SAFE OF ZEEF?

Nieuwe wetgeving moet

‘Zolang ik niet gehackt word, is er niets aan de hand’. Misschien hebben wel meer huisartsen deze gedachte. Maar ze vergissen zich. De nieuwste wijziging van de Wet bescherming persoonsgegevens verplicht u namelijk om zogenaamde *datalekken* te melden op straffe van behoorlijke boetes. Misschien een reden om de praktijkvoering nog eens kritisch door te lichten?

ROELF NORG
ROELFNORG@MEDITTA.NL

Huisartsen zijn verwerkers van persoonsgegevens en vallen dus onder de regelgeving van de Wet bescherming persoonsgegevens. De huisarts dient deze persoonsgegevens te beveiligen, zodat ze niet verloren gaan of in handen (of onder ogen) van onbevoegden komen. Gebeurt dit tóch, dan spreekt men van een datalek. Zo’n datalek dient sinds 1 januari jongstleden gemeld te worden aan de Autoriteit Persoonsgegevens (AP), het vroegere College bescherming persoonsgegevens.

Extra zorgvuldigheid

De wet heeft betrekking op geautomatiseerde en niet-geautomatiseerde gegevens die in een bestand zijn opgenomen (zoals het papieren archief). Persoonsgegevens zijn gegevens waarmee iemand geïdentificeerd kan worden, direct (naam) of indirect (bijvoorbeeld ‘twaalfjarige jongen met leukemie’). De wet benoemt enkele soorten bijzondere persoonsgegevens. De voor de huisarts belangrijkste zijn gegevens over gezondheid, ras en seksueel leven. Het verwerken hiervan vereist extra zorgvuldigheid.

Potentiële datalekken

Waar zijn dit soort gegevens te vinden? Als eerste denkt elke huisarts waarschijnlijk aan zijn HIS. Deze vormt immers de administratieve spil van de praktijk. Maar er zijn meer plekken waar persoonsgegevens worden geregistreerd. In een boekhoudprogramma, waarin declaraties en bankoverschrijvingen worden verwerkt. In een spreadsheet voor het bijhouden van passanten, overledenen en nieuwingekomenen. Maar denk ook aan de spirometer, het ecg-apparaat, de 24-uursbloeddrukmeter en de fotocamera voor de teledermatologie. Al deze apparaten kunnen persoonsgegevens opgeslagen hebben (bijvoorbeeld het ecg of spirogram dat van een naam of geboortedatum is voorzien of een herkenbare foto).

Overal veilig?

Hoe veilig is de website? Welke gegevens zijn zichtbaar als er online afspraken gepland worden? Hoe is de beveiliging van e-mailconsulten geregeld? Maar ook: de onlinegegevensuitwisseling via programma’s voor ketenzorg, teleconsultatie en patiënt-zelfmanagement. Er zijn steeds meer websites waarop patiënt én huisarts medische gegevens delen. Hoe is de beveiliging hiervan geregeld?
Werkt de huisarts thuis? Hoe logt hij in op de praktijk? Gebruikt hij ASP (*application service provider*) of een VPN-programma (*virtual private network*)? En hoe zijn de inlogcodes en wachtwoorden beveiligd (automatisch invullen)? Wordt de privé-e-mail gebruikt om bestanden met patiëntgegevens over te sturen (benchmarkcijfers of indicatoren)? (Zie ook *SynthesHis* 2013, nummer 3.)

u extra alert maken

De aios neemt video-opnames mee voor beoordeling en nabespreking. De coassistent downloadt wellicht patiëntgegevens voor de stageopdracht. De diëtiste vindt het handig om 'even' enkele medicatieoverzichten mee te nemen, enzovoort.

Datalekken

De wet gebruikt het woord 'datalek' zelf niet, maar spreekt over een 'inbreuk op de beveiliging van de persoonsgegevens', waardoor er persoonsgegevens verloren zijn gegaan of onrechtmatig verwerkt (lees: in verkeerde handen zijn gevallen). De Autoriteit Persoonsgegevens noemt als concrete voorbeelden van datalekken een kwijtgeraakte usb-stick, een gestolen laptop, een inbraak door een hacker, een malware-besmetting en een calamiteit in een datacentrum, zoals een brand.[1]

Maar denk ook aan de niet goed opgeschoonde usb-stick van de coassistent of de computer die naar de afvalverwerking gebracht is of een tweede kans heeft gekregen in een schoolklas; de video-opname van de aios die op de harde schijf van de huisartsopleiding is terechtgekomen; de gedeelde cloud-opslag van privégegevens, waaronder zich het overzicht van de indicatoren bevindt; de 'lege' back-up die pas wordt ontdekt als de harde schijf gecrasht is.

Het zijn voorbeelden van onachtzaamheid, criminaliteit en domme pech. Geen voorbeelden van opzet of duidelijke schuld. Toch verwacht de wet actie.

Wie is verantwoordelijk?

