek niet
- weten niet waarom het belangrijk is om een datalek te melden
- weten niet waar en hoe ze een datalek moeten melden.

Deze toolkit bevat verschillende praktische tools:
- **Voor medewerkers:** het meldproces. Dit maakt medewerkers bewust van de gevaren en laat zien wat ze moeten doen bij een (mogelijk) datalek.
- **Voor informatieveiligheidsprofessionals:** een voorbeeldproces. Wat moet je doen als je een melding van een (mogelijk) datalek ontvangt.
- **Template vragenformulier:** melden (mogelijk) datalek.

Deze tools zijn ook apart te **downloaden** op de website van het programma Informatieveilig gedrag in de zorg. Ook is hier een handige **animatie** te vinden die je met medewerkers in jouw organisatie kan delen. Deze kun je op de volgende pagina ook alvast bekijken.
We hopen dat deze tools jou en jouw collega's gaan helpen. Door het signaleren, melden en dichten van datalekken maken we de zorgorganisatie samen steeds veiliger!

"Door deel te nemen aan de werkgroep 'Melden Datalek' hebben we de mogelijkheid gehad om met diverse organisaties in het zorgveld (cure and care) te kijken naar de richtlijnen van AP en daar met zijn allen, mooie praktische tools voor op te zetten. Tools om collega's en medewerkers te informeren en tools die meer diepgang en richting bieden omtrent de werkwijze 'Melden Datalek' naar de Privacy Officers toe.

De onderlinge samenwerking, de ondersteuning vanuit en begeleiding van ECP hierin hebben wij als zeer waardevol ervaren. We hebben in een kort tijdsbestek, concrete en daadkrachtige slagen kunnen maken. Waar het AP informatie biedt, bieden deze ontwikkelde tools meer houvast, richting én dus advies.

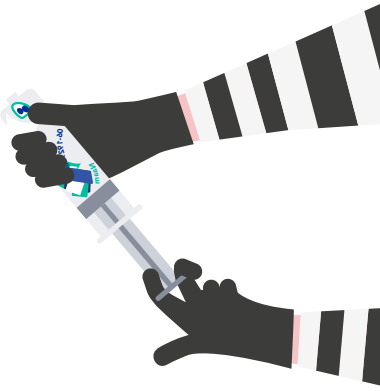
Hopelijk van waarde voor vele zorgorganisaties!"

Danique Arendonk-de Ruijter
Beleidsadviseur Kwaliteit & Veiligheid
Dé Provinciale Kraamzorg | Lunavi Kraamzorg

Agnes Verbruggen
Security Officer

Melden datalek

Datalek gemeld? Leren is wat telt!



START

Is dit een (mogelijk) datalek?

Voorbeelden

Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

Ja

Melden

Tip

Bij twijfel vraag je wie hier binnen jouw organisatie meer van weet.

Melden is eenvoudig en vraagt weinig tijd.

Waarom snel melden?

- je beperkt de gevolgen van het datalek
- we sporen kwetsbaarheden in proces, werkwijzen of systeem op
- we leren en verbeteren

Wat gebeurt er met je melding?

Mogelijke acties

Leren en verbeteren

De collega die jouw melding in behandeling heeft genomen zet acties uit om herhaling te voorkomen. Bijvoorbeeld een waarschuwing op het intranet of aanpassing van een werkproces of systeem.

Goed bezig! Veiligheid van persoonsgegevens staat voorop!

Voorbeelden van een datalek

Het zorgdossier inzien zonder dat er een behandelrelatie is.

Niet-versnipperde baxter-zakjes met alle patiënt- of cliëntgegevens in een open prullenbak.

Medische persoonsgegevens delen via WhatsApp en na gelezen te hebben vergeten te verwijderen.

Patiënt- of cliëntgegevens toevoegen aan het verkeerde dossier.

Phishing e-mails openen, op de link klikken en persoons-gegevens achterlaten.

Werktelefoon, laptop, tablet of usb-stick kwijtraken.

E-mail met medische persoonsgegevens met externe adressen in de cc in plaats van de bcc.

Sollicitatiebrieven weg-gooien bij het oud papier.

Patiënt- of medewerkers-gegevens bij de printer laten liggen.

Gegevens over een patiënt of cliënt op een (wegwerp) handschoen schrijven.

Terug naar figuur

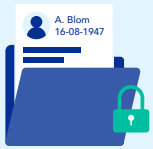
Mogelijke acties na melden datalek

Datalek melden bij de Autoriteit Persoonsgegevens.

Herstelacties uitvoeren.

Patiënt/cliënt of medewerker van wie persoonsgegevens zijn gelekt informeren.

Terugkoppeling aan de melder van het datalek en eventueel betrokken collega's.



Maatregelen nemen om werkwijze, proces of systeem te verbeteren om datalek in de toekomst te voorkomen.

