- Concept -

Factsheet

Mobiel werken

Het implementatieteam van ActiZ en GGD Nederland ondersteunt organisaties om een goed werkend digitaal dossier voor de jeugdgezondheidszorg (DD JGZ) te realiseren. Als onderdeel van deze ondersteuning adviseert het implementatieteam bij de benodigde aanpassingen voor het mobiel werken.

JGZ-medewerkers werken niet altijd vanuit dezelfde vaste locaties. Ze hebben contactmomenten op andere locaties, zoals op scholen of gaan op huisbezoek bij hun cliënten. Ook hebben zij regelmatig overleg rondom bijvoorbeeld Zorg Advies Teams. Het werken met de digitale dossiers vraagt daarom om technische flexibiliteit. Het principe van 'mobiel werken' (oftewel plaatsonafhankelijk werken) geeft hier invulling aan. JGZ medewerkers willen – en kunnen - niet altijd op de standaard werkplek zitten. Zij zoeken de cliënten op en willen daarbij wel toegang tot het DD JGZ. Zij moeten in iedere situatie effectief en efficiënt met digitale dossiers kunnen werken.

Ook al wordt het met de huidige technische mogelijkheden steeds eenvoudiger - en daarmee gewenster - om mobiel te werken, er blijven verschillende aandachtspunten. Met deze factsheet geven we hier meer inzicht in. Te beginnen bij de benodigdheden voor mobiel werken om vervolgens door te gaan op mogelijke manieren van mobiel werken.

Benodigdheden mobiel werken

Om mobiel te kunnen werken zijn de JGZ-organisaties afhankelijk van de technische mogelijkheden. En ondanks de snelle ontwikkeling van de techniek blijven er de nodige (technische) aandachtspunten wat betreft hardware, verbinding en beveiliging. In deze volgorde bespreken we deze ook.

Hardware

Om mobiel te werken is in de ideale situatie een aantal hardware noodzakelijk.

- Een mobiele computer. Voorkeur bij mobiel werken gaat uit naar een computer die handzaam is, bijvoorbeeld een notebook of netbook (klein formaat notebook).
- Een draadloze netwerkkaart (WiFi) die voldoet aan de IEEE 802.11 standaarden.
- Een USB antenne, expresscard- of PCMCIA-kaart om toegang te hebben tot het internet via UMTS/HSDPA/HSUPA.
- Eventuele software voor beveiligde verbindingen of het werken op afstand via een Terminal Service Cliënt als Citrix.
- Afhankelijk van de soort beveiliging (zie factsheet informatiebeveiliging) is een "token" nodig voor toegang tot het eigen netwerk.
- Op het moment dat de JGZ-organisatie aangesloten wordt op het Landelijk Schakelpunt (LSP) moet de organisatie UZI-houder zijn en de JGZ medewerker in het bezit zijn van een UZI-pas. De UZI-pas is een elektronisch authenticatiemiddel ontwikkeld voor de zorg. De pas vormt het elektronische paspoort voor onder andere JGZ medewerkers. Op deze wijze kunnen medewerkers aantonen wie ze zijn en welke functie ze hebben, en dus welke toegang ze hebben tot informatie.
- Dit alles gecombineerd in een handzame mobiele koffer/tas houdt de hardware bij elkaar. De losse componenten zijn nadelig voor de JGZ medewerker bij verplaatsing. Het risico van verlies en/of diefstal is bij mobiel werken hoog, waardoor het gebruik van een beveiligingskabel tegen diefstal noodzakelijk is.

Verbinding

Het op een veilige manier verbinding maken met het DD JGZ is noodzakelijk. Dit is op verschillende manieren mogelijk. Leidraad hierbij is dat de applicatie de mogelijkheden ondersteunt. Dit betekent dat wanneer de JGZ-medewerker wil werken met het DD JGZ er een beveiligde verbinding moet zijn. Dit is mogelijk door het gebruik van een zogenoemde 'Terminal Service Cliënt'. Deze cliënt legt een beveiligde verbinding door het gebruik van een portal met het digitale dossier. Een tweede optie is om te werken met een beveiligde 'https-verbinding'. Deze verbinding is overal te benaderen maar geeft uitsluitend toegang aan de mensen die gemachtigd zijn. Toegang tot beide manieren kan met een wachtwoord of 'token'. Het mobiel werken via het C2000-netwerk - het digitale communicatienetwerk voor de Nederlandse hulpverleningsdiensten waaronder ambulancediensten en meldkamers - is door beperking in dataoverdracht niet mogelijk.[1]

Zonder deze beveiligde verbinding kan en mag er niet mobiel worden gewerkt. Sommige netwerken staan het niet toe dat bepaalde beveiligde verbindingen worden gelegd. Het openstellen van de juiste 'poort' op een firewall waardoor de verbinding wordt gelegd, lost het probleem vaak op.

Beveiliging

Wat betreft het mobiel werken met het DD JGZ spelen er op beveiligingsniveau dezelfde issues als bij de normale informatiebeveiliging. Ook de mobiele computer moet voldoen aan de beveiligingsnormen die in GBZ en NEN7510 staan vermeld. Deze normen stellen dat digitale gegevensdragers – waaronder mobiele computers - zich bijvoorbeeld altijd in een inbraakwerende ruimte moeten bevinden. De factsheet informatiebeveiliging gaat verder in op de beveiligingsnormen van informatie.