Verantwoordelijk voor de goede beveiliging van de persoonsgegevens is de huisarts of (ook) de eventuele bestuurder in een gezondheidscentrum. Veel huisartsen maken gebruik van een waarnemer of gedetacheerde praktijkondersteuner en hebben mensen in opleiding. Ze laten huurders toe tot de praktijk, zoals een diëtiste of podotherapeut. Het is dan verstandig een clausule op te nemen in de waarneem-, opleidings-, huur- of detacheringsovereenkomst waarin plichten ten aanzien van het voorkomen en rapporteren van datalekken door de externe medewerker zijn opgenomen.

Maatregelen ter voorkoming van datalekken

De verwerker van persoonsgegevens moet zorgen voor 'preventieve, detectieve, repressieve en correctieve' maatregelen. Hij moet datalekken voorkomen, vroegtijdig signaleren en de schadelijke gevolgen beperken.

Hij wordt ook geacht bij de Autoriteit Persoonsgegevens melding te maken van een datalek en 'correctieve' maatregelen te nemen om nieuwe problemen te voorkomen. Er wordt hiermee dus een gesloten kwaliteitscirkel verwacht.

Bewerkersovereenkomst

In het kader van de meldplicht datalekken in de Wet bescherming persoonsgegevens, die op 1 januari in werking is getreden, bent u als gebruiker verantwoordelijk voor het aangaan van een bewerkersovereenkomst met de HIS-leverancier. Uw gebruikersvereniging kan deze taak van u overnemen door een relatie te leggen tussen de mantelovereenkomst en deze bewerkersovereenkomst. Atlas is met Promedico zo goed als klaar om dit te realiseren en start dit proces met CGM op. Waarschijnlijk zullen andere gebruikersverenigingen een soortgelijke strategie volgen.
Zo blijkt dat uw gebruikersvereniging er is om u, met zo min mogelijk inspanning, een goede en verantwoorde positie te geven richting uw softwareleverancier en daarmee aan uw verplichting te voldoen, zonder dat u zelf actie hoeft te ondernemen. U blijft zelf binnen de praktijk verantwoordelijk voor het voorkomen, registreren en melden van eventuele datalekken.

Leo van Rooijen (vrooijen@hagrozwijndrecht.nl)
voorzitter gebruikersvereniging Atlas

Met de billen bloot

Tijdens de evaluatie van de Wet bescherming persoonsgegevens is vastgesteld dat er sprake is van een maatschappijbreed 'nalevingstekort'. Op twee manieren moeten beheerders van persoonsgegevens worden gestimuleerd om werk te maken van privacybescherming, die ik de 'billen-bloot'- en de 'gebrande billen'-sancties zou willen noemen. 'Billen-bloot' betekent dat de mensen van wie de gegevens in een 'gelekt' bestand waren opgenomen persoonlijk geïnformeerd moeten worden. U zult dus bijvoorbeeld uw patiënten moeten laten weten dat er uit uw praktijk een computer met patiëntgegevens gestolen is. De term 'gebrande-billen' slaat op 'de dreigende en afschrikwekkende werking van een bestuurlijke boete', die 'node werd gemist'.[2] De maximale boete is opgehoogd van 4.500 euro naar 810.000 euro (of 10% van de omzet van bv's). De gemiddelde huisartsenpraktijk zal zo'n hoog boetebedrag niet gauw opgelegd krijgen.

Maar duidelijk is wel dat de regering met deze bepaling een serieus signaal wil afgeven. Wel erkent de minister dat een datalek zich ook kan voordoen als de persoonsgegevens adequaat beveiligd zijn. Dan is een boete vanwege het datalek zelf niet aan de orde. Wél kan een boete worden opgelegd voor het niet melden van het datalek aan de AP en aan de gedupeerden (meestal zullen dat de patiënten zijn).[3] Zo kan een verloren usb-stick u toch nog duur komen te staan.

Voorkom problemen

Er zijn diverse manieren waarop datalekken kunnen ontstaan. De juridische gevolgen kunnen groot zijn. Het is van belang om de praktijk nog eens door te lopen op de mogelijke risico's en hier en daar de afspraken nog eens aan te scherpen. Dat kan veel problemen voorkomen. ■

Roelf Norg is huisarts in Haelen en jurist

BRONNEN

1. Autoriteit Persoonsgegevens. De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) – Beleidsregels voor toepassing van artikel 34a van de Wbp. (via https://www.cbpweb.nl/, geraadpleegd d.d. 17-12-2015)
2. Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid. Tweede nota van wijziging. Kamerstuk 33662 nr. 9. (https://zoek.officielebekendmakingen.nl/kst-33662-9.html, geraadpleegd d.d. 17-12-2015)
3. Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid. Memorie van Antwoord. Kamerstuk 33662 nr. C. (https://zoek.officielebekendmakingen.nl/kst-33662-C.html, geraadpleegd d.d. 17-12-2015)