Inspectie Gezondheidszorg en Jeugd
Ministerie van Volksgezondheid, Welzijn en Sport

Rapportage van het inspectiebezoek in het kader van het toezicht op e-health aan Stichting Aafje Thuiszorg Huizen en Zorghotels te Rotterdam op 1 februari 2024

Utrecht, 28 mei 2024

Bedrijfsgevoelige informatie

Inhoud

1 Inleiding

De Inspectie Gezondheidszorg en Jeugd (de inspectie) bezocht op 1 februari 2024 Stichting Aafje (Aafje). Aafje is een zeer grote zorgaanbieder in Rotterdam en omstreken die zorg van A-Z levert. Dit wil zeggen dat zij naast verpleging en verzorging ook thuiszorg, revalidatiezorg, crisisopvang en dagbesteding aanbieden. De cliëntendoelgroep van Aafje is daardoor divers. De inzet van digitale zorg vindt met name plaats in de intramurale setting en in de thuiszorg. De raad van bestuur van Aafje bestaat uit twee personen. Een persoon van de raad van bestuur heeft het onderwerp digitale zorg specifiek in diens portefeuille. De raad van bestuur is onderdeel van het directieteam waar ook vijf directeuren, een controller en een secretaris onderdeel van zijn.

Het onderwerp van het bezoek was de inzet van informatie- en communicatietechnologie (ICT) in de zorg. Dit heet ook wel 'e-health' of 'digitale zorg'. De inspectie toetste of de zorgaanbieder bij het gebruik van e-health zorgt voor de nodige voorwaarden voor goede en veilige zorg, die volgen uit wetten, (veld)normen en richtlijnen op dit gebied.

1.1 Aanleiding en belang

Onder e-health verstaat de inspectie: de inzet van hedendaagse ICT, in het bijzonder internettechnologie, om de gezondheid en gezondheidszorg te ondersteunen of te verbeteren.

Voorbeelden hiervan zijn elektronische patiëntendossiers (EPD's of ECD's) en elektronische uitwisseling van gegevens. Met e-health bedoelt de inspectie dus ook de meer traditionele zorg-ICT. Maar ook patiëntenportalen, medische apps, monitoring van chronische patiënten[1] op afstand, en inzet van onlinebehandeling of begeleiding.

De inspectie is positief over de mogelijkheden die e-health kan bieden. E-health kan de zorg minder laten afhangen van tijd en plaats. Ook kan het de communicatie tussen patiënt (of cliënt/bewoner) en zorgverlener helpen. En die tussen zorgverleners. Dit wordt belangrijker nu de patiënt vaker te maken krijgt met een netwerk van zorgaanbieders.

Tegelijk vindt de inspectie het belangrijk dat de inzet van e-health doordacht gebeurt. Ook bij de inzet van e-health moet de zorgaanbieder de kwaliteit en veiligheid van de zorg bewaken. Vooral grote organisaties leunen steeds meer op e-health. Dat vraagt erom dat de zorgaanbieder zorgt voor goede voorwaarden in de zorgaanbieder.

De nieuwe mogelijkheden kennen helaas ook risico's. Denk bijvoorbeeld aan cyberaanvallen, de uitval van systemen, fouten ontstaan door systeemupdates of gebruikersfouten. Ook ontwikkelen de wetgeving en normering zich verder. Daarom kijkt de inspectie bij zorgaanbieders naar e-health. Daarbij toetst de inspectie of de zorgaanbieder zorgt voor de goede randvoorwaarden voor digitale zorg. In het toezicht op e-health betrekt de inspectie verschillende wetten, veldnormen en richtlijnen op het gebied van ICT in de zorg (zie 1.3).

[1] Waar in dit document gesproken wordt over de patiënt kan ook cliënt of bewoner worden gelezen.

1.2 Onderzoeksvragen

Het doel van het bezoek was om te toetsen of de zorgaanbieder bij de inzet van informatie- en communicatietechnologie (e-health) zorgt voor de nodige voorwaarden voor goede en veilige zorg, die volgen uit wetten, (veld)normen en richtlijnen op dit gebied.

1.3 Onderzoeksmethode en toetsingskader

Bij het bezoek gebruikte de inspectie een toetsingskader, dat is gepubliceerd op de website van de IGJ[2].

Een toetsingskader moet praktisch bruikbaar zijn. Daarom heeft de inspectie tijdens het bezoek gekeken naar de volgende vijf onderwerpen. Daarin zijn de verschillende normen en richtlijnen meegenomen.

Onderwerp	**Uitleg**
Goed bestuur en verantwoord innoveren	Het bestuur van de zorgaanbieder moet 'in control' zijn, ook op het gebied van e-health. Dit vraagt om een helder en gedragen beleid. Het bestuur moet de verantwoordelijkheden goed regelen bij inzetten van technische innovaties, zoals e-health. Ook een goede inrichting van de besluitvorming hoort daarbij.
Invoering en gebruik van e-health-producten en -diensten	De zorgaanbieder moet bij invoering en gebruik van e-health-producten en -diensten zorgen voor goede voorwaarden. De zorgaanbieder zorgt bijvoorbeeld voor duidelijke eisen aan producten en diensten. Ook moet de zorgaanbieder goed omgaan met mogelijke risico's. Belangrijke voorwaarden zijn verder goede training, goed testen en goed onderhoud.
Patiëntparticipatie	De patiëntenzorg wordt steeds afhankelijker van e-health. Daarom is het belangrijk dat de zorgaanbieder de cliëntenraad raadpleegt over het beleid. De zorgaanbieder kijkt hoe geschikt e-health-producten en -diensten zijn voor patiënten. Ook zorgt de zorgaanbieder voor goede informatie en begeleiding voor patiënten.
Samenwerken in het netwerk en elektronisch vastleggen en uitwisselen van gegevens	E-health kan andere vormen van samenwerken mogelijk maken tussen zorgverleners. Daarbij is het belangrijk dat de zorgaanbieder duidelijke afspraken maakt met andere zorgaanbieders over digitale samenwerking. Daarbij moet de zorgaanbieder zorgen voor goede organisatorische en technische maatregelen.
Informatiebeveiliging en continuïteit	De groeiende afhankelijkheid van ICT vraagt erom dat de zorgaanbieder zorgt voor de continuïteit. Daar horen goede afspraken en maatregelen bij voor informatiebeveiliging.

