Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3617

Vragen van het lid **Van Haga** (Groep Van Haga) aan de Minister van Volksgezondheid, Welzijn en Sport over *het opslaan van medische gegevens van Nederlanders door externe softwareleveranciers* (ingezonden 20 juli 2023).

Antwoord van Minister **Kuipers** (Volksgezondheid, Welzijn en Sport) (ontvangen 12 september 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 3341.

Vraag 1
Hebt u kennisgenomen van het bericht «Zonder hun medeweten worden de medische dossiers van miljoenen Nederlanders gekopieerd en «ergens» opgeslagen» van NRC?[1]

Antwoord 1
Ja.

Vraag 2
Aangezien de Autoriteit Persoonsgegevens al in 2018 onderzoek deed naar het kopiëren van de medische gegevens van Nederlanders naar een commercieel systeem, kan dan geconcludeerd worden dat u al jaren op de hoogte was van deze grootschalige en mogelijk juridisch oneigenlijke dataverzameling in de Nederlandse zorg? Zo ja, kunt u dan uitleggen waarom hieraan niet eerder ruchtbaarheid is gegeven? Waarom is het Nederlandse volk hierover niet eerder grootschalig ingelicht?

Antwoord 2
Ik ben ervan op de hoogte dat de Autoriteit Persoonsgegevens (AP) in 2018 een vooronderzoek heeft uitgevoerd. De AP zag destijds geen aanleiding tot vervolgonderzoek. De reden om geen vervolgonderzoek te doen was tweeledig. De AP constateerde dat de geëxtraheerde gegevens meteen automatisch worden versleuteld en alleen toegankelijk zijn voor de huisarts (die de sleutel heeft). De softwareleverancier en de ketenzorggroep hebben geen sleutel. Daarnaast worden medische gegevens niet met externen gedeeld, voor bijvoorbeeld wetenschappelijk onderzoek of statistiek.

[1] NRC, 18 juli 2023, «Zonder hun medeweten worden de medische dossiers van miljoenen Nederlanders gekopieerd en «ergens» opgeslagen» (https://www.nrc.nl/nieuws/2023/07/18/zonder-hun-toestemming-worden-de-medische-dossiers-van-miljoenen-nederlanders-gekopieerd-en-ergens-opgeslagen-a4170063).

ah-tk-20222023-3617
ISSN 0921 - 7398
's-Gravenhage 2023

Ten aanzien van het geven van ruchtbaarheid ligt de verantwoordelijkheid voor het informeren van betrokkenen over gegevensverwerkingen – in het algemeen en in deze casus – bij de betrokken huisartsen. Zij zijn verwerkingsverantwoordelijken in de zin van de Algemene verordening gegevensbescherming (AVG). Verwerkingsverantwoordelijken moeten richting betrokkenen en desgevraagd aan de AP – als onafhankelijke toezichthouder op de naleving van het gegevensbeschermingsrecht – kunnen aantonen dat zij in overeenstemming met de AVG persoonsgegevens verwerken.
De AP is een onafhankelijk zelfstandig bestuursorgaan (ZBO) en dat betekent onder meer dat zij niet verplicht is om mij te informeren over bepaalde gegevensverwerkingen waarnaar al dan niet onderzoek wordt verricht. Daarnaast gaat de AP zelf over de openbaarmaking van bij haar berustende informatie over bijvoorbeeld onderzoeken die naar bepaalde verwerkingen plaatsvinden.

Vraag 3
Kunt u uitleggen waarom in de Nederlandse (huisartsen)zorg op een dusdanig grootschalige manier gebruik wordt gemaakt van deze software(leveranciers), terwijl de medische privacy van mensen hierdoor in het geding komt en er juridische onduidelijkheid is over de validiteit van deze manier van dataverzameling?

