
1 2 3
4 5 6
7 8 9
0 *

IGJ onderzoekt informatiebeveiliging

‘Werk stap voor stap aan verbetering’

Iedere huisartsenpraktijk moet voldoen aan NEN 7510, de norm voor informatiebeveiliging. De Inspectie Gezondheidszorg en Jeugd (IGJ) is bezig met een onderzoek daarnaar en heeft vijftig praktijkhouders een digitale vragenlijst gestuurd. Wat houdt die norm in, hoe zorg je dat je daaraan voldoet en wat doet IGJ met de onderzoeksresultaten? Huisarts en LHV-bestuurder Mariëtte Willems geeft uitleg.

TEKST: BERBER BIJMA / BEELD: AAD GOUDAPPEL

Goed omgaan met patiëntgegevens is sinds jaar en dag onderdeel van het werk van huisartsen, zegt Mariëtte Willems. Wat dat betreft dus weinig nieuws onder de zon. Maar door het uitdijende aantal systemen dat huisartsen gebruiken, de toenemende interactie met andere zorgverleners en de groei van het aantal medewerkers in praktijken, wordt die standaardtaak steeds complexer. Over het nut van de beveiliging van de gegevens die huisartsen van patiënten hebben, is geen discussie, stelt Willems. ‘Wij werken met hele gevoelige patiëntgegevens, die veel verder gaan dan naam, adres en BSN. We moeten én willen ervoor zorgen dat niemand anders daarbij kan dan degenen voor wie die informatie is bedoeld. Patiënten moeten erop kunnen vertrouwen dat hun gegevens veilig zijn bij de huisarts. Dat betekent niet alleen dat systemen zo weerbaar mogelijk moeten zijn tegen een cyberhack, maar bijvoorbeeld ook dat er geen patiëntgegevens op een bureau moeten liggen als de schoonmaker aan het werk is. Gedrag blijft een belangrijke component bij gegevensbeveiliging.’

De norm waaraan zorgorganisaties moeten voldoen op het gebied van informatiebeveiliging, staat beschreven in NEN 7510. Willems: ‘Die norm gaat zowel over eisen aan systemen als over eisen aan zorgverleners. En behalve dat je moet voorkomen dat gegevens door derden worden ingezien, gaat het ook om de continuïteit van zorg: informatie moet altijd beschikbaar zijn als die nodig is om goede zorg te kunnen leveren.’

IGJ-ONDERZOEK

IGJ doet dit najaar onderzoek naar de stand van zaken rond informatiebeveiliging in huisartsenpraktijken. Daarvoor hebben vijftig praktijkhouders een digitale vragenlijst toegestuurd gekregen. De vragenlijst is niet bedoeld om sancties op te leggen als een praktijk niet (geheel) aan NEN 7510 voldoet, benadrukt

‘Je hoeft als praktijkhouder zeker geen expert te worden in informatiebeveiliging’

Willems. ‘IGJ wil met dit onderzoek een beeld krijgen van de informatiebeveiliging in huisartsenpraktijken. De praktijken die geselecteerd zijn, krijgen na het invullen van de lijst een brief van IGJ waarin staat hoe hun praktijk ervoor staat en welke stappen de betreffende praktijk kan nemen om de beveiliging te verbeteren. Het onderzoek is dus bedoeld om ervoor te zorgen dat praktijken gestructureerd aan de slag gaan met de beveiliging van hun patiëntgegevens.’
De eisen die NEN 7510 stelt, zijn fors. ‘Deze norm is in eerste instantie bedoeld voor grote zorgorganisaties. Er zitten onderdelen in die ingewikkeld zijn voor huisartsenpraktijken. Ook het taalgebruik sluit niet altijd aan bij wat voor huisartsen gebruikelijk is. We zijn daarom onder andere met IGJ in gesprek om te zorgen dat de eisen praktisch en reëel zijn voor huisartsenpraktijken. Het onderzoek en de brief die IGJ daarna stuurt, moeten bijdragen aan bewustzijn rond informatiebeveiliging en huisartsen aanzetten tot actie, in plaats van hen af te schrikken. Om dat averechtse effect te voorkomen zijn we dus in gesprek.’



Dit doet de LHV om informatiebeveiliging werkbaar te maken

Voldoen aan NEN 7510 is geen eenvoudige opgave. De LHV zet zich op meerdere manieren ervoor in dat de eisen werkbaar zijn in de dagelijkse praktijk: zowel in gesprekken met landelijke partners als met hulpmiddelen voor individuele praktijken.

De LHV heeft regelmatig contact met IGJ over het lopende onderzoek onder vijftig praktijken, op basis van feedback van huisartsen die aan dit onderzoek meedoen. Doel is dat een volgende vragenlijst meer aansluit op de dagelijkse praktijk in de huisartsenzorg.

Daarnaast zijn we in gesprek over het ‘groeimodel’ waar IGJ aan werkt. Dit is een stappenplan waarmee huisartsenpraktijken concreet aan de slag kunnen om gaandeweg steeds volledieger te voldoen aan NEN 7510.

Bij meer complexe onderdelen kan ondersteuning vanuit de regionale huisartsenorganisatie helpen, bijvoorbeeld bij het inrichten en borgen van een structurele verbetercyclus.

De LHV is met VWS in gesprek over de norm zelf, die in eerste instantie is ontworpen voor grote zorgorganisaties. Zij hebben te maken met bijvoorbeeld complexere ketenrisico’s en contractstructuren. De LHV bespreekt met VWS of het mogelijk is om voor kleinere zorgaanbieders de norm zodanig vorm te geven dat de RHO’s een deel van de eisen realiseren, bijvoorbeeld door de inzet van een C(M)IO. Ook landelijk kan wellicht een deel van de eisen worden ‘afgevangen’, bijvoorbeeld met een leveranciersbeoordeling. Andere eisen, zoals veilig gedrag en het in kaart brengen van risico’s, spelen hoe dan ook op praktijkniveau.

■ BETREK HET HELE TEAM

Wanneer voldoet een praktijk eigenlijk aan de normen? ‘Je hoeft als praktijkhouder zeker geen expert te worden in informatiebeveiliging’, zegt Willems. ‘Net zo goed als dat we geen financiële experts hoeven te zijn als huisartsen. Tegelijk zijn we wel verantwoordelijk voor een goede boekhouding en ook voor goede informatiebeveiliging. Je kunt externe deskundigheid inhuren en natuurlijk ook gebruikmaken van hulpmiddelen en advies vanuit zowel de LHV als de regionale huisartsenorganisatie.’
Informatiebeveiliging is grofweg in te delen in vier stappen: de risico’s in kaart brengen (te beginnen met de meest cruciale systemen en informatiestromen), maatregelen voor de beveiliging nemen, die maatregelen vastleggen en vervolgens steeds blijven controleren en verbeteren.
Voldoen aan NEN 7510 is niet een traject dat op een bepaald moment helemaal ‘af’ is, zegt Willems. ‘Omdat systemen, risico’s en gedrag voortdurend veranderen, is informatiebeveiliging een doorgaande activiteit. Wellicht ga je zo nu en dan met een nieuwe ict-toepassing werken, krijg je nieuwe medewerkers of veranderen de dreigingen, bijvoorbeeld door AI. Je moet dus voortdurend met beveiliging bezig blijven. Soms in technische zin: het generieke wachtwoord “Welkom01” voor alle medewerkers kan bijvoorbeeld echt niet meer. Andere keren gaat het meer om gedrag. Je kunt bijvoorbeeld een *phishing mail* laten versturen om het bewustzijn van medewerkers hoog te houden.’
Het hele team betrekken is van groot belang, benadrukt Willems. ‘Je bent als praktijkhouder weliswaar eindverantwoordelijk voor de veilig-

Weten waar je nu staat?

Informatiebeveiliging begint met een goed beeld van de huidige stand van zaken. Op de LHV-site vind je scans die helpen dat beeld scherp te krijgen.

Met de **Privacyscan** onderzoek je of in jouw praktijk alleen bevoegden toegang hebben tot (persoonlijke) gegevens. Privacy gaat ook over transparantie: houd jouw systeem bij wie wanneer een patiëntendossier heeft ingezien en zijn die gegevens beschikbaar voor patiënten? Daarnaast gaat privacy over wat je doet als het misgaat.

Met een **Integriteitsscan** kijk je naar de nauwkeurigheid, volledigheid en consistentie van de dossiervorming. Daarnaast gaat integriteit over traceerbaarheid: is duidelijk wie informatie heeft ingevoerd of gewijzigd?

Tot slot kun je de **Beschikbaarheidsscan** uitvoeren. Hiermee kijk je of een patiëntendossier altijd beschikbaar is op de plek en het tijdstip waar dat nodig is om de patiënt zorg te kunnen verlenen.

Let op! Met het uitvoeren van een of meer van deze drie scans verbeter je de informatiebeveiliging van jouw praktijk niet. Ze geven je alleen een eerste beeld van wat er moet gebeuren om die veiligheid te verbeteren en aan de wettelijke eisen te voldoen.

Concreet aan de slag!
In het webdossier Informatiebeveiliging vind je verschillende hulpmiddelen voor een betere informatiebeveiliging.

Met de **Handleiding Risicoafweging** breng je stapsgewijs in kaart welke informatiestromen er in de praktijk zijn, variërend van je HIS tot data verzameld door medische apparatuur en van medicijnverpakkingen met NAW-gegevens tot verslagen van functioneringsgesprekken. De handleiding helpt je om zicht te krijgen op de risico's van al die informatiestromen en die risico's af te wegen. De uitkomsten van de risicoafweging kun je verwerken in een beleidsplan. Op de site vind je tips voor het opstellen van een beleidsplan.

Bewustwording binnen het team is essentieel voor een veilige omgang met (patiënt)gegevens. We geven diverse tips waarmee je ervoor kunt zorgen dat in jouw praktijk informatiebeveiliging voortdurende aandacht heeft bij alle medewerkers. Denk bijvoorbeeld aan afspraken die je met nieuwe of vertrekkende medewerkers maakt of informatieveiligheid als terugkerend onderwerp bij teamoverleggen.

Met een **Privacyverklaring** laat je patiënten op jouw website weten hoe je met hun gegevens omgaat. Op onze site vind je een voorbeeld van zo'n verklaring.

Ondanks alle voorzorgsmaatregelen kan het misgaan: jouw praktijk kan te maken krijgen met een datalek. In de **LHV-handleiding Datalek in de huisartsenpraktijk** lees je wat je dan kunt en moet doen.

Het webdossier Informatiebeveiliging krijgt de komende weken een update.

heid van patiëntgegevens, maar die kun je niet in je eentje realiseren. Iedereen moet zich ervan bewust zijn dat er geen geprinte gegevens moeten rondslingeren, dat je niet op een link moet klikken waarvan je niet zeker weet dat die veilig is, dat je niet bij je scherm moet weglopen terwijl je ingelogd bent, enzovoorts. Veilig gedrag vraagt steeds weer aandacht.'

■ HULPMIDDELEN

Veel huisartsenspoedposten hebben er het afgelopen jaar voor gekozen om zich te laten certificeren voor een veilige omgang met patiëntgegevens. Voor huisartsenpraktijken is dat niet nodig, benadrukt Willems, maar ze moeten wel kunnen aantonen dat ze aan de normen voldoen. 'De eisen zitten overigens deels in de NHG-accreditatie verwerkt. We werken nu samen met de NPA om informatiebeveiliging een steviger onderdeel te maken in hun audits en de NPA-wegwijzer.
Dat betekent dus niet dat je met accreditatie volledig voldoet aan NEN 7510.'
De LHV heeft al diverse hulpmiddelen om de informatiebeveiliging in een praktijk te verbeteren (zie kader). Die worden de komende tijd verder verbeterd en uitgebreid, vertelt Willems. 'Verder zien we dat veel regionale huisartsenorganisaties praktijken ondersteunen op het gebied van veiligheid. Vanuit de LHV praten we met landelijke partijen, waaronder dus IGJ, om te zorgen voor reële eisen en een goede ondersteuning. Een praktijk die gestructureerd, stap voor stap werkt aan steeds betere informatiebeveiliging, moet zich geen zorgen hoeven maken.' ¶