WERKINSTRUCTIE

Auteur	Sandra van Roermund
Afdeling	Beleidsmedewerker
Autorisatie door	Bart Hugen, directeur
Bestemd voor	Alle medewerkers
Status / Versie	Vastgesteld
Geldig tot	31-12-2022
Gerelateerde documenten / evt. wet- en regelgeving	AVG , Werkinstructie rechten zorgvrager privacywet , Toestemmingsformulier (https://www.ghz.nl/voorbereiden-op/informatiefilms-en-cliëntenfolders/algemene-folders/)
Vindplaats bronbestand / Aantal en vindplaats hardcopies	Algemene schijf

Inhoud

1 Samenvatting

Informatie delen mag alleen met:

nedap

ons

Point

Siilo.

ZorgDomein

Veilig verzenden

Wat mag of moet wel:

- Informatie verwerken met toestemming van de cliënt
- Je computer en telefoon vergrendeld achter laten als je weg loopt

Wat mag niet:

- Onbeveiligd e-mailen naar iemand buiten de organisatie
- E-mailen naar privé adressen
- Persoonsgegevens delen als dat niet strikt noodzakelijk is
- Thuis verwerken van cliënt-gegevens zonder toestemming van je leidinggevende, en niet zonder beveiligde verbinding

2 Omschrijving

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. In deze wet staan rechten van betrokkenen (zoals cliënten of medewerkers) en plichten van zorgaanbieders benoemd waar iedereen zich aan moet houden. In deze memo kun je lezen wat dit voor jou als medewerker van ZorgBrug betekent.

3 Aandachtspunten

In welke gevallen mag je gegevens gebruiken?
De AVG stelt dat gegevens niet gebruikt mogen worden, tenzij er een rechtsgrond voor is. Bij ZorgBrug is de rechtsgrond meestal dat er zorg verleend wordt, waarvoor bepaalde zaken, zoals het Burger Service Nummer (BSN) geregistreerd móeten worden. Wanneer het niet gaat om zorgverlening, maar om bijvoorbeeld het geven van scholing, dan mogen er geen privacygevoelige gegevens worden verwerkt. Het woord verwerken betekent in de AVG: opslaan, bewaren, gebruiken, inzien, verspreiden, etc. Dus ook het hebben van gegevens wordt gezien als 'verwerken'.

Welke gegevens mag je gebruiken?
Je mag uitsluitend gegevens verwerken wanneer dat noodzakelijk is voor het kunnen uitoefenen van de zorgverlening (incl. declaraties). Er wordt hierbij onderscheid gemaakt tussen 'gewone' en 'bijzondere' persoonsgegevens. Alle vormen van persoonsgegevens kunnen ertoe leiden dat je een individuele persoon kunt herleiden, maar de bijzondere persoonsgegevens zijn extra gevoelig van aard en moeten daarom met extra voorzichtigheid behandeld worden. Dit zijn:

- NAW-gegevens
- Geboortedatum
- Geslacht
- Cliëntnummer
- BSN (dit is een bijzonder persoonsgegeven)
- Gezondheid (dit is een bijzonder persoonsgegeven)

Met deze gegevens kan een persoon gevonden worden door derden, en dit betreft dus privacygevoelige informatie. ZorgBrug moet dus uitermate voorzichtig omgaan met deze gegevens, want cliënten vertrouwen ZorgBrug met die gegevens.

Hoe ga je om met het doorgeven van gegevens?
Gegevens mogen doorgegeven worden aan zorgverleners die direct bij het uitvoeren van de zorgovereenkomst betrokken zijn, indien dat voor het uitvoeren van hun taak noodzakelijk is. Bijvoorbeeld: je hebt met een cliënt besproken dat je hem doorverwijst naar een andere zorgverlener. Indien gegevens, zoals een BSN-nummer, niet noodzakelijk zijn dan mag het niet doorgegeven worden. Hierbij is een goede vuistregel "als de cliënt er logischerwijs van uit kan gaan dat zijn gegevens worden doorgegeven, dan hoef ik geen toestemming aan de cliënt te vragen". Dat is bijvoorbeeld zo bij een verwijzing, maar niet bij het geven van scholing.

