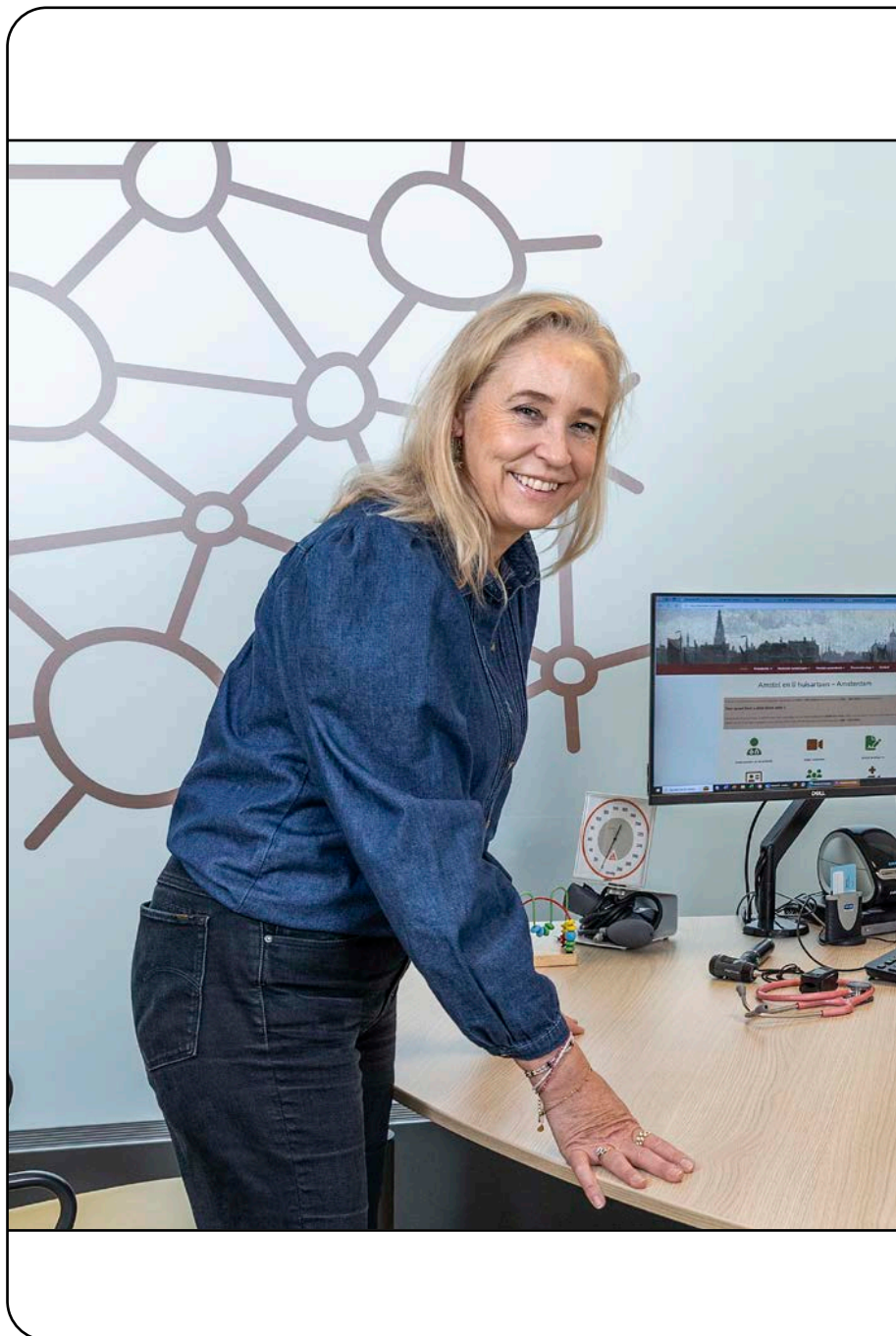


Informatie- beveiliging: houd de aandacht vast

Leuker wordt het misschien niet, maar belangrijker wel: als huisarts moet je de beveiliging van persoonsgegevens en medische informatie goed op orde hebben. Gelukkig hoef je dat niet alleen te doen. De regionale huisartsenorganisatie kan vaak een belangrijke rol spelen. De LHV bracht onlangs samen met InEen en NHG een nieuw webdossier uit, met daarin onder meer drie scans die een eerste indruk geven van hoe jouw praktijk ervoor staat.

