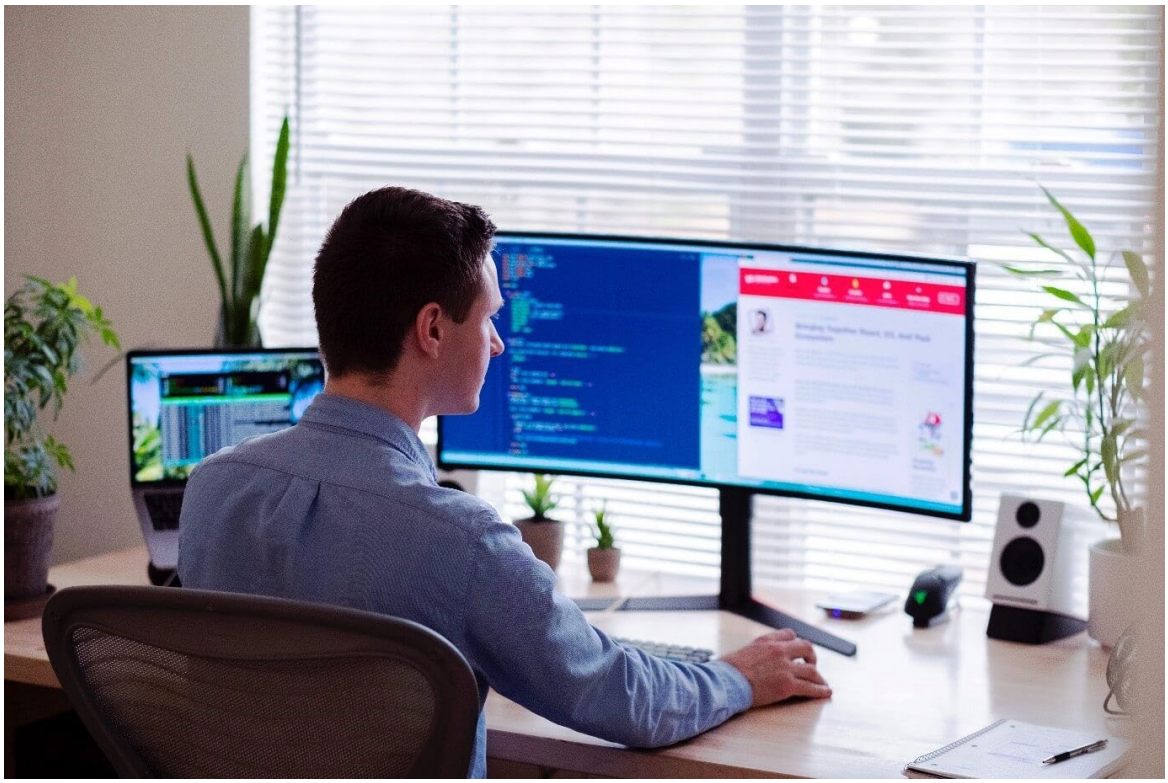


DATALEK IN DE ZORG

AAN DE SLAG MET DIGITALE VAARDIGHEDEN
TRAINING: INFORMATIEBEVEILIGING & PRIVACY

DIGIVAARDIG IN DE ZORG

Voorkomen van datalekken in de zorg

In de zorg wordt gewerkt met privacygevoelige persoonsgegevens die je niet zomaar met anderen mag delen. In het nieuws hoor je steeds vaker over het gevaar van een datalek. In 2020 kwamen bij de Autoriteit Persoonsgegevens de meeste datalekmeldingen (37% = 24.000) uit de sector gezondheid en welzijn. (Bron: AP, 2021)

Vaak wordt er gewaarschuwd over dreigingen van buitenaf: *phishing, hacking of ransomware*. Maar de meeste datalekken in de zorg hebben een interne oorzaak in plaats van inbreuk van buitenaf. (Bron: ICT&Health, 2019)

In dit werkblad ga je aan de slag met informatie over het voorkomen van datalekken in de zorg. Wat is een datalek? Wat kun je doen om dit te voorkomen? En wat moet je doen als er een datalek wordt geconstateerd. Je kunt dit werkblad alleen of samen maken.

Wat is een datalek?

Je spreekt over een datalek als de persoonsgegevens die je als zorgorganisatie verzamelt over cliënten en werknemers, onbedoeld onder ogen komen of in handen vallen van derden. Dat kan gebeuren door rondslingerende briefjes met persoonsgegevens erop. Of door een 'digitaal lek'.

Wat zijn persoonsgegevens? Onder persoonsgegevens valt alle informatie die direct of indirect naar een persoon te herleiden is.

Opdracht 1

Kruis aan wat persoonsgegevens zijn. De antwoorden kun je vinden aan het einde van dit werkblad.

