Vlaams Parlement

SCHRIFTELIJKE VRAAG

nr. 263
van **ELKE SLEURS**
datum: 14 maart 2019

---

aan **JO VANDEURZEN**
VLAAMS MINISTER VAN WELZIJN, VOLKSGEZONDHEID EN GEZIN

Ziekenhuizen van de toekomst - Big data en digitale beveiliging

In het groenboek 'Ziekenhuis van de toekomst' lezen we dat big data zowel voor de zorgactoren (huisartsen, thuisverpleegkundigen, ziekenhuisartsen, verpleegkundigen enzovoort) als de patiënten een rode draad zullen zijn. Het gebruik van een elektronisch patiëntendossier is in de gezondheidzorg al geïntegreerd. De uitwisseling van data tussen patiëntendossiers en de analyse daarvan is nog een grote uitdaging. Een handvol ziekenhuizen is mee op de digitale trein gesprongen maar nog lang niet allemaal. Daar komt nog bij dat de nood aan geïntegreerde informatiedeling groot is, waarbij zorgactoren actief kunnen zijn binnen één patiëntvolgend dossier, waardoor de digitale kloof alsmaar dieper wordt. Die geïntegreerde data geven de artsen de mogelijkheid om te anticiperen op de behoeften van de patiënt om proactief zorg toe te dienen en preventie te stimuleren. Het laat ook toe de kennisvertaling van de onderzoeken bij de patiënten sneller te interpreteren. Big data maakt namelijk suggesties op basis van real-timeanalyse van patiëntengegevens. Hierdoor kan zeer kort op de bal gespeeld worden.
De keerzijde van de big datamedaille is de gegevensbeveiliging, het beschermen van de vertrouwelijkheid van gegevens. De opstellers van het groenboek benadrukken dat cyberinbreuken een grote bedreiging vormen voor de ziekenhuizen van de toekomst. Digitale beveiliging van ziekenhuizen of cybersecurity is immers zeer belangrijk en bovendien gevoelig voor hackers.

In Nederland heeft men hier onlangs onderzoek naar gedaan. Een van de conclusies is dat kleine ziekenhuizen beter beveiligd zijn dan grote ziekenhuizen omdat zij op modernere softwareprogramma's draaien.

1. Zijn onze Vlaamse ziekenhuizen klaar om de digitale omslag te maken, om big data toe te laten in hun technologische systemen? Indien niet, waar liggen de knelpunten?
2. Zullen de gebruikte softwareprogramma's op punt worden gesteld om cyberaanvallen tegen te gaan? Kan een cybersecuritybedrijf (zoals men in Nederland heeft gedaan) worden ingeschakeld om de digitale beveiliging te testen? Indien niet, waarom niet?

JO VANDEURZEN
VLAAMS MINISTER VAN WELZIJN, VOLKSGEZONDHEID EN GEZIN

ANTWOORD
op vraag nr. 263 van 14 maart 2019
van **ELKE SLEURS**

---

1. We hebben er geen zicht op of de Vlaamse ziekenhuizen op dit ogenblik klaar zijn om big data toe te laten in hun technologische systemen. Vele big data analyses kunnen geanonimiseerd gebeuren, zonder enig gevaar voor de privacy van de personen wiens data wordt gebruikt. Real-time beslissingen zijn gebaseerd op heuristieken die uit dergelijke analyses komen, maar dat is voorlopig nog toekomstmuziek. Wat ook een verklaring is waarom het is opgenomen in het groenboek 'Ziekenhuis van de toekomst'. Voor zover we weten wordt dergelijke proactieve beslissings-ondersteuning nog niet in Vlaanderen ingezet.

2. Systemen die de blootstelling aan cyberaanvallen kunnen minimaliseren zijn zeer kostelijk. De kost van ICT in de ziekenhuizen bedroeg in 2015 560 miljoen, waarvan 65 miljoen rechtstreeks gefinancierd via de meaningful use financiering van het EPD. Sindsdien zijn de kosten enkel nog maar gestegen, mede omwille van de extra investeringen in geïntegreerde EPD's.

   Een audit kan maar dit zal leiden tot bijkomende kosten voor de ziekenhuizen. Zowel wat big data betreft als digitale veiligheid kan financiering een belangrijke belemmering of stimulans zijn. De financiering van de ziekenhuizen is de bevoegdheid van de Federale overheid.

   Voor zover we weten is het aantal privacy accidenten vooralsnog zeer beperkt en deze moeten onder de GDPR-wetgeving (General Data Protection Regulation) ook onmiddellijk aan de gegevensbeschermingsautoriteit (GBA) gemeld worden.