Titel	**: Datalekken**
Type document	: Procedure voor HCT en ECT
Versie	: 1.0
Doelgroep	: werkzame personen HCT en ECT
Datum vaststelling	: 19-09-2018
Datum laatste evaluatie	: 10-02-2022
Herzieningsdatum	: 10-02-2023
Beheerder	: Martijn Leeflang / Tim van Tuil

Doel:
Weten wanneer er sprake is van een datalek en wat moet je in dat geval moet doen.

Doelgroep:
Alle medewerkers, inhuur en derden

Definities:
Datalek: Met een 'datalek' doelen we in deze toelichting op het lekken van persoonsgegevens van patiënten. Dit kunnen zowel geautomatiseerd verwerkte persoonsgegevens zijn, maar ook persoonsgegevens die op papier staan.

FG: Functionaris Gegevensbescherming

Taken, verantwoordelijkheden, bevoegdheden:
De verwerkingsverantwoordelijke (praktijkhouder) van persoonsgegevens is altijd verantwoordelijk voor het melden van een datalek aan de Autoriteit persoonsgegevens. De FG is verantwoordelijk voor juiste advisering en informatie. Iedere medewerker is verantwoordelijk om een beveiligingsincident te melden via de VIM procedure.

Van alle beveiligingsincidenten kunnen we leren. Door beveiligingsincidenten te melden kunnen we leren wat er misging en acties inzetten om deze te voorkomen. Hierdoor kunnen wij ervoor zorgen dat kleine incidenten in de toekomst geen grote incidenten worden. Het is dus belangrijk dat alles wat mis gaat te melden via ons VIM systeem.

Mocht het incident een datalek zijn dan moet dit gemeld worden aan de Autoriteit Persoonsgegevens. De praktijkmanager meldt dit in overleg met de Manager geïntegreerde zorg en/of de FG van de HAP.

Melden Datalekken
Onderstaand poster geeft aan wat je wel en niet moet melden. Wat moet je als medewerker melden via de VIM procedure? Dat is alles waarvan er sprake is van vernietiging, verlies, wijziging of delen van persoonsgegevens zonder dat dat de bedoeling was. Bij twijfel hierover gewoon altijd melden. Een datalek hoeft niet per se opzettelijk te zijn, zoals bij hacking. Er kan ook sprake zijn van onopzettelijke datalekken, bijvoorbeeld als persoonsgegevens per abuis worden gedeeld met de verkeerde persoon. Het hoeft daarbij niet te gaan om persoonsgegevens van duizenden mensen, een datalek kan ook betrekking hebben op slechts één persoon. Zie voor voorbeelden datalekken: Bijlage 1.

Wij zijn verplicht een verwerkersovereenkomst te sluiten met onze verwerkers. Als er bij onze verwerker een datalek plaatsvindt met betrekking tot de gegevens die hij voor ons verwerkt, dan moet hij dit aan ons melden. En wij weer melden aan de Autoriteit Persoonsgegevens.

Patiëntrisico’s en datalekken
Wanneer persoonsgegevens niet op een behoorlijke en zorgvuldige manier zijn verwerkt of langer worden bewaard dan noodzakelijk of als de beveiliging van gegevens niet deugt, kan informatie letterlijk op straat komen te liggen.

Evaluatie
De effectiviteit van het protocol wordt middels een interne audit getoetst.
Bijlage 1: Voorbeelden van datalekken

Brief/ mail of pakketje naar verkeerde ontvanger
Een brief (verwijs, afspraken) bevat meestal persoonsgegevens; het bevat immers informatie die specifiek bedoeld is voor de ontvanger. Een dergelijke brief kan per ongeluk naar de verkeerde persoon worden gestuurd. Die persoon kan, zonder enige kwaad in de zin te hebben, de brief openen omdat hij denkt dat de inhoud voor hem is bestemd. In dat geval is er sprake van een datalek. Immers, persoonsgegevens zijn toegankelijk gemaakt voor iemand die daar geen toegang toe mocht hebben. Dit geldt trouwens ook voor een e-mail naar de verkeerde ontvanger.

Let wel, als een brief naar de verkeerde ontvanger wordt gestuurd, maar ongeopend retour komt, dan is dat geen datalek. De persoonsgegevens in de brief zijn namelijk niet openbaar of toegankelijk gemaakt, aangezien de brief niet is geopend.

