Privacy geldt waar gezondheid telt!

‘Een toetsing van het beleid en de werkwijze van de GGD aan huidige- en in de toekomst in te voeren privacywet- en regelgeving’

Bijlagen

GGD Hart voor Brabant

Marlin van Dinther

Den Bosch, 9 januari 2017

Inhoudsopgave bijlagen

Bijlage I. Beleidsplan onderdeel informatieveiligheid 2015-2017

Beleidsplan onderdeel informatieveiligheid 2015 – 2017

Doel 2017: Basisniveau informatieveiligheid bereikt en certificeringsrijp

Missie

Definitie van informatieveiligheid:
Het voldoende beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tegen de mogelijke manifestatie van bedreigingen.

Visie

Wij willen dat onze klanten en medewerkers kunnen bouwen en vertrouwen op een betrouwbare informatievoorziening en hun privacy wordt beschermd. Dit doen we door de bedrijfsvoering op die onderdelen veilig te stellen die met informatievoorziening te maken hebben en wettelijke verplichtingen na te komen.

Succesbepalende Factoren (SBF'en)

- Directie als probleemeigenaar staat voor het informatieveiligheidsbeleid en draagt dat actief uit.
- Medewerkers zijn zich bewust (awareness) wat informatieveiligheid inhoudt.
- Medewerkers handelen volgens gemaakte afspraken informatieveiligheid.
- Een goed ingericht incidentmeldingssysteem en verbetercyclus.
- Externen conformeren zich aan informatieveilig-heidsbeleid.

Focuspunten 2015

1. Medewerkers gaan zorgvuldig om met informatie en leveren daarmee een bijdrage aan informatieveiligheid.
2. Het Information Security Management System (ISMS) is ingebed in het kwaliteitsmanagementsysteem (KMS).
3. Organisatie is continu bewust waar risico's zitten en neemt (zo nodig) passende maatregelen.
4. Klanten, leveranciers en partners zijn geïnformeerd en/of betrokken bij de afspraken rondom informatieveiligheid.
5. Privacy van cliënten en medewerkers is gewaarborgd.

1. Leiderschap

- Richting geven aan informatieveiligheid. (2–3)
- Ambassadeurschap, het actief ondersteunen en uitdragen van informatieveiligheid. (1)
- Tonen van voorbeeldgedrag en elkaar hierop aanspreken. (1)
- Erkennen en toekennen van verantwoordelijkheden. (2– 3)
- Ruimte maken voor inrichting van informatieveiligheids-organisatie. (2– 3)

3. Management van medewerkers

- Versterken van awareness bij medewerkers. (1)
- Duidelijk maken van de verantwoordelijkheden van de medewerker zelf. (1)
- Vastleggen van rollen en bevoegdheden van informatieveiligheidsfunctionarissen/ contactpersonen informatieveiligheid. (1-2)
- Adviseur IB belasten met toezicht op uitvoering van informatieveiligheidsbeleid. (2)

2. Strategie en beleid

- Opstellen en onderhouden van informatieveiligheids-beleid. (2)
- Toetsen van informatiebeleid en –architectuur (PURA) op informatieveiligheidsrichtlijnen. (2-3)
- Opstellen jaarlijks informatieveiligheidsplan. (2)
- Opstellen en onderhouden communicatieplan informatieveiligheid. (1-2-4)
- Inrichten van een lean ISMS met behulp van NEN7510. (2)
- Informatieveiligheid opnemen in de directiebeoordeling. (2)

4. Management van middelen

- Vrijmaken van tijd en middelen voor het inventariseren, labelen en classificeren van bedrijfsmiddelen. (2)
- Vrijmaken van tijd en middelen voor de uitvoering van risicoanalyses. (1-2-3)
- Beschikbaar stellen van ondersteunende applicaties/ ICT-tools om de verbetercyclus efficiënter te laten verlopen. (2-3)
- Inrichten van cliënt- en personeelssystemen zodat privacy, autorisatie en authenticatie op goede wijze geregeld zijn. (1-3-5)

