Nieuwe wet gegevensbescherming

Privacyschending patiënt strenger bestraft

Privacy is een groot goed. Zeker in de zorg willen patiënten dat hun gegevens beschermd en beveiligd zijn. Bestaande wetgeving voor bescherming van persoonsgegevens wordt vanaf 25 mei vervangen door de Europese privacywet, de Algemene Verordening Gegevensbescherming (AVG). Op datalekken staan strenge sancties.

Tekst Loek Kusiak

Geen branche waar partijen zoveel gevoelige persoonsgegevens uitwisselen als in de zorg. Hierdoor kent de sector een hoog risico op privacyschendingen. De zorg was in 2017 verantwoordelijk voor bijna 30 procent van de meldingen bij de Autoriteit Persoonsgegevens (AP) over datalekken. Daarvan was driekwart te herleiden op een persoonlijke fout van een medewerker.
"Een datalek kan het gevolg zijn van een computerhack. Maar wat ook als datalekken worden aangemerkt zijn het niet maken van een back-up van patiëntgegevens, het doorsturen van een e-mail naar de verkeerde personen of het in de trein laten liggen van een zorgplan met patiëntgegevens. En op datalekken staan boetes." Aan het woord is Peter Schell, voorzitter van de Stichting Privacyzorg, een non-profitorganisatie die circa duizend geabonneerde zorgaanbieders – huisartspraktijken, apothekers, ziekenhuizen - helpt bij het beschermen van patiëntgegevens en te laten voldoen aan Europese wetgeving inzake de 'Algemene Verordening Gegevensbescherming' (AVG) die op 25 mei van kracht wordt en voor alle sectoren geldt. De AVG vervangt in Nederland de huidige Wet bescherming persoonsgegevens (Wbp) en geeft de AP bevoegdheid om hogere boetes uit te delen. Dus ook aan de arts die patiëntgegevens aan een farmaceut verkoopt.

Aanscherping

Onder de Wbp was de AP nog terughoudend met het uitdelen van boetes. Het bleef bij waarschuwingen. Onder de nieuwe wetgeving zal de AP vrijwel zeker strenger optreden, verwacht Schell. Boetes van nu nog maximaal 820.000 euro kunnen dan oplopen tot 20 miljoen, hoewel dat bedrag vooral multinationals moet afschrikken de nieuwe privacywet niet te ontduiken.

> "Op datalekken staan boetes"

Schell: "Een aantal eisen van de AVG zit al in bestaande zorgspecifieke wetgeving voor geneeskundige behandeling en cliëntenrechten. De AVG zorgt voor een aanscherping, voor een grotere verantwoordelijkheid bij de zorgaanbieder. De zorgaanbieder moet zowel naar de patiënt als naar de AP en de Inspectie Gezondheidszorg en Jeugd met een administratie bewijzen dat voldaan wordt aan de privacyregels en dat ICT-systemen, ofwel de informatiebeveiliging, geen risico's opleveren bij de verwerking van persoonsgegevens."

Registerplicht

In grote lijnen gaat het bij de AVG om een beoordeling door de zorgorganisatie op het effect van risicovolle verwerkingen van persoonsgegevens (*privacy impact assessment*). Dat is belangrijk bij het ontwerp van systemen en het aanleggen van databestanden (*privacy by design*). Ook geldt een 'registerplicht' voor alle verwerkingsactiviteiten van persoonsgegevens. Daarnaast moet in een 'verwerkersovereenkomst' tussen de zorgverlener en partijen met wie deze samenwerkt, vastgelegd worden wie geautoriseerd is tot het inzien van patiëntgegevens. Ziekenhuizen delen ook veel medische gegevens van patiënten voor wetenschappelijk onderzoek, bijvoorbeeld met KWF Kankerbestrijding. Ze zijn voortaan verplicht hiervan een overzicht bij te houden.

Schell: "Zorgorganisaties raad ik aan persoonsgegevens te versleutelen en een tweefactorauthenticatie in te voeren, ofwel een extra beveiliging die jou als enige toegang geeft, ook al weet een ander het wachtwoord." Het melden van datalekken aan de AP kan de Stichting Privacyzorg namens de zorgorganisatie doen. "Wij schrijven en versturen ook de brief naar de patiënt om hem over het datalek te informeren."
De AVG verplicht organisaties die veel persoonsgegevens verwerken, zoals in de zorg, tot de aanstelling van een Functionaris Gegevensbescherming (FG). Dit is een onafhankelijk, aan geheimhouding gehouden persoon die toezicht houdt op de naleving van de privacyregels en klachten afhandelt. Om het voor kleine zorgorganisaties betaalbaar te houden, vervult Stichting Privacyzorg voor hen ook de rol van FG.
Schell: "Omdat de mens de zwakste schakel is in de informatiebeveiliging besteden we daar op voorlichtingsavonden voor zorgmedewerkers ook aandacht aan." ●