Persoonsgegevens bij het oud papier
Werk je veel met persoonsgegevens op papier, dan zou het zomaar kunnen dat je bepaalde documenten niet meer nodig hebt en bij het oud papier gooit. Echter, zet je dat oud papier aan de straat of breng je het weg naar het milieupark, dan zou het zomaar kunnen zijn dat het (onbedoeld) in de verkeerde handen valt. Zelfs als dat niet gebeurt is er nog steeds sprake van een datalek, de persoonsgegevens zijn namelijk openbaar toegankelijk gemaakt.

Werk je met persoonsgegevens op papier dan altijd een (gecertificeerde) shredder of een papiervernietigingsbedrijf gebruiken. Of neem andere maatregelen om ervoor te zorgen dat persoonsgegevens niet letterlijk op straat komen te liggen.

Persoonsgegevens op oud apparaat
Heb je een nieuwe laptop, smartphone of welk ander apparaat dan ook, zorg er dan voor dat de gegevens op het oude apparaat volledig worden verwijderd als je het apparaat weg doet. Het mag namelijk niet zo zijn dat een ander die het apparaat, al dan niet kwaadwillend, in gebruik neemt en allerlei vertrouwelijke gegevens kan inzien. Ook hier geldt weer, het feit dat er persoonsgegevens op een oud apparaat staan dat jij niet meer onder je hebt is al een datalek, tenzij je kunt aantonen dat de gegevens écht niet toegankelijk zijn. Hint: enkel een wachtwoord op het apparaat is daarvoor niet genoeg.

Persoonsgegevens delen met verkeerde ontvanger
Er kan ook sprake zijn van een datalek *binnen* een organisatie/praktijk op het moment dat persoonsgegevens van een medewerker worden gedeeld met een andere medewerker, die geen inzage mocht hebben. Bijvoorbeeld het verkeerde arbeidscontract wordt aan een medewerker gegeven.

Een ander voorbeeld is wanneer een persoon/patiënt zijn recht op inzage in de persoonsgegevens die wij van hem verwerken verzoekt. Jij moet verifiëren dat die persoon recht op inzage heeft. Met andere woorden, als Pietje verzoekt om inzage van zijn gegevens, dan moeten wij ervoor zorgen dat het ook echt Pietje is waar je inzage aan verleent en niet per ongeluk Jantje die zich voordoet als Pietje.

Apparaat met persoonsgegevens kwijtraken
Bijvoorbeeld verlies/diefstal van laptop.

Een onherstelbaar defect apparaat
Als je geen back-ups maakt van je gegevens en het apparaat waarop je de gegevens verwerkt stopt permanent met werken, dan is er sprake van een datalek. De gegevens zijn weliswaar voor niemand toegankelijk, maar ze zijn ook niet meer beschikbaar. Mensen kunnen in dat geval dan bijvoorbeeld hun rechten met betrekking tot hun persoonsgegevens niet meer uitoefenen.

Sleutel voor versleutelde gegevens is verloren
Een goede manier om gegevens te beveiligen is om ze te versleutelen. Op dat moment worden de gegevens een reeks cijfers en letters die nietszeggend zijn. Alleen als je de sleutel hebt kun je de gegevens inzien. Echter, raak je de sleutel kwijt, dan kan je niet meer bij de gegevens. Anderen ook niet natuurlijk, maar feit blijft dat de gegevens dus onbeschikbaar zijn en dat is ook een datalek.

Toegang door ongeautoriseerde partij
De afdeling/praktijk gaat verhuizen naar een mooier en groter pand. De inboedel, inclusief archiefkasten met allerlei persoonsgegevens, worden verhuisd door een professioneel bedrijf. De volgende dag trekt een ander bedrijf in je oude kantoor en komt erachter dat de verhuizers één archiefkast zonder slot zijn vergeten te verhuizen. Of het nieuwe bedrijf in die archiefkast heeft gekeken of niet, maakt op dat moment niet meer uit. Het feit dat die gegevens beschikbaar waren voor dat nieuwe bedrijf maakt het al een datalek. Dit geldt ook voor eventuele ander huurders of bedrijven, praktijken in hetzelfde pand. Kunnen zij bij jullie persoonsgegevens?