5. Management van processen

- Inrichten van informatie-veiligheidsprocessen. (2-3)
- Inventariseren en classificeren van bedrijfsmiddelen. (2-3)
- Uitvoeren van risicoanalyses (2-3).
- Bepalen van benodigde set van veiligheidsmaatregelen op basis van uitgevoerde risicoanalyse. (2-3)
- Inrichten van een rapportage-systeem. (2-3)
- Maken van afspraken op gebied van informatieveiligheid met externe dienstverleners. (3-4)
- Inrichten proces dat relevante (privacy)wet- en regelgeving vertaalt naar organisatie. (1-2-3-4-5)
- Monitoren en borgen van (wijzigingen in) wet- en regelgeving door adviseur IB. (1-2-3-4-5)
- Meenemen van informatieveiligheidsaspecten bij risicoanalyse door kwaliteit van primaire processen. (2)

7. Medewerkers

- % medewerker weet wat informatieveiligheid inhoudt.
- % informatieveiligheidsfunctionarissen weet welke rol en bevoegdheden ze hebben.
- # personeels- en cliëntsystemen die afdoende veilig zijn (privacy, autorisatie en authenticatie).
- Verantwoorde functiescheiding is geregeld.

6. Klanten en partners

leveranciers

- # afspraken rondom informatieveiligheid zijn gemaakt.
- # partijen waarmee informatie veilig wordt uitgewisseld.
- # cliënt- en personeelssystemen die afdoende veilig zijn (privacy, autorisatie en authenticatie).

8. Maatschappij

- Géén negatieve publiciteitsgevallen i.v.m. informatieveiligheid/privacy.

9. Bestuur en financiers

Bestuur als toezichthouder
Informatieveiligheid maakt deel uit van de bestuursrapportage.

Accountant
Op- en aanmerkingen uit accountantsverslag zijn meegenomen in informatieveiligheidsplan.
De actiepunten zijn uitgevoerd.

IGZ/CBP
De veiligheid van klant- en medewerkersdossiers is geborgd.

Organisatie

Resultaat

Verbeteren en vernieuwen

Bijlage II. Veilig gedrag op de werkplek intranet van de GGD

Bijlage II

Veilig gedrag op de werkplek

Iedereen werkt steeds meer plaats- en tijdonafhankelijk, ook op kantoor. Je kunt ervan uitgaan dat je in een veilige omgeving werkt. Maar mogen jouw collega's altijd meekijken in jouw werk? En spreek jij mensen aan die je niet kent in ons gebouw? Laten we samen alert blijven zodat we informatie beschermen!

Wil jij weten hoe? Denk aan clean desk werken, je pc vergrendelen, je smartphone beveiligen! Lees Veilig Internetten voor allerlei tips.

Clean desk

- Laat vertrouwelijke informatie niet onbeheerd rondslingeren.
- Bewaar gevoelige informatie in afgesloten kasten of ruimtes.
- Laat druppels en sleutels niet onbeheerd slingeren.
- Bewaar sleutels in afgesloten lades.

Clean screen

- Vergrendel je pc als je even van je werkplek gaat met: Windows-toets + L-toets.
- Stel je screensaver zo kort mogelijk in, bijvoorbeeld op 5 minuten.
- Bewaar geen zakelijke documenten op een geleende USB-stick.

In het gebouw

- Sluit beveiligde deuren, laat ze niet openstaan.
- Begeleid bezoekers binnen het gebouw.
- Vergeet niet om na het kopiëren, faxen of scannen het origineel mee te nemen.
- Vind je een print, retourneer deze aan de eigenaar, manager of gooi hem in de blauwe container.
- Zie je onbekenden onbegeleid in het kantoorgebied lopen, vraag dan even of je ze kunt helpen.
- Ontvang je gasten? Meld ze aan bij de receptie. Ontvang ze zelf bij de receptie en wandel na afloop nog even met ze mee. Lukt het niet om je gast zelf op te halen? Vraag een collega.