[2] Zie https://www.igj.nl/documenten/toetsingskaders/2018/11/15/toetsingskader-inzet-van-e-health-door-zorgaanbieders

De inspectie heeft het bezoek kort van tevoren bekend gemaakt. Dit was nodig om de zorgaanbieder de mogelijkheid te geven gesprekspartners vrij te maken.
Ook heeft de inspectie gevraagd om een aantal documenten ter voorbereiding op te leveren. Een overzicht staat in bijlage 2 van dit rapport.

Tijdens het bezoek heeft de inspectie met verschillende betrokkenen gesproken over de thema's van het toetsingskader. Dit waren personen in de volgende rollen:

- Raad van bestuur;
- Directeur Bedrijfsvoering;
- Manager ICT;
- Informatiemanager;
- Adviseur Kwaliteit en Veiligheid;
- Accountmanager Zorgtechnologie en Innovatie Wijkverpleging;
- Key-user ECD;
- Digicoach;
- Wijkverpleegkundige;
- Functioneel beheer Verpleeg Oproep Systeem (VOS);
- Maatschappelijke Medewerker Zorg
- Teammanager diensten;
- Lid centrale en lokale cliëntenraad;

Ook heeft de inspectie tijdens het bezoek twee e-health-toepassingen bestudeerd. Het gaat om de volgende voorbeelden:

1. Virtuele Thuiszorg, van leverancier Mobile Care. Binnen dit pakket aan Virtuele Thuiszorg kan de zorgaanbieder verschillende e-health toepassingen aanbieden aan hun cliënten. Tijdens het inspectiebezoek is gekeken naar de inzet van de medicatiedispenser die onderdeel is van het Mobile Care virtuele thuiszorg pakket.
2. Verpleeg Oproep Systeem (VOS), van het platform IQmessenger. De zorgaanbieder heeft dit systeem samen met AMR ICT partner geïmplementeerd op verschillende locaties. Tijdens het inspectiebezoek is gekeken naar de locatie Smeetsland.

Naast deze toepassingen gebruikt de zorgaanbieder nog diverse andere digitale producten en diensten, zoals dossier applicaties ONS (Nedap) en Ysis en andere relevante e-health toepassingen die ingezet worden in de thuissituatie.
Waar relevant worden deze apart in het document benoemd.

De resultaten van het inspectiebezoek staan in hoofdstuk 4 van dit rapport.
De beoordeling bij elk onderwerp volgt een vierpuntsschaal: afwezig, aanwezig, operationeel, geborgd. Zie bijlage 1 voor een uitleg over deze begrippen.

2 Conclusie

De inspectie concludeert dat de zorgaanbieder bij de inzet van ICT in de zorg (e-health) voor het merendeel zorgt voor de juiste randvoorwaarden voor goede en veilige zorg. In positieve zin vallen onder meer de heldere aanpak van de invoering en beproeving van innovaties op. Ook is er veel aandacht voor draagvlak, zowel bij cliënten als medewerkers. Bij de aanschaf van toepassingen betrekt de zorgaanbieder nog niet altijd de cliëntvertegenwoordiging, cliënten of hun naasten. De zorgaanbieder is actief in de regio als het gaat om gegevensuitwisseling. Gelet op het thema informatiebeveiliging is de zorgaanbieder actief bezig met de opzet van een werkende PDCA-cyclus. De zorgaanbieder heeft diverse audits uitgevoerd en is op dit moment bezig met de verbeteracties, her-audits en borging.

De inspectie komt tot de volgende deelconclusies:

De zorgaanbieder heeft een duidelijke visie op het thema digitale zorg. Dit is verwerkt in een koersplan. Ook zijn de verantwoordelijkheden duidelijk beschreven.
De zorgaanbieder heeft een visie opgesteld in het koersplan 2024-2028. De visie richt zich op digitaal tenzij. Het thema digitale zorg is bij meerdere niveaus in de organisatie belegd. Ook houdt de zorgaanbieder rekening met digitale zorg in haar begroting.

De invoering van digitale producten en diensten verloopt zorgvuldig en is in lijn met de visie.
De inzet van digitale zorg moet volgens de zorgaanbieder ondersteunend zijn aan de medewerker. Voor de aanschaf van digitale toepassingen worden vaste formats gebruikt. De zorgaanbieder besteedt aandacht aan scholing, testen en onderhoud.

De zorgaanbieder betrekt cliënten bij de invoering van digitale zorg. Bij de aanschaf van toepassingen betrekt de zorgaanbieder nog niet altijd structureel de cliëntvertegenwoordiging, cliënten of hun naasten.
De zorgaanbieder hanteert een visie op digitale zorg die de medewerker moet ondersteunen. De zorgaanbieder kiest bewust waar zij de cliënt en/of vertegenwoordiger wel bij of juist niet bij willen betrekken. Hierdoor kunnen cliënten, de cliëntvertegenwoordiging of naasten van de cliënten niet altijd meebeslissen over de aanschaf van de digitale zorg toepassingen. Het thema digitale zorg staat nog niet standaard op de agenda van de cliëntenraad.

Digitale uitwisseling voorziet in de behoeften, de zorgaanbieder is regionaal betrokken bij nieuwe ontwikkelingen.
De zorgaanbieder volgt naast het principe ‘digitaal tenzij’, ook het principe ‘regio tenzij’. De zorgaanbieder is vertegenwoordigd in diverse regionale samenwerkingen. De zorgmedewerkers beschikken over de juiste informatie om de zorg te kunnen leveren.