Over het doorgeven van gegevens aan zorgverleners of andere derden van wie de zorgvrager niet logischerwijs weet dat die partij de gegevens zal ontvangen, moet

de zorgvrager geïnformeerd worden. Dit is bijvoorbeeld het geval bij het terugkoppelen van gezondheidsinformatie informatie aan de huisarts. In zulke gevallen moet een cliënt expliciet toestemming geven voor het delen van de informatie, en die toestemming moet worden vastgelegd in het dossier van de cliënt. Hier voor kan op de website van het GHZ een toestemmingsformulier gevonden worden.

Met welke middelen mag je informatie delen?
Zowel voor interne als externe communicatie is het van belang om de juiste middelen te gebruiken voor het veilig versturen van persoonsgegevens, zeker als het gaat om bijzondere persoonsgegevens. Hiervoor bestaan de volgende mogelijkheden:

1. Binnen het GHZ kan beveiligde mail (de knop Veilig Verzenden in Outlook) gebruikt worden. Dit moet voor externe communicatie **altijd** gebruikt worden.
2. Zorgmail (binnen Surface). Dit kan ook voor externe communicatie gebruikt worden.
3. In Nedap kan je 'berichten' sturen naar je collega's en contactpersonen. Dit is voor interne communicatie, of gerichte externe communicatie naar contactpersonen van cliënten.
4. Point
5. Zorgdomein
6. Siilo
7. Fax (liever niet, tenzij je zeker weet dat de fax bij de ontvanger in een afgesloten ruimte binnen komt)

LET OP: Waar moet je verder rekening mee houden?

1. Persoonsgegevens mogen nooit gedeeld worden met derden (dus buiten ZorgBrug of het GHZ) via een onbeveiligde e-mail.
2. Persoonsgegevens mogen nooit naar een privé e-mailadres van een medewerker of collega-zorgverlener gestuurd worden.
3. Indien je thuis wilt werken en daarbij persoonsgegevens van cliënten gaat verwerken, is daarvoor toestemming nodig van je leidinggevende. Je moet hiervoor tevens thuis in kunnen loggen op je @zorgbrug.nl mailbox, of je @ghz.nl mailbox. Je mag, zoals in lid 2 al gezegd, geen gegevens naar je privé e-mailadres sturen. Verder moet je ervoor zorgen dat je laptop of PC beveiligd is met een wachtwoord zodat gezinsleden of anderen die de computer in handen krijgen niet bij de informatie kunnen, en moet je ervoor zorgen dat persoonsgegevens niet lokaal op de computer worden opgeslagen (denk bijvoorbeeld aan de map Downloads als je een bestand download, en de Prullenbak).
4. Zorgvragers hebben het recht om te weten welke gegevens van hen worden gebruikt en kunnen bijvoorbeeld een verzoek doen tot het inzien of het verwijderen van hun gegevens. Hiervoor is op de Afdelingsschijf een aparte werkinstructie beschikbaar, de Werkinstructie rechten zorgvrager privacywet. Hierin staat omschreven welke rechten de betrokkenen precies hebben en hoe ZorgBrug handelt als iemand een beroep doet op zo'n recht.