☐ Locatiegegevens GSM	☐ Het ras van iemand	☐ Wachtwoord
☐ Browsergeschiedenis	☐ IP-adres	☐ Email

Verschil beveiligingsincident en datalek

Soms kan het voorkomen dat bepaalde informatie door een lek in de beveiliging onbedoeld naar buiten komt. Dit noem je een beveiligingsincident. Dat hoeft niet altijd te betekenen dat er ook een datalek ontstaat. Er is alleen sprake van een datalek als er bij het beveiligingsincident een aanmerkelijke kans bestaat dat persoonsgegevens verloren zijn gegaan of onrechtmatige verwerking van de gegevens niet redelijkerwijs is uit te sluiten.

Opdracht 2

Een beveiligingsincident hoeft dus niet altijd een datalek te beteken. Kruis hieronder aan in welke situatie er **wel** sprake is van een datalek. De antwoorden kun je vinden aan het einde van dit werkblad.

☐ **1)** Een brief met daarin cliëntgegevens wordt naar een verkeerd adres gestuurd. De brief wordt ongeopend retour gestuurd.

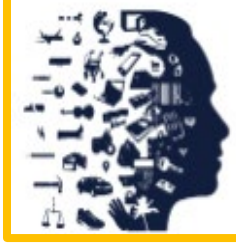
☐ **2)** Een cliënt vraagt om zijn of haar medicatielijst. Deze wordt uitgeprint en in een enveloppe meegegeven. Bij thuiskomst constateert de cliënt dat de medicatielijst van een andere cliënt is en meldt dit.

☐ **3)** Een zorgverlener is zijn of haar pas verloren waarmee kan worden ingelogd op een werkcomputer.

☐ **4)** Er is een werklaptop gestolen met gegevens van meer dan 200 cliënten. De laptop heeft een wachtwoord. Maar het bestand van cliëntgegevens is niet versleuteld.

De algemene verordening gegevensbescherming (AVG)

Het is wettelijk vastgelegd dat zorgprofessionals zorgvuldig om moeten gaan met privacygevoelige informatie van cliënten en/of patiënten. Juist nu veel informatie gedigitaliseerd wordt verzameld.



De zorgorganisatie waar jij werkt heeft een verantwoordingsplicht naar de Autoriteit Persoonsgegevens (AP) waarmee zij moeten kunnen aantonen dat de juiste technische en organisatorische maatregelen zijn genomen om de persoonsgegevens van cliënten te beveiligen.

Informatiebeveiliging in een organisatie is zo sterk als de zwakste schakel. Elke medewerker heeft daarom ook een verantwoordelijkheid om veilig te werken met persoonsgegevens. Bekijk de factsheet *Veilig thuiswerken* om een datalek vanuit huis te voorkomen.

TIP! de AVG-helpdesk voor Zorg, Welzijn en Sport heeft alle informatie op het gebied van AVG, privacy en datalekken op één website gebundeld. www.avghelpdeskzorg.nl

Wat moet je doen als je een datalek ontdekt?

Zorgorganisaties zijn verplicht om binnen 72 uur een **risicovolle** datalek te melden bij de AP. Voordat een melding wordt gedaan worden er intern een aantal stappen genomen. Bij iedere zorgorganisatie kan dat anders verlopen.

Opdracht 3

Je hebt een mail ontvangen van een collega met persoonsgegevens van een cliënt die jij niet kent. Kruis aan wat je hoort te doen.

1. Eerst mail ik ☐ **de collega /** ☐ **functionaris gegevensbescherming** wat er is gebeurd
2. Daarna ☐ **maak een printscreen van de mail /** ☐ **ik verwijder de mail direct**

Functionaris gegevensbescherming

Als jij als zorgprofessional een datalek vermoedt of ontdekt, meld je dit niet zelf bij het AP. Zorginstellingen en zorgorganisaties zijn verplicht om een functionaris gegevensbescherming (FG) aan te stellen. Deze persoon houdt toezicht op de toepassing en naleving van de Algemene Verordening Gegevens Bescherming (AVG) en maakt de afweging om een melding te maken bij het AP en/of de betrokkenen en gedupeerden op de hoogte te brengen.

Maar er zijn meer personen waar jij een datalek kunt melden. Per organisatie verschilt dit. Zoek uit hoe je de volgende personen kunt bereiken en vul de contactgegevens in.

Functionaris Gegevensbescherming	**Contactpersoon:** **Email:** **Telefoon:**
Leidinggevende	**Contactpersoon:** **Email:** **Telefoon:**
ICT service desk	**Contactpersoon:** **Email:** **Telefoon:**

Gevolgen van een datalek

In de zorg wordt gewerkt met persoonsgegevens en bijzondere persoonsgegevens die bij wet beschermd zijn zodat ieders recht op privacy is gewaarborgd. Wat zijn de gevolgen voor verschillende betrokkenen van een datalek?

