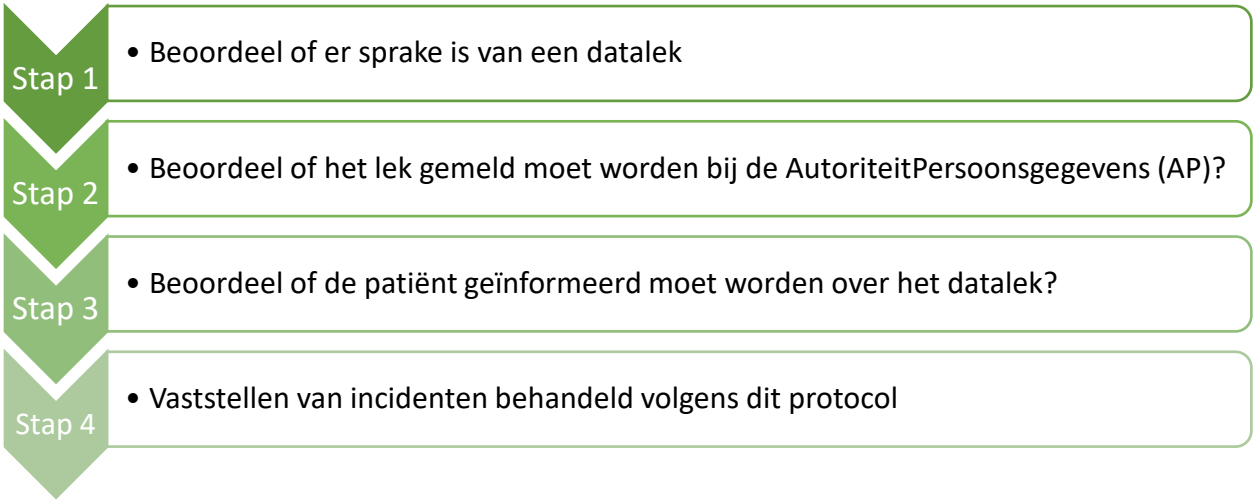
Protocol Datalek melden Praktijk voor Fysiotherapie Michelle Schut

Doel: weten wanneer een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) en de patiënt en weten waar we de behandeling van een (potentieel) datalek bewaren in de praktijk.

Eerste Hulp bij datalekken

Een datalek betekent dat er persoonsgegevens waar wij verantwoordelijk voor zijn, door onbevoegden zijn ingezien of verloren zijn gegaan. Sinds 1 januari 2016 is er een wet van kracht die in zulke gevallen om adequaat handelen vraagt.

Bij een vermoeden van een datalek bestaat ons protocol uit 3 stappen.



Stap 1; beoordeel of er sprake is van een datalek

Beoordeel of er sprake is van een datalek, bij bijv. de volgende beveiligingsincidenten:

- Diefstal van een laptop
- Verlies van een USB stick
- Verlies van een mobiele telefoon
- Gestolen (papieren) patiëntendossier
- Onjuiste adressering van e-mail of post
- Inzien van persoonsgegevens door onbevoegde
- Open papiercontainer met daarin persoonsgegevens
- Archiefopslag waar onbevoegden persoonsgegevens inzien
- Datacenter waar een lek in de beveiliging ontstaat

•

Datalek	Geen datalek
•Sprake van inbreuk op de beveiliging •Persoonsgegevens zijn verloren gegaan •Wij kunnen niet uitsluiten dat persoonsgegevens onrechtmatig zijn verwerkt (in verkeerde handen zijn gekomen)	•Geen insprake van inbreuk op de beveiliging •Wij kunnen redelijkerwijs uitsluiten dat de persoonsgegevens onrechtmatig zijn verwerkt

Niet ieder beveiligingsincident is ook een datalek. Als er alleen sprake is van een zwakke plek in de beveiliging is het een beveiligingslek en niet een datalek. Dat wordt niet gemeld, maar wel aangepakt.