Antwoord 3
De Nederlandse zorgsector is gefragmenteerd, waardoor ook de zorg-ICT-markten gefragmenteerd zijn. Mede hierdoor is een beperkt aantal leveranciers actief op de markt voor EPD/ECD-systemen in de eerstelijnszorg. Bovendien komen patiënten in hun zorgpad vaak veel verschillende zorgverleners tegen. Dit vereist dat artsen en zorgverleners de nodige patiëntgegevens makkelijk met elkaar kunnen delen en uitwisselen, iets wat in veel van hun ICT-systemen (nog) niet mogelijk is. Daarom kiezen steeds meer regionale samenwerkingsverbanden van huisartsen gezamenlijk voor VIPLive, een ICT-systeem dat informatie automatisch en eenvoudig uitwisselt, wat bovendien ook de administratieve lasten voor huisartsen verlaagt. De AP houdt als onafhankelijk toezichthouder toezicht op hoe VIPLive patiëntgegevens opslaat en deelt. Het is niet aan mij om te beoordelen of onderhavige gegevensdeling onrechtmatig is.

Vraag 4
Zijn er geen andere manieren om medische gegevens, indien nodig voor de behandeling van een patiënt, te delen met lokale behandelaars? Is er actief werk gemaakt van het onderzoeken van deze mogelijkheid en zo ja, welke analyses en afwegingen kwamen daaruit? Zo nee, waarom is er niet gezocht naar alternatieve methoden om de zorg voor patiënten in de regio anders te organiseren?

Antwoord 4
Binnen de ketenzorg werken meerdere zorgverleners vanuit verschillende organisaties samen aan de behandeling van één patiënt (bijvoorbeeld voor diabetes en COPD). Iedere organisatie heeft een eigen informatiesysteem, maar voor een integraal patiëntbeeld moet men ook de informatie van elkaar hebben. Er zijn verschillende methoden om medische gegevens te delen met andere behandelaars.
Regionaal en sectoraal zijn daardoor in de afgelopen jaren verschillende zorginfrastructuren ontstaan, waarbinnen medische gegevens worden uitgewisseld en opgeslagen. Deze zorginfrastructuren hebben zelf afspraken gemaakt over de wijze waarop de wet- en regelgeving wordt ingevuld. Op basis van hun rol van verwerkingsverantwoordelijke in de zin van de AVG is het aan de betrokken zorgaanbieders om te boordelen en vast te stellen of de gekozen oplossing – in dit geval Topicus/Calculus – voldoet aan de geldende wetgeving en normen ten aanzien van de AVG en informatiebeveiliging, dat Topicus/Calculus beschikt over de benodigde certificeringen voor de NEN 7510 en ISO 27001 en voldoet aan de normen van de NEN 7512 en NEN 7513.

Vraag 5
Waarom worden op een dusdanig grootschalige manier medische gegevens van zoveel Nederlanders opgeslagen, terwijl de gegevens van veel van deze mensen helemaal niet verzameld en gedeeld hoeven worden, aangezien daar geen medische noodzaak voor is? Waarom kan dit niet gerichter gebeuren en is de Nederlandse overheid hierover niet in gesprek gegaan met de partijen die aan dergelijke dataverzameling en opslag doen?

Antwoord 5
In het NRC-artikel wordt benoemd dat de patiëntgegevens uit VIPLive worden gekopieerd. In de moderne en «digitale» huisartspraktijk van nu is het digitaal werken en de bijbehorende centrale opslag van data nodig om het dagelijks werk en de patiëntenzorg goed en effectief uit te voeren. De nodige zorgvuldigheid in de omgang en het gebruik van patiëntengegevens is een aspect waar medewerkers in de zorg en ik ons dagelijks bewust van zijn. De desbetreffende data wordt opgeslagen in verschillende datacenters binnen de Europese Economische Ruimte (EER). Daarbij wordt data per praktijk strikt gescheiden opgeslagen.
Het is niet aan mij om te beoordelen of Topicus/Calculus voldoet aan de geldende wetgeving en normen ten aanzien van de AVG en informatiebeveiliging. Dit oordeel behoort toe aan de AP (en eventueel aan de rechter).

