Tekst: Daan Marselis
Beeld: Shutterstock

Meldplicht datalekken

Met de Wet meldplicht datalekken kunnen praktijkhouders niet langer achteroverleunen als het om informatiebeveiliging gaat. Ze moeten een actieve houding aannemen, anders riskeren ze een boete.

De Wet meldplicht datalekken, die op 1 januari 2016 in werking treedt, verplicht zorgprofessionals een melding te doen bij de Autoriteit Persoonsgegevens als de beschikbaarheid en veiligheid van persoonsgegevens in het geding is geweest. Dat kan gaan om een kwijtgeraakte usb-stick met patiëntgegevens, een gestolen laptop of inbraak in het ict-systeem door een hacker. Het gaat niet alleen om digitale gegevensdragers. Ook medische dossiers die door het raam van een geparkeerde auto te lezen zijn, geeltjes met persoonsgegevens die op monitors hangen en bezorglijsten die bij de prullenbak achter de apotheek rondslingeren gelden als een potentieel lek.

Omdat patiëntgegevens voor de continuïteit van bedrijfsvoering en dienstverlening essentieel zijn, is er ook sprake van een datalek wanneer deze gegevens door bijvoorbeeld brand in een datacentrum niet meer beschikbaar zijn. “Het niet beschikbaar zijn van het dossier is namelijk direct van invloed op de patiëntenzorg”, zegt VvAA’s compliance officer Anton Belt die er vanuit zijn functie voor zorgt dat VvAA zich aan geldende wet- en regelgeving houdt. “Zorg dus voor een back-up.”

In sommige gevallen moet het datalek ook aan de betrokkene worden gemeld, bijvoorbeeld bij mogelijk ongunstige gevolgen voor diens persoonlijke levenssfeer. Denk aan stigmatisering als medische gegevens op straat komen te liggen.

Logboek

Zorgverleners moeten alle incidenten in een logboek gaan bijhouden, zegt Belt. Voor zover bekend is dat logboek vormvrij. De praktijkhouder noteert wat is voorgevallen, hoe het heeft kunnen gebeuren, of hij stappen heeft gezet om het een volgende keer te voorkomen en waarom hij het incident wel of niet aan de toezichthouder of betrokkene meldt.

De richtlijnen voor het melden waren bij het ter perse gaan van dit magazine nog niet vastgesteld. Kijk voor actuele informatie op de site van het College Bescherming Persoonsgegevens, de voorganger van de Autoriteit Persoonsgegevens.

Deze nieuwe autoriteit kan forse boetes opleggen. Hoewel dat afschrikwekkend klinkt, zeggen Belt en zijn collega security officer Paul van de Berg, die bij VvAA verantwoordelijk is voor onder meer informatiebeveiliging, dat praktijkhouders niet hoeven te panikeren. Hebben zorgverleners (en andere ondernemers) de beveiliging van hun data op orde en gaan ze zorgvuldig met patiëntgegevens om, dan zal de autoriteit niet snel een boete uitdelen. Doel van de meldplicht is vooral om zicht te krijgen op aard en omvang van incidenten. Op basis van die informatie zal de autoriteit ook best practices opstellen. Bovendien is informatiebeveiliging helemaal niet zo moeilijk als het klinkt. “Met kleine ingrepen kun je de beveiliging snel naar een hoger niveau tillen”, zegt Van de Berg.

Hardnekkige misverstanden

Dat moet praktijkhouders als muziek in de oren klinken. “Velen vinden informatiebeveiliging namelijk een ver-van-mijn-bedshow”, zegt Hossein Seyed Nabavi, een afgestudeerd medicus die zorgprofessionals bewust wil maken van het belang van informatiebeveiliging. Sinds 2009 is zijn Stichting Informatiebeveiliging Gezondheidszorg (IBGZ) actief. “Talloze hardnekkige misverstanden omgeven het begrip informatiebeveiliging”, verzucht Nabavi. Naast bewustwording wil hij met zijn stichting ook de beveiliging van gegevens makkelijker maken.