Er is sprake van een datalek als er bij het beveiligingsincident een aanmerkelijke kans bestaat dat persoonsgegevens verloren zijn gegaan of als onrechtmatige verwerking van de persoonsgegevens niet uitgesloten kan worden.

Stap 2; melden bij het AP?

Als er patiëntgegevens zijn gelekt, moeten we binnen 72 uur melden bij de AP. Bij twijfel ook. Ten onrechte niet melden kan leiden tot hoge boete.

> Als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens moet melden wij dit aan de AP

De melding moet gedaan worden door de verantwoordelijke, bij ons is dat de huisarts: dit kan via meldloket datalekken AP: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage

Dus melden als:

- Persoonsgegevens van gevoelige aard zijn gelekt, bijv medische gegevens van een patiënt
- Gebruikersnamen, wachtwoorden en andere inloggegevens zijn gelekt
- Gegevens die iemand kunnen identificeren zijn gelekt (bv kopie ID en het BSN)

Hiervan is ook sprake als

- Er per persoon veel persoonsgegevens zijn gelekt
- Er ingrijpende beslissingen genomen worden op basis van gegevens (met financiële gevolgen voor de patiënt)
- De persoonsgegevens binnen een keten worden gedeeld

Wat wordt er gemeld?

De volgende informatie wordt verstrekt:

- De aard van de melding (eerste melding of vervolg op eerdere melding)
- Het wettelijk kader voor deze melding (AVG)
- Algemene informatie en contactgegevens

- Gegevens over het datalek

Beveiligingslekken worden bijgehouden met de ondernomen acties om die in te toekomst te voorkomen

- Naar aanleiding van het datalek getroffen vervolgacties
- Informatie over het inlichten van patiënten
- Getroffen technische maatregelen
- Internationale aspecten
- Of er nog een vervolgmelding zal volgen

Stap 3; melden aan de patiënt?

Als er patiëntgegevens zijn gelekt moeten we de patiënten ook onverwijld informeren. Zij kunnen zo nodig maatregelen nemen om zich te beschermen tegen de gevolgen van het datalek.

Volg het stroomschema op de volgende pagina om te zien of er wel of niet gemeld moet worden.