Informatiebeveiliging is deels in lijn met de wettelijke norm NEN 7510. De zorgaanbieder is op dit moment bezig met de borging.
De zorgaanbieder heeft in 2023 onafhankelijke audits uitgevoerd op respectievelijk beide delen van de wettelijk verplichte norm NEN 7510. De zorgaanbieder heeft een jaarplan waarin de aandachtspunten die uit deze audits voortkomen, beschreven. De zorgaanbieder is nu bezig met de borging op de verbeteracties. Een nieuwe onafhankelijke beoordeling op de gehele norm zal ook nog plaats moeten vinden. De zorgaanbieder heeft een nieuw crisisplan en zal de komende tijd werken aan meer bewustzijn bij medewerkers over dit crisisplan en continuïteit.

3 Handhaving

3.1 Maatregelen

De inspectie kan maatregelen nemen wanneer een zorgaanbieder nog niet voldoet aan een norm. Deze maatregelen zijn verschillend van aard. Welke maatregelen de inspectie kan nemen staat beschreven in haar interventiebeleid.[3]

De inspectie verwacht dat de zorgaanbieder aantoonbaar voldoet aan de wettelijk verplichte norm NEN 7510.
Voldoen aan de NEN 7510 is wettelijk verplicht. Dit vereist dat een zorgaanbieder een lerend managementsysteem heeft voor informatiebeveiliging. Dit staat voor voortdurende evaluatie en verbetering. De zorgaanbieder moet aantonen dat dit lerende systeem in de praktijk functioneert. De zorgaanbieder kan dit aantonen met het resultaat van een onafhankelijke beoordeling van het managementsysteem voor informatiebeveiliging en een uitgewerkt verbeterplan (zie verder paragraaf 3.3).

3.2 Aanbevelingen

De inspectie heeft geen aanbevelingen anders dan deze in het rapport als aandachtspunten zijn benoemd. De inspectie verwacht dat de raad van bestuur deze ter harte zal nemen.

3.3 Vervolgacties inspectie

De zorgaanbieder heeft al veel stappen gezet richting het aantoonbaar voldoen aan de norm NEN 7510. Ook heeft de zorgaanbieder al een aantal audits en onafhankelijke beoordelingen laten uitvoeren op de NEN 7510. Uit deze beoordelingen komen verbeteracties om aantoonbaar te kunnen voldoen aan de norm. Omdat de zorgaanbieder nu nog niet voldoet, blijft de inspectie de zorgaanbieder volgen. Naar aanleiding van een reactie van de raad van bestuur op het rapport volgde een gesprek tussen de inspectie en de zorgaanbieder. Met elkaar werden de volgende afspraken gemaakt. Deze afspraken volgen de planning van de zorgaanbieder.

- Uiterlijk **2 september 2024** stuurt de zorgaanbieder een verbeterplan met tijdslijn, betreffende het aantoonbaar voldoen aan de NEN 7510, naar de inspectie.
    - De zorgaanbieder stelt dit verbeterplan op naar aanleiding van de verbeteracties die naar voren kwamen uit de onafhankelijke beoordeling van de NEN 7510 deel 1 en 2.
    - In dit verbeterplan komt duidelijk naar voren welke verbeteracties nodig zijn en wie verantwoordelijk is voor het oppakken van deze verbeteracties.
    - Ook schetst de zorgaanbieder hier een duidelijke tijdslijn voor het voldoen aan de NEN 7510. Hierin worden in ieder geval meegenomen: de risicoanalyse(s), interne audits, directiebeoordeling en externe audits.

[3] IGJ interventiebeleid | Publicatie | Inspectie Gezondheidszorg en Jeugd

- De inspectie ontvangt uiterlijk **31 maart 2025** een terugkoppeling over de resultaten van de interne audits op de verbeteracties NEN 7510.
    - De zorgaanbieder informeert de inspectie over de resultaten van de interne audits. Dit doet zij door middel van een terugkoppeling op de resultaten en de stand van zaken betreffende het aantoonbaar voldoen aan de norm NEN 7510.

- Uiterlijk **1 maart 2026** informeert de zorgaanbieder de inspectie over de resultaten van de integrale onafhankelijke beoordeling die zij in het vierde kwartaal van 2025 uit zal voeren op de gehele norm NEN 7510.

4 Resultaten

4.1 Goed bestuur en verantwoord innoveren

Getoetste normen:

- De raad van bestuur heeft de controle over de e-health-ontwikkelingen. De zorgaanbieder heeft een beleid voor e-health en heeft hierbij de mensen betrokken die er belang bij hebben. Hij heeft taken en verantwoordelijkheden belegd in de zorgaanbieder. Hij regelt een duidelijke besluitvorming. De zorgaanbieder heeft aandacht voor risicomanagement en kwaliteitsborging van de e-health/ICT-omgeving. Het bestuur krijgt stuurinformatie.

	Afwezig	Aanwezig	Operationeel	Geborgd
Goed bestuur en verantwoord innoveren				√

Uitleg:

De zorgaanbieder is sinds de aanschaf van het elektronisch cliënten dossier in 2014 bezig met de ontwikkeling van een visie op digitale zorg. In 2019 lieten zij een digitale strategie formuleren door projectbureau Quint. In deze strategie stond centraal hoe digitale en innovatieve toepassingen een toegevoegde waarde konden zijn voor de medewerkers van Aafje. Deze visie heeft de zorgaanbieder overgenomen een koersplan genaamd Aafje op reis van 2020-2024. Hierin worden zes strategische pijlers beschreven:

- Verdieping van persoonsgerichte benadering,
- Verbinding met medewerker,
- Verbijzondering van doelgroepen,
- Vasthouden en verder verbeteren van de kwaliteit,
- Vernieuwing van en met technologie en
- Verbetering van het woon- en werkklimaat.

De pijler *Vernieuwing van en met technologie* beschrijft dat de zorgaanbieder innovaties inzetten die als eerste het werk voor de medewerkers makkelijker en leuker maken. Slimme digitale middelen zijn hiermee een hulpmiddel.

Deze visie trekt de zorgaanbieder door in het nieuwe koersplan genaamd Aafje op reis 2024-2028. Hierin is de pijler vernieuwing van en met technologie aangepast naar digitaal tenzij, leest de inspectie in de ontvangen documentatie.
De zorgaanbieder vertelt het beleid in de toekomst voort te zetten. Ook in regioverband wordt de inzet van digitale toepassingen uitgebreid. In het nieuwe koersplan van 2024-2028 heeft de zorgaanbieder aandacht voor risico’s ten aanzien van de informatiebeveiliging in de ketensamenwerking. Hiervoor hanteert de zorgaanbieder het vijf lagen model van Nictiz.

De zorgaanbieder benoemt zichzelf als fast follower. Hiermee bedoelt de zorgaanbieder dat zij technologie inzetten als deze vernieuwend en bewezen is. Het primaire proces is leidend voor de inzet van digitale zorg. De ICT-afdeling, bestaande uit 33 fte is hierbij ondersteunend. Naast de ICT-afdeling heeft de zorgaanbieder ook een afdeling informatiemanagement van 4fte. De afdelingen zijn los van elkaar georganiseerd. Beide vallen onder de verantwoordelijkheid van de directeur Bedrijfsvoering. Deze directeur rapporteert via het directieteam aan de raad van bestuur.

Ideeën voor innovaties en de inzet van technologie kunnen uit alle teams en/of medewerkers naar voren komen, vertellen gesprekspartners. In de wijkverpleging hanteert de zorgaanbieder accounthouders die de ideeën verzamelen en prioriteren. In de intramurale setting komen de meeste ideeën binnen bij de afdeling ICT of de afdeling informatiemanagement. Dit loopt dan meestal via de teammanagers.
De zorgaanbieder heeft voor de meeste applicaties en toepassingen een key-user en voor alle applicaties en toepassingen ook een functioneel beheerder. Ook maakt de zorgaanbieder gebruik van digicoaches. Deze medewerkers hebben meer kennis van digitale toepassingen op de werkvloer en ondersteunen daarmee medewerkers die vragen hebben over deze digitale toepassingen.

Voor de toepassing van Mobile Care heeft de inspectie gezien dat er gewerkt wordt met een projectvoorstel dat door de directie moet worden goedgekeurd.
De afwegingen en voorwaarden op basis waarvan besluitvorming plaatsvindt en de daadwerkelijk besluitvorming heeft de inspectie niet gezien. Wel is gezien dat er aan de stuurgroep in een voortgangsrapportage besluitvorming gevraagd is en inzicht in voortgang wordt gegeven.

De zorgaanbieder heeft een Informatiebeveiligingsbeleid vastgesteld in 2022. Er is een concept van een aangepaste versie van dit beleid met de inspectie gedeeld. Hierin zijn wijzigingen voorgesteld onder meer voortkomend uit de audit op NEN 7510 (zie ook 4.5). In dit beleid zijn onder meer rollen en verantwoordelijkheden vastgelegd. Ook ketensamenwerking en verantwoord gebruik van generatieve AI zijn hierin opgenomen.

In de presentatie die de bestuurder geeft tijdens het inspectiebezoek leest de inspectie dat de zorgaanbieder jaarlijks ruimte vrijmaakt op de begroting voor de investering in ICT-producten. Ook maakt de zorgaanbieder 1 miljoen per jaar vrij om te besteden aan (ICT) projecten. De bestuurder heeft de beschikking over uiteenlopende informatie over de inzet en het gebruik van e-health en zorgtechnologie. Leveranciers leveren daar informatie voor aan, die ook, zo nodig, aan de orde kan komen in het directieteam van de zorgaanbieder.

4.2 Invoering en gebruik van e-health-producten en -diensten

Getoetste normen:

- De zorgaanbieder heeft een proces afgesproken voor de invoering van e-health-producten of -diensten. Hij brengt daarbij de nodige experts samen. De zorgaanbieder stelt programma's van eisen op. De zorgaanbieder doet risicoanalyses. Hij zorgt voor training van gebruikers en testen van producten en diensten voor het in gebruik nemen. Ook regelt de zorgaanbieder het onderhoud.

	Afwezig	Aanwezig	Operationeel	Geborgd
Invoering en gebruik van e-health-producten en -diensten				✓

Uitleg:

De zorgaanbieder hanteert een projectmatige aanpak voor het aanschaffen en invoeren van e-health-diensten of producten. De inspectie ziet en leest dit terug in de verschillende documentatie die zij voorafgaand aan het bezoek heeft gekregen. In de gesprekken komt naar voren dat dit proces aansluit bij de door de zorgaanbieder opgestelde visie voor de inzet van digitale zorg. Bij de aanschaf kijkt men naar de toegevoegde waarde van de e-health-diensten of producten voor de medewerker.

De wens van het in gebruik nemen of toepassen van een (nieuwe) digitale toepassing wordt geprioriteerd in een projectgroep ~~ICT.~~ De zorgaanbieder zet dan een projectgroep op waarbij medewerkers vanuit verschillend functies, waaronder ICT, bij aansluiten. Deze projectgroep schrijft een projectplan met onder andere doelstellingen en de scope van het project. De inspectie hoort van de gesprekspartners dat zij in de meeste gevallen ook gebruik maken van een Proof of Concept (POC). Dit wordt deels uitgevoerd door de projectleider ICT. Het gaat hier met name om de technische realisatie. In de documenten ten aanzien van de aanschaf van een nieuw VOS leest de inspectie dit ook terug.

De zorgaanbieder stelt per project een pakket van eisen op voor de aanschaf en het invoeren van een e-health-product-of -dienst. De andere eisen in het pakket van eisen worden opgesteld aan de hand van een projectaanpak. Het projectteam stelt de eisen op samen met de zorgmedewerkers die de toepassing moeten gaan gebruiken. Dit ziet de inspectie terug in de documenten voor de aanschaf van een nieuw verpleegoproep systeem (VOS 2.0). Een van de eisen die de zorgaanbieder heeft geformuleerd voor dit oproepsysteem op basis van de veiligheid van de medewerkers is locatiebepaling van de medewerker

De zorgaanbieder heeft ervoor gekozen om met één samenwerkingspartner voor innovatie en technologie in de thuiszorg te werken. Deze partner is expert op dit gebied.

In de gesprekken met de zorgverleners hoort de inspectie dat zij geschoold worden in het gebruik van e-health toepassingen. De scholingen zijn fysiek en digitaal in de vorm van een e-learning. In de scholingen en/of cursussen geeft men aandacht aan de eerste introductie, maar er is bij belangrijke toepassingen ook aandacht voor training van latere gebruikers en het bijstellen van trainingsmateriaal en hertraining en/of aanvullende training. De inspectie hoort dat dit voornamelijk gebeurt bij wijzigingen in het proces of als medewerkers zelf aangeven hier behoefte aan te hebben. De zorgaanbieder maakt voornamelijk gebruik van train the trainer.

Diverse leercoaches en digicoaches zijn aanwezig op de locaties om medewerkers te trainen.

De zorgaanbieder besteedt aandacht aan testen voorafgaand aan ingebruikname. Bij toepassingen als het ECD gebeurt dit deels door de leverancier van het ECD. Bij andere toepassingen wordt er in de implementatiefase aandacht besteed aan het testen. In het VOS 2.0 traject hoort de inspectie dat testen na implementatie alleen voorkomt bij signalen of meldingen van niet functioneren van het systeem. Er vindt geen periodieke test plaats voor de e-health toepassingen. Bij de invoering van VOS 2.0 op een locatie heeft de organisatie tijd geïnvesteerd in het observeren van onder andere de locatiebepaling van het signaal uit het VOS. Dit was een belangrijke stap om de inzet van deze technologie aan te laten sluiten bij de behoeften van de medewerkers.

Over het onderhoud van de meeste e-health-producten of -diensten maakt de zorgaanbieder afspraken met de leveranciers. Dit hoort de inspectie terug in de gesprekken met de betrokkenen. Daarnaast ziet de inspectie dat er overeenkomsten zijn gesloten met de leveranciers over het gebruik en onderhoud van de toepassingen. Controles op naleving van onderhoudsafspraken vinden plaats door middel van leveranciersmanagement (zie ook paragraaf 4.5)

4.3 Patiëntparticipatie

Getoetste normen:

- De zorgaanbieder bespreekt de keuzes over e-health met patiëntvertegenwoordigers. De zorgaanbieder kijkt wanneer en e-health-product of -dienst wel of niet geschikt is. Daarbij houdt hij rekening met de zorgbehoefte van patiënten en de eigenschappen van de e-health-dienst. Patiënten krijgen voldoende informatie. Zo kunnen zij beslissen of een e-health-product of -dienst past bij hun zorgbehoefte. Ze zijn dus ook op de hoogte van mogelijke risico's. De zorgaanbieder maakt duidelijk hoe patiënten hulp kunnen krijgen bij e-health.

	Afwezig	**Aanwezig**	**Operationeel**	**Geborgd**
Patiëntparticipatie			√	

Uitleg:

De zorgaanbieder heeft een centrale cliëntenraad (CCR) en lokale cliëntenraden gekoppeld aan locaties en de thuiszorg. Leden uit de lokale cliëntenraad zijn ook in de CCR vertegenwoordigd. Leden van de cliëntenraad worden betrokken bij de implementatie van digitale zorg. Zij hebben in de meeste gevallen een laatste stem als het gaat om de invoering van de digitale zorg. Dit hoort de inspectie van een van de leden dat zij de invoering van sensoren bij een specifieke doelgroep en locatie hebben tegengehouden omdat dit niet passend was op die locatie.

Tijdens verschillende gesprekken hoort de inspectie dat de toepassing van digitale zorg in eerste instantie altijd vanuit de behoefte van de medewerker dient plaats te vinden. Op deze manier bestaat er meer aandacht voor de cliënt op andere vlakken, geeft een lid van de CCR aan. Ook draagt het bij aan meer zelfredzaamheid in de thuiszorg, zegt een ander lid van de lokale cliëntenraad. Het thema digitalisering en de inzet van digitale zorg staat niet standaard op de agenda van de cliëntenraad.

Bij de inzet van virtuele thuiszorg ziet en hoort de inspectie dat gekeken is naar de ondersteuning van de medewerker. De cliënt heeft geen directe inspraak gehad in de aanschaf van de soorten en merken van virtuele thuiszorg. De zorgverleners geven aan dat er bij de inzet van de virtuele thuiszorg, zoals de medicatiedispenser, gekeken wordt naar de cognitie van de cliënt en of de cliënt in staat is om het apparaat te gebruiken.

Tijdens het bezoek zag de inspectie een voorbeeld van de inzet van het verpleeg oproepsysteem (VOS). De aanschaf van een nieuw VOS is gedaan omdat de locatie van de medewerker niet duidelijk weergegeven kon worden. Gelet op de complexiteit van de doelgroep van de locatie was het van belang dat een nieuw oproepsysteem zou komen. De cliënten en hun naasten zijn niet betrokken geweest bij de implementatie van het VOS 2.0. De inspectie hoort dat zij zijn geïnformeerd via een brief. De zorgaanbieder heeft de cliënten en hun naasten wel geïnformeerd over de wijzigingen ten opzichte van het eerdere systeem. De inspectie hoort in een van de gesprekken van de gesprekspartners dat de cliënt en hun naasten mogelijk niet altijd goed op de hoogte zijn van de inzet van het systeem.

