Privacybewust werken

Je bent nieuw bij het team Bron- en Contactonderzoek van GGD Zaanstreek Waterland.

In jouw rol ga je met vertrouwelijke gegevens van onze burgers om. Dit kunnen persoonsgegevens zijn (bijvoorbeeld naam, adres woonplaats, email, telefoonnummer) gevoelige gegevens (BSN nummer) of bijzondere persoonsgegevens (bijvoorbeeld medische gegevens).

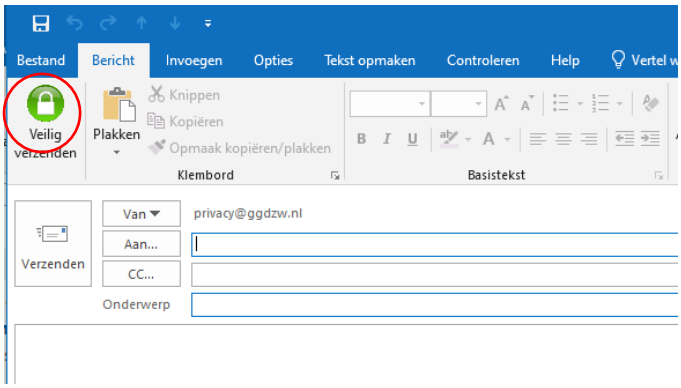
Elke medewerker van onze GGD moet op een juiste manier omgaan met deze gegevens. Je deelt de informatie die je inziet niet met vrienden en familie of andere derden. Je kijkt alleen in het dossier van een burger als je een contactonderzoek start. Je hebt ook een geheimhoudingsverklaring ondertekend. Je leest hier wat dit betekent in de praktijk. Het belangrijkste is dat je je bewust bent dat wij bij de GGD met heel veel data werken die zeer vertrouwelijk is en ook als dusdanig behandeld moet worden. Je werkt onder de verantwoordelijkheid van een arts. Mocht er iets met de data gebeuren, dan wordt deze arts verantwoordelijk gehouden. Zorg er dus voor dat de privacy van onze burgers geborgd is!

1. Communicatie

1a Veilig e-mailen / verzenden

Als je iets vertrouwelijks verstuurd, gebruik dan altijd de optie veilig verzenden. Denk hierbij aan een mail waarin je persoonsgegevens deelt of andere vertrouwelijke gegevens.

Het systeem vraagt automatisch om een 06 nummer als je veilig verzendt. De ontvanger ontvangt de code op het ingevoerde 06 nummer.