Vraag 6
Hoe worden de medische gegevens die worden opgeslagen door deze leverancier(s) beschermd? Weet u wat er met deze gegevens gebeurt, wat de betrokken investeringsmaatschappij precies doet en op welke manier zij kan beschikken over de medische gegevens die worden verzameld, waar deze precies zijn opgeslagen, om hoeveel en welke gegevens het precies gaat en of deze gegevens wellicht ook met andere partijen worden gedeeld, verkocht worden aan derden, of voor andere doeleinden worden gebruikt?

Antwoord 6
Nederlandse zorginstellingen zijn wettelijk verplicht om te voldoen aan de norm voor informatiebeveiliging in de zorg, de NEN 7510. De NEN 7510 geeft richtlijnen voor controlemaatregelen en stelt eisen aan het informatiebeveiligingssystemen. Bij de inzet van ICT-producten die medische gegevens verwerken, eisen zorgaanbieders van de softwareleveranciers van deze ICT-producten dat ook zij voldoen aan de NEN 7510 en de AVG. Voor de NEN 7510 dienen softwareleveranciers dit aan te tonen door middel van het hebben van een certificaat. Aan het voldoen aan de eisen van de AVG wordt invulling gegeven door het sluiten van een verwerkersovereenkomst, waarin duidelijk gezamenlijk is vastgelegd hoe de softwareleverancier de medische gegevens verwerkt en dat deze verwerking voldoet aan de AVG. De Inspectie Gezondheidszorg en Jeugd (IGJ) en de AP houden hier toezicht op.

Vraag 7
Hoe reflecteert u op de kritiek en de zorgen die artsen uiten over deze manier van dataopslag door een commerciële partij, zonder dat huisartsen daar per patiënt en per medisch dossier invloed op kunnen uitoefenen? Vindt u het geoorloofd dat de autonomie over deze datasharing niet bij de behandelaar, maar bij een softwareleverancier ligt?

Antwoord 7
Over het algemeen is het acceptabel dat zorgaanbieders commerciële softwareleveranciers – als verwerkers in de zin van de AVG – inschakelen die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerken. In dat kader moeten verwerkersovereenkomsten met de softwareleveranciers worden gesloten, waarin gezamenlijk afspraken worden gemaakt over de bescherming en beveiliging van persoonsgegevens (artikel 28 AVG). Uiteraard geldt daarbij ook dat verwerkers zich moeten houden aan de AVG. Dat betekent onder meer dat verwerkers (hier: de softwareleveranciers) de persoonsgegevens niet voor eigen/andere doeleinden mogen gebruiken. Op grond van de AVG blijft de arts – als verwerkingsverantwoordelijke – de zeggenschap houden over de wijze waarop de verwerking plaatsvindt.

Vraag 8
Hoe rijmt u deze grootschalige medische dataopslag, die ook nog plaatsvindt zonder informed consent van de patiënt, met de privacywetgeving, die voorschrijft dat er juist zo weinig mogelijk gevoelige persoonsgegevens verzameld en opgeslagen mogen worden? Kunt u uitleggen waarom dergelijke bedrijven blijkbaar wordt toegestaan om buiten de wet te handelen?

Antwoord 8
Het is niet aan mij om een oordeel te geven over de rechtmatigheid van de gegevensverwerkingen die hier aan de orde zijn. Dat vergt onder meer een gedegen onderzoek naar de feiten en omstandigheden en hoe die zich verhouden tot het relevante wettelijke kader. Dat is aan de AP, als onafhankelijke toezichthouder op de naleving van het gegevensbeschermingsrecht.

Vraag 9
Vindt u het geoorloofd dat commerciële softwareleveranciers met elkaar concurreren om privacygevoelige, medische data van mensen? Vindt u niet dat er hierdoor perverse prikkels en belangen ontstaan, ten koste van burgers, die hierdoor niets meer te zeggen hebben over hun eigen medische gegevens?