De cliënt geeft aan dat hij bij zijn zorgverleners terecht kan bij vragen over de e-health producten. Het lid van de cliëntenraad vertelt dat zij ook informatie verzamelen van de cliënten op de locaties over zowel medische als technische vragen met betrekking tot e-health.

4.4 Samenwerken in het netwerk en elektronische vastleggen en uitwisselen van gegevens

Getoetste normen:

- De zorgaanbieder kent de andere zorgaanbieders met wie hij samen zorg levert aan patiënten. Hij spreekt met hen de (zorginhoudelijke) informatie af die daarbij nodig is. Hij regelt dat de zorgverleners deze informatie kunnen uitwisselen. De zorgaanbieder legt afspraken over elektronische uitwisseling vast. De zorgaanbieder vraagt de patiënt toestemming voor elektronische uitwisseling als dat moet. De zorgaanbieder regelt samen met de mede-zorgaanbieders in de regio de medicatieoverdracht.

	Afwezig	Aanwezig	Operationeel	Geborgd
Samenwerken in het netwerk en elektronisch uitwisselen van gegevens				√

Uitleg:

De zorgaanbieder maakt deel uit van verschillende regionetwerken. Hierbij hanteren zij het principe 'regio tenzij' De bijdrage van de zorgaanbieder in regionale samenwerking is gericht op de toegankelijkheid van de zorg, in verdeling van schaarste. Zo heeft de zorgaanbieder een netwerk als het gaat om gezamenlijk capaciteitsmanagement, gezamenlijke zorgpaden, een samenwerking met de VVT-aanbieders in de regio op avond, nacht en weekend (ANW) diensten, spoedzorg (Spoedzorg010), verwijshulp (verwijshulp010) en geven zij een impuls op het maken van gezamenlijke keuze VVT-breed. Voor dit laatste zijn zij onderdeel van de architectuurboard Rijnmondnet. De zorgaanbieder maakt ook gebruik van het zorgplatform Digizorg. In dit zorgplatform werkt de zorgaanbieder samen met andere zorgorganisaties, zoals ziekenhuizen en huisartsen, aan een nieuwe

regionale ontwikkeling voor domein overstijgende ketensamenwerking.
De zorgaanbieder heeft deelgenomen aan het programma VIPP InZicht.
De zorgaanbieder heeft hierbij een start gemaakt met de verpleegkundige e-overdracht regionale ziekenhuizen en VVT. Wegens een minimale beschikbaarheid van de overdracht heeft de zorgaanbieder het traject stopgezet. Er zijn plannen om weer met elkaar aan tafel te gaan zitten en het traject te herstarten. Men ervaart toegevoegde waarde van een regionale samenwerkingsorganisatie, ook op andere thema's dan uitwisseling, zoals informatiebeveiliging.

De belangrijkste vormen van informatie die met de omgeving uitgewisseld worden zijn volgens de zorgaanbieder medische informatie te denken aan brieven, verpleegkundige dossiers en medicatie. De zorgaanbieder is voornemens het delen van meerdere vormen van informatie uit te breiden. De artsen schrijven digitaal voor in het EPD met gebruik van Medimo.

Medewerkers geven aan voor het uitvoeren van hun werk voldoende informatie digitaal beschikbaar te hebben. Wel zijn er wensen om informatie eenvoudiger vanuit bepaalde applicaties in andere systemen te krijgen, zoals het ECD, of gegevens meer gestructureerd in het ECD te willen hebben.

De zorgaanbieder gebruikt verwerkersovereenkomsten bij alle leveranciers die persoonsgegevens verwerken. De zorgaanbieder geeft aan dit standaard op te stellen bij elke samenwerking. De inspectie heeft de verwerkersovereenkomst met Point en Nedap ontvangen. Bij het afsluiten van de zorgovereenkomst vraagt de zorgaanbieder toestemming gevraagd voor gegevensuitwisseling.

In de algemene voorwaarden staat dat toestemming niet meer met formulier gevraagd wordt. Dit wordt mondeling gevraagd en in een formulier in ONS vastgelegd.

4.5 Informatiebeveiliging en continuïteit

Getoetste normen:

- Informatiebeveiliging: het bestuur heeft gezorgd voor het inrichten, invoeren, onderhouden en aldoor verbeteren van een managementsysteem voor informatiebeveiliging. De zorgaanbieder heeft een continuïteitsstrategie afgesproken, gedocumenteerd, ingevoerd en getest.

	Afwezig	Aanwezig	Operationeel	Geborgd
Informatiebeveiliging en continuïteit			√	

Uitleg:

Informatiebeveiliging
De zorgaanbieder is sinds 2016 actief bezig met het uitvoeren van audits met als thema informatiebeveiliging. In 2019 heeft er een eerste audit plaatsgevonden op basis van de NEN7510 en de AVG. De zorgaanbieder heeft deze onafhankelijke audit in april 2023 en in november 2023 opnieuw uit laten voeren op de NEN7510. In april vond de audit op deel 1 van de NEN 7510 (Information Security Management System, het ISMS) plaats en in november was de audit van deel 2 van de NEN 7510. (de beheersmaatregelen). De audits zijn uitgevoerd door concern control in samenwerking met EDPendent Audit & Control. Concern control is een onafhankelijke afdeling binnen Aafje, die direct rapporteert aan de raad van bestuur en niet betrokken is bij de (zorg)processen. De zorgaanbieder heeft nog geen besluit genomen over het al dan niet certificeren voor NEN 7510. Hierin ziet de aanbieder voor- en nadelen.

In de rapportage van de audit van NEN 7510-1 en de NEN 7510-2 leest de inspectie verbeteracties ten aanzien van het ISMS en de beheersmaatregelen. Zo leest de inspectie in het rapport van de audit van NEN 7510-1 dat een organisatie-brede risicoanalyse ten aanzien van informatiebeveiliging, met bijbehorende risicobeoordelings- en behandelprocedure ontbreekt. In de rapportage van de audit van NEN 7510-2 leest de inspectie dat het informatiebeveiligingsbeleid nog niet de zorg specifieke eisen die de norm vraagt, bevat. Ook leest de inspectie dat beleid nog geen onderdeel is van de P&C cyclus. Aanvullend leest de inspectie dat de zorgaanbieder informatiebeveiliging en informatie-uitwisseling nog geen onderdeel heeft gemaakt van beleidsontwikkeling en audits. En dat de informatiebeveiligingscontinuïteit niet regelmatig wordt geëvalueerd.

De inspectie kan op dit moment nog niet volledig vaststellen welke verbetermaatregelen ten aanzien van het ISMS en de beheersmaatregelen opgepakt zijn en worden geborgd. Een plan van aanpak of verbeterplan om aantoonbaar aan de norm te voldoen was ten tijde van het bezoek nog niet volledig beschikbaar.[4] Wel leest de inspectie in het vernieuwde informatiebeveiligingsbeleid dat er aanpassingen zijn gedaan voor de beheersmaatregelen over het informatiebeveiligingsbeleid. Dit aan de hand van de tekortkomingen uit de audit NEN 7510-2.

Rollen en verantwoordelijkheden ten aanzien van informatiebeveiliging
De zorgaanbieder heeft sinds 2022 een CISO. Voorheen had de manager ICT de rol van CISO. De CISO werkt volgens een jaarplanning, welke is ingezien door de inspectie. Het jaarplan van de CISO vormt de kapstok van de PDCA-cyclus ten aanzien van informatiebeveiliging en de NEN 7510. Zowel het jaarplan als het jaarverslag van de CISO wordt in het Directieteam besproken en vastgesteld. In het (halfjaar)verslag van de CISO wordt de voortgang van het jaarplan, inclusief actuele ontwikkelingen beschreven, ziet de inspectie. Niet duidelijk is welke besluiten genomen worden op basis van de halfjaarlijkse rapportage van de CISO en welke acties hieruit voortkomen. Een verbeterplan waarin acties voortkomende uit risicoanalyse, audits, rapportages en eventuele incidenten zijn vastgelegd is niet aanwezig.

Ook heeft de organisatie een Security Advisory Board (SAB). Deze heeft de rol van een IBMF en komt elke twee weken bij elkaar, vertellen gesprekspartners. Doel van deze board is om informatiebeveiliging integraal en planmatig te organiseren. Het SAB beoordeelt nieuwe beveiligingsrisico's, bespreekt data-incidenten en fungeert ook als werkgroep die helpt om het beveiligingsbeleid van de zorgaanbiedervorm te geven. De SAB bestaat uit CISO, Privacy Officer, manager ICT, Adviseur Informatiemanagement, medewerker ICT-systeembeheer en medewerker ICT-applicatiebeheer.

Continuïteit
De zorgaanbieder heeft sinds januari 2024 een nieuw Informatiebeveiliging (IB) Beleid waarin wordt verwezen naar een afzonderlijk continuïteitsplan. Medewerkers zijn nog niet altijd goed op de hoogte van dit plan, hoort de inspectie tijdens de gesprekken. De zorgaanbieder streeft ernaar om meer aan de bewustwording te doen van medewerkers.

[4] De zorgaanbieder heeft in de periode tussen het bezoek en de publicatiedatum van het rapport een plan van aanpak aangeleverd. Ook heeft de inspectie een gesprek gevoerd met de Chief Information Security Officier (CISO). Zowel het plan van aanpak als het gesprek in de bijlage van dit rapport heeft de inspectie meegenomen in haar eindconclusie en handhaving.

In het IB Beleid leest de inspectie dat alle zorg-locaties redundant zijn ontsloten richting het datacenter en zijn voorzien van een lokale breakout naar internet. Het datacenter zelf is ook redundant ingericht (richting interne netwerk en het internet). De SaaS-applicaties hebben hun eigen uitwijk, de verbinding die nodig is om de SaaS-oplossing te benaderen kan via Wifi en 4G. De zorgaanbieder heeft een Servicedesk die ook buiten kantooruren bereikbaar is. Voor noodsituaties is een 1e en 2e-lijns bereikbaarheidsdienst beschikbaar.

De zorgaanbieder heeft een analyse gemaakt van de diverse systemen die zij gebruiken voor het leveren van de zorg. Deze systemen noemen zij kroonjuwelen. Ten aanzien van deze kroonjuwelen hoort de inspectie dat de zorgaanbieder met leveranciers van deze digitale producten en diensten afspraken maakt over beheer, onderhoud en het omgaan met storingen. Dit leveranciersmanagement is belegd bij de eigenaars van specifieke applicaties (het eigenaarschap van applicaties is belegd bij organisatieonderdelen waar deze in gebruik zijn) en deels ook bij de afdeling ICT.

Bijlage 1: Algemene uitleg van de beoordelingen

Niveau	Uitleg
Afwezig	De zorgaanbieder besteedt niet aantoonbaar aandacht aan het onderwerp en/of heeft geen herkenbaar proces. Er ligt niets vast.
Aanwezig	De zorgaanbieder besteedt aantoonbaar aandacht aan het onderwerp. Er kan een gedocumenteerd proces zijn, maar in de praktijk kent niet iedereen dit. Of medewerkers volgen het niet altijd.
Operationeel	De zorgaanbieder heeft een gedocumenteerd proces. Medewerkers kennen dit en volgen het ook.
Geborgd	De zorgaanbieder heeft een gedocumenteerd proces. Medewerkers kennen dit en volgen het ook. De zorgaanbieder kijkt naar de resultaten en brengt verbeteringen aan waar mogelijk.

Bijlage 2: Overzicht van documenten die zijn bestudeerd

Voor en/of tijdens het inspectiebezoek zijn de volgende documenten bestudeerd:

- Aafje Kaderbrief 2024, Aafje, 2023;
- Aafje Digitale strategie (2019) Quint, 2019;
- Aafje Innovatie platform (2020) Aafje, 2020;
- Aafje op reis 2024 - 2028 Aafje;
- Aafje op reis 2020 - 2024, Aafje;
- Aafje Organogram, Aafje, 2024;
- Aafje Informatiebeveiligingsbeleid, Aafje, 2022;
- Aafje Integraal Crisisplan, Aafje, 2024;
- Crisisplan - Table top oefening, Aafje, 2023;
- Aafje Auditrapport IB NEN 7510-2, Concerncontrol, 2023 ;
- Aafje Inschatting Toetsingskader e-Health, Aafje, 2021;
- Verwerkingsovereenkomst Nedap - Aafje, Aafje, 2018;
- Verwerkingsovereenkomst Aafje - Point, Aafje, 2022;
- Mantelovereenkomst Point - Rijnmondnet, Aafje, 2023;
- Mantelovereenkomst Point - Rijnmondnet - Addendum Inzicht Regeling, Aafje, 2023;
- Mantelovereenkomst Point - Rijnmondnet - Addendum Orderformulier, Aafje, 2023;
- Aafje ingevulde vragenlijst IGJ e-Health, Aafje, 2024;
- Projectvoorstel Ons Medicatie verzorgingshuizen, Aafje, 2021;
- Decharge Ons Medicatie verzorgingshuizen, Aafje, 2023;
- Projectvoorstel Asset Tracking, Aafje, 2022;
- Leveranciersselectie Asset Tracking , Aafje, datum onbekend;
- Acceptatiecriteria PoC Asset Tracking, Aafje, 2023;
- Uitkomsten PoC Asset Tracking, Aafje, 2023;
- Uitkomsten PoC/Advies VOS 2.0, Aafje, 2021;
- PoC VOS 2.0 Technische inrichting, Aafje, 2021;
- PvE VOS 2.0, Aafje, 2021;
- Projectvoorstel VOS 2.0, Aafje, 2021;
- Projectvoorstel VOS 2.0 locatie Slinge, Aafje, 2022;
- Informatiefolder Dzep(Dementie en Zeer Ernstig Probleemgedrag), Aafje, datum onbekend;
- Projectplan Ons Wondzorg, Aafje, 2021;
- Decharge Ons Wondzorg, Aafje, 2022;
- Evaluatie en Borging Ons Wondzorg, Aafje, 2022;
- Projectplan Mobile Care, Aafje, 2021;
- Voortgangsrapportage Mobile Care, Aafje, 2021;
- Mobile Care Dashboard, Aafje, 2023;
- Informatiefolder Project Virtuele Thuiszorg, Aafje, datum onbekend;
- Mobile Care afwegingen, Aafje, datum onbekend;
- Onderzoek medicatie dispensers, Aafje, datum onbekend;
- Werkplan Borging Mobile Care, Aafje, 2023;
- Catalogus Aafje - Mobile Care 24/25, Aafje, 2024;
- Projectvoorstel Mobile Care Intramuraal, Aafje, 2022;
- NEN 7510 - 01 Auditrapport Informatiebeveiliging april 2023, Concerncontrol, 2023;
- NEN 7510 - 02 Auditrapport Informatiebeveiliging november 2023, Concerncontrol, 2023;
- Jaarplan CISO 2023, Aafje, 2023;
- Rapportage 2023 Q1 en Q2 CISO, Aafje, 2023 ;
- Informatiebeveiligingsbeleid - aangepast, Aafje, 2024;
- Rapportage privacy Q1Q2 2023, Aafje, 2023;
- Escalaties Q1 2023 presentatie, Aafje, 2023;

Bijlage 3: Samenvatting gesprek Chief Information Security Officer (CISO)

Op 16 april 2024 voerde de inspectie een gesprek met de CISO van Aafje, Hieronder de samenvatting van dit gesprek welke door Aafje gecorrigeerd is op een feitelijke onjuistheid.

Samenvatting gesprek

In het gesprek is allereerst gesproken over het jaarplan 2024 van de CISO en hoe de verschillende processen, zorg en ICT, op elkaar aansluiten. De inspectie hoort dat het thema informatiebeveiliging belegd is bij ICT maar ook in de zorgprocessen. Volgens de gesprekspartner sluit dit aan bij de werkwijze van Aafje en is het daardoor niet alleen een onderwerp dat leeft op ICT-niveau. Verder hoort de inspectie dat er op proces en/of projectniveau een risicoanalyse is uitgevoerd door de zorgaanbieder. Er is nog geen overkoepelende risicoanalyse aanwezig op organisatieniveau. De inspectie hoort dat er wel plannen zijn om een organisatie brede risicoanalyse uit te voeren.

In het gesprek stelde de inspectie vragen over het opvolgen van incidenten en het bepalen van prioriteiten voor audits. De inspectie hoort van de gesprekspartner dat de incidenten besproken worden in het SAB en worden bijgehouden in een register. De CISO stelt rapportages op over verbeteracties en incidenten en bespreekt deze eens per twee weken met de manager bedrijfsvoering en de manager ICT. Deze rapportages bespreekt men vervolgens ook op directieniveau. Een aantal keer per jaar wordt de raad van toezicht ook betrokken bij dit proces.

De zorgaanbieder heeft drie audits ingepland omtrent het thema informatiebeveiliging. Een grote audit zal zich richten op het continuïteitsplan van de organisatie. De inspectie hoort dat de CISO op hoofdlijnen heeft aangegeven uit welke onderdelen de audits moeten bestaan. De audits worden uitgevoerd door concerncontrol.

Afsluitend vraagt de inspectie of de organisatie een onafhankelijke beoordeling heeft laten uitvoeren op de gehele norm NEN 7510. De gesprekspartner geeft aan dat er op dit moment geen totale beoordeling aanwezig is op beide delen van de NEN 7510. Deel 1 van de norm is getoetst in april 2023 en deel 2 van de norm is getoetst in november 2023. De inspectie hoort dat de organisatie dit jaar wil werken naar een audit op het geheel.