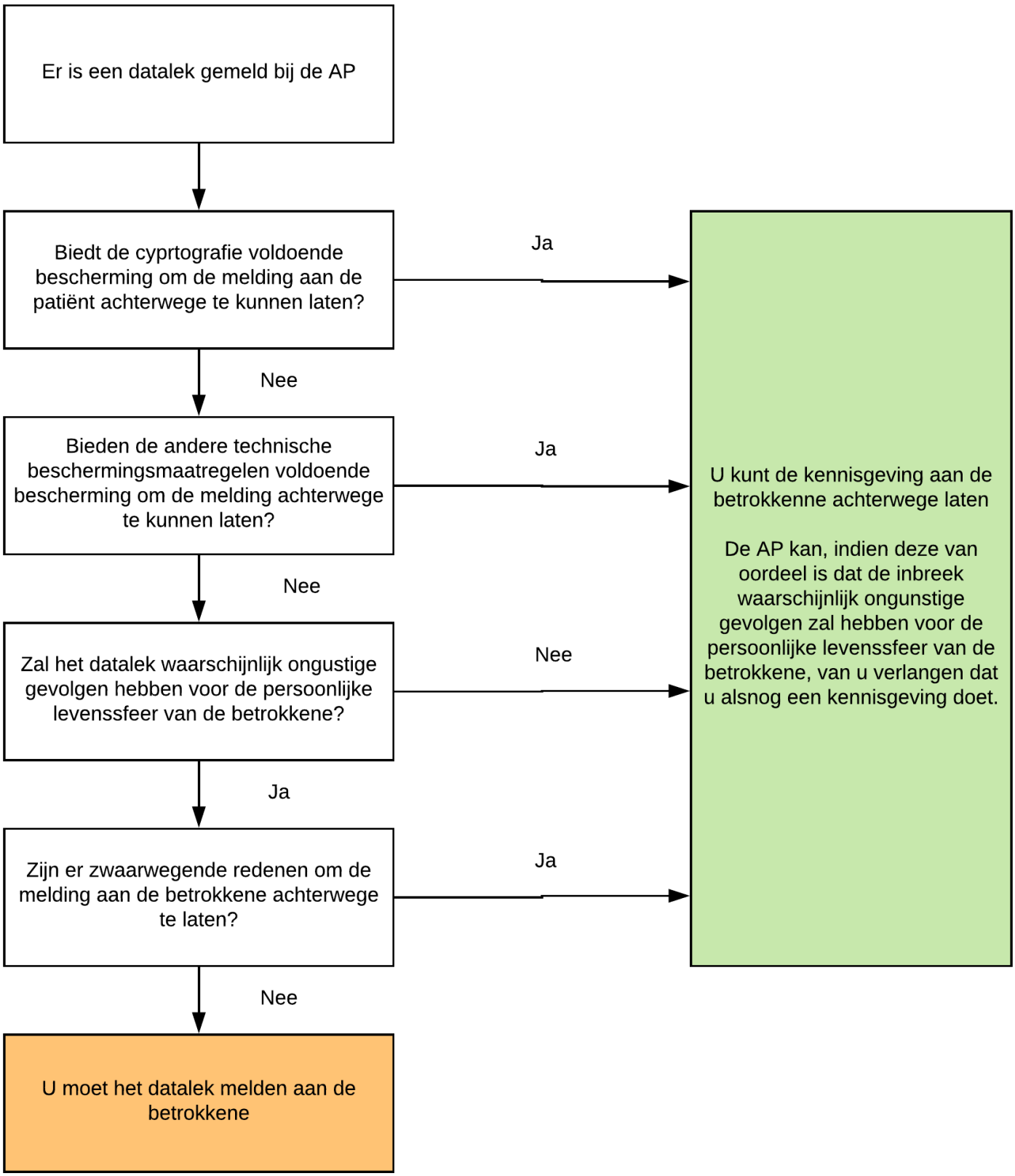
Wat wordt er gemeld?

Een melding aan patiënt bevat:

1. Informatie over wat er aan de hand is:
   Leg in duidelijke en eenvoudige taal uit wat er aan de hand is en wat mogelijk gevolgen voor hen kunnen zijn. Neem daarin mee:
   - Om wat voor soort datalek gaat het; zijn er gegevens in handen van onbevoegden gekomen, verloren gegaan of iets anders?
   - Wat is er precies gebeurd?
   - Staat het vast dat er gegevens zijn gelekt? Is het zeker dat “mijn” gegevens gelekt zijn?
   - Wat voor soortgegevens zijn er gelekt: “gewone” (NAW) gegevens of “gevoelige” gegevens (medisch, BSN)?
   - Van hoeveel personen zijn gegevens gelekt?
   - Uit welke bestanden zijn gegevens gelekt?
   - Wat voor misbruik zou iemand van de gelekte gegevens kunnen maken
   - Hoe groot is het risico dat dit ook echt gebeurt?
   - Welke maatregelen zijn getroffen om de eventuele nadelige gevolgen te beperken?
   - Welke maatregelen zijn er getroffen of worden voorgenomen om het datalek te verhelpen?
2. Informatie over waar patienten terecht kunnen met vragen:
   → Bij de huisartspraktijk
3. Informatie over wat patienten zelf kunnen doen:
   → Informeer wat zij in aanvulling op de al genomen acties zou kunnen doen. Bijvoorbeeld: het wijzigen van een wachtwoord.

Stap 4; bijhouden beveiligs- en datalekken

Vul het formulier 'bijlage protocol datalek' in. Deze is te vinden op onze gedeelde schijf in het mapje privacy. Sla het ingevulde formulier op in hetzelfde mapje.



Gebaseerd op: *Handreiking Meldplicht datalekken in de eerstelijns zorg* (LHV-NHG-INEEN-KNMP) jan 2017