Een paar misverstanden wil Nabavi daarom meteen ontkrachten. Zo gaat het niet alleen om bescherming van de privacy van patiënten. Anno 2015 is informatie cruciaal voor de zorgverlening en bedrijfsvoering. De informatie moet dus altijd beschikbaar zijn, anders komen kwaliteit en continuïteit in gevaar. Voor veilige informatieverwerking is geen diepgaande technologische kennis noodzakelijk. “Je hoeft geen automonteur te zijn om veilig auto te kunnen rijden”, zegt Nabavi. “Evenmin hoef je een ict-er te zijn om de gegevens van je patiënten goed te beschermen. Het gaat om organisatie en techniek.”

Bij organisatorische veiligheid gaat het bijvoorbeeld om goede afspraken met medewerkers. “Zorg ervoor dat na kantooruren de dossierkasten zijn afgesloten, dat patiëntendossiers niet rondslingeren op bureaus en er geen geeltjes met patiëntgegevens op monitors zijn geplakt. In de avonduren komt namelijk de schoonmaker en die kan dat allemaal lezen. Huisartsen die visite rijden, moeten eventuele papieren patiëntendossiers uit het zicht leggen of ten minste met de tekst naar beneden op de bijrijdersstoel, zodat ze niet te lezen zijn door passanten. Praktijkhouders geven hun medewerkers ieder een eigen gebruikersnaam en wachtwoord. Anders hebben ontslagen of anderszins vertrokken medewerkers nog altijd toegang tot de gegevens. En een tweede internetlijn kan de kans op storingen aanzienlijk verkleinen.”

Nabavi roept zorgprofessionals ook op om goede bewerkersovereenkomsten af te sluiten met softwareleveranciers. Vroeger hadden praktijken de patiëntgegevens in eigen beheer. Die stonden op een server in de gangkast. Tegenwoordig staan de gegevens vaak in datacentra van de leverancier van het informatiesysteem. Belangrijk is dat er afspraken worden gemaakt over geheimhouding, het actief signaleren van datalekken door de leverancier, het beveiligen van gegevens, in hoeverre medewerkers van de leverancier toegang hebben tot de patiëntendossiers, wat er gebeurt bij faillissement van de leverancier en wie aansprakelijk is als gegevens lekken of niet beschikbaar zijn.

Bij technische veiligheid gaat het bijvoorbeeld om het gebruik van een firewall en systemen die up-to-date zijn. En hier wordt het meteen een stuk moeilijker, zegt huisarts Adriaan Mol die tevens voorzitter is van NedHIS, de koepelorganisatie van gebruikersverenigingen van huisartsinformatiesystemen. “De individuele huisarts komt er nooit achter of de leveranciers van zijn informatiesysteem (HIS) en zijn business intelligence systeem volledig veilig werken. Er zijn geen keurmerken voor en ga maar eens controleren of zo’n bedrijf de gegevens echt wel direct na verwerking van zijn servers verwijdert.”

Er is ook sprake van een datalek wanneer gegevens niet meer beschikbaar zijn

Toch zijn er wel waarborgen, stelt hij. “Informeer daartoe bij de gebruikersvereniging. Die laat de bewerkersovereenkomsten opstellen door juristen die er verstand van hebben. En wij van NedHIS bevragen de leveranciers ook op veiligheid, maar we sturen geen specialist naar binnen om het echt te controleren.”

Financiële gevolgen

Ook VvAA’ers Belt en Van de Berg wijzen erop dat absolute veiligheid niet te garanderen is. “Waar gewerkt wordt, kan een datalek ontstaan”, zegt Belt. “De wetgever eist vanaf nu vooral een actieve houding. Het gaat erom dat je uit kunt leggen wat je allemaal hebt gedaan om de data van je patiënten te beschermen.” Financiële gevolgen van datalekken kunnen sinds kort verzekerd worden via een speciale cyberverzekering, zoals ook VvAA aanbiedt. “Die verzekering helpt tevens bij het herstellen van schade”, zegt Belt.

Van de Berg stelt dat informatiebeveiliging maatwerk is. Aan grote praktijken en ketens worden hogere eisen gesteld dan aan de fysiotherapeut op de hoek. “Benader het onderwerp vanuit een risicoperspectief”, zegt hij. “Is de ict op orde, hoe staat het met de beveiliging van het pand, zijn de collega’s geïnstrueerd hoe ze met patiëntgegevens moeten omgaan? Het gaat om goed vaderschap en inzet van de middelen die je tot je beschikking hebt.”

Meer informatie

vvaa.nl/cyber; College Bescherming Persoonsgegevens: cbpweb.nl; Stichting IBGZ: ibgz.nl