Handreiking meldplicht datalekken in de eerstelijns zorg

Deel 1: Schema "Wat te doen bij een datalek in de eerstelijns zorg?"

	Een datalek wil zeggen dat er vanuit of binnen uw praktijk persoonsgegevens van patiënten (data) op straat zijn gekomen, 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. De eerste reactie bij een vermoeden van een datalek bestaat uit 3 stappen.		
1	**Beoordeel of er echt sprake is van een datalek**	Er is sprake van een datalek als door een inbreuk op de beveiliging, vertrouwelijke gegevens verloren kunnen zijn gegaan. Of als niet uitgesloten is dat deze door onbevoegden zijn verwerkt, binnen of buiten de beschermde omgeving van de praktijk of van de service provider.	Voorbeelden:[1] een USB-stick of pc op straat,[2] UZI-pas met pincode kwijt,[3] inbreuk door een hacker,[4] diefstal van dossiers,[5] fout van een medewerker.[6] Ook kan een andere (zorg)partij of gegevensbewerker melden dat uw gegevens zijn gelekt.[7]
2	**Beoordeel of u het lek moet melden bij de Autoriteit Persoonsgegevens (AP)**	Als er patiëntgegevens zijn gelekt, moet u dat binnen 72 uur na het bekend worden ervan melden bij de AP. Bij twijfel meldt u ook; u kunt een melding later altijd weer intrekken. Ten onrechte niet melden kan leiden tot hoge boete.	U meldt een datalek via het Meldloket Datalekken van de AP: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
3	**Beoordeel of u uw patiënten moet informeren over het lek**	Als er patiëntgegevens zijn gelekt moet u uw patiënten ook onverwijld informeren. Zij moeten zo nodig maatregelen kunnen nemen om zich te beschermen tegen de gevolgen van het datalek.	U informeert uw patiënten (individueel of in combinatie met algemene voorlichting) over de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en de maatregelen die u de betrokkene aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken, zoals het veranderen van gebruikersnamen en wachtwoorden. De aard van de inbreuk mag u algemeen omschrijven. U vermeldt uw contactgegevens zodat de betrokkene u kan bereiken als hij of zij vragen heeft over het datalek.

[1] In de volgende voetnoten verwijzen we naar de casuïstiek in deel 3 van deze handreiking: 'Overzicht cases datalekken'.
[2] Vgl. casus nr. 12, 13.
[3] Vgl. casus nr. 23.
[4] Vgl. casus nr. 11, 21
[5] Vgl. casus nr. 13.
[6] Vgl. casus nr. 1 t/m 7, 23.
[7] Vgl. casus nr. 10, 21.