1b Appen

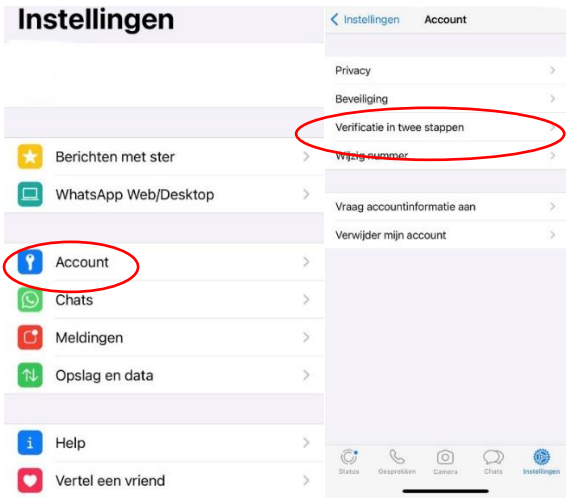
WhatsApp

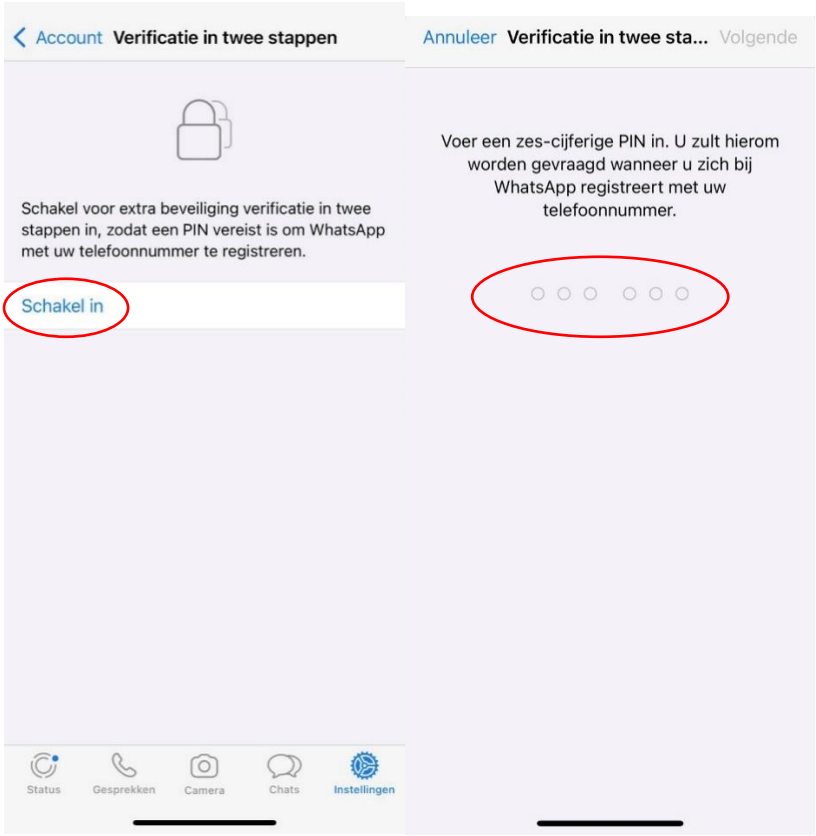
Het gebruik van WhatsApp is niet veilig en mag niet gebruikt worden om persoonsgegevens of andere vertrouwelijke gegevens te delen! Voor medische informatie mag alleen Siilo worden gebruikt. Dat wordt verderop beschreven.

Als je het gebruikt, volg dan onderstaande instructies:

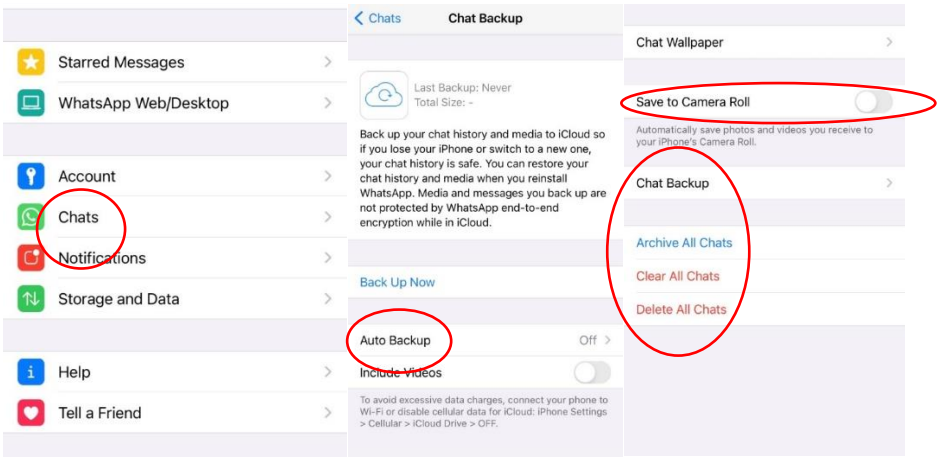
A. Zet de beveiliging aan,
B. Wis je chat regelmatig
C. Sla media niet automatisch op

A: Beveiliging (verificatie in twee stappen)





B + C: sla je chats en media niet op en wis regelmatig



Siilo

Siilo is een veilig alternatief voor zorgprofessionals.

