Zaanstreek-Waterland

Privacybewust werken

GGD Zaanstreek-Waterland

Privacybewust werken

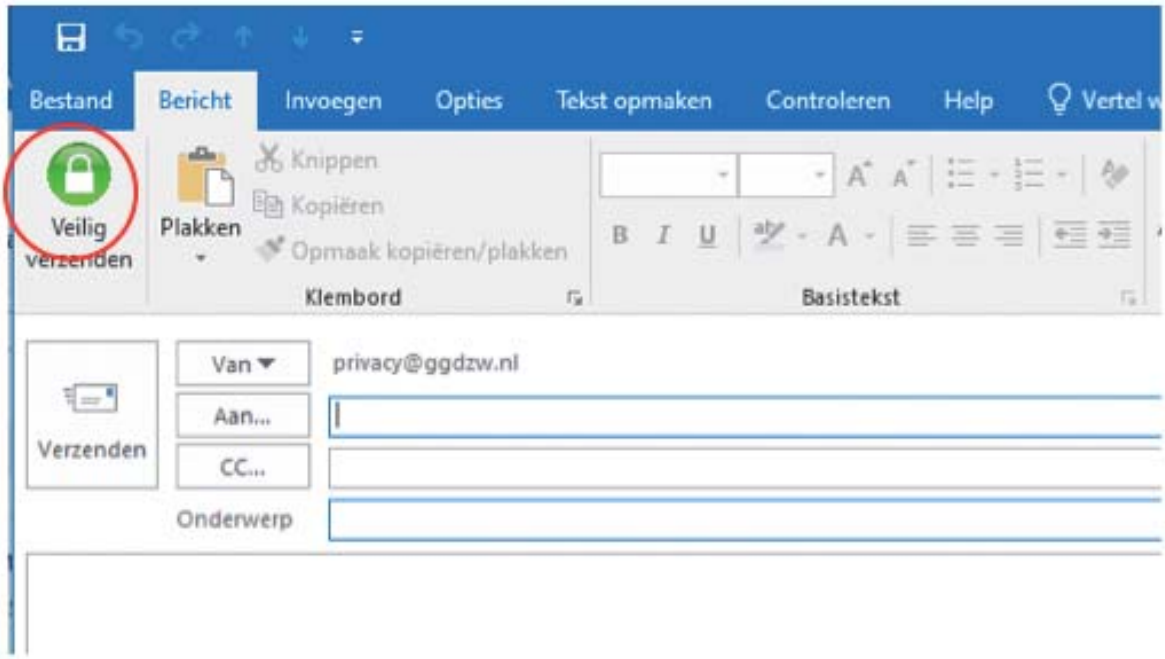
Je werkt bij de sector corona van GGD Zaanstreek Waterland.
In jouw rol ga je met vertrouwelijke gegevens van onze klanten om.
Dit kunnen persoonsgegevens zijn (bijvoorbeeld naam, adres, woonplaats, e-mail, telefoonnummer), gevoelige gegevens (BSN nummer) of bijzondere persoonsgegevens (bijvoorbeeld medische gegevens). Elke medewerker van onze GGD moet op een juiste manier omgaan met deze gegevens.

Je deelt de informatie die je ziet en hoort niet met vrienden en familie of andere derden. Je kijkt alleen in het dossier van een burger als dit noodzakelijk is voor het uitvoeren van de werkzaamheden die horen bij jouw functie. 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 informatie werken die zeer vertrouwelijk is en die je ook zo moet behandelen. Als vertrouwelijke informatie kwijtraakt of bij een persoon terecht komt waarvoor het niet is bedoeld, kan dit voor grote problemen zorgen. Bijvoorbeeld voor de burger die het betreft. Ook kan het vertrouwen in onze organisatie beschadigd raken. Daarnaast wordt de arts, onder wiens verantwoordelijkheid je werkt, in deze gevallen verantwoordelijk gehouden. Bescherm daarom de privacy van onze burgers!

1 Communicatie

1a Veilig e-mailen / verzenden

Als je iets vertrouwelijks verstuurt, 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 je niet gebruiken om persoonsgegevens of andere vertrouwelijke gegevens te delen! Voor medische informatie mag je alleen Siilo gebruiken. Je vindt een beschrijving in dit document.

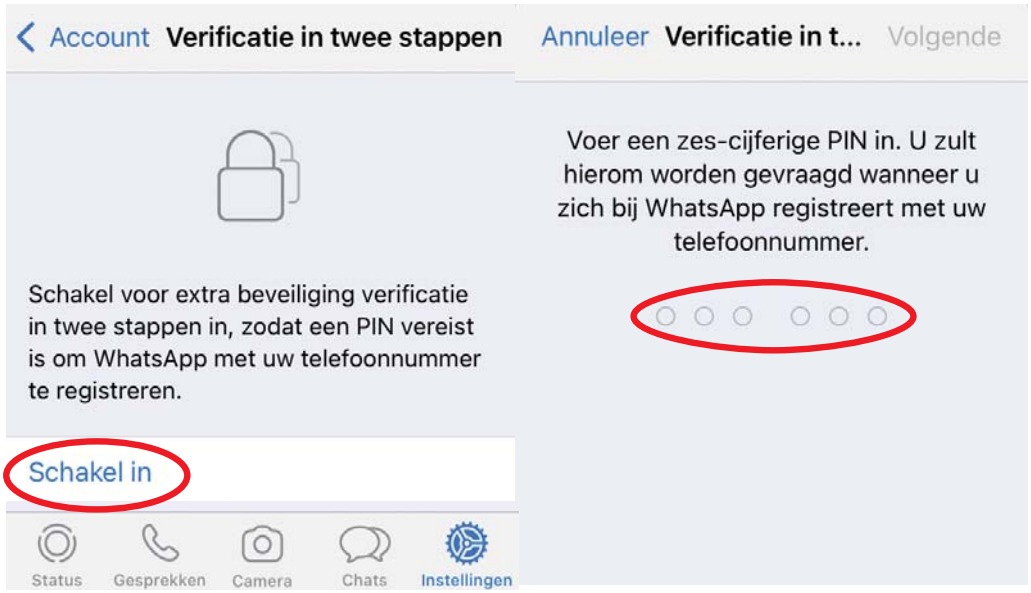
Als je WhatsApp gebruikt, volg dan onderstaande instructies:

A zet de beveiliging aan;

B wis je chat regelmatig;

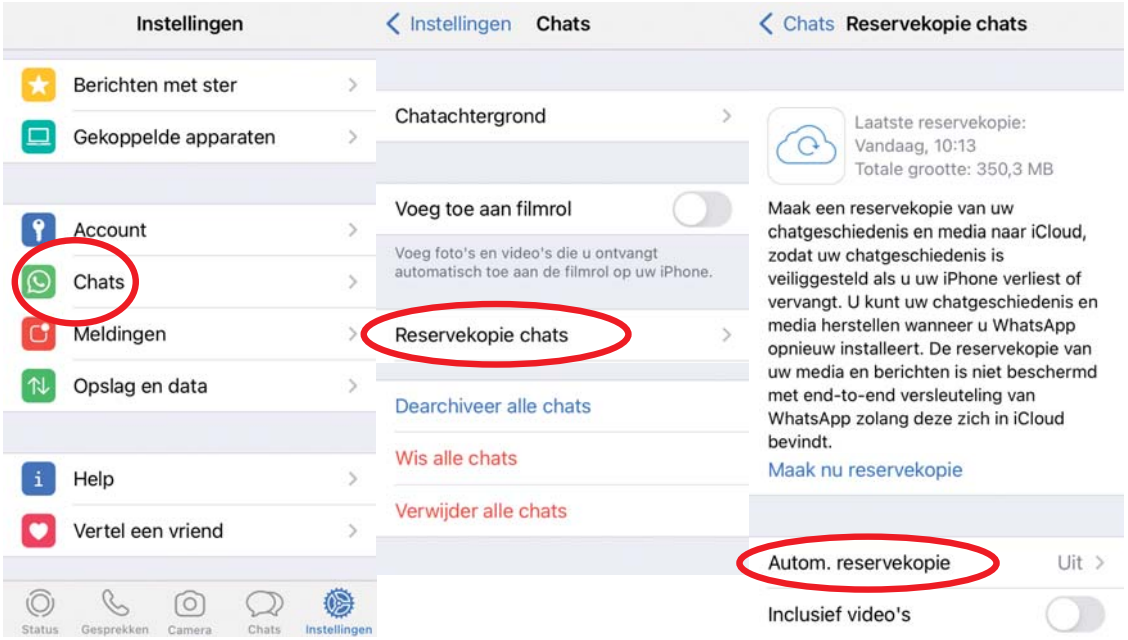
C sla media niet automatisch op.

A: Beveiliging (**verificatie in twee stappen**)



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

In de afbeelding hieronder zie je de instructies voor Iphone. Voor Android doorloop je de volgende stappen: **Instellingen** > **Chats** > **Chat back up** > Back-up maken naar Google Drive: kies optie '**Nooit**'. Onder '**Chats**' vind je ook '**Chatgeschiedenis**', wis die regelmatig.



Siilo

Siilo is een veilig alternatief voor zorgprofessionals. Siilo wist het gesprek automatisch na 30 dagen en heeft een koppeling met geverifieerde zorgprofessionals. Het is end-to-end beveiligd; het is zo versleuteld dat alleen de zender en ontvanger de inhoud van berichten kunnen lezen. Ook zie je geen notificaties zodat berichten zijn afgeschermd.
Je kunt Siilo downloaden via Google Play en App Store

1c Telefonie

Misschien maak je voor je werk veel gebruik van de telefoon. Bijvoorbeeld als medewerker bron- en contactonderzoek: je bevraagt telefonisch een index en contacten, zodat je ze kunt adviseren over hoe te handelen bij een mogelijke besmetting en om de bron van de infectie op te sporen.

Hou je aan de scripts zoals in de werkinstructies beschreven en vraag niet meer. 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. Als er iets met je telefoon gebeurt, 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 bijvoorbeeld 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;
- papieren aantekeningen kwijtgeraakt;
- inloggegevens door iemand anders gebruikt;
- 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

De GGD registreert toegang tot dossiers 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 tot hebt, neem dan contact op met je 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;
- een testuitslag checken voor iemand die je kent (terwijl je niet op de casus werkt), ook al heb je toestemming.

Als je een casus ziet van iemand die je kent, raden we je aan om deze casus aan een collega over te dragen.

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

Tot slot:

Ook als je uit dienst treedt blijft de geheimhoudingsverklaring van toepassing. Dat betekent dat je ook dan geen gegevens van de GGD, haar medewerkers of klanten mag delen of gebruiken.
We hebben ook de gedragscode Digitale Communicatiemiddelen. Deze is voor alle 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!