Richtlijn voor mobiel werken

Er zijn momenteel diverse mogelijkheden om via een beveiligde verbinding mobiel te werken met het DD JGZ. Wij behandelen de mogelijkheden die geschikt zijn voor de JGZ-organisaties. Het gaat dan om de mogelijkheden die voor de JGZ medewerker het meest ideaal zijn. In deze volgorde zullen deze ook behandeld worden. In de ideale situatie is er een continue online verbinding met het DD JGZ via het landelijke draadloze netwerk. Wanneer dit niet mogelijk is kan overgeschakeld worden op het netwerk van derden. Als dit niet mogelijk blijkt, is het gewenst om offline te werken waarna de JGZ medewerker zo snel mogelijk synchroniseert met het online DD JGZ wanneer deze hiertoe in de mogelijkheid is. Wanneer dit niet tot de opties behoort kan de JGZ organisatie eventueel gebruik maken van de computers van derden. En als laatste optie werkt de JGZ medewerker in een papieren template die later in het DD JGZ ingevoerd/geüpload wordt.

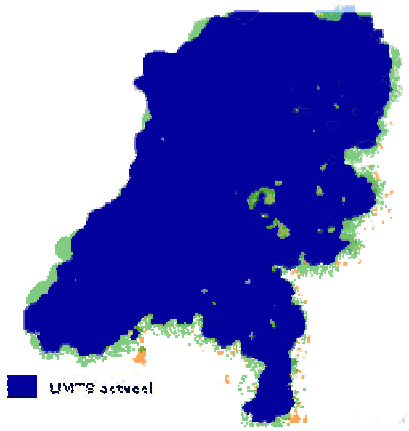
1) Continue online verbinding met het DD JGZ

De grotere landelijke netwerkoperators (KPN/Vodafone/T-Mobile) geven aan te beschikken over een vrijwel landelijke UMTS/HSDPA dekking (90%). Dit netwerk behoort tot de snelste in haar soort. Hierdoor kan vrijwel overal mobiel gewerkt kan worden. KPN heeft momenteel zelfs als enige een dekking van 90% op het nieuwe – en nog meer snelle - HSUPA netwerk. HSUPA staat voor High-Speed Uplink Packet Access en is – net als UMTS en HSDPA - een protocol voor het mobiele netwerk.

[1] Kijk voor meer informatie over Mobiel Werken via het C2000-netwerk op het forum op http://invoeringddjgz.ning.com/ onder Mobiel Werken.

Wanneer het UMTS/HSDPA/HSUPA signaal te zwak is (door beperking in de dekking), schakelt het netwerk automatisch over op het langzamere GPRS. Het GPRS netwerk is niet toereikend voor mobiel werken. Het digitaal dossier kan in dit geval niet goed geraadpleegd/bewerkt worden, wat gevolgen heeft voor het werkproces. De JGZ medewerker kan niet online werken en moet dus alternatieven zoeken.

In de praktijk blijkt dat de kwaliteit van het UMTS, HSDPA of HSUPA-netwerk in veel gebieden niet zorgt voor een prettige en effectieve manier van werken. De dekking van 90% is niet gebaseerd op het werken in afgesloten ruimten/gebouwen. In de praktijk blijkt (toetsing in Leiden en Gouda) dat het bereik van het netwerk rond de 40% ligt. Dit houdt in dat een continue online verbinding momenteel nog erg onzeker is. Hoewel de techniek zich in hoog tempo blijft ontwikkelen waardoor de kwaliteit van de verbinding steeds verder verbetert, is deze nu nog ontoereikend om volledig op te vertrouwen.



Figuur 1: UMTS-dekking KPN, 2009 (buiten)

2) Gebruik van een netwerk van derden

Het werken op een netwerk van derden (bijvoorbeeld een school of consultatiebureau) kan als tweede optie een oplossing zijn van dit probleem. Het levert daarnaast ook onzekerheden op. Doordat het DD JGZ privacygevoelige informatie bevat zijn de JGZ-organisaties verplicht gebruik te maken van een streng beveiligde omgeving. De beveiligde verbinding die gelegd moet worden met het DD JGZ moet allereerst door de applicatie ondersteund worden maar daarnaast ook door het netwerk van derden mogelijk zijn. Bij het gebruik van een externe online omgeving – bijvoorbeeld de Citrix omgeving – is het niet altijd mogelijk om vanuit een netwerk van derden een verbinding te leggen, omdat a) de 'quality of service' (QoS)[2] van de verbinding van het netwerk onvoldoende is en/of b) de gehanteerde veiligheidsnorm van de JGZ-organisatie niet aansluit bij de externe omgeving (bijvoorbeeld de beveiliging en calamiteitenregeling).

