Inspectie Gezondheidszorg en Jeugd
Ministerie van Volksgezondheid, Welzijn en Sport

Extra aandacht nodig voor ICT in de jeugdzorg

Breng de basis op orde en benut kansen

Inleiding

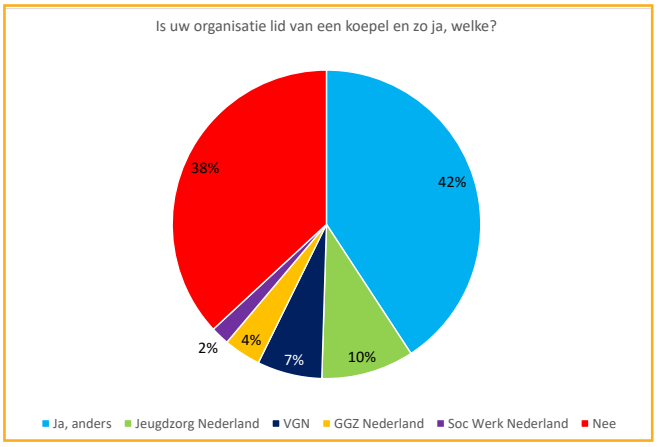
Informatie- en communicatietechnologie wordt ook in de jeugdhulp steeds belangrijker. Voorbeelden van ICT in de jeugdhulp zijn elektronische cliëntendossiers, elektronische gegevensuitwisseling, het gebruik van apps en sociale media, monitoring van cliënten op afstand, toezichthoudende domotica (bewegingssensoren, camera's en personenalarmering) en virtual reality. Dit biedt de sector kansen en ruimte voor innovatie maar brengt tegelijkertijd ook nieuwe risico's met zich mee.

In het voorjaar van 2019 vond een incident rondom informatiebeveiliging in de jeugdzorg plaats. Door een datalek kwamen dossiers met hierin de bijzondere persoonsgegevens van meer dan 2500 kwetsbare jeugdigen in handen van derden. Voor jeugdigen, hun ouders, de professionals in de sector en alle overige betrokkenen is een dergelijk incident zeer onwenselijk.
Cliënten moeten erop kunnen vertrouwen dat gevoelige informatie alleen op de juiste momenten en met de juiste personen wordt gedeeld. Professionals moeten ook op het gebied van informatiebeveiliging voldoende worden ondersteund om hun werk goed te kunnen doen. Het datalek was aanleiding voor de Tweede Kamer om zich nader te laten informeren over de stand van zaken met betrekking tot de informatie- en communicatietechnologie (hierna: ICT) en informatiebeveiliging in de jeugdhulp.

De inspectie besloot een breed onderzoek te doen. Informatiebeveiliging was een specifiek onderdeel van dit onderzoek. Voor dit onderzoek werd een enquête uitgezet onder een grote groep jeugdzorgorganisaties in Nederland. Daarnaast organiseerde de inspectie een focusgroep om de resultaten van de enquête te bespreken. Tot slot bracht de inspectie toezichtbezoeken aan een grote jeugdhulpaanbieder en een gecertificeerde instelling.
Ook zijn in opdracht van VWS zogenaamde penetratietesten uitgevoerd door een externe partij bij jeugdhulpaanbieders. De resultaten hiervan zijn op hoofdlijnen meegenomen.

Enquête

In het najaar van 2019 vroeg de inspectie aan 1342 jeugdhulpaanbieders[1], inclusief de zestien gecertificeerde instellingen, om anoniem een webbased vragenlijst in te vullen over het gebruik van ICT en informatiebeveiliging. 563 organisaties vulden de vragenlijst in (42% respons). Daarnaast organiseerde de inspectie een focusgroep om de resultaten van de enquête te bespreken. Vertegenwoordigers van zowel kleinere als grotere jeugdhulpaanbieders namen hieraan deel. Ook bracht de inspectie twee verkennende toezichtbezoeken in de sector en toetste de instellingen aan het door de inspectie opgestelde toetsingskader e-health. De uitkomsten zijn meegenomen in deze factsheet.
De respondenten vormen een goede afspiegeling van de sector; er reageerden veel kleine jeugdhulpaanbieders. Bijna 60% van de respondenten heeft maximaal 10 medewerkers (fte) in dienst. Aanbieders met meer dan 100 medewerkers komen weinig voor: 15%. De respondenten leveren diverse vormen van jeugdhulp, variërend van ambulante hulp tot jeugdhulp met verblijf en gesloten jeugdhulp. In de analyse van de vragenlijst is de invloed van de grootte van een jeugdhulpaanbieder op de uitkomsten meegenomen. Van de respondenten is de meerderheid (62%) lid van een brancheorganisatie, zoals Jeugdzorg Nederland, de Vereniging Gehandicaptenzorg Nederland of de Federatie Landbouw en Zorg.



