NEN EN NTA

Een nieuwe norm voor veilig mailen

In mei 2019 publiceerde het NEN de NTA 7516 met als titel *Medische Informatica – Eisen voor veilige e-mail en chat-applicaties (uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie)*. NTA, NEN, wat zijn dat eigenlijk?

CAROLINE NORG-SCHULPEN
PRAKTIJK.NORG@HOME.NL

NEN is de afkorting voor *Nederlandse Norm* en is tevens de naam van het Nederlands Normalisatie-instituut. Normalisatie betekent dat betrokken partijen in overleg een norm vaststellen over een product, dienst of proces. Die norm is een op consensus gebaseerde afspraak, dus geen wet. Het is een 'best practice' die op vrijwillige basis gevolgd kan worden. Het instituut NEN is het kennisnetwerk dat de partijen ondersteunt bij het vaststellen van deze normen.
NTA staat voor Nederlandse Technische Afspraak, een variant (of voorloper) van een norm. Als er niet per se consensus nodig is van alle belanghebbenden of snelle ontwikkelingen binnen de technologie hier geen tijd voor bieden, kan er voor een NTA worden gekozen.
Door zich te houden aan NEN en NTA kan een (zorg)instelling aangeven dat er vertrouwen gesteld kan worden in de betreffende dienst.

Richtlijnen

In *SynthesHis* nummer 3 van 2017 staat een artikel over het op een veilige manier versturen van vertrouwelijke informatie via e-mail. Dit ging vooral over de technische vereisten. Wat voegt de NTA 7516 hier nog aan toe voor de huisarts? We zetten enkele opvallende zaken uit het 52 pagina's tellende document op een rijtje.
De NTA 7516 stelt dat een huisartsenpraktijk zijn patiënten een veilig middel ter beschikking moet stellen om contact op te nemen met de praktijk. Dit kan een veilige e-mailoplossing zijn, een contactformulier of een patiëntenportaal. Op de website moet duidelijk kenbaar worden gemaakt hoe de patiënt contact kan opnemen.
In de NTA staan ook richtlijnen voor de aanbieders van de software voor e-mail en patiëntenportaal. Zij moeten in hun productinformatie duidelijk maken aan welke van de volgende criteria zij voldoen:

- De ontvanger (een andere zorgverlener of de patiënt) moet meteen kunnen zien wie de afzender is van een bericht. Een e-mailadres moet er dus uitzien als piet@huisartsenpraktijk.nl en niet als ph2ghjr@iuveu.tr.
- Het beantwoorden van een door de huisarts aan de patiënt of andere zorgverlener gestuurd bericht moet automatisch veilig zijn. Het op een veilige manier doorsturen van het bericht is de verantwoordelijkheid van de eerste ontvanger. Deze moet er wel op gewezen worden dat dit mogelijk niet veilig is.
- Het berichtenverkeer (de techniek) moet 99,8% per jaar beschikbaar zijn, oftewel mag maximaal 17,5 uur per jaar ongepland uitvallen.
- De maximale geplande aaneengesloten uitvalduur (bijvoorbeeld bij onderhoud) is 24 uur.

EEN E-MAILADRES MOET ER DUS UITZIEN ALS PIET@HUISARTSENPRAKTIJK.NL EN NIET ALS PH2GHJR@IUVEU.TR

Betrouwbaarheidsniveau

In uw huisartsenpraktijk moet gedocumenteerd worden wat voor de praktijk de vastgestelde minimale eisen zijn voor beschikbaarheid, integriteit, gebruiksvriendelijkheid en interoperabiliteit voor de software.
Als het gaat om het uitwisselen van medische gegevens ('spreekkamerinformatie') is het betrouwbaarheidsniveau 'hoog' vereist voor de authenticatie. Dit betekent minimaal tweefactorauthenticatie. Voor de informatie die minder risico's heeft met betrekking tot de vertrouwelijkheid, 'wachtkamerinformatie', kan de verzender een aparte risicoafweging maken.
Vervolgens moeten er in de praktijk regels zijn over het werken met de e-mail, het patiëntenportaal of de chat. Wie heeft er toegang tot de functionele berichtenbox (bijvoorbeeld info@huisartsenpraktijk.nl)? Hoe zit het met waarneemsituaties? Hoe lang worden mails bewaard? Waar worden berichten opgeslagen?
Let ook op het gebruik van geautomatiseerde functies (auto-reply, leesbevestiging): gebeurt dit ook veilig? ■