Wanneer derden bereid zijn de JGZ-organisaties te faciliteren in het openstellen of aanleggen van een toereikende verbinding, is er technisch gezien geen probleem om een online verbinding te leggen met het DD JGZ. Het is daarom van belang vooraf duidelijke afspraken te maken met derden wat betreft de mogelijkheden van netwerkgebruik. De eisen die de applicatie stelt wat betreft QoS en de beveiligingseisen die worden gesteld aan het werken met het DD JGZ zijn hierbij leidend.

3) Gebruik van een mix tussen offline en online werken

Wanneer het leggen van een verbinding met het DD JGZ niet mogelijk is doordat het netwerk niet beschikbaar en/of toereikend is, kan ook er (afhankelijk van de applicatie) offline gewerkt worden. De informatie die de JGZ medewerker offline verwerkt kan direct gesynchroniseerd worden wanneer de medewerker een online verbinding legt met het DD JGZ. Door op deze manier te werken bestaat er geen risico van het wegvallen van een verbinding of beperkte beveiliging van het netwerk van derden. Bijkomend voordeel is dat de korte verbindingstijd en beperkte data-overdracht zorgt voor lagere kosten.

[2] Onder de onvoldoende QoS vallen onder andere: een niet toereikende bandbreedte, optredende vertraging en kwaliteitsverlies van de verbinding.

Toch bestaan er ook verschillende kanttekeningen bij deze manier van werken. Doordat medewerkers lokaal werken en wellicht informatie opslaan op de eigen computer is het risico groter dat informatie verloren gaat. Het is belangrijk dat JGZ medewerkers daarom goed zijn uitgerust met de kennis en vaardigheden om dit risico te minimaliseren. Een tweede aandachtspunt is de complexiteit van het synchronisatieproces van het offline werken met het DD JGZ en het actuele – online - DD JGZ. JGZ medewerkers die beide in de offline variant werken aan hetzelfde dossier "botsen" bij online synchronisatie met het DD JGZ. In de praktijk is de kans dat deze situatie zich voordoet erg klein. Toch is het belangrijk dat de applicatie hier een oplossing voor biedt. Dit moet daarom meegenomen zijn in het programma van eisen dat wordt neergelegd bij de applicatieleverancier. Een derde aandachtspunt bij offline werken is de vraag hoe recent de informatie is die op een bepaald moment in het digitaal dossier staat. Doordat offline gewerkt wordt aan informatie over een cliënt is het belangrijk voor dat collega's hiervan op de hoogte zijn. Bij het ontwikkelen van de applicatie moeten daarom mogelijkheden meegenomen worden om een dossier 'in gebruik' te nemen, waardoor collega's er tijdelijk niet in kunnen werken. Door identificatie van de medewerker kunnen JGZ medewerkers eenvoudig zien wie er aan het document werkt en wanneer dit gebeurt/is gebeurd.

4) Gebruik van een computer van derden

Een derde alternatief voor het continu online zijn is het werken op computers van derden. Er is zo geen eigen laptop nodig, uitsluitend een beveiligde verbinding met het DD JGZ. Het maken van goede afspraken met organisaties (bijvoorbeeld scholen en consultatiebureaus) over het gebruik van hun faciliteiten is hierbij noodzakelijk. Iedere school is bijvoorbeeld verplicht om een computer beschikbaar te hebben met internetverbinding waardoor de technische mogelijkheid bestaat om met het DD JGZ te werken. Of het gewenst is om te werken op computers van derden is per situatie afhankelijk. Indien een beveiligde verbinding tot stand gebracht kan worden zijn er technisch gezien geen beperkingen en moet dit geen problemen opleveren. Er moet echter goed gekeken worden of het gebruik van de vaste computer/werkplek een goede omgeving is voor de JGZ medewerker om contact te hebben met de cliënt. Daar komt bij dat ook de computers van derden weer dienen te voldoen aan alle beveiligingseisen die de JGZ organisaties moeten volgen.

5) Gebruik van papieren templates

Wanneer voorgaande situaties niet mogelijk zijn, kunnen JGZ medewerkers werken met een tijdelijke papieren template die op een later tijdstip verwerkt wordt in het DD JGZ. Deze manier van werken heeft als voordeel dat er geen technische verbinding tot stand gebracht hoeft te worden, maar zal leiden tot productieverlies.

Conclusie

Er moet verschillende hardware aangeschaft worden om mobiel te werken. Hierbij is het noodzakelijk dat de online verbinding met het DD JGZ goed beveiligd is en dat de mobiele computer aan dezelfde beveiligingsnormen voldoet (GBZ en NEN7510) als een vaste computer. Meer informatie hierover is te vinden in de factsheet informatiebeveiliging.

In de ideale situatie is er een continue online verbinding met het DD JGZ via het landelijke draadloze netwerk. Dit is in de praktijk echter niet mogelijk waardoor overgeschakeld moet worden op het netwerk van derden of offline gewerkt moet worden waarna de JGZ medewerker zo snel als mogelijk synchroniseert met het online DD JGZ. Wanneer dit alles ook niet tot de opties behoort kan de JGZ organisatie eventueel nog gebruik maken van de computers van derden. Als laatste optie werkt de JGZ medewerker in een papieren template die later in het DD JGZ ingevoerd/geüpload wordt.