Boete voor zorgorganisaties

Het niet, of niet op tijd, melden van een datalek bij de AP kan leiden tot een boete van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet. De AP mag de hoogte van de boete bepalen.

Deze zorgorganisaties kregen al eens een boete:

Boete orthodontiepraktijk vanwege onbeveiligde patiëntenwebsite
12.000 euro (10 juni 2021)

Boete OLVG voor slechte beveiliging patiëntendossiers
440.000 euro (11 februari 2021)

Boete HagaZiekenhuis voor slechte beveiliging patiëntendossiers
460.000 euro (16 juli 2019)

Imagoschade

Zorgorganisaties willen goede zorg leveren. Daar hoort het beschermen van persoonsgegevens ook bij. Voor een organisatie kan een datalek een enorme imagoschade aanrichten. Zijn mijn gegevens daar nog wel veilig?

Daarnaast kunnen de gelekte gegevens van de gedupeerden ook voor hen zorgen voor imagoschade. In een tijd waarin social media ontzettend groot is en nieuws als een snel vuurtje gaat, wil je niet dat jouw zorggegevens zo maar op het internet belanden.

Gijzelen van gegevens

Als het datalek komt door een inbreuk van buitenaf, een hack, dat kan het gebeuren dat de hackers vragen om losgeld. Het lijkt een ongeschreven regel onder hackers dat je zorginstellingen moet ontzien. Helaas is dat niet altijd het geval. Lees het gehele artikel via: https://tweakers.net/nieuws/181680/ransomware-aanvallers-ierse-zorg-eisen-losgeld-maar-premier-weigert-te-betalen.html

Ransomware-aanvallers Ierse zorg eisen losgeld, maar premier weigert te betalen

In de zaak van de ransomware-aanval op de Ierse publieke gezondheidsdienst is inmiddels losgeld geëist, maar Ierland zegt dat het niet van plan is om dat te betalen. Hoe groot het losgeldbedrag is, is niet bekend.

Dat standpunt is ingenomen door de Ierse premier Micheál Martin, zo schrijft Reuters. "We zijn er heel duidelijk in: we gaan geen losgeld betalen". Verder liet de *Director-general* van de Ierse *Health Service Executive* op de radio weten dat het om de Conti-ransomware zou gaan en tegenover Reuters meldde hij dat er een zeroday-kwetsbaarheid uitgebuit is. Ossian Smyth, de Ierse minister van *eGovernment*, omschrijft het als 'mogelijk de meest significante cyberaanval op de Ierse staat'.

Voorkomen is beter dan genezen

Natuurlijk hopen we dat je nooit betrokken raakt bij een datalek. En dat je door dit werkblad meer informatie hebt gekregen over het voorkomen van een datalek in de zorg.

We weten dat kennis en bewustwording niet altijd leiden tot verandering in gedrag. Je hebt weinig tijd en verstuurt een mail met cliëntgevens toch niet versleuteld naar een ketenpartner. Of je loopt zonder te denken naar de printer zonder jouw laptopscherm te vergrendelen. Normaal ben je altijd scherp op het checken van de afzender, maar je trapt nu toch in een phishingmail (hackers worden hier ook steeds beter in).

Informatieveilig gedrag in de zorg heeft een Wegwijzer *'Aan de slag met informatieveilig gedrag'* ontwikkeld. Hiermee kun je zelf aan de slag met het stimuleren van informatieveilig gedrag. Door deze werkwijze te volgen, kun je al snel stappen zetten richting een informatieveiligere organisatie. https://www.informatieveiliggedragzorg.nl/

De antwoorden van de opdrachten staan op de volgende pagina

Deze module is gemaakt door Xiomara Vado Soto voor Digivaardig in de Zorg in samenwerkeing met Daan Brinkhuis van 's Heerelenoo.

Heb je opmerkingen of vragen over dit lesmateriaal? Mail dan naar info@digivaardigindezorg.nl.

Antwoorden:

Opdracht 1
Wel persoonsgegevens: Locatiegegevens GSM, IP-adres, E-mail

Ras is een **bijzonder** persoonsgegeven en extra bescherm door de wet. Wachtwoord en browsergeschiedenis is niet direct te herleiden naar één persoon.

Opdracht 2

1) Is geen datalek, de brief is niet geopend teruggestuurd

2) Is wel een datalek, de cliënt heeft de medicatielijst van een ander kunnen bekijken

3) Dit is geen datalek als de kan worden bewezen dat er na verlies van pas niet mee is ingelogd en pas wordt geblokkeerd.

4) Dit is wel een datalek, ondanks dat de laptop een wachtwoord heeft valt onrechtmatige verwerking van gegevens niet uit de sluiten omdat deze niet vergrendeld zijn.

Opdracht 3

1. Functionaris gegevensbescherming (je kunt jouw collega daarna op de hoogte stellen van de fout)
2. Verwijder de mail direct (tenzij de FG anders adviseert)