Het registreren van een datalek in een datalekregister van de eigen organisatie is wettelijk verplicht. Noot: deze registratie is niet bedoeld voor sancties of dossieropbouw.

Analyseren en evalueren van (bijna) datalekken. Ook van verschillende ogenschijnlijk kleine incidenten wordt geleerd en kunnen acties worden genomen om een datalek in de toekomst te voorkomen.

Terug naar figuur

Voorbeeldproces Melden datalek

Datalek gemeld? Leren is wat telt!

START

1 Je ontvangt een melding van een (mogelijk) datalek

2 Beoordeel de melding

Tip
Bekijk de video van de Autoriteit Persoons-gegevens (AP)

3 Zijn er persoons-gegevens gelekt?

Nee

Ja

Is informatie gedeeld met een betrouwbare bron?

Ja → Geen melding aan AP

Grootschaligheid en gevoeligheid van gelekte data kan alsnog een reden zijn tot actie

Tip
Uitleg over (bijzondere) persoons-gegevens

Nee

4 Zijn er bijzondere persoonsgegevens gelekt?

Ja

Nee

5 Beoordeel de omvang van het datalek. Is het datalek grootschalig?

Ja

Nee

6 Lopen één of meer personen een groot (persoonlijk) risico door dit lek?

Ja

Nee

Maak eerste risicoinschatting voor afweging melden AP

Informeer:

- Betrokkene(n)
- Melder
- AP

Tip
Zo informeer je slachtoffers

Tip
Datalek: wel of niet melden. Autoriteit Persoonsgegevens

7 Neem acties om gevolgen datalek te beperken

8 Tref maatregelen om herhaling te voorkomen

9 Evaluëer afhandeling datalek en koppel terug aan de melder

GEREED

Template vragenformulier Melden (mogelijk) datalek

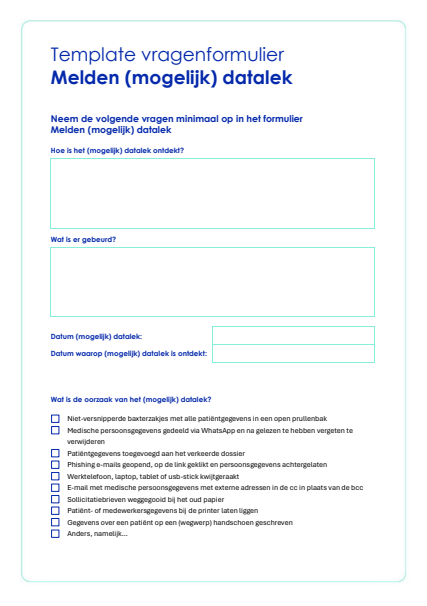
Gebruik van dit template
Dit template is een hulpmiddel voor de Informatieveiligheidsprofessional (IVP). De vragen in dit formulier zijn bedoeld als input om zelf een (digitaal) meld-formulier te maken. Kies de vragen die jij passend vindt bij jouw organisatie, meldproces en medewerkers.

Waarom deze vragen?
Zorgmedewerkers kunnen via dit formulier snel en eenvoudig een (mogelijk) datalek melden. En de IVP ontvangt voldoende en relevante gegevens om met de melding aan de slag te gaan.

Uitgangspunt is dat de gegevens van de melder (naam, emailadres, telefoon-nummer) door de digitale melding automatisch gegenereerd zijn. Dit wordt dus niet uitgevraagd.

Je kunt dit meldformulier met vragen beschikbaar stellen aan medewerkers op een passende manier in jouw organisatie. Bijvoorbeeld als digitaal formulier op intranet of via een ticketsysteem.

Download het formulier hier.


Template vragenformulier
Melden (mogelijk) datalek

Neem de volgende vragen minimaal op in het formulier Melden (mogelijk) datalek

Hoe is het (mogelijk) datalek ontdekt?

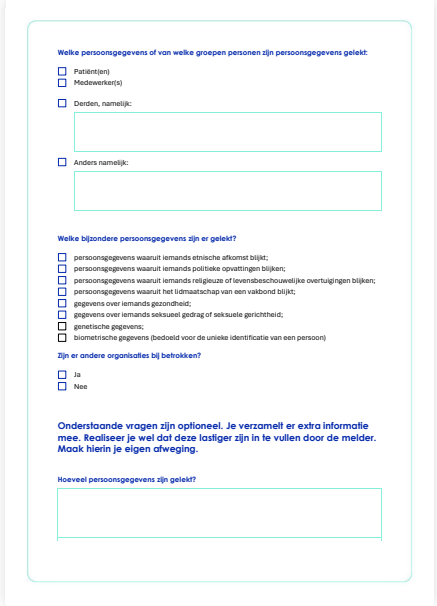
Wat is er gebeurd?