Buiten het gebouw

- Bewaar je werkgerelateerde documenten of laptop niet achter in je auto.
- Laat je smartphone/tablet/laptop nooit onbeheerd achter.

- Beveilig je smartphone/tablet/laptop/USB-stick met een pincode.
- Let op wat je waar/wanneer aan wie vertelt, ben je bewust van ‘meekijkers’ en ‘meeluisteraars.’
- Gooi werkgerelateerde documenten niet thuis weg bij het afval, maar op je werk in de blauwe container.
- Gebruik geen onbeveiligd wifi-netwerk (b.v. in een café) om werk gerelateerde documenten te verzenden en ontvangen.
- Laat je druppel niet rondslingeren.

  Heb je vragen over veilig werken? Stel ze gerust!

  Martin Moritz en Erika Neumann

Bijlage III. Prestatie-indicatoren

Bijlage I

Tabel uitwerking prestatie-indicatoren

Indicator	**Doel**	**Hoe te meten**	**Verantwoordelijke uitvoering meting**
Informatieveiligheids-afspraken met externe ICT-partners zijn gemaakt en vastgelegd	- Verkleinen van risico's op data-lekken. - Checken of externe ICT-partners aan informatieveiligheids-eisen voldoen.	- Aantal datalekken waarbij oorzaak bij externe ICT-leverancier en -dienstverlener ligt. - SLA's/contracten controleren. - Informeren en afspraken maken.	Adviseurs informatieveiligheid
Cliënt- en personeels-systemen voldoen aan veiligheidseisen	- Verkleinen van risico's op data-lekken. - Checken of gebruikte systemen afdoende beveiligd zijn.	- Aantal datalekken of informatieveiligheid-incidenten die betrekking hebben op de systemen. - Actueel overzicht van systemen en gebruikers. - Autorisatie geregeld? - Authenticatie geregeld? - Functiescheiding geregeld?	Adviseurs informatieveiligheid

Bijlage IV. Schematische weergave gevoerde gesprekken

Systeem	Welke (persoons) gegevens	Doel geformuleerd door mede-werker (artikel 7 Wbp)	Grond (artikel 8 Wbp)	Autorisatie	Delen gegevens	Bewaartermijn/vernietigen	inzagerecht
Kidos	NAW, Contactgegevens, BSN, geboortedatum, sociaal-medische gegevens, woon-gezinsituatie, mediche gegevens	Dat er altijd met de juiste gegevens wordt verwerkt	Op consultatiebureau wordt toestemming gevraagd. Het is niet duidelijk waarvoor specifiek toestemming wordt gevraagd aan de ouders. Toestemming aan kinderarts tijdens consult of het verwerken van toestemmings-vraag in gesprek met zorgteam	Alle medewerkers die toegang hebben tot Kidos kunnen bij de zelfde informatie. Niet iedereen kan evenveel aanpassen. Daarvoor heb je specifieke autorisatie nodig.	Intern worden gegevens betreffende de gezondheid gedeeld binnen het team. Voor extern delen wordt mondeling toestemming gevraagd aan de betrokkene.	Bewaartermijn is volgens de KNMG richtlijn. Op dit moment worden er geen gegevens vernietigd na die termijn.	Betrokkene kan verzoeken het dossier in te zien of een uitdraai van het dossier te krijgen.
HP Zone	Bij binnenkomende telefoontjes enkel naam, postcode en soms telefoonnummer Melders m.b.t. infectieziekten zijn soms meldingsplichtig. Dan naam, geboortedatum, BSN en de infectieziekte Meldingen van	Niet geformuleerd	Wet publieke gezondheid. (wettelijke plicht, artikel 8 grond c)	2 artsen + functioneel beheerder hebben toegang tot alle gegevens. Verder is er per persoon/functie een aparte autorisatie. Medewerkers kunnen dus enkel bij de nodige	Onderling tussen artsen bij gezamenlijke behandelrelatie. Soms huisarts, maar dan moet er toestemming zijn van de cliënt.	Onduidelijk. 10 of 15 jaar. Op dit moment wordt alles bewaard. Een casus kan worden gesloten. Dan komt de casus niet meer actief in beeld, maar nooit vernietigd.	Nog nooit voorgekomen.