5. Het is te allen tijde van belang dat wij zorgvuldig met gegevens van zorgvragers omgaan. Dit houdt bijvoorbeeld in dat:
    a. Papieren dossiers in principe niet meer gebruikt/gemaakt worden. Er wordt alleen nog digitaal gewerkt in NOVA/Nedap/inSight etc. Indien er een archief bestaat van papieren dossiers moet dit zoveel mogelijk gedigitaliseerd worden. Indien dat niet mogelijk is, en de bewaartermijn nog niet is verstreken, dan is het toegestaan om het papieren dossier in een afgesloten kast te bewaren.
    b. Je niet bij een computer of iPad wegloopt zonder die eerst te vergrendelen;
    c. Je ook in je e-mail oplet wat daarin wordt geschreven, opgeslagen en hoe lang.
        1. Schrijf alleen persoonsgegevens die strikt noodzakelijk zijn om te delen. Kan je het doel waarvoor je een e-mail schrijft ook bereiken door gegevens niet te delen? Dan mag je geen aanvullende gegevens noteren.
        2. Als je een e-mail over of van een zorgvrager ontvangt of verstuurt, en het is van belang om deze te bewaren, voeg deze toe aan het elektronisch cliëntendossier of rapporteer erover. De e-mail verwijder je uit je inbox, verzonden items en verwijderde items.
           Loop je inbox af en toe door aan de hand van de regels rondom bewaartermijnen (zie bijlage). Verwijder die gegevens waarvan de bewaartermijn is verstreken.

Een datalek kan vervelende gevolgen hebben voor de betrokkenen. Zo kan het voor een cliënt betekenen dat zijn identiteit gestolen wordt, en voor ZorgBrug kan het betekenen dat er flinke kosten gemaakt moeten worden om de gevolgschade van het datalek te beperken of dat ZorgBrug een boete krijgt. Maak er daarom een gewoonte van om je werkplek, inclusief computer en telefoon, altijd vergrendeld achter te laten en handel zorgvuldig bij het uitwisselen of opslaan van informatie.

4 Meldplicht datalekken

Het is aan iedereen de taak om ervoor te zorgen dat de kans op een datalek geminimaliseerd wordt.
In het geval dat er tóch een datalek is geweest (op welke manier dan ook ontstaan) moet er DIRECT een melding gemaakt worden bij het MT (Bart Hugen of Wouter Steenwoerd). Zij beoordelen dan samen met de sleutelfiguur privacy (Sandra van Roermund) of het lek dusdanig grote gevolgen kan hebben dat er melding van gemaakt moet worden bij de Autoriteit Persoonsgegevens. Mocht dit het geval zijn, moet die melding binnen 72 uur gemaakt worden. Het is dus van belang dat het MT bij een datalek (of een vermoeden van een lek) zo snel mogelijk (uiterlijk binnen vier uur na de ontdekking) bericht ontvangt, zodat er voldoende tijd is om het risico van de melding te beoordelen. Dit geldt ook buiten kantoortijden en op zon- en feestdagen.

De melding kan via e-mail (met Hoge Urgentie en in de onderwerpregel vermeld dat het om een datalek gaat) of mondeling/telefonisch gedaan worden:

- Bart Hugen (bart.hugen@ghz.nl, tel:0182-505432 / 06-29017881)

- Wouter Steenwoerd (wouter.steenwoerd@ghz.nl, tel: 0182-5055432 / 06-21504339)

5 Verwijzingen

- Werkinstructie rechten zorgvrager privacywet
- Toestemmingsformulier delen gegevens / uitwisselen gegevens met derden (GHZ.nl)

6 Samenvatting

- Met alle persoonsgegevens moet zorgvuldig omgegaan worden, in het bijzonder met BSN en gegevens omtrent gezondheid.
- Gebruik voor het doorgeven van gegevens de toegestane beveiligde vormen van communicatie.
- Vergrendel computers en tablets of telefoons en zorg voor een zorgvuldige omgang met papieren dossiers.
- Bij (het vermoeden van) een datalek dient zo snel mogelijk een melding bij het MT gedaan te worden.

7 Vragen?

Voor vragen kun je terecht bij Sandra van Roermund (sandra.van.roermund@ghz.nl).