Bevindingen over ICT

De meeste jeugdhulpaanbieders (68%) onderschrijven het belang van ICT voor de kwaliteit van de jeugdhulp. Ook ziet men het gebruik van ICT binnen de eigen organisatie groeien. Dit heeft impact op de kwaliteit van jeugdhulp én kan een middel zijn om die kwaliteit in beeld te krijgen.

Er zijn ook risico's aan verbonden: 88% geeft aan zich bewust én voorbereid te zijn op de risico's die de groeiende inzet van ICT met zich meebrengt. Het merendeel van de jeugdhulpaanbieders lijkt tevreden met de inzet van ICT voor de eigen medewerkers. Een kwart van de respondenten stelt echter ook dat men meer met ICT moet doen, zodat de jeugdhulp meer bij de tijd blijft.

Het digitaal bijhouden van dossiers is gemeengoed in de sector. Bijna alle (98%) respondenten werken (deels) digitaal, waarvan 72% via een ECD en 25% met algemene software zoals Word of Excel. Digitale gegevensuitwisseling met andere partijen is ook gebruikelijk, zoals met gemeenten (69%), andere jeugdhulpaanbieders (65%) en overige organisaties (22%) waaronder bijvoorbeeld huisartsen, rechtbanken en de raad voor de kinderbescherming.

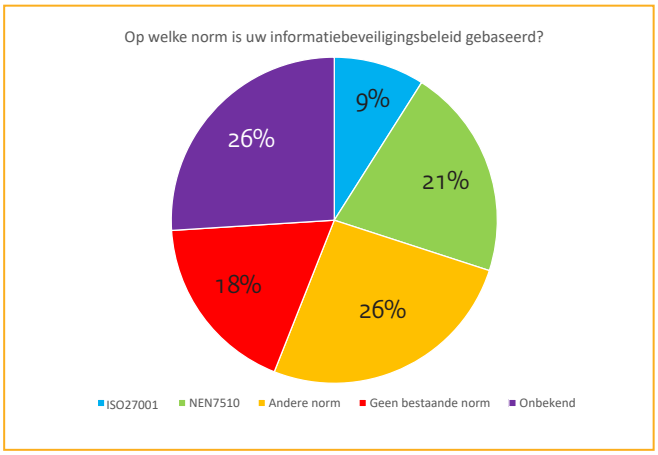
Hoewel er wel aandacht is voor uitwisseling van gegevens, kwam uit de focusgroep (waarover hieronder meer) naar voren dat het digitaal bijhouden van cliëntgegevens in dossiers en het uitwisselen van die gegevens niet op een gestandaardiseerde wijze gebeurt. Dit belemmert een gestructureerde uitwisseling van gegevens tussen jeugdhulpaanbieders en kan daarmee een risico vormen voor de kwaliteit van jeugdzorg.

Bijna 70% van de respondenten geeft aan beleid op het gebied van ICT te hebben geformuleerd. Van deze groep geeft de helft aan hierbij wel aandacht te hebben voor het thema 'samenwerken in het netwerk en elektronisch vastleggen en uitwisselen van gegevens'. Ook de andere thema's uit het toetsingskader e-health komen veelal terug in het beleid zoals 'informatiebeveiliging & continuïteit' (63%), 'invoering en gebruik van ICT-producten en –diensten' (41%) en 'cliënten-participatie' (32%). Slechts 2% besteedt geen aandacht aan een van de genoemde thema's uit het toetsingskader.