	scholen/kinderdagverblijven, enkel de aandoening, niet identificeerbaar, dus geen persoonsgegevens. Lab uitslagen worden opgeslagen in dit systeem. Komt binnen via zorgmail.			gegevens.		Conclusie: geen bewaartermijn	
Orion Globe	Digitaal: BSN, NAW, telefoonnummer, naam, geboortedatum, nationaliteit, contactgegevens en geslacht. Papier: Gegevens betreffende de gezondheid. Er wordt gewerkt aan digitalisering van dit systeem.	Zo gezond mogelijk op reis en weer terug laten komen van klanten. Zo goed mogelijk advies geven.	Als wordt ingestemd met behandelplan gaan zij uit van instemmen met verwerken van persoonsgegevens. Soms wordt verwezen naar de website over informatieveiligheid.	3 personen met gehele toestemming. Beheerders van het systeem. Verder autorisatie per persoon geregeld.	Delen enkel met cliënt of intern via inloggen. Lastig punt is wanneer cliënt in buitenland zit en zijn vaccinatieboekje kwijt is. Dan is opsturen per post geen optie.	Alles wordt bewaard.	Niets over geregeld. Staat op de agenda. waarschijnlijk kunnen cliënten straks inloggen en eigen vaccinatieboekje zien.
Orion Forensisch	NAW, medische gegevens, BSN, geboortedatum, geslacht, nationaliteit.	Patiënten zo goed mogelijk kunnen helpen	Wettelijke grondslag	Iedereen met autorisatie kan in het systeem en kan bij alle gegevens.	Medicijngebruik wordt gedeeld met politie middels overdrachts-formulier. Intern casuïstiek-bespreking, dit gebeurt anoniem.	Papieren dossiers worden na 15 jaar vernietigd. Digitaal is hierover nog niets geregeld.	Aanvraagformulier. De betrokkene kan dan aanvinken of inzage of een kopie gewenst is.

Topdesk KCC	Bij binnenkomend telefoongesprek: Naam en e-mailadres. Binnenkomende e-mails worden opgeslagen. In deze mails staan vaak (bijzondere)persoons-gegevens. Patiëntgegevens worden opgeslagen in het kind dossier bijvoorbeeld.	Het in beeld houden van meldingen. Worden ze juist behandeld en doorgezet?	Mensen sturen de gegevens zelf. Er wordt dus van de toestemming uitgegaan.	Front-office mensen hebben toegang tot alle gegevens die in het systeem zitten. Zij hebben hier een autorisatie voor gekregen. Bij afdeling reizigers op KCC wordt op elkaars accounts gewerkt. Zij zien NAW gegevens, afspraken en de reis van cliënt.	Intern worden de binnenkomende gegevens doorgezet naar de juiste afdelingen/ systemen. Extern verwijzen ze bij twijfel door naar het consultatiebureau. Bij dossiers met geheime adressen altijd naar consultatiebureau.	Voor de digitale systemen is nog geen bewaartermijn vastgesteld.	Cliënten kunnen een formulier invullen dat heet “aanvraag persoonsgegevens” Hierop kunnen zij aanvinken welke gegevens zij willen ontvangen. Ze kunnen het volledige medische dossier opvragen.
Tubis	NAW gegevens, verzekeringsgegevens, huisartsonderzoek, patiëntendossier met daarin medische gegevens.	Waarborgen van de gezondheid	Niet bekend. Er wordt geen toestemming gevraagd.	Autorisatie middels gebruikersnaam en wachtwoord. Iedereen met autorisatie kan bij alle gegevens, maar dat moet ook zo zijn volgens medewerker	Extern wordt in principe niets gedeeld. Dit kan wel op verzoek van cliënt, bijvoorbeeld naar huisarts. Voor het COA worden screenings gedaan bij asielzoekers.	Volgens een richtlijn. Onlangs de papieren dossiers nog gesaneerd. Digitaal wordt er niets verwijderd. Er is geen optie om op grotere schaal dossiers te verwijderen en geen tijd om dit individueel	Hier zijn richtlijnen voor. Bij de balie ligt een folder. Mensen kunnen dat daar zien.