WERKINSTRUCTIE

Bijlage 1: Lijst bewaartermijnen

Bron: Fundis

LIJST BEWAARTERMIJNEN wettelijk kader

Document/gegevens	Bewaartermijn
Zorggerelateerd	
Cliëntdossier	*Minimaal 15 jaar vanaf de datum dat het dossier is aangemaakt.*
BOPZ dossier	*Minimaal 5 jaar na beëindiging van de BOPZ behandeling.*
Actueel medicatieoverzicht	*Minimaal 15 jaar.*
Medicatietoedieningslijsten	*Minimaal 2 maanden ingaande na einddatum van de betreffende lijst. Indien iets bijzonders is voorgevallen, is het bewaartermijn tenminste 2 jaar.*
Temperatuurlijsten medicatieopslag (medicijnkoelkast)	*Minimaal 2 jaar.*
Personeelsgegevens	
Sollicitatiebrieven, sollicitatieformulieren, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag	*Na beëindiging sollicitatieprocedure: maximaal 4 weken **zonder toestemming** sollicitant maximaal 1 jaar **met toestemming** sollicitant.*
Arbeidsovereenkomst en wijzigingen	*Maximaal 2 jaar na einde dienstverband.*
Verslagen van functioneringsgesprekken	*Maximaal 2 jaar na einde dienstverband.*
Verslaglegging in het kader Wet Verbetering Poortwachter	*Maximaal 2 jaar na einde dienstverband.*
Loonbelastingverklaringen en kopieën van identiteitsbewijzen	*Minimaal 5 jaar na einde dienstverband.*
Afspraken betreffende salaris en arbeidsvoorwaarden	*Minimaal 7 jaar na einde dienstverband.*
Burgerlijke staat werknemer	*Minimaal 7 jaar na einde dienstverband.*
Loonbeslagen	*Tot opheffing.*

BEWAARTERMIJNEN

Algemene bedrijfsmatige documenten	
Jaarrekening, accountantsverklaring, e.d.	*Minimaal 7 jaar vanaf datum opstellen.*
Winst- en verliesrekening	*Minimaal 7 jaar vanaf datum opstellen.*
Administratie na ontbinding rechtspersoon	*Minimaal 7 jaar na ontbinding.*
Dividendnota's	*Minimaal 5 jaar na opstellen.*
Gegevens bedrijfsmatig onroerend goed	*Minimaal 9 jaar volgend op het jaar waarin men het onroerend goed is gaan gebruiken.*
Ledenadministratie van een coöperatie met aansprakelijkheid van de leden	*Minimaal 10 jaar na aanvraag van het lidmaatschap.*
Subsidie administratie	*Minimaal 7 jaar vanaf datum administreren.*
Fiscale documenten	
Grootboek, debiteuren- en crediteuren-administratie, in- en verkoopadministratie, voorraadadministratie en loonadministratie	*Minimaal 7 jaar vanaf 1 januari na het jaar van opstellen.*
Facturen i.v.m. de omzetbelasting	*Minimaal 7 jaar na opstellen c.q. ontvangst.*
Identificatiebewijs (op grond van Wet Identificatieplicht)	*Minimaal 5 jaar na einde dienstverband.*
Videobeelden van personeel	
Beveiligingscamera's	*Maximaal 4 weken na start opname, tenzij een incident heeft plaatsgevonden.*
Opsporingscamera's t.b.v. fraude, diefstal en dergelijke	*Zo lang als nodig is voor het doel.*
Logfiles computersystemen / e-mail en internetmonitoring	
Computersystemen	*Maximaal 6 maanden.*
E-mail / internetmonitoring	*Maximaal 6 maanden.*
Toegangscontrolesystemen / tijdregistratiesystemen	
Gegevens m.b.t. tijdsregistratie	*Minimaal 52 weken vanaf de dag van registratie.*
Gegevens m.b.t. toegangscontrole	*Maximaal 6 maanden nadat recht op toegang is vervallen.*

fundis