Naast het digitaal vastleggen en uitwisselen van gegevens zijn er binnen de jeugdhulp diverse andere toepassingen in gebruik. Opvallend is het hoge percentage respondenten dat gebruik maakt van chat en 'messaging' mogelijkheden om digitaal contact met clienten en andere betrokkenen te hebben (73%). Minder gebruikelijk zijn digitale middelen zoals behandelplatforms, veilige communicatiekanalen en persoonlijke gezondheidsomgevingen. Specifieke aandacht is er vaak wel voor het gebruik van sociale media in de jeugdhulpsector; 69% van de respondenten heeft beleid of afspraken over het gebruik van sociale media.

Bevindingen over informatiebeveiliging en privacy

Voor informatiebeveiliging en de omgang met digitale privacy heeft 88% van de respondenten beleid geformuleerd. Via inwerkprogramma's en andere methoden nemen medewerkers kennis van het beleid. De grootte van een organisatie speelt hierbij nagenoeg geen rol. Het beleid is bij een derde van de jeugdhulpaanbieders gebaseerd op de gangbare wettelijke normen (ISO 27001 en/of NEN7510).



Opvallend is dat een deel van de sector zich niet bewust is van de gangbare normen. 42% van de respondenten die aangeven beleid te hebben opgesteld voor informatiebeveiliging heeft dit niet gebaseerd op een gangbare norm (18%) óf men weet de gehanteerde norm niet te noemen (26%).

Bijna 80% van de respondenten heeft een verantwoordelijke voor informatiebeveiliging aangewezen. De rest heeft geen verantwoordelijke aangewezen. Bij grotere jeugdhulpaanbieders was die verantwoordelijkheid vaker belegd dan bij kleine jeugdhulpaanbieders.

Naast een verantwoordelijke voor informatiebeveiliging heeft ook de functionaris gegevensbescherming (hierna: FG) een belangrijke rol bij informatiebeveiliging. Soms is deze rol verplicht op basis van de Algemene Verordening Gegevensbescherming (hierna: AVG), bijvoorbeeld wanneer er sprake is van grootschalige verwerking van bijzondere persoonsgegevens[2].

De FG is bij 34% van de respondenten niet aanwezig, waarbij grotere aanbieders logischerwijs vaker een FG hebben dan kleinere. Verder blijkt dat zowel de verantwoordelijke voor informatiebeveiliging als de FG bij de meeste jeugdhulpaanbieders maar beperkt tijd te hebben voor hun rol, al is het aantal uren bij grote aanbieders wel iets hoger.

Voor informatiebeveiliging is het noodzakelijk een actueel beeld te hebben van de risico's op dit gebied. In 60% van de organisaties was de afgelopen drie jaar minimaal één keer een risicoanalyse uitgevoerd. Echter, 40% deed geen analyse. Opvallend is dat bij 38% van de respondenten die aangaven wél de risico's op dit vlak te kennen en hierop voorbereid te zijn, geen risicoanalyse is gedaan.

Een middel om informatiebeveiligingsbeleid te toetsen is een onafhankelijke audit. De geldende normen voor informatiebeveiliging vragen dit ook. Bij bijna de helft van de respondenten is de afgelopen drie jaar minstens eenmaal een onafhankelijke audit op het gebied van informatiebeveiliging uitgevoerd. Bij meer dan de helft ontbrak dit dus. De omvang van de organisatie is hier ook van invloed. Een dergelijke audit kan eventueel leiden tot het verkrijgen van een certificaat op basis van de ISO27001 of de NEN7510.

Focusgroep

In januari 2020 organiseerde de inspectie een focusgroep om het beeld dat uit de enquête naar voren was gekomen, te toetsen en te verrijken. De aanwezigen vertegenwoordigden zowel kleine als grote jeugdhulpaanbieders en reflecteerden samen met de inspectie op de resultaten uit de vragenlijst. De volgende punten kwamen hierbij naar voren:

- Aanwezigen zagen een groot probleem in de vele verschillen in werkwijzen en afspraken in de sector; de eisen voor ICT zijn bovendien niet eenduidig; standaardisatie ontbreekt. Soms moeten jeugdhulpaanbieders met tientallen gemeenten en andere partijen steeds weer andere afspraken maken. Zowel bij het digitale dossier als bij de rapportages en verantwoording wordt de ICT hierdoor problematisch. Er zijn veel systemen in gebruik die onderling maar beperkt informatie (kunnen) uitwisselen. In diverse processen is gegevensuitwisseling nodig, zoals het aanleveren van beleidsinformatie, declareren, verantwoorden en ook de overdracht van zorginhoudelijke cliëntinformatie. Er is een gebrek aan standaardisatie en samenwerking op ICT-vlak waardoor partijen zelf het wiel uit (moeten) vinden. Vernieuwing en innovatie komen hierdoor niet van de grond. Het gebrek aan standaarden in de sector wordt door aanwezigen als een groter risico voor de kwaliteit van de jeugdhulp beoordeeld dan de informatiebeveiligingsrisico's. Als het gaat om de kwaliteit van de jeugdhulp wordt het gebrek aan standaarden en daarmee versnippering als een groter risico voor de kwaliteit ervaren dan onvoldoende informatiebeveiliging.

- ICT-thema's als informatiebeveiliging of e-health en innovatie zijn met name voor kleinere jeugdhulpaanbieders moeilijk om zelfstandig aan te pakken. Deze jeugdhulpaanbieders hebben ondersteuning nodig om hun ICT op een hoger plan te brengen en volgens de geldende normen te werken. Regionale serviceorganisaties die kleinere aanbieders 'ontzorgen' op ICT gebied, werden genoemd als oplossingsrichting.

- Aanwezigen gaven aan dat de kwaliteit van ICT in de jeugdhulp omhoog moet. Complex hierbij is dat het niet helder is wie binnen de sector de regie kan nemen op het gebied van digitale ontwikkelingen. Er bestaan meerdere koepels dan wel brancheorganisaties met verschillende mogelijkheden. Een centraal geregisseerd overlegorgaan, zoals het Informatieberaad dat bekend is in andere zorgsectoren, functioneert nog niet voor de jeugdhulp.

- Digitale deskundigheid is volgens de aanwezigen een aandachtspunt. Dit speelt zowel bij de kleine jeugdhulpaanbieders als bij de grotere organisaties.

- Het gebruik van sociale media door jeugdigen is een aandachtspunt. Het biedt kansen, maar heeft ook risico's. Diverse jeugdhulpaanbieders hebben hiervoor beleid opgesteld. Aanwezigen geven aan dat het lastig is en blijft om jeugdigen bewust te maken van de risico's omtrent sociale media, waarmee de vraag blijft hoe effectief en doeltreffend dit beleid is.

- Digitalisering of e-health biedt ook kansen en ruimte voor innovatie. Een bekend voorbeeld hiervan is het platform Garage2020, waar een aantal innovatieve initiatieven ontplooid worden.

Toezichtbezoeken

Eind 2019 bezocht de inspectie een grote jeugdhulpaanbieder en een gecertificeerde instelling. De bezoeken waren verkennend van aard. De inspectie gebruikte bij deze bezoeken het toetsingskader e-health[3]. De rapporten van deze bezoeken heeft de inspectie separaat gepubliceerd op haar website[4]. Uit beide toezichtbezoeken kwam naar voren dat ICT van toenemend belang is voor de (kwaliteit van) jeugdhulp. Er was sprake van ICT-beleid met een nauwe relatie met de bredere doelstellingen van de organisaties en zowel voor cliënten als voor medewerkers zijn ICT middelen in toenemende mate van belang. In beide gevallen waren verbeteringen mogelijk, onder andere op het vlak van informatiebeveiliging. Hierbij valt te denken aan het aantoonbaar voldoen aan de geldende normen, maar ook aan het meer gestandaardiseerd werken bij de invoering van nieuwe ICT-toepassingen.

Conclusies van de inspectie

De inspectie heeft op basis van het gehele onderzoek twee grote zorgen binnen de jeugdzorgsector als het gaat om ICT en informatiebeveiliging:

1. Informatiestandaarden ontbreken waardoor digitale uitwisseling en samenwerking onvoldoende van de grond komt.
2. Er is onvoldoende kennis aanwezig van en zicht op de risico's op het gebied van ICT en informatiebeveiliging. Ook heeft de sector onvoldoende middelen voorhanden.