						te doen.	

Bijlage V. Gevoerde gesprekken

Bijlage III Gevoerde gesprekken

22 september, HP Zone, Angelique Theuws.

1. *Welke persoonsgegevens worden er verwerkt op deze afdeling en in dit systeem?*

In dit systeem worden telefoongesprekken verwerkt van mensen die bellen met vragen. Dan vragen ze alleen postcode en naam, soms telefoonnummer. Ze zetten een melding in. Mensen met bepaalde infectieziekte zijn soms meldingsplichtig, naam, geboortedatum, bsn nummer ; infectieziekte worden genoteerd

Dan heb je nog meldingen van kinderdagverblijven en scholen etc. die melden meerder meldingen van huiduitslag. Dan alleen gegevens van de melder. Niet van de personen die de aandoening hebben.

De labuitslagen krijgen ze of vanuit ziekenhuis of vanaf huisartslaboratorium via zorgmail. Die gegevens opgeslagen in HP Zone.

2. *Wat is het doel waarvoor de gegevens worden opgeslagen? 7Wbp*

Dat ligt in de wet publieke gezondheid. Die gegevens moeten gemeld worden aan ons. Ook verplicht om de gegevens te noteren. Daar waar alleen vragen gesteld worden door mensen hoeven ze niet perse dingen te noteren. Ze vragen dan postcode, hoeft niet, het mag ook anoniem als mensen dat niet fijn vinden.

3. *Wat is de grond waarop jullie gegevens verwerken? 8 Wbp, wordt er bijvoorbeeld toestemming gevraagd?*

Wettelijke grondslag uit wet publieke gezondheid.

4. *Hoe beschermen jullie en/of het systeem de verwerkte gegevens?*

Iedere persoon die toegang krijgt tot het systeem wordt geautoriseerd door een van de artsen die beheerder is. Iedereen heeft individueel wachtwoord.

5. *Wie heeft er toegang tot de verwerkte gegevens?*

Zie volgende vraag

6. *Wie hoort er toegang te hebben tot de verwerkte gegevens?*

Administratieve krachten mogen wel gegevens invoeren maar kunnen een heleboel dingen niet zien die artsen en verpleegkundigen wel kunnen zien. 2 artsen en zij hebben toegang als soort van beheerder dus kunnen overal bij.

7. *Komen alle gegevens van een persoon direct naar boven bij het zoeken naar persoonsgegevens, of alleen het noodzakelijke?*

Als je zoekfunctie ‘naam’ gebruikt moet je de juiste aanklikken en daar krijg je de juiste gegevens van. Ze ontmoedigen om niet op naam te zoeken, maar op bsn of geboortedatum.

8. *Delen jullie (bijzondere) persoonsgegevens?*
   zo ja, Met wie?
   Hebben jullie intern afspraken over het al dan niet delen van deze informatie?

Medische gegevens. Artsen hebben soms gezamenlijke behandelrelatie dan kun je makkelijker gegevens delen. Maar als je melding krijgt van huisarts vragen ze of er toestemming is van patiënt om gegevens te delen.

9. *Hebben jullie in beeld wanneer sprake is van een datalek en waar meld je dat in zo’n situatie?*

Omdat het een online systeem is hoeven er geen gegevens op draagbare gegevensdrager. Als er sprake zou zijn van een datalek dat opgemerkt wordt. Dan zouden ze het bij ICA melden.