Siilo wist automatisch de conversatie na 30 dagen, heeft een koppeling met geverifieerde zorgprofessionals en is end-to-end beveiligd. Ook zie je geen notificaties zodat berichten zijn afgeschermd.

Siilo is te downloaden via de Playstore en de Appstore.

1c Telefonie

Je maakt voor je werk veel gebruik van de telefoon. Je gaat een index en contacten bevragen om ze enerzijds van advies te dienen hoe te handelen bij een mogelijke besmetting en anderzijds om de bron van de infectie op te sporen.

Hou je aan de scripts zoals in de werkinstructies beschreven en vraag niet meer uit. Een belangrijk onderdeel van privacy is dat je alleen de informatie vraagt die je nodig hebt. Niet meer en niet minder.

Wis op het einde van je dienst de gebelde nummers. Mocht er iets met je telefoon gebeuren, dan zijn de nummers van de gebelde burgers in ieder geval voor niemand toegankelijk.

2. Datalekken

Meld dit via de knop 'Melding intern incident' op intranet of privacy@ggdzw.nl.

Wanneer is er sprake van een datalek?

- Per ongeluk in het verkeerde dossier gekeken (noteer dit ook in het dossier!)
- Per ongeluk de verkeerde persoon een e-mail gestuurd
- Dossier open laten staan op je computer en je werkplek onbeheerd achtergelaten
- Dossier per ongeluk uitgeprint
- Gegevens uit het ene dossier per ongeluk in het andere dossier gezet (foutief)

- Papier met persoonsgegevens niet in bak vertrouwelijk papier gedaan
- Je papieren aantekeningen kwijtgeraakt
- Iemand anders heeft je inloggegevens gebruikt
- Je telefoon is onbeheerd en niet op slot achtergebleven.

Het lijkt alsof iets een datalek is als er ook daadwerkelijk informatie (ongeoorloofd) lekt. Niets is minder waar. Ook het open laten staan van je beeldscherm is al een datalek. Dus 'de mogelijkheid om ongeoorloofd toegang te hebben' is ook al een datalek.

TIP: Snel je scherm op slot bij het (kort en lang) verlaten van de werkplek:

3. Digitale veiligheid

Toegang tot dossiers wordt geregistreerd om misbruik te voorkomen. Dit heet zogenaamde 'logging'.
Wanneer je een dossier per ongeluk opent, registreer dan in het dossier waarom je erin bent geweest.

De regel is dat je alleen een dossier opent als dit nodig is voor de casus waar je op dat moment in werkt.

Wat kan wel:

- Met je eigen gegevens inloggen
- De identiteit van de beller controleren, zie hiervoor de werkinstructies op GGD GHOR Academy. Als je hier geen toegang to hebt, neem dan contact op met je dag coördinator.
-

Wat kan niet:

- Je login gegevens afgeven of die van een ander gebruiken
- Informatie afgeven aan iemand over een ander
- Inloggen in programma's met patiëntendossiers als je niet bent ingeroosterd
- Printen of printscreens maken
- Persoonsgegevens van klanten of collega's delen op social media
- Via welke media dan ook iets delen dat de GGD, collega's of klanten kan schaden

- Als je een casus ziet van iemand die je kent raden we je aan om deze casus aan een collega over te dragen
- Een testuitslag checken voor iemand die je kent (terwijl je niet op de casus werkt), ook al heb je toestemming

Heb je vragen over privacy? Stel ze aan je leidinggevende of stuur een mail naar privacy@ggdzw.nl.

Tot slot:

Ook bij uitdiensttreding blijft de geheimhoudingsverklaring van toepassing. Dat betekent dat ook dan geen gegevens van de GGD, haar medewerkers of klanten gedeeld of gebruikt mogen worden.

We hebben ook de gedragscode Digitale Communicatiemiddelen beschikbaar gesteld. Deze is opgesteld voor de reguliere medewerkers van de GGD en dus niet specifiek voor de sector Corona. Je kan er wel veel informatie uit halen op het gebied van Privacy en Informatieveiligheid!