Informatiebeveiliging: óók een kwestie van boerenverstand

Natuurlijk moeten patiëntgegevens en andere gevoelige informatie digitaal achter slot en grendel. Maar veilig omgaan met gegevens in de huisartsenpraktijk is 'zeker niet alleen high tech', zegt Johan Snijders, ICT-beleidsmedewerker bij de LHV. 'Kunnen patiënten niet meekijken op het scherm van de assistente? Laat niemand papieren met medische gegevens achter bij de printer? Informatiebeveiliging gaat voor een belangrijk deel over gedrag en is daarom ook een kwestie van boerenverstand.'

TEKST: BERBER BIJMA // ILLUSTRATIE: AAD GOUDAPPEL

'Als zorgverlener en praktijkhouder ben je hoeder van belangrijke medische en persoonlijke informatie. Je bent niet alleen verplícht daar goed mee om te gaan, maar zorgverleners wíllen er ook goed mee omgaan. Je wilt echt niet dat de gegevens van je patiënten op straat komen te liggen.'
Johan Snijders houdt zich als ICT-beleidsmedewerker bij de LHV bezig met de eisen aan en het adviseren over de informatiebeveiliging in huisartsenpraktijken. Hij ziet dat er zowel huisartsen zijn die zich er té druk om maken als huisartsen die zich er niet druk genoeg om maken. 'Sommige huisartsen hebben het gevoel dat ze niet genoeg technologische vaardigheden hebben om het allemaal precies goed te doen. Aan de andere kant van het spectrum zie je huisartsen die denken dat ze het allemaal wel aardig goed hebben geregeld en die zich er daarom niet zo druk om maken. Die houding is risicovoller, want je moet voortdurend bewust en kritisch blijven kijken naar de processen in de praktijk. Net als met de VIM-procedure voor medische incidenten en bijna-incidenten, is het ook goed om bijna-incidenten met informatiebeveiliging onder de loep te nemen. Veilig omgaan met gegevens is geen noodzakelijk kwaad, maar een onderdeel van de praktijkvoering. Het hoort simpelweg bij het huisartsenvak om zorgvuldig met patiëntgegevens om te gaan. Dat was vroeger al het uitgangspunt; toen bewaarde de huisarts de papieren patiëntendossiers óók achter een slot.'

'Het is aan de huisarts om te bedenken wie waarbij moet kunnen'

STAPPENPLAN

In de Praktijkwijzer Informatiebeveiliging hebben LHV, NHG, en InEen samen op een rij gezet wat er bij veilig omgaan met gegevens komt kijken. 'In die handleiding zitten alle hulpmiddelen die wij kunnen bedenken om de zaken goed te regelen volgens de NEN-normen' vertelt Snijders. 'Het is daardoor een vrij uitgebreide handleiding geworden, maar het is niet nodig alles in één keer door te lezen. Ik raad huisartsen doorgaans aan om met één onderwerp te beginnen. Je kunt beter twee kleine stappen zetten dan alles in één keer perfect proberen te krijgen.' De globale volgorde die in de handleiding staat beschreven is: breng de informatiestromen in kaart, onderzoek de risico's daarin, regel wat je zelf kunt regelen en zoek zo nodig ondersteuning bij andere acties.
De informatiestromen binnen een praktijk gaan voor een deel via computersystemen. 'Niet voor ieder systeem is een verwerkersovereenkomst nodig', vertelt Snijders. 'Als het bijvoorbeeld gaat om een applicatie waarin geen persoonsgegevens worden verwerkt, hoef je niet zo'n overeenkomst te sluiten. Op de LHV-site staat een beslisboom die duidelijk maakt wanneer er wel en niet een verwerkersovereenkomst nodig is én een checklist met voorwaarden waaraan de overeenkomst moet voldoen.'
De toegang tot diverse informatiesystemen moet goed beveiligd zijn. 'Het is aan de huisarts om te bedenken wie waarbij moet kunnen. Het technische deel van de inlogbeveiliging wordt meestal geregeld door de vaste ict-ondersteuner of de zorggroep in de regio.'

BREED KIJKEN

Bij het onderzoeken van risico's in informatiestromen is het belangrijk zo breed mogelijk te kijken, adviseert Snijders, juist omdat het om veel meer gaat dan techniek. 'Een patiënt die kan meekijken op het scherm van de assistente is een informatierisico dat je meestal vrij gemakkelijk kunt oplossen, bijvoorbeeld door de computer een kwartslag te draaien of een deel van een raam af te plakken.'
Om allerlei risico's op te sporen, kan het handig zijn een paar medewerkers daar specifiek voor in te zetten.

Deze veiligheids-stappen zijn snel gezet

Print zo weinig mogelijk

Zorg dat patiënten niet onbedoeld op een computerscherm kunnen meekijken

Vergrendel altijd uw computer bij het verlaten van uw werkplek

Laat apparatuur met informatie (laptop, smartphone, usb-stick) nooit onbeheerd achter

Sluit nooit privé-apparatuur aan op praktijknetwerken, óók niet om op te laden

Gebruik sterke wachtwoorden en verander uw wachtwoorden eens per halfjaar

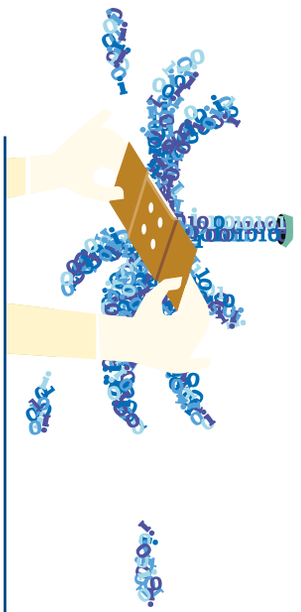
Gebruik eventueel een wachtwoordmanager, zodat u zelf maar één wachtwoord hoeft te onthouden

Stuur mails alleen via beveiligde systemen

Laat 1 of 2 medewerkers eens een dag 'speuren' naar informatielekken en onveilig gedrag in de praktijk

Zet informatiebeveiliging regelmatig op de agenda van het werkoverleg

Meer tips over informatiebeveiliging leest u in de Praktijkwijzer Informatiebeveiliging, een gezamenlijke uitgave van LHV, NHG en InEen, op www.lhv.nl.



Snijders: 'Vraag bijvoorbeeld de praktijkmanager en een assistente om een dag of een paar dagen heel bewust om zich heen te kijken: wat slingert er eventueel rond in de praktijk of wat is zichtbaar voor mensen die het niet zouden moeten zien. Informatiebeveiliging is vaak de taak van de praktijkmanager – als die er is – gemaakt, maar het is goed om ervoor te zorgen dat uiteindelijk iederéén zich ervoor verantwoordelijk voelt. En juist door meer mensen erbij te betrekken, haal je meer risico's boven water, want iedereen ziet vanuit de eigen functie andere dingen. De assistente zou bijvoorbeeld kunnen zien dat de verschillende huisartsen van één praktijk net wat anders werken en daardoor verschillend omgaan met gevoelige informatie.'

■ INFORMATIEPROTOCOL

Om risico's te verkleinen is het uiteraard van belang de technische beveiliging van gegevens goed op orde te hebben, met toepassingen als twee-factor-authenticatie. Om ook informatielekken door risicovol gedrag zoveel mogelijk te beperken, kan een 'informatieprotocol' zinvol zijn. 'Zeker als er nieuwe medewerkers in de praktijk komen, is het handig hen zo'n protocol te kunnen overhandigen. Tegelijk is natuurlijk duidelijk: met alleen het opschrijven en opslaan van hoe je met gevoelige informatie wilt omgaan, bereik je weinig. Verantwoord gedrag moet onderdeel van het dagelijks werk worden en dus een terugkerend onderwerp bij werkoverleggen. Mocht er sprake zijn van een echt datalek, dan is de huisarts in veel gevallen verplicht

INFORMATIEBEVEILIGING IN DE HUISARTSENPRAKTIJK

Duidelijke regels én voortdurende aandacht

Sandra Groot-Metz is praktijkmanager bij Gezondheidscentrum Holendrecht in Amsterdam. Samen met een van de huisartsen is ze verantwoordelijk voor de informatieveiligheid in de praktijk. 'Dat betekent dat we continu aandacht houden voor het belang van privacybescherming.' De technische kant daarvan is grotendeels in handen van de stichting GAZO, waar Gezondheidscentrum Holendrecht onder valt. 'GAZO regelt bijvoorbeeld ons HIS en heeft er ook voor gezorgd dat we externe werkplekken hebben. Als er een computer wordt gestolen, staat daar geen gevoelige informatie op, want alles staat op die externe werkplek.'

Naast de techniek zijn het de praktische werkprocessen die de privacy moeten garanderen. 'We hebben duidelijke afspraken over heel veel verschillende dingen. Bijvoorbeeld: communicatie via WhatsApp mag niet tot een persoon herleidbaar zijn, je vergrendelt je computer als je je werkplek verlaat, van urinepotjes haal je de naamsticker af voor je 'm bij het afval gooit, bij het papierafval scheiden we gevoelige en niet-gevoelige informatie, niemand neemt praktijkpost mee naar huis.'

De regels gaan soms behoorlijk ver. 'Patiënten die verhuizen, willen soms zelf hun dossier ophalen om het aan hun nieuwe huisarts over te dragen. Als ze dan hun zoon of dochter sturen, geven wij het alleen mee als die een machtigingsformulier met handtekening heeft. Daarnaast hebben we de afspraak dat aan de balie geen achternamen van patiënten worden genoemd, omdat het in onze praktijk niet helemaal te voorkomen is dat geluid van de balie de wachtkamer bereikt.'

En dan nog zijn er genoeg valkuilen. 'Huisartsen die visites doen, nemen soms een visitekaart mee met medicatie-informatie.

dat te melden bij de Autoriteit Persoonsgegevens, die altijd zal vragen: wat heb je gedaan om dit in de toekomst te voorkomen? Ook een bijna-datalek moet daarom altijd aanleiding zijn om in gesprek te gaan. Het zou bijvoorbeeld kunnen gebeuren dat alle patiënten van de praktijk een mail krijgen en iemand op het laatste moment voor verzending ontdekt dat de mailadressen in CC staan in plaats van BCC. Dan ga je in gesprek over hoe het kon dat dat bijna fout ging en hoe je ervoor kunt zorgen dat het de volgende keer niet écht fout gaat – bijvoorbeeld door een extern mailprogramma te gaan gebruiken.'

■ NIET GEK LATEN MAKEN

Veilig omgaan met gegevens steekt nauw: een foto naar een specialist appen of een geboortekaartje in de wachtkamer hangen in plaats van in de personeelskamer, zijn zaken die niet kunnen. 'Je moet weten waar de grens ligt, maar je tegelijk ook realiseren dat niet alles meteen een groot probleem is', zegt Snijders. 'Je kunt het onderwerp dus niet naast je neerleggen onder het mom "daar ben ik niet van", maar je moet je tegelijk ook niet gek laten maken. Begin simpelweg met een paar kleine stappen uit de handleiding Informatiebeveiliging en zet het onderwerp regelmatig op de agenda, zodat er meer bewustzijn komt. Daarmee werk je toe naar de gedachte áchter de AVG – die onterecht nog vaak wordt gezien als een "moetje" – dat goed omgaan met gevoelige informatie een standaard plek in de praktijkvoering heeft.' ¶

Wat nu als die op de terugweg uit je jaszak valt?' Een goed privacybeleid is daarom vooral een kwestie van voortdurende aandacht, zegt Groot. 'Na een tijdje trapt iedereen toch weer in valkuilen. Informatieveiligheid komt daarom bij ons vrijwel iedere maand ter sprake en twee keer per jaar hebben we een 'Week van de privacy' waarbij er dagelijks aandacht is, bijvoorbeeld door te laten zien wat er mis kan gaan.' Privacy is een serieus onderwerp, maar in gezondheidscentrum Holendrecht benaderen ze het ook graag met humor. Wie zijn of haar computer onbeheerd achterlaat, kan bij terugkomst een bordje '#datalek' op het toetsenbord vinden. 'Dat mag iedereen bij een collega neerzetten. #datalek klinkt met opzet een beetje catchy. We willen het onderwerp ook graag een beetje luchtig en bespreekbaar houden, zonder al te veel met de vinger te wijzen.'

'Transparantie over fouten geeft vertrouwen'

Voor Jonathan Bouman is zorgvuldige informatiebeveiliging een belangrijk element van zijn werk als huisarts. 'Vertrouwen in de basis van ons vak. Als de patiënt mij niet vertrouwt, kan ik die patiënt niet goed helpen. Ik tik de hele dag door dingen in systemen. Als daarin een lek ontstaat en dat lek wordt niet zorgvuldig gedicht, dan verlies ik mogelijk het vertrouwen van de patiënt.'
Bouman is waarnemend huisarts in Amsterdam en een van de bestuursleden van het CMIO-netwerk, een netwerk van chief medical information officers: huisartsen die zich naast hun medische werk ook actief bezighouden met informatisering in de zorg. Het netwerk voor de eerste lijn is vorig jaar opgericht. De leden hebben bovengemiddelde kennis van informatietechnologie én zijn thuis in de medische wereld. Dat maakt het netwerk de ideale partij om bruggen te slaan tussen die beide werelden, zegt Bouman, die ook actief is als ethisch hacker.
De technologische kennis die de leden van het CMIO-netwerk hebben, heeft niet iedere huisarts nodig, benadrukt hij. 'Een goede oplossing is een CMIO binnen de zorgroep of regio-organisatie die zorgt dat de basis op orde is. Als waarnemer kom ik overal en nergens en ik krijg nog regelmatig een wat verfrommeld papiertje in handen gedrukt met een algemeen account met wachtwoord, waar alle waarnemers in die praktijk gebruik van maken. Dat moet bijvoorbeeld een gepersonaliseerd account zijn.'
De meest voorkomende datalekken zijn toch nog altijd de spreekwoordelijke 'dossiers die in de winkelwagen worden achtergelaten'. 'Alleen al daarom is een belangrijke stelregel: print zo weinig mogelijk, het is heel vaak niet nodig. En áls er iets misgaat, bepaalt de manier waarop je daarmee omgaat, het vertrouwen van patiënten. Een recent voorbeeld is het datalek bij de GGD in het bron- en contactonderzoek – dat is echt schadelijk. Het lek was begin november al bekend en werd eind januari pas verholpen. Onze patiënten verwachten niet dat alles waterdicht is, maar wel dat de informatieveiligheid morgen beter is dan vandaag en dat wij daar als zorgverleners transparant over zijn.'
Begin juni organiseren de LHV Academie, Technische Universiteit Eindhoven en het CMIO Netwerk Eerste Lijn een tweedaagse masterclass voor huisartsen die de rol van CMIO (willen) vervullen. Heeft u belangstelling voor het netwerk of de masterclass? Dan vindt u meer informatie op www.cmionetwerk.nl.