10. *Zien jullie zelf risico's in de manier waarop nu persoonsgegevens worden verwerkt?*

Zijn allemaal redelijk bewust dat ze daar zorgvuldig mee omgaan, dus niet echt.

11. *Hoelang worden gegevens bewaard, en is hier ook een reden voor?*

Veel twijfel over. 10 of 15 jaar en wat betekent dit voor dossiers? En welke gegevens wel en welke niet. Op dit moment wordt alles bewaard. Je kunt een casus sluiten zodat hij niet meer actief in beeld komt maar hij is nog wel op te roepen.

12. *Is er ook iets afgesproken over de manier en het tijdstip van vernietiging van de gegevens?*

Nee

13. *Hebben jullie procedures als het gaat om het inzagerecht van betrokkene?*

Is nog nooit gebeurd. Mensen kunnen die vraag stellen. Ze proberen het altijd zo te doen dat mensen het zelf ook begrijpen.

14. *Worden er alleen gegevens van klant opgeslagen of ook van bijvoorbeeld familie? Is dit dan ook daadwerkelijk nodig?*

Vaak ook gegevens van anderen zoals de melder.

13 september 2016, Orion Globe, Annemarie de Gouw

1. *Welke persoonsgegevens worden er verwerkt op deze afdeling en in dit systeem?*

Digitaal worden BSN, NAW, telefoonnummer, naam, geboortedatum, nationaliteit, contactgegevens en geslacht verwerkt.
In papieren dossiers worden gegevens betreffende de gezondheid verwerkt. Er wordt gewerkt aan digitalisering van dit systeem.

2. *Wat is het doel waarvoor de gegevens worden opgeslagen? 7Wbp*

Het doel van het opslaan van de gegevens is het zo gezond mogelijk op reis en weer terug laten komen van klanten. Zo goed mogelijk advies geven.

3. *Wat is de grond waarop jullie gegevens verwerken? 8 Wbp, wordt er bijvoorbeeld toestemming gevraagd?*

Er wordt geen expliciete toestemming gevraagd voor het verwerken van de persoonsgegevens. Er wordt vanuit gegaan dat als men instemt met het behandelplan, men ook instemt met de verwerking van persoonsgegevens. Soms wordt er verwezen naar de website waarop staat hoe wordt omgegaan met informatieveiligheid.

4. *Hoe beschermen jullie en/of het systeem de verwerkte gegevens?*

De verwerkte gegevens worden beschermd door het systeem, omdat er toestemming moet zijn om in bepaalde gegevens te kunnen. Er zijn op heel de afdeling 3 personen die in alle gegevens kunnen, dat is mevrouw De Gouw zelf, applicatiebeheerder en de vervanger. In het systeem kan worden aangevinkt wie er bij welke gegevens van de klant kan.

5. *Wie heeft er toegang tot de verwerkte gegevens?*

Zie vraag hierboven.

6. *Wie hoort er toegang te hebben tot de verwerkte gegevens?*

De personen die nu toegang hebben behoren volgens mevrouw De Gouw ook toestemming te hebben. Zij kunnen dit flexibel veranderen. Er hoeft niet meer te gebeuren dan de autorisatie voor een bepaald account intrekken om te voorkomen dat iemand toegang heeft tot gegevens waartoe zij geen toegang behoorde te hebben.

7. *Komen alle gegevens van een persoon direct naar boven bij het zoeken naar persoonsgegevens, of alleen het noodzakelijke?*

Alleen de noodzakelijke. Je kunt zoeken op geboortedatum, BSN nummer, naam. Als je hierop zoekt moet je nog het balkje aanklikken om in het dossier van de gezochte persoon te komen. je komt dus niet zomaar het hele dossier tegen als je aan het zoeken bent. Bovendien moet je geautoriseerd zijn om in een dossier te kunnen. Medische gegevens (staan dus ook digitaal) vormen weer een categorie apart, waardoor je hier zeker niet zomaar bij kunt komen.

