**AVG - privacy**

Hoe wij binnen JouwPad-MijnZorg omgaan met AVG-privacy

**Algemeen deel**

**Vertrouwelijke informatie**

Vertrouwelijke informatie is informatie over de bedrijfsvoering van JouwPad-MijnZorg en persoonlijke informatie over hulpvragers en medewerkers. Als vertrouwelijke informatie (mogelijk) ter inzage is geweest voor mensen waarvoor de informatie niet bedoeld is, spreken we van een datalek.

**Vertrouwelijke informatie op een (memo)briefje**

Je mag vertrouwelijke informatie niet zomaar in de prullenbak gooien, omdat je niet weet wie erbij kan en wat zij ermee doen. Wanneer je iets op een memobriefje hebt geschreven om af te stemmen moet je er voor zorgen dat je de memo veilig opbergt of je zorgt dat dit versnipperd wordt. Daarnaast is het belangrijk om zo min mogelijk vertrouwelijke informatie op het memobriefje te zetten. Zelf moet je wel begrijpen waar het over gaat, maar een ander niet.

**Vertrouwelijke medewerkersgegevens**

Privégegevens van medewerkers zijn vertrouwelijk en mag je daarom niet delen met anderen. Wanneer je bijvoorbeeld een collega een kaartje wil sturen dan mag dit alleen als de collega toestemming heeft gegeven voor het delen van het adres.

**Meld datalekken en beveiligingsincidenten**

Wanneer je ontdekt dat een document met persoonsgegevens onbeheerd is achtergelaten onderneem je altijd actie. Als je weet van wie de afdruk is dan breng je de afdruk naar de persoon of de betreffende afdeling toe. Is hier niemand of weet je niet van wie de afdruk is dan versnipper je de afdruk of gooi je het in een papiercontainer voor vertrouwelijke informatie.

Daarnaast moet je altijd melding maken van dergelijke situaties, zodat beoordeeld kan worden of sprake is van een datalek.

Een datalek moeten wij binnen 72 uur doorgeven aan de Autoriteit Persoonsgegevens, het is daarom belangrijk om een melding zo snel mogelijk te doen.

**Wachtwoorden**

Wachtwoorden zijn persoonlijk en houd je altijd voor jezelf. Dit betekent dat je wachtwoorden niet op mag schrijven in je agenda of op een (memo)briefje. Heb je een moeilijk wachtwoord en heb je deze vergeten? Dan kan je altijd een nieuw wachtwoord aanvragen.

Ook is het niet toegestaan om in te loggen met het wachtwoord van iemand anders.

**Phishing mail herkennen**

Ondanks de beveiligingsmaatregelen die we nemen kunnen er soms phishing mails in je mailbox terecht komen. Het is belangrijk dat je deze kan herkennen en niet op de link in de mail klikt. Ook wanneer in ongevraagde mails naar vertrouwelijke informatie gevraagd wordt om bijvoorbeeld een lening of erfenis te krijgen gaat het in veel gevallen om phishing.

Kenmerken phishingmail:

- Afzender meestal niet bekend;

- Taalfouten in de tekst of rare zinsopbouw;

- Aanhef is vaak algemeen, zoals ‘Beste heer/mevrouw’;

- Je wordt gevraagd om op een link te klikken, een bijlage te openen of vertrouwelijke informatie op te sturen.

Phishing mails kunnen ervoor zorgen dat schadelijke software geïnstalleerd wordt, dat je naar een valse website geleid wordt of dat zij met jouw persoonsgegevens aan de haal gaan ‘identiteitsfraude’.

**Veilig mailen**

Wanneer je informatie naar een hulpvrager, verwant of een andere zorgaanbieder moet sturen dan moet dit altijd op een veilige manier gebeuren. Voor het mailen naar “buiten” moeten aanvullende maatregelen worden genomen om veilig te kunnen mailen. Je mag dus niet zonder aanvullende maatregelen naar een privéadres van jezelf, een hulpvrager of verwant mailen. Dit geldt ook voor mailen naar andere zorgaanbieders, gemeenten en CIZ.

**Whatsapp**

De Whatsapp-verbinding is beveiligd (met de zogeheten end-to-end encryptie), maar de provider houdt zich het recht voor om de gegevens te gebruiken voor andere doeleinden. Dit is in strijd met de privacywetgeving, waardoor wij Whatsapp niet mogen gebruiken voor het uitwisselen van cliëntgerelateerde gegevens. Alleen wanneer gegevens niet te herleiden zijn naar een hulpvrager mogen we het gebruiken.