Datum (mogelijk) datalek:

Datum waarop (mogelijk) datalek is ontdekt:

Wat is de oorzaak van het (mogelijk) datalek?

- ☐ Niet-versnipperde baxterzakjes met alle patiëntgegevens in een open prullenbak
- ☐ Medische persoonsgegevens gedeeld via WhatsApp en na gelezen te hebben vergeten te verwijderen
- ☐ Patiëntgegevens toegevoegd aan het verkeerde dossier
- ☐ Phishing e-mails geopend, op de link geklikt en persoonsgegevens achtergelaten
- ☐ Werktelefoon, laptop, tablet of usb-stick kwijtgeraakt
- ☐ E-mail met medische persoonsgegevens met externe adressen in de cc in plaats van de bcc
- ☐ Sollicitatiebrieven weggegooid bij het oud papier
- ☐ Patiënt- of medewerkersgegevens bij de printer laten liggen
- ☐ Gegevens over een patiënt op een (wegwerp) handschoen geschreven
- ☐ Anders, namelijk...


Welke persoonsgegevens of van welke groepen personen zijn persoonsgegevens gelekt:

- ☐ Patiënt(en)
- ☐ Medewerker(s)
- ☐ Derden, namelijk:
- ☐ Anders namelijk:

Welke bijzondere persoonsgegevens zijn er gelekt?

- ☐ persoonsgegevens waaruit iemands etnische afkomst blijkt;
- ☐ persoonsgegevens waaruit iemands politieke opvattingen blijken;
- ☐ persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken;
- ☐ persoonsgegevens waaruit het lidmaatschap van een vakbond blijkt;
- ☐ gegevens over iemands gezondheid;
- ☐ gegevens over iemands seksueel gedrag of seksuele gerichtheid;
- ☐ genetische gegevens;
- ☐ biometrische gegevens (bedoeld voor de unieke identificatie van een persoon)

Zijn er andere organisaties bij betrokken?

- ☐ Ja
- ☐ Nee

Onderstaande vragen zijn optioneel. Je verzamelt er extra informatie mee. Realiseer je wel dat deze lastiger zijn in te vullen door de melder. Maak hierin je eigen afweging.

Hoeveel persoonsgegevens zijn gelekt?

Tips

- Zorg dat je volledig bent in het uitvragen van gegevens die je nodig hebt, zodat er geen extra gesprek of extra vragenlijst nodig is.
- Gebruikt je organisatie een ticketsysteem voor het melden van (mogelijke) datalekken? Vraag dan het ticketnummer uit op het formulier.
- Stel korte vragen. Het invullen moet voor de melder weinig tijd kosten en makkelijk zijn.
- Is het meldformulier geïntegreerd in een systeem? Onderzoek dan of het telefoonnummer en emailadres van de melder automatisch ingevuld kan worden (o.b.v. inlogaccount).
- Werk zoveel mogelijk met gesloten vragen of meerkeuzevragen (bijv. ja/nee, een lijst met aan te vinken van voorbeelden van datalekken).

Colofon

De toolkit Melden datalek is een uitgave van het programma Informatieveilig gedrag in de zorg.

Het programma Informatieveilig gedrag in de zorg wordt uitgevoerd door stichting ECP | Platform voor de Informatiesamenleving in opdracht van het ministerie van VWS. De brancheorganisaties ActiZ, de Nederlandse ggz, NFU, NVZ en VGN zijn bij het programma betrokken.

Gebaseerd op werkgroep methodiek Vliegwielcoalitie (digitale transformatie in de zorg).

Auteurs
Mariët de Waal, ECP | Platform voor de Informatiesamenleving
Bettine Pluut, ECP | Platform voor de Informatiesamenleving
Meelezer: Daan Brinkhuis, Z-CERT

Communicatie
Demi van Spronssen, ECP | Platform voor de Informatiesamenleving

In samenwerking met werkgroep Melden datalek

Hiske de Vries	Senior beleidsadviseur bij RAV Haaglanden
Pieter Jan Visser	CISO bij Zonnehuisgroep Amstelland
Monica Bassie	Privacy Officer bij Jong JGZ
Spencer Burger	Information Security Officer bij Antoni van Leeuwenhoek
Lisanne Reurings	Privacy Officer bij Antoni van Leeuwenhoek
Bianca Bogers	Information security officer bij GGZ Westelijk Noord Brabant
Sharon van den Hemel	Privacy Officer bij Korian
Petra Waelepoel	Ervaringsdeskundige patiëntenzorg
Hilde van Ras	Beleidsadviseur bij Laverhof
Marije Kraan	Communicatieadviseur bij Zozijn
Agnes Verbruggen	Security Officer bij Kempenhaeghe
Danique Arendonk-de Ruijter	Beleidsadviseur Kwaliteit & Veiligheid bij Dé Provinciale Kraamzorg	Lunavi Kraamzorg