PEILSTATIONS

Bescherming patiëntgegevens door tandartsen

Met de Algemene verordening gegevensbescherming (AVG), zie ook pagina 26 in dit *Nt*, worden per mei 2018 de regels rond de bescherming van persoonsgegevens flink aanscherpt en uitgebreid. Medio 2016 deed de KNMT onderzoek naar de uitwisseling van patiëntgegevens in tandartspraktijken. In *Nt* 7/2017, p. 41 is belicht hoe vaak en op welke manieren dit gebeurt. Deze bijdrage is gewijd aan de beveiliging van digitale patiëntgegevens.

Bijna alle (99%) tandartsen hebben hiervoor maatregelen getroffen. De tabel laat zien welke dit zijn. Veruit de meeste ondervraagden hebben dit gedaan rond de kwaliteit en beveiliging van het (computer)netwerk tegen externe invloeden (86%) en/of rond de toegang van externe partijen (73%). En waar het gaat om de interne beveiliging heeft 76% beleid met betrekking tot het computergebruik door de medewerkers. Veel minder tandartsen noemen maatregelen voor de interne kwaliteit en beveiliging van het (computer)netwerk (51%) en/of voor procedures inzake hun medewerkers (36%). Denk bijvoorbeeld aan een protocol voor het melden van datalekken (21%).

Alle nieuwe beveiligingseisen die de wetgever stelt, zijn voor de beroepsgroep geen sinecure. Maar ook aan de al bestaande eisen wordt nog niet altijd voldaan. Zo is de Meldplicht datalekken al per 2016 van kracht, maar heeft nog slechts een vijfde van de tandartsen hiervoor in de praktijk een protocol of procedure.

Maatregelen tegen misbruik van digitale patiëntgegevens, naar vijf aspecten van beveiliging #1	
kwaliteit en beveiliging van het (computer)netwerk (extern)	**86%**
- modern en veilig wifi-netwerk (met eventueel aparte of geen toegang voor gasten)	68%
- computernetwerk heeft een up-to-date (next generation) firewall	64%
- e-mails worden beveiligd verstuurd (versleuteld of via elektronische berichtendienst)	17%
beveiliging van de externe toegang	**73%**
- externe partijen (zoals softwareleveranciers) hebben geen onbeperkte toegang	61%
- externe toegang tot computernetwerk is versleuteld via VPN of SSL-VPN	37%
- leveranciers voldoen aan de huidige beveiligingseisen (nagegaan en vastgelegd)	12%
kwaliteit en beveiliging van het (computer)netwerk (intern)	**51%**
- automatische schermbeveiliging (‘clear screen’) wanneer niet wordt gewerkt	43%
- bijhouden van een ‘logging’ in alle digitale systemen en regelmatige controle van de data	17%
computergebruik door medewerkers	**76%**
- beleid voor gedifferentieerde toegang tot het computersysteem	60%
- beleid voor wachtwoordbeveiliging	44%
- beleid voor gebruik van usb-sticks / externe disks	35%
procedures inzake medewerkers	**36%**
- gebruik van in- en uit-dienstprocedures (accounts blokkeren e.d.)	23%
- gebruik van een interne procedure/protocol voor het melden van datalekken	21%

n = 266
#1 meer antwoorden mogelijk
bron: Project Peilstations, Omnibus-enquête najaar 2016