**Zorg gerelateerd deel**

**Informatieverzoeken van derden**

In de praktijk kan het voorkomen dat je gebeld wordt door iemand die graag informatie wil over een hulpvrager van jou. Cliëntgegevens zijn echter vertrouwelijk en wij hebben een beroepsgeheim. Dit betekent dat wij niet zomaar cliëntgegevens mogen delen met anderen. Wij mogen pas informatie over de hulpvrager delen als wij daar van de hulpvrager toestemming voor hebben gekregen. Dit geldt ook voor de toegang van gemeenten.

**Social media**

Het delen van cliëntgegevens via social media is niet toegestaan vanwege het feit dat deze niet voldoende beveiligd zijn. Hierdoor lopen wij het risico dat onbevoegden inzage krijgt in de informatie.

**Veilig omgaan met IT-middelen**

Wanneer je in het bezit bent van een telefoon, laptop of iPad dan ga je daar natuurlijk goed mee om. Ook dan kan het gebeuren dat jij iets verliest of bestolen wordt. In zo’n geval moet je direct contact opnemen met JouwPad-MijnZorg. Wanneer je iets belangrijks bij een cliënt hebt laten liggen dan haal je dat direct op.

**Netwerken**

**Openbare netwerken**

Netwerken in openbare ruimten, zoals een bibliotheek, vliegveld, camping of hotel zijn openbare netwerken. Soms zijn deze wel beveiligd met een wachtwoord, maar iedereen die inlogt komt op datzelfde netwerk, ook mensen met apparaten die jij niet kent. Wanneer je inlogt op een openbaar netwerk bestaat altijd het risico dat iemand met jou meekijkt. Het is daarom niet toegestaan om via een openbaar netwerk te werken. Wij adviseren om in jouw privésituatie ook zelf geen activiteiten als internetbankieren of bijvoorbeeld inloggen bij DigiD/mail etc te doen.

**Databundel (3G of 4G)**

Het gebruik van een databundel is wel veilig, omdat het hier gaat om een eigen verbinding met het netwerk. Alleen jouw telefoon maakt via jouw route contact met het netwerk van jouw provider.

**Thuiswerken**

Wanneer je inlogt op je eigen computer is het belangrijk dat je daarbij veilig werkt. Neem in ieder geval de volgende maatregelen in acht:

• Zorg voor een veilige netwerkomgeving, zorg dus voor een wifi-netwerk met een eigen wachtwoord dat niet door anderen dan jou en jouw gezin wordt gebruikt of maak gebruik van een internetkabel ;

• Zorg voor antivirussoftware, een malwarescanner en een firewall en houd deze up to date ; • Wees altijd voorzichtig met vage mails (mogelijk phising) ;

• Sla geen vertrouwelijke bedrijfsinformatie en cliëntgegevens op je eigen computer op ;

• Zorg ervoor dat vertrouwelijke bedrijfsinformatie en cliëntgegevens niet inzichtelijk zijn voor huisgenoten.

**Veilig werken**

Als je op een computer werkt met vertrouwelijke gegevens dan moet je bij het verlaten van je werkplek er altijd voor zorgen dat de toegang tot je computer wordt afgesloten. Dit kan je doen door je computer te vergrendelen via de Start-knop of door gebruik te maken van Windows + L. Wanneer iemand bij jou komt staan dan zorg je dat de vertrouwelijke informatie niet meer zichtbaar is op het scherm. Dit kan je doen door de applicatie of het document te minimaliseren of af te sluiten

**Gegevens uitwisselen binnen het sociaal domein**

Het verstrekken van het cliëntdossier aan een gemeente is niet toegestaan. Het dossier van een hulpvrager bevat alle inhoudelijke informatie en mag niet, ook niet met toestemming van de hulpvrager, gedeeld worden met de gemeente. De toestemming van de hulpvrager is in deze gevallen niet voldoende omdat de hulpvrager afhankelijk is van de gemeente voor het ontvangen van zorg of ondersteuning.

Wanneer in het kader van (her-)beschikking bepaalde informatie nodig is mogen wij dit wel verstrekken, maar daarbij mag alleen die informatie verstrekt worden die noodzakelijk is om een nieuwe beschikking af te geven. Het is bijvoorbeeld niet noodzakelijk om het hele plan van een hulpvrager te sturen, vaak is alleen een evaluatie op bepaalde doelen voldoende.

Uiteraard gebeurt dit alleen als de hulpvrager hiervoor toestemming heeft gegeven.

Ook voor het bespreken van hulpvrager in een wijkteam geldt dat de hulpvrager hiervoor toestemming moet geven. Alleen in bijzondere gevallen kan hiervan worden afgeweken, om bijvoorbeeld de veiligheid van hulpvrager en/of zijn omgeving te kunnen garanderen.