8. *Delen jullie (bijzondere) persoonsgegevens?*
   zo ja, Met wie?
   Hebben jullie intern afspraken over het al dan niet delen van deze informatie?

Extern worden er geen gegevens gedeeld, alleen intern door in te loggen. Wel is het soms lastig als een klant in het buitenland zit en bijvoorbeeld zijn vaccinatieboekje kwijt is. Het versturen per post is dan niet mogelijk. Het is dan erg aantrekkelijk om een print screen te maken en deze per mail te versturen, maar dit doen ze niet. Dit wordt wel als een lastig punt ervaren.

9. *Hebben jullie in beeld wanneer sprake is van een datalek en waar meld je dat in zo'n situatie?*

Nee. Niet in beeld wanneer precies sprake is van een datalek en ook niet op de hoogte waar dit gemeld moet worden of wat voor protocol er gevolgd moet worden.

10. *Zien jullie zelf risico's in de manier waarop nu persoonsgegevens worden verwerkt?*

Alles blijft intern. Het is wel aantrekkelijk om info te sturen aan de persoon die daarom vraagt. Willen ze per post gaan doen. Het gaat hierbij om de persoon van wie het dossier is.

11. *Hoelang worden gegevens bewaard, en is hier ook een reden voor?*

Gegevens worden in principe niet verwijderd. Er is geen termijn om gegevens te bewaren. Op dit moment zitten gegevens vanaf 2001 in het systeem, omdat er toen sprake is geweest van digitalisering.

12. *Is er ook iets afgesproken over de manier en het tijdstip van vernietiging van de gegevens?*

In principe blijven gegevens bewaard. Dit is nodig voor het voortschrijdend inzicht. Als vaccinaties verlopen zijn worden ze wel verwijderd uit het systeem.

13. *Hebben jullie procedures als het gaat om het inzagerecht van betrokkene?*

Die zijn ze aan het opstellen. Staat voor de volgende vergadering op de agenda. Ze willen dit per post gaan doen als klanten om eigen gegevens vragen. Het gaat hierbij bijna altijd om het vaccinatieboekje dat opgevraagd wordt door klanten. In een systeem dat ze waarschijnlijk gaan gebruiken gaat het mogelijk zijn om een digitaal vaccinatieboekje te maken. De klant kan op deze gegevens inloggen en kan dan bij zijn eigen vaccinatieboekje.

14. *Worden er alleen gegevens van klant opgeslagen of ook van bijvoorbeeld familie? Is dit dan ook daadwerkelijk nodig?*

Alleen gegevens van klant. Als je bijvoorbeeld belt, worden wel je gegevens ook genoteerd.

21 september 2016, Kidos, Aukje Westhof

1. *Welke persoonsgegevens worden er verwerkt op deze afdeling en in dit systeem?*

Basisregistratie persoonsgegevens. NAW gegevens via gemeente, bsn en gba nummers. Overlijden, geboren etc. worden doorgegeven via een automatische koppeling met de gemeente. Gemeente transporteert naar kidos, dus ook wie de ouders zijn bijvoorbeeld.

2. *Wat is het doel waarvoor de gegevens worden verwerkt? 7Wbp*

Het doel van het verwerken van de gegevens is dat er altijd met de juiste gegevens wordt gewerkt .

3. *Wat is de grond waarop jullie gegevens verwerken? 8 Wbp, wordt er bijvoorbeeld toestemming gevraagd?*

Ouders gaan naar consultatiebureau. Daar wordt aan de ouders om toestemming gevraagd voor het doorsturen en verwerken van gegevens.

4. *Hoe beschermen jullie en/of het systeem de verwerkte gegevens?*

Dit is middels authenticatie. Er wordt een gebruikersnaam, wachtwoord en verificatiecode gevraagd. Het is niet toegestaan om op elkaars accounts te werken. Hier wordt op gehamerd, maar ze zijn er niet zeker van dat dit op alle onderdelen ook daadwerkelijk gebeurt. Vooral bij kcc zijn ze hiervoor bang.