TEKST: BERBER BIJMA, BEELD: MIRJAM VAN DER LINDEN



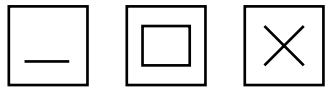
Om meteen maar een misverstand uit de wereld te ruimen: huisartsen zijn niet te klein om interessant te zijn voor hackers. Johan Snijders, senior beleidsmedewerker ICT bij de LHV, kent helaas verhalen van kleinere zorgverleners die slachtoffer werden van digitale criminelen. ‘Vorig jaar was er nog een ransomware-aanval bij een groep tandartsen, die wel een week duurde en bij mijn weten de tandarts aardig wat losgeld heeft gekost. Hackers worden slimmer, dus de bedreiging neemt toe. Informatiebeveiliging blijft daardoor een ingewikkeld onderwerp, maar je ziet aan zo’n voorbeeld tegelijk hoe belangrijk het is, want je wilt echt

geen hack of datalek.’

Mede door de nare voorbeelden die in het nieuws komen, ziet Snijders dat de bewustwording bij huisartsen de laatste jaren is toegenomen. ‘Zeker wanneer huisartsen zaken gaan doen met een nieuw bedrijf, zijn ze alert op de veiligheid van persoonlijke gegevens van patiënten. Dat is absoluut winst. Maar informatiebeveiliging gaat ook over: wat als je backup-systeem niet werkt, wat gebeurt er als de stroom plotseling uitvalt, hoe gaan medewerkers om met gevoelige gegevens?’

■ LAAGDREMPELIGE VEILIGHEIDSSCANS

Om een eerste antwoord op die



vragen te krijgen, heeft de LHV samen met InEen en NHG drie laagdrempelige scans uitgebracht die een globaal antwoord geven op de vraag: hoe staat mijn praktijk ervoor qua informatiebeveiliging? De eerste scan is een privacyscan, waarbij het gaat om vragen als: hebben alleen bevoegden toegang tot het dossier, wordt bijgehouden wie wanneer een patiëntendossier heeft geraadpleegd, kan de patiënt dat ook opvragen en wat doe ik als het fout gaat? De integriteitsscan gaat over de nauwkeurigheid, volledigheid en consistentie van de dossiervorming en over traceerbaarheid: is het altijd duidelijk wie informatie heeft ingevoerd of gewijzigd? De laatste scan gaat over de beschikbaarheid van gegevens: kan

een praktijkmedewerker erop vertrouwen dat er relevante informatie uit het dossier tevoorschijn komt, op de plek en tijd waar dat nodig is? Iedere scan bestaat uit een paar vragen, die via de LHV-site beantwoord kunnen worden. 'De uitkomst laat zien wat je al hebt geregeld en wat nog niet', legt Snijders uit. 'Zo kun je bepalen wat vervolgstappen zijn en besluiten wat je prioriteit wilt geven. Wat die prioriteiten zijn, hangt af van wat je al hebt gedaan, maar ook van hoe de praktijk eruitziet. Kan een bezoeker bijvoorbeeld bij de computer van een balie-medewerker? Dan kun je besluiten daar allereerst maatregelen voor te nemen. Daarnaast werken de vragen van de scans natuurlijk ook als

AMSTERDAM:

Coöperatie en koploperpraktijken plaveien de weg

De Regionale Organisatie Huisartsen Amsterdam (ROHA) is volop aan de slag met informatiebeveiliging. In eigen huis, maar ook bij de 150 aangesloten huisartsenpraktijken. 'Informatiebeveiliging staat bij ons hoog in het vaandel', vertelt Ben Stoltenborg, security officer bij de ROHA. Hij wijst erop dat 'NEN 7510', de norm voor informatiebeveiliging in de zorg, expliciet benoemd staat in het Integraal Zorgakkoord (IZA). 'In 2025 moeten alle zorgorganisaties in Nederland – dus ook huisartsenpraktijken – aan die norm voldoen. Voor een individuele praktijk is dat niet te doen: het gaat om maar liefst 117 beheersmaatregelen.'

Vijf 'koploperpraktijken' in Amsterdam zijn sinds afgelopen zomer onder begeleiding van de ROHA bezig met het traject dat komend voorjaar tot de NEN-certificering moet leiden. De praktijk van huisarts Pieter Jan van Empel, met een vestiging in Amsterdam-Noord en een vestiging in het Amstelkwartier, is een van de koploperpraktijken. 'Ict heeft altijd mijn interesse gehad', vertelt hij. 'Toen ik in 2016 een nulpraktijk opende, kon ik de ict meteen zo modern en veilig mogelijk opzetten. Bovendien zit ik in het ROHA-bestuur. Vanuit die rol wil ik het goede voorbeeld geven. Vandaar dat ik heb ingestemd toen Ben mij vroeg een van de koploperpraktijken te zijn.'

De ROHA en de koploperpraktijken plaveien momenteel samen de weg voor de andere praktijken die op een later moment het certificeringstraject doorlopen. Van Empel: 'Afgelopen maanden hebben we het voortraject voor de nulmeting gehad. De ROHA had een checklist opgesteld die wij als koploperpraktijken hebben doorlopen en van commentaar voorzien. Zo ligt er nu een goede checklist voor de nulmeting bij andere praktijken.'

■ 'WELKOM123'

De checklist maakt duidelijk wat er nog moet gebeuren voor een praktijk aan de NEN-norm voldoet. Stoltenborg: 'Deels zijn dat dingen die we op coöperatieniveau regelen, zoals een risicoanalyse, het leveranciersmanagement, een verwerkingsregister. Andere zaken moet je juist binnen de praktijk regelen.'

Van Empel somt een heel aantal voorbeelden op: 'Is de 2-factorauthenticatie goed geregeld, wie heeft toegang tot welke gegevens, wat is er geregeld voor als iemand uit dienst gaat en dus niet meer moet kunnen inloggen, hoe sla je documenten op, mag iemand een

‘Het goede nieuws: je hoeft het niet alleen te doen én niet alles hoeft niet in één keer’

trigger: je realiseert je bij het invullen wat er allemaal bij komt kijken bij informatieveiligheid.’

De scans zijn onderdeel van een nieuw webdossier over informatiebeveiliging, vertelt Snijders. ‘Tot voor kort hadden we een praktijkboek informatiebeveiliging. Het webdossier dat we nu hebben, is actueler, toegankelijker en praktischer. Zo hopen we dat de drempel om met informatiebeveiliging aan de slag te gaan, lager is.’

■ TREK SAMEN OP MET DE REGIO-ORGANISATIE

Of je op dit moment al veel of weinig hebt geregeld op het gebied van informatiebeveiliging, ‘het kan altijd beter dan gisteren’, zegt Snijders. ‘Je móet er dus mee aan de slag, ook als het potentieel veel werk is. Vergelijk het met het kwaliteitsmanagement, waar ook iedere praktijk aan hoort te werken. Het goede nieuws is dat je het

niet alleen hoeft te doen én dat alles niet in één keer hoeft. Ik adviseer huisartsen altijd om samen op te trekken met hun regionale huisartsenorganisatie. Daar zit meestal veel deskundigheid op het gebied van informatiebeveiliging.’

Het is verstandig om binnen de praktijk één medewerker aan te stellen die informatiebeveiliging in zijn of haar portefeuille heeft. ‘Diegene kan bijvoorbeeld het beleidsplan informatiebeveiliging opstellen – dat klinkt overigens zwaarder dan het is. In veel praktijken is het de praktijkmanager die over informatiebeveiliging gaat, maar het kan ook iemand anders zijn. Belangrijk is wel dat de anderen daarmee niet denken: fijn, dat is dan geregeld. Informatiebeveiliging is een onderwerp dat iedereen aangaat, vooral omdat het ook over menselijk gedrag gaat. Daarom is het goed om het regelmatig op het teamoverleg terug te laten komen.’ 

usb-stick gebruiken, staat de schermbeveiliging aan tijdens de lunch?’ Met dat laatste raakt Van Empel aan wat hij ‘het meest ingewikkeld’ vindt aan informatiebeveiliging: bewustwording en gedrag. ‘Jonge waarnemende huisartsen zijn zich lang niet altijd bewust van de gevaren van hun omgang met gevoelige gegevens en de mogelijke schade voor patiënten. Wij vragen waarnemers altijd om met hun UZI-pas in te loggen. Dat levert vaak weerstand op, want ze zijn gewend om in te loggen met een waarnemerspas. Gebruikersnaam Waarnemer1, wachtwoord Welkom123. Daarmee kan zoveel méér misgaan dan met je persoonlijke UZI-pas. Die UZI-pas is ook veel handiger, want je kunt makkelijker terugvinden wie wanneer heeft gewerkt en welke patiënten heeft gezien.’

Ook bij assistenten blijft Van Empel erop hameren dat ze veilig met persoonsgegevens omgaan. ‘We hebben bijvoorbeeld de duidelijke regel: geen medische gegevens op het bureaublad van een computer. Maar toch vind ik er nog weleens een brief van het ziekenhuis. Of zelfs een eigen salarisstroom. Bij een waarnemend huisarts trof ik een keer een hypotheekovereenkomst aan op het bureaublad. Wat mij betreft geen probleem als je tussen het werk door even iets voor je privé doet, maar als je je eigen persoonlijke gegevens al op het bureaublad achterlaat, hoe kan ik er dan op vertrouwen dat je veilig met patiëntgegevens omgaat? Patiënten zelf zijn soms ook slordig, trouwens. We hebben meegemaakt dat een patiënt heel graag een papieren uitdraai van zijn dossier wilde en dat we die even later terugvonden in de wachtkamer.’

■ BEWUSTWORDINGSCAMPAGNE

Bewustzijn en veilig gedrag wordt een belangrijk onderdeel van het certificeringstraject dat de ROHA begeleidt, vertelt Stoltenborg. ‘We gaan een campagne organiseren en materiaal verspreiden dat bedoeld is om alle medewerkers van de praktijk alert te houden.’ Lonneke Reuser, manager Zorg en Innovatie bij de ROHA, hoopt dat Van Empel en de andere ‘koploperhuisartsen’ na het eerste traject hun collega’s enthousiast zullen maken. ‘De andere 145 praktijken hoeven niet allemaal vanaf nul te beginnen, natuurlijk. De meeste hebben echt al wel iets geregeld. Maar zij – en wij – moeten nog wel flink wat werk verrichten om in 2025 aan de NEN-norm te voldoen. Overigens betekent dat “voldoen” niet dat dan alles geregeld moet zijn, maar vooral dat je continu werkt aan verbetering, en dat ook blijft doen na 2025. Met de koploperpraktijken ontwikkelen wij daar momenteel een goede werkwijze voor. En we staan er zeker voor open om de producten die wij nu ontwikkelen, zoals de checklist voor de nulmeting, te delen met andere regionale huisartsenorganisaties.’



Scan jouw praktijk

Benieuwd hoe de informatiebeveiliging in jouw praktijk ervoor staat? Met drie scans krijg je een eerste indruk hoe het nu geregeld is en welke verbeteringen je kunt doorvoeren: de privacyscan, de integriteitsscan en de beschikbaarheidsscan. Vul de scans in en je krijgt jouw uitkomsten en verbeter-tips in je mailbox. Je vindt de scans op onze website.