Antwoord 9
In Nederland is bewust gekozen voor een vrije markt, zodoende ook in de zorg-ICT. Ik ben van mening dat dit de ontwikkeling van innovatieve oplossingen ten goede komt. Zonder commerciële partijen zou het nodige ontwikkel- en innovatieklimaat niet bestaan. De commerciële softwareleveranciers zijn – net als niet-commerciële partijen – gebonden aan privacywetgeving. Ten aanzien van de inspraak die de patiënt behoort te hebben, is vastgelegd dat zorgverleners hun patiënten informeren dat hun medische gegevens worden opgeslagen en moeten zij hier tevens toestemming aan de patiënt voor vragen.

Vraag 10
Waarom kan het opslaan van medische gegevens om de zorg voor (chronisch) zieke mensen te verbeteren en (regionaal) te stroomlijnen niet gebeuren via een overkoepelend systeem van het Rijk, waarop alle zorgverleners in Nederland kunnen worden aangesloten? Vindt u niet dat dit een publieke voorziening zou moeten zijn, in plaats van dit over te laten aan de markt?

Antwoord 10
In de nationale visie is vastgesteld dat we naar een integraal georganiseerd gezondheidsinformatiestelsel moeten groeien, waarin data beschikbaar, bereikbaar en bruikbaar moet zijn voor preventie, het primaire zorgproces en secundair datagebruik. Daarvoor moeten burgers, zorgverleners, zorgaanbieders, onderzoekers en beleidsmakers vertrouwen hebben in elkaar en in het zorgvuldig gebruik van data. Om dat vertrouwen een rotsvaste basis te geven is regie vanuit VWS nodig.
Om deze basis te creëren zet ik in op de standaardisatie van taal en techniek en de implementatie van generieke functies. Standaardisatie maakt het mogelijk de huidige en nieuwe infrastructuren te verbinden waardoor een landelijk dekkend netwerk ontstaat. Voor een uitgebreide uiteenzetting van mijn beleidslijn om te
komen tot een landelijk dekkend netwerk van infrastructuren verwijs ik u graag naar mijn Kamerbrief van 13 april 2023 «Landelijk dekkend netwerk van infrastructuren».[2]

Vraag 11
Nu u weet dat de manier waarop medische gegevens worden opgeslagen voor veel huisartsen een (moreel) bezwaar is, bent u dan van plan om toch een vervolgonderzoek te laten doen naar deze dataverzameling?

---

[2] Kamerstuk 27 529, nr. 293.

Antwoord 11
De AP heeft in 2018 een vooronderzoek uitgevoerd. De AP zag destijds geen aanleiding tot verder onderzoek. De redenen hiervoor zijn in de beantwoording al eerder door mij benoemd. Het is uitdrukkelijk niet aan mij om aanvullend onderzoek te doen naar de rechtmatigheid van de gegevensverwerkingen die hier aan de orde zijn. Dat is aan de AP. Ik kan de AP ook niet vragen om dat onderzoek te doen, omdat de AP als onafhankelijke toezichthouder zelf beslist of zij al dan niet onderzoek doet naar bepaalde gegevensverwerkingen.

Vraag 12
Wat gaat u doen om Nederlanders actief op de hoogte te brengen van het feit dat hun medische gegevens op grote schaal worden verzameld door externe partijen? Indien u niets gaat doen, kunt u dan uitleggen waarom u dit niet nodig acht?

Antwoord 12
Ten aanzien van het geven van ruchtbaarheid ligt de verantwoordelijkheid voor het informeren van betrokkenen over gegevensverwerkingen – in het algemeen en in deze casus – bij de betrokken huisartsen. Zij zijn verwerkingsverantwoordelijken in de zin van de AVG. Verwerkingsverantwoordelijken moeten richting betrokkenen en desgevraagd aan de AP – als onafhankelijke toezichthouder op de naleving van het gegevensbeschermingsrecht – kunnen aantonen dat zij in overeenstemming met de AVG persoonsgegevens verwerken.

Vraag 13
Gaat u zorgen dat er duidelijke juridische kaders komen voor dergelijke medische dataverzameling en bent u voornemens om daarin op te nemen dat alleen medische gegevens die strikt noodzakelijk zijn voor de behandeling van een patiënt heel gericht verzameld en opgeslagen mogen worden en dat er duidelijke doeleinden worden verbonden aan het gebruik daarvan en wie daarover beschikking mogen hebben?

Antwoord 13
Er is al wet- en regelgeving die vereist dat medische gegevens goed worden beschermd. Zo is er de AVG en de Uitvoeringswet AVG (UAVG), op basis waarvan gezondheidsgegevens niet zomaar mogen worden verwerkt en waarin is geregeld dat betrokkenen in beginsel op de hoogte moeten worden gehouden van de verwerking van hun persoonsgegevens. Daarnaast stelt genoemde wetgeving eisen aan de verwerking van persoonsgegevens, zoals dat de verwerking rechtmatig, behoorlijk en transparant moet zijn.[3] Ook bepaalt de AVG dat er passende technische en organisatorische waarborgen moeten worden getroffen, zodat de gegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Dit laatste is in nationale wet- en regelgeving nader ingevuld. Zo is in het Besluit elektronische gegevensverwerking door zorgaanbieders bepaald dat zorgaanbieders moeten voldoen aan de informatiebeveiligingsnormen NEN 7510, NEN 7512 en NEN 7513. De AP houdt toezicht op de naleving van de AVG en andere (nationale) privacywetgeving in Nederland.
Daarnaast geldt het medisch beroepsgeheim, dat met zich brengt dat een hulpverlener in beginsel moet zwijgen over alles dat aan hem door de patiënt wordt toevertrouwd. Het belang van het wettelijk beroepsgeheim wordt benadrukt door de strafbaarstelling van schending ervan. Voor softwareleveranciers die als verwerker ten behoeve van de zorgaanbieder persoonsgegevens verwerken, geldt een afgeleid medisch beroepsgeheim. Dat betekent dat voor hen dezelfde (geheimhoudings)regels gelden als voor hulpverleners. Al deze regels borgen dat commercieel gebruik van medische gegevens niet zomaar is toegestaan.

[3] Uitzonderingen op art. 9 AVG (verbod op verwerking bijzondere persoonsgegevens) zijn te vinden in art. 24 en art. 30 UAVG.

Deze regels moeten worden nageleefd. Het is primair aan zorgaanbieders om te zorgen dat voldaan wordt aan de internationale en nationale wet- en regelgeving en daar de nodige voorzieningen voor te treffen.

Vraag 14
Hoe gaat u ervoor zorgen dat huisartsen niet aansprakelijk kunnen worden gesteld voor oneigenlijk gebruik en verspreiding van de medische gegevens van hun patiënten die zijn opgeslagen, aangezien zij op dit moment eindverantwoordelijk zijn voor de medische gegevens van hun patiënten en de veiligheid en bescherming daarvan?

Antwoord 14
Dat is niet aan mij. Of een huisarts tuchtrechtelijk en/of civielrechtelijk of uit anderen hoofde aansprakelijk of aanspreekbaar is vanwege overtreding van bepaalde wet- en regelgeving, hangt af van de relevante wet- en regelgeving en de concrete feiten en omstandigheden. Daarin kan ik niet treden. Overigens maak ik mij wel hard voor informatieveiligheid. Dit doe ik onder andere met het programma «Informatieveilig gedrag». Dit programma heeft als doel dat veel meer zorgorganisaties effectieve interventies kiezen om gedragsverandering bij zorgprofessionals te bereiken op het gebied van informatieveiligheid.

Vraag 15
Aangezien veel huisartsen op dit moment niet eens op de hoogte zijn van het feit dat de medische gegevens van hun patiënten via het softwaresysteem op wekelijkse basis worden gekopieerd en opgeslagen bij een externe partij, gaat u alle huisartsen in Nederland hier actief over informeren? Bent u voornemens om het voor huisartsen makkelijker te maken over te stappen naar een andere leverancier en transparant en inzichtelijk te maken wat de verschillen zijn tussen de verschillende softwareleveranciers die diensten aanbieden voor dataverzameling- en sharing en op welke manier zij weer verbonden zijn met andere partijen, zoals bijvoorbeeld zorgverzekeraars?

Antwoord 15
Huisartsen zijn zelf verantwoordelijk voor welke ICT-systemen zij gebruikmaken. Ook zijn huisartsen verantwoordelijk voor het bewaren en beschermen van medische gegevens van hun patiënten. Overstappen naar een andere softwareleverancier is voor zorgaanbieders bovendien altijd ingrijpend. Met het Actieplan zorg-ICT-markt probeer ik de markt opener, eerlijker en toekomstgericht te maken. Meer specifiek wil ik door inrichting van een catalogus van zorg-ICT-systemen, zorgaanbieders en ICT-inkopers in staat stellen om ICT-producten en diensten met elkaar te vergelijken, bijvoorbeeld op basis van functionaliteiten of keurmerken. Bovendien zal ik brancheorganisaties als NHG en InEen vragen om opslag en uitwisseling van elektronische patiëntgegevens en ICT-inkoopbeslissingen bij hun achterban onder de aandacht te brengen.

Vraag 16
Aangezien de handelwijze van Calculus in strijd lijkt te zijn met de privacywetgeving, omdat deze voorschrijft dat er niet op dusdanig grote schaal en op dezelfde plek dit soort gevoelige data opgeslagen mag worden, bent u voornemens om consequenties te verbinden aan deze gang van zaken? Zo ja, welke sancties gaat u stellen? Zo nee, waarom niet?

Antwoord 16
Dat er sprake is van overtreding van privacywetgeving staat niet vast, zolang de AP – als onafhankelijke toezichthouder – geen onderzoek heeft gedaan naar de relevante feiten en hoe die zich verhouden tot wet- en regelgeving inzake het gegevensbeschermingsrecht. Het verbinden van consequenties door mij is dan ook niet aan de orde. Als er sprake zou zijn van overtreding van privacywetgeving, dan is het aan de AP om al dan niet onderzoek in te stellen en/of eventueel handhavingsmaatregelen op te leggen.

Vraag 17
Heeft u een risicoanalyse gemaakt met betrekking tot een mogelijk datalek, of een hack? En weet u wat de gevolgen zouden (kunnen) zijn als deze medische gegevens van burgers op straat komen te liggen, of in handen vallen van criminelen?

Antwoord 17
Het maken van risicoanalyses en het eventueel treffen van risicomitigerende maatregelen is aan de organisatie die verantwoordelijk is voor de grootschalige verwerking van patiëntgegevens (de verwerkingsverantwoordelijke) en/of de verwerker zelf. Deze organisaties zijn onder omstandigheden verplicht hiertoe een gegevensbeschermingseffectbeoordeling (DPIA) te verrichten. Hierin moeten de risico's van de gegevensverwerking worden geïdentificeerd, evenals de maatregelen die moeten worden getroffen om die risico's weg te nemen.
De gevolgen van een datalek kunnen ernstig zijn.[4] Een gevolg hiervan kan financiële schade voor betrokkenen zijn, zoals identiteitsfraude en oplichting. Daarnaast kan een betrokkene als gevolg van een datalek immateriële schade lijden, wanneer gevoelige informatie over (mentale) gezondheid of problemen in de thuissituatie zijn gelekt.
Met betrekking tot het algemene dreigingsbeeld voor de zorgsector publiceert Z-CERT, het Computer Emergency Response Team voor de zorg, jaarlijks een cybersecurity dreigingsbeeld. In dit dreigingsbeeld worden trends, dreigingen en risico's voor de Nederlandse zorgsector beschreven[5]. In het laatst gepubliceerde dreigingsniveau typeert Z-CERT het risico op een datalek als «medium». Het risico op een hack wordt aangemerkt als «hoog». Zorginstellingen zijn in de eerste plaats zelf verantwoordelijk om deze risico's te beperken en de impact van incidenten te mitigeren. Dit neemt echter niet weg dat ik me ook inzet op het verkleinen van de risico's en de impact hiervan. Dit doe ik door te zorgen voor meer bewustwording, duidelijke normen en kaders, en het ondersteunen van Z-CERT.

Vraag 18
Worden er controles uitgevoerd op de systemen waarmee de medische gegevens van burgers worden verzameld, om de veiligheid van deze systemen te waarborgen en zo ja, is de Nederlandse overheid betrokken bij deze toetsing?

Antwoord 18
De softwareleveranciers van deze systemen zijn zelf verantwoordelijk voor de eigenschappen van het systeem voor wat betreft de informatiebeveiliging. Zij kunnen desgewenst hun systemen onafhankelijk laten toetsen aan gangbare normen op het gebied van informatiebeveiliging, zoals de ISO 27001 en de NEN 7510. Ook kunnen zij hiervoor desgewenst certificaten behalen, zodat zij kunnen aantonen dat zij volgens deze normen werken. Een certificering is niet verplicht. De certificerende partij moet daarvoor geaccrediteerd zijn door de Raad voor de Accreditatie, een private stichting.
Zorgaanbieders zijn zelf verantwoordelijk om te voldoen aan wet- en regelgeving op het gebied van gegevensbescherming (AVG) en informatiebeveiliging (o.a. de NEN 7510). De NEN 7510 stelt regels over informatiebeveiliging in leveranciersrelaties: alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke softwareleverancier die informatie van de organisatie verwerkt en/of opslaat. De zorgaanbieder kan daarbij bijvoorbeeld eisen van een softwareleverancier dat een certificaat aanwezig is.
De AP ziet toe op de naleving van de AVG. De AP en de IGJ houden beide toezicht op informatiebeveiliging bij zorgaanbieders en gaan daarbij uit van de norm NEN 7510. De AP richt zich daarbij primair op gevallen waar het zwaartepunt op de verwerking van persoonsgegevens ligt. De IGJ richt zich primair op gevallen waar het zwaartepunt op de kwaliteit van zorgverlening

[4] AP_Rapportage_datalekken_2022.pdf.
[5] Z-CERT_RapportDreigingsbeeld2022.pdf.

ligt. De AP en de IGJ hebben samenwerkingsafspraken gemaakt en vastgelegd in een Samenwerkingsprotocol[6].

Vraag 19
Wat gaat u doen indien er naar aanleiding van dit onderzoek van NRC grootschalig klachten worden ingediend door burgers/patiënten, die niet willen dat hun medische gegevens zonder hun toestemming zijn verzameld en opgeslagen door een externe partij? Op welke manier gaat u huisartsen hierbij ondersteunen en beschermen?

Antwoord 19
Ik ben niet direct betrokken bij de behandeling van klachten aan het adres van zorgaanbieders. Klachten dienen betrokkenen direct in bij een zorgaanbieder of diens klachtenfunctionaris of functionaris voor gegevensbescherming. Daarnaast kunnen betrokkenen klachten indien bij de AP.
Verder zijn huisartsen en andere zorgverleners zelf verantwoordelijk voor de keuze voor en inkoop van ICT-systemen en horen daarom afwegingen te maken hoe en waar de elektronische patiëntgegevens op worden geslagen. Zoals eerder ook al benoemd zal ik bij brancheorganisaties als NHG en InEen vragen om de opslag en uitwisseling van elektronische patiëntgegevens bij hun achterban onder de aandacht te brengen.

[6] Samenwerkingsprotocol AP-IGJ.