5. *Wie heeft er toegang tot de verwerkte gegevens?*

Iedereen kan bij de zelfde informatie komen. Niet iedereen kan evenveel aanpassen, daarvoor moet je een autorisatie hebben. Maar iedereen met een autorisatie voor kidos kan bij alle gegevens.

6. *Wie hoort er toegang te hebben tot de verwerkte gegevens?*

Dit zou meer gespecificeerd moeten en kunnen worden. Nu kan iedereen bij de gegevens en dat is niet nodig. Er zijn mensen die hier niet bij zouden hoeven kunnen komen. Hier wordt op dit moment landelijk naar gekeken.

7. *Komen alle gegevens van een persoon direct naar boven bij het zoeken naar persoonsgegevens, of alleen het noodzakelijke?*

Alleen NAW-gegevens en de gekoppelde GGD. Er is alleen toegang tot de gegevens bij de eigen GGD. Dat gaat dus om de GGD die gekoppeld is aan het dossier.

8. *Delen jullie (bijzondere) persoonsgegevens?*
   zo ja, Met wie?
   Hebben jullie intern afspraken over het al dan niet delen van deze informatie?

Ja, medische gegevens, gegevens betreffende de gezondheid. Deze worden intern gedeeld binnen het team. Voor het extern delen van bijzondere persoonsgegevens wordt de uitdrukkelijke toestemming gevraagd van de betrokkene. Dit wordt mondeling afgesproken. Er wordt hierover dus niets schriftelijk vastgelegd.

9. *Hebben jullie in beeld wanneer sprake is van een datalek en waar meld je dat in zo'n situatie?*

Men heeft er geen idee van wanneer sprake is van een datalek. Als ze het zouden constateren zouden ze naar servicedesk ICA gaan.

10. *Zien jullie zelf risico's in de manier waarop nu persoonsgegevens worden verwerkt?*

Alles is controleerbaar. Om die reden zien zij nu geen risico's in de verwerkig van persoonsgegevens. Er is terug te zien wie op welk moment welk dossier heeft geraadpleegd.

11. *Hoelang worden gegevens bewaard, en is hier ook een reden voor?*

Gegevens worden heel lang bewaard. Hierover moet ik vragen stellen aan Simone Klok of Elise Buiting.

12. *Is er ook iets afgesproken over de manier en het tijdstip van vernietiging van de gegevens?*

Er wordt niks verwijderd. Soms worden dingen gearchiveerd. Maar het is een wettelijke plicht om alle dossiers te bewaren.

13. *Hebben jullie procedures als het gaat om het inzagerecht van betrokkene?*

Ja, er wordt een afspraak gemaakt met de betrokkene. Die kan dan het dossier inzien en eventueel een uitdraai van het dossier meekrijgen.

14. *Worden er alleen gegevens van klant opgeslagen of ook van bijvoorbeeld familie? Is dit dan ook daadwerkelijk nodig?*

Als het te maken heeft met de gezondheid van het kind worden ook gegevens van andere, zoals bijvoorbeeld de biologische ouders verwerkt. Het gaat daarbij dan om gegevens betreffende de gezondheid van de ouder(s).

11 ktober 2016, Kidos, Elise Buiting

1. *Hoelang worden gegevens bewaard, en is hier ook een reden voor?*

Bewaartermijnen zijn volgens de KNMG richtlijn. Er wordt op dit moment niets vernietigd, enkel gearchiveerd.

2. *Wie hoort er toegang te hebben tot de verwerkte gegevens?*

De autorisatie zou strikter geregeld kunnen worden. Artsen hebben toegang tot alle dossiers, ook die van patiënten van andere artsen. De functioneel beheerder heeft ook toegang tot alle gegevens.

20 september 2016, Topdesk KCC, Lianne de Rooij.

1. *Welke persoonsgