AH 474
2026Z17530

Antwoord van minister Hermans (Volksgezondheid, Welzijn en Sport) (ontvangen 27 oktober 2026)

Zie ook Aanhangsel Handelingen, vergaderjaar 2026-2027, nr. 69

Vraag 1.

Bent u bekend met het artikel 'China bestormt Europa nu ook met medische apparaten'[1] naar aanleiding van de podcast Dagkoers van het Financieel Dagblad?

Antwoord 1.

Ja, daar ben ik mee bekend.

Vraag 2.

Wordt er in Nederlandse ziekenhuizen momenteel gebruik gemaakt van Chinese medische technologie? Zo ja, om wat voor technologie gaat het en worden er ook gevoelige persoonsgegevens verwerkt, behandeld of opgeslagen? Wie voert de updates uit en doet het onderhoud van deze technologie?

Antwoord 2.

Ja, meerdere Nederlandse ziekenhuizen beschikken over medische technologie van Chinese leveranciers, waaronder patiëntbewakingssystemen, echoapparatuur en infuuspompen. Of en welke patiëntgegevens worden verwerkt, waar deze gegevens worden opgeslagen en wie toegang heeft, is afhankelijk van het specifieke hulpmiddel en de technische inrichting binnen het ziekenhuis. Ook updates en onderhoud kunnen verschillend zijn georganiseerd. De updates en het onderhoud kunnen worden uitgevoerd door (de serviceorganisatie van) de fabrikant, een geautoriseerde servicepartij of de technische dienst van het ziekenhuis.

Vraag 3.

Klopt het dat het St. Antonius Ziekenhuis gebruikmaakt van patiëntmonitoren van een Chinees bedrijf? Zo ja, wat vindt u hiervan, hoe wordt bescherming van patiëntgegevens gewaarborgd? Zijn er (Europese) alternatieven?

---

[1] Het Financieel Dagblad, 25 augustus 2026, 'China bestormt Europa nu ook met medische apparaten', https://fd.nl/economie/1609835/china-bestormt-europa-nu-ook-met-medischeapparaten?utm_medium=email&utm_source=nieuwsbrief&utm_campaign=fd ochtendnieuwsbrief&utm_content=1352427_52160_20260825&utm_term=A

Antwoord 3.

Ja, dat klopt.

Ziekenhuizen zijn zelf verantwoordelijk voor de inkoop van medische hulpmiddelen, waaronder patiëntmonitoren. Bij de aanschaf van medische technologie worden verschillende factoren afgewogen, waaronder kwaliteit, veiligheid, kosten en de beschikbaarheid van een betrouwbare serviceorganisatie, onderhoud en onderdelen. Bij netwerkverbonden medische technologie wordt daarnaast beoordeeld welke risico's ontstaan op het gebied van continuïteit van zorg, cybersecurity en gegevensverwerking. Dit gebeurt op basis van de geldende wet- en regelgeving en richtlijnen voor de veilige toepassing van medische technologie, privacy en dataveiligheid.

In het specifieke geval van de patiëntmonitoren binnen het St. Antonius Ziekenhuis acht het kabinet de risico's voor patiëntgegevens beperkt, omdat de monitoren geen patiëntengegevens verzamelen of opslaan. Meerdere leveranciers bieden mobiele patiëntmonitoring aan. De geschiktheid van een alternatief is echter wel afhankelijk van de beoogde toepassing en de technische en organisatorische context van het ziekenhuis.

Het kabinet begrijpt dat zorginstellingen mogelijk zorgen hebben over de veiligheid van medische gegevens. Wanneer zij vragen hebben over de beveiligings- en privacyaspecten van gegevensdoorgifte buiten de EU, zijn bij verschillende instanties relevante hulpmiddelen en informatie beschikbaar. Zo publiceert de Autoriteit Persoonsgegevens (AP) informatie over het gebruik en delen van gezondheidsgegevens. Ook het Nationaal Cyber Security Centrum (NCSC) publiceert kennisproducten over dit onderwerp. Tot slot vervult Z-CERT niet alleen een rol bij de afhandelingen van beveiligingsincidenten, maar zet de organisatie zich ook preventief in. Z-CERT deelt informatie over dreigingen en kan zorgorganisaties waarschuwen wanneer zorginstellingen met risico's te maken hebben of kunnen krijgen. Het waarschuwen voor dreigingen is een van de wettelijke taken van Z-CERT op grond van de Cyberbeveiligingswet (Cbw).

Vraag 4.

Op welke wijze is gewaarborgd dat medische gegevens van Nederlanders niet in handen komen van niet Europese bedrijven of organisaties?

Antwoord 4.

Het kabinet erkent de zorgen die hierover leven in het veld. Fabrikanten zijn op grond van de Europese Verordening Medische Hulpmiddelen (MDR) verplicht om de medische software die zij op de markt brengen te beschermen tegen ongeoorloofde toegang. Daarnaast stelt de AVG zeer strikte voorwaarden aan de verwerking en doorgifte van persoonsgegevens, waaronder patiëntendata. Het is

in de eerste plaats aan zorgaanbieders en hun toeleveranciers om binnen dit kader te borgen dat buitenlandse wetgeving niet leidt tot onrechtmatige toegang tot patiëntendata.

Wanneer (zorg)data wordt ondergebracht bij een buitenlandse aanbieder (buiten AVG gebied), dan moet verplicht een toets worden gedaan of de geldende wet- en regelgeving binnen dat land een voldoende beveiligingsniveau biedt. Hieruit volgt dat een jurisdictie toets gedaan moet worden. Immers, moet een opdrachtgever eerst weten welke jurisdictie van toepassing is voordat deze kan worden getoetst.

Tot slot wil het kabinet benadrukken dat zorginstellingen zelf verantwoordelijk zijn voor het in kaart brengen van risico's in relatie tot gegevensbescherming en deze verantwoordelijkheid ziet ook op het maken van afgewogen keuzes om genoemde risico's te beperken door aanvullende maatregelen te nemen zoals versleuteling van medische data. Er moet langs verschillende lijnen maatregelen worden genomen om ongeoorloofde toegang tot medische gegevens, bijvoorbeeld door hacks of cyberaanvallen, te voorkomen.

Vraag 5.

Deelt u de zorgen omtrent spionage, misbruik en privacy bij het gebruik van medische technologie van Chinese aanbieders? Zo nee, waarom niet?

Antwoord 5.

Het kabinet begrijpt dat er zorgen zijn omtrent spionage, misbruik en privacy bij het gebruik van medische technologie uit derde landen gezien de huidige geopolitieke situatie. Zorgaanbieders zijn zelf verantwoordelijk voor het in kaart brengen van deze risico's en voor het maken van afgewogen keuzes, waarmee zij invulling kunnen geven aan hun digitale autonomie.

Er zijn verschillende hulpmiddelen beschikbaar die zorgaanbieders kunnen ondersteunen bij het in kaart brengen en beoordelen van risico's. Zo biedt NEN een risicotool voor NEN 7510, waarmee zorgaanbieders ook aspecten van digitale autonomie en afhankelijkheid van leveranciers kunnen meenemen in hun risicoafweging. Daarnaast kunnen zij de Cybercheck van de AIVD, het NCSC, CIO Rijk en de NCTV gebruiken om risico's in de digitale toeleveringsketen te signaleren en te beoordelen.

Vraag 6.

Welke bevoegdheden hebt u om te garanderen dat medische informatie niet in Chinese handen komt te vallen? Als deze bevoegdheden onvoldoende zijn, aan welke mogelijkheden denkt u om dit wel te kunnen garanderen?

Antwoord 6.

De AVG regelt juridisch de beveiliging en doorgifte van persoonsgegevens af. Zorgaanbieders zijn op grond van de AVG verantwoordelijk voor het adequaat beschermen van medische informatie en moeten daarbij de risico's van het gebruik van niet-Europese leveranciers zorgvuldig afwegen. Binnen Nederland is daarnaast wettelijk geregeld dat organisaties die medische persoonsgegevens verwerken op grond van de norm voor informatiebeveiliging in de zorg, de NEN 7510, een risicoanalyse moeten doen. De AP en IGJ hebben de bevoegdheid om toezicht op de naleving van deze regels te houden.

Vraag 7.

Deelt u de wens dat Nederland en Europa voor medische technologie niet te afhankelijk mogen worden van Chinese aanbieders? Zo ja, wat doet u hieraan?

Zo nee, waarom niet?

Vraag 8.

Deelt u de wens dat het goed zou zijn om waar mogelijk te investeren in Nederlandse en Europese alternatieven zodat zorginstellingen, zoals ziekenhuizen, kunnen kiezen voor veilige alternatieven? Zo nee, waarom niet?

Antwoord 7 en 8.

Het kabinet vindt het van belang om de mogelijke gevolgen van het toenemende marktaandeel van Chinese medische technologiebedrijven voor de Europese industriële basis en risicovolle strategische afhankelijkheden nauwlettend te volgen. Aan de andere kant kan deze groei bijdragen aan lagere kosten en meer keuzemogelijkheden voor zorginstellingen, wat de toegankelijkheid en betaalbaarheid van medische technologie ten goede kan komen.

Het kabinet werkt in algemene zin aan de weerbaarheid van ons zorgsysteem en hanteert hierin geen landenspecifieke aanpak. Zo trekt het kabinet bijvoorbeeld € 102,5 miljoen uit voor versterking van de Nederlandse MedTech-sector. Deze publiek-private investering komt als reactie op het Groeiplan MedTech, onderdeel van het rapport Wennink. Het kabinet werkt samen met de sector toe naar één MedTech-ecosysteem, met aandacht voor start-ups, midden- en kleinbedrijf (mkb), kennisinstellingen, technische universiteiten, zorginstellingen, en het grootbedrijf. Dit plan, genaamd MedTech 2035, heeft de ambitie dat Nederland in 2035 het sterkste MedTech-ecosysteem in Europa heeft. Daarin dienen onderzoek, zorg en industrie naadloos samen te werken aan een toekomstbestendig en passend zorgsysteem voor Nederland en economische impact.

Daarnaast voert het ministerie van VWS een marktconsultatie uit naar mogelijkheden voor opschaalbare productiecapaciteit van persoonlijke beschermingsmiddelen in Nederland. Deze productie zou de weerbaarheid van het Nederlandse zorgsysteem verder vergroten.