   Het onderzoek van de inspectie richtte zich primair op ICT en informatiebeveiliging. Uit de gesprekken met de focusgroep komt naar voren dat het gebruik van sociale media door jeugdigen kansen biedt maar daar ook (nieuwe) risico's worden gezien. De inspectie ziet hier een belangrijk punt en formuleert daarom nog een derde conclusie:
3. Onvoldoende beeld van de doeltreffendheid van beleid op het gebied van sociale media.

Aanbevelingen van de inspectie

1. **Op het gebied van uitwisseling van gegevens:**
   De inspectie realiseert zich dat het niet één partij is die de basis in de sector als geheel op orde kan brengen. Dit neemt echter niet weg dat alle organisaties in de sector zelf verantwoordelijkheid dragen om te zorgen voor een goede digitale uitwisseling en samenwerking. De problematiek kan daarnaast geagendeerd worden in het overleg Branches Gespecialiseerde Jeugdhulpaanbieders Jeugdhulp (BGZJ) en het Informatieprogramma Sociaal Domein (ISD).

   De inspectie spreekt graag verder met de sector over het uitwisselen van gegevens. Een volgende focusgroep of bijeenkomst waar wordt ingegaan op de belangrijkste randvoorwaarden voor uitwisseling zoals samenwerking tussen ketenpartners, ondersteuning van processen en het maken van afspraken over structuur en inhoud van informatie is hiervoor passend[5].

2. Op het gebied van informatiebeveiliging:
De uitkomsten van de door VWS uitgevoerde penetratietesten laten zien waar een gebrekkig informatiebeveiliging toe kan leiden: hoge risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van dossiers in de jeugdhulp. De inspectie roept alle jeugdzorg instellingen op om de informatiebeveiliging op orde te brengen conform de hiervoor geldende normen, te weten de ISO27001 en/of de NEN7510. De geldende normen zijn onvoldoende bekend in de sector. De inspectie roept daarom brancheorganisaties uit de sector, zoals bijvoorbeeld Jeugdzorg Nederland, de Federatie Landbouw & Zorg, Keurmerk Gezinshuizen en Gezinshuis.com, maar ook de Vereniging van Nederlandse Gemeenten op om deze normen expliciet onder de aandacht te brengen van hun leden. Deze oproep geldt ook voor alle andere brancheorganisaties en koepels uit de sector.

3. Op het gebied van sociale media:
De inspectie roept alle jeugdzorg instellingen op om beleid te formuleren voor het gebruik van sociale media. Ook roept de inspectie alle jeugdzorg instellingen op om dit beleid te toetsen op doeltreffendheid.

Toezicht van de inspectie

De inspectie realiseert zich dat de sector tijd nodig heeft om de basis van ICT en informatiebeveiliging op orde te brengen en opvolging te geven aan bovengenoemde aanbevelingen. De inspectie verwacht wel dat de sector in de komende periode de ICT en informatiebeveiliging verder professionaliseert conform de daarvoor geldende normen. De inspectie neemt het thema 'ICT en informatiebeveiliging in de jeugdhulp' vooralsnog alleen reactief mee in haar toezicht. Dit betekent dat bij de analyse van meldingen zal worden meegewogen of de kwaliteit van ICT een rol heeft gespeeld of zou moeten spelen. De inspectie zal waar nodig breed informeren over best practices, met name op het gebruik van sociale media.

1 Ten behoeve van de leesbaarheid wordt, waar ook de gecertificeerde instellingen worden bedoeld, alleen de term jeugdhulpaanbieder gebruikt.
2 Een functionaris gegevensbescherming is in een aantal situaties verplicht. De Autoriteit Persoonsgegevens beschrijft welke en geeft daarbij een richtlijn hoe hiermee in de zorg moet worden omgegaan. Zie daarvoor onder andere: https://autoriteitpersoonsgegevens.nl/nl/nieuws/uitleg-begrip-%E2%80%98grootschalig%E2%80%99-verduidelijkt-voor-alle-zorgaanbieders
3 De inspectie maakt haar toetsingskaders openbaar. Het toetsingskader e-health is hier in te zien: https://www.igj.nl/documenten/toetsingskaders/2019/10/18/toetsingskader-inzet-van-e-health-door-zorgaanbieders
4 https://www.toezichtdocumenten.igj.nl
5 Zie ter illustratie het interoperabiliteitsmodel van Nictiz: https://www.nictiz.nl/standaardisatie/interoperabiliteit

Bijlage

