Tekst: Jan Bos
Beeld: Marcel Leuning

Ik zal geheimhouden wat mij is toevertrouwd – onderdeel van de eed die iedere arts heeft afgelegd. Geestelijk vader van de artseneed is Hippocrates. Had hij kunnen vermoeden dat patiëntengegevens ooit digitaal zouden worden opgeslagen, dan had hij dit onderdeel van de eed wellicht wat actiever geformuleerd. Want in deze tijd van internet vraagt het beroepsgeheim meer dan zwijgen over wat je is toevertrouwd.

Digitale veiligheid in de praktijk

Huisarts Willem Vaarkamp (59) voert sinds 1985 een praktijk in Badhoevedorp. “Ik doe het in m’n eentje, dat komt niet veel meer voor. Ik ben dan ook een solist”, zegt hij over zichzelf. Hij maakt lange werkweken waarbinnen hij ook tijd moet vinden om de steeds complexer wordende administratie op orde te houden. Daarbij maakt hij dankbaar gebruik van moderne digitale systemen. Dat aan het werken met die systemen ook de nodige risico’s zijn verbonden, bijvoorbeeld omdat vertrouwelijke informatie in verkeerde handen kan vallen, is hij zich nauwelijks bewust. “Er is nog nooit iets gebeurd”, zegt hij terwijl hij bezwerend op zijn houten bureau klopt, “dus ik hoop maar dat het regionale informatiesysteem waarbij ik ben aangesloten goed beveiligd is.”

Hoewel Vaarkamp zelf slachtoffer is geweest van fraude met zijn bankpas, heeft hem dat ten aanzien van zijn patiëntengegevens niet alerter gemaakt. Hij weet bijvoorbeeld niet wat er in het contract met de leverancier van het systeem staat over de beveiliging van patiëntengegevens. Het wachtwoord heeft hij in de vier jaar dat hij met het informatiesysteem werkt, nimmer gewijzigd. Elke ochtend logt hij in en pas aan het eind van de werkdag logt hij uit, waardoor de gegevens tijdens zijn patiëntenbezoeken door kwaadwillenden zijn te raadplegen. “Als ik er overdag even niet ben, kunnen de mensen in de wachtkamer in mijn computer”, geeft hij toe, “maar wie heeft daar nou belang bij? Dat is misschien naïef, maar ik kan me gewoon niet voorstellen dat iemand in mijn gegevens zou willen snuffelen.”

De huisarts realiseert zich dat zijn houding ten opzichte van digitale veiligheid niet strookt met het beroepsgeheim. “Dat wringt, maar ik denk al snel dat het zo’n vaart niet zal lopen. En ik word er ook nooit op aangesproken. Als gekwalificeerd huisarts moet je aan allerlei eisen voldoen, je moet bijvoorbeeld je verslagen volgens bepaalde richtlijnen opstellen, maar nog nooit heeft iemand mij gevraagd hoe ik de gegevens in de computer opsla.”

Aansprakelijk

“Schokkend.” Zo kwalificeert hoogleraar Digitale Beveiliging Bart Jacobs de manier waarop huisarts Vaarkamp met digitale veiligheid omgaat. “Het is goed dat hij daar openhartig over praat, maar vanuit mijn vakgebied is het natuurlijk verschrikkelijk”, gruwt de cyber security-expert in zijn kamer op de tweede verdieping van de Radboud Universiteit. “Ik begrijp heel goed dat artsen het beheer van hun dossiers uitbesteden, maar dat ontslaat ze niet van hun verantwoordelijkheid. Zij blijven ook in juridische zin aansprakelijk voor een goed dossierbeheer.”

Voor Jacobs zou het een koud kunstje zijn om in het informatiesysteem van Vaarkamp in te breken. “Ik zou hem een mailtje sturen met een besmette bijlage, bijvoorbeeld een fictieve uitnodiging voor een congres”, fantaseert hij hardop. “Zodra hij die bijlage opent, wordt er malware geïnstalleerd en krijg ik inzicht in de toetsen die hij aanslaat en heb ik dus ook het wachtwoord. Dat is helemaal niet zo moeilijk.”

Jacobs hamert erop dat een gebrekkige beveiliging veel meer schade kan aanrichten dan men zich lijkt te realiseren. “Je moet je voorstellen dat op straat komt te liggen wie een psychiatrisch verleden heeft of wie een geslachtsziekte heeft opgelopen. Dat kan grote consequenties hebben voor iemands loopbaan. Bovendien kunnen gegevens ook worden verwijderd of aangepast. En een eventuele schadeclaim gaat dan naar de arts, niet naar de softwareleverancier, want de arts is verantwoordelijk voor de bescherming van de privacy van zijn patiënten.”

Ondanks het beroepsgeheim gaan artsen soms slordig om met persoonlijke gegevens, weet Jacobs uit eigen ervaring. “Mijn eigen tandarts vroeg een keer naar mijn burgerservicenummer (BSN), maar hij checkte niet of het nummer dat ik gaf wel klopte. ‘Ik ben toch geen politieagent’, zei hij toen ik hem erop aansprak. Door zo’n lakse houding loop ik zelf ook een risico, bijvoorbeeld wanneer iemand mijn BSN opgeeft en niet gecontroleerd wordt. Ik vind zo’n laconieke opstelling strijdig met het beroepsgeheim. Artsen moeten zich veel meer inspannen om gegevens te beschermen.”

Wisselwerking

Jacobs noemt het evident dat digitale veiligheid onder zorgverleners veel meer aandacht behoeft, de discussie over het epd ten spijt. “Iedereen steekt zijn kop in het zand”, constateert de hoogleraar. “Het epd voorzag ook in normen en richtlijnen voor uitwisseling van gegevens, maar die zijn nu van tafel verdwenen. Alsof de problemen daarmee zijn opgelost. Ondertussen gaat de uitwisseling natuurlijk gewoon door. De overheid moet zorgen voor duidelijke normen en voor een betrouwbare ICT-infrastructuur, maar de minister loopt weg voor die verantwoordelijkheid. Ik vind dat zorgelijk. De overheid zorgt toch ook voor normen voor brandveiligheid, waarom dan niet voor digitale veiligheid?”

De beveiligingsexpert ziet de oplossing vooral in een wisselwerking tussen ICT-systemen en bewustzijn. “Bij het gebruik van informatiesystemen moeten artsen met de risico’s worden geconfronteerd, bijvoorbeeld dat je alleen kunt inloggen met een pasje. Op die manier word je vanzelf gedwongen om op een veilige manier te werken.”

Huisarts Willem Vaarkamp zou al blij zijn wanneer de beroepsvereniging voorlichtingsavonden over cyber security zou organiseren. “Dit zet me wel aan het denken”, erkent hij, “maar het zou centraal opgepakt moeten worden. Als het Genootschap een scholingsavond organiseert, ben ik zeker van de partij.”

Tips

- Verstuur geen vertrouwelijke gegevens per e-mail.
- Leg afspraken over beveiliging vast in de overeenkomst met de leverancier van een informatiesysteem.
- Spreek met medewerkers over het belang van digitale beveiliging.
- Installeer antivirusprogramma’s en een firewall op alle computers.
- Kies voor een sterk wachtwoord van minstens 12 tekens en gebruik geen woorden, maar combinaties van cijfers, letters en tekens.
- Beveilig het draadloze netwerk met een sterk wachtwoord.
- Zorg ervoor dat software en hardware altijd bijgewerkt zijn door updates direct te installeren.
- Gebruik per toepassing een verschillend sterk wachtwoord.
- Verander de wachtwoorden regelmatig.
- Raadpleeg een externe partij wanneer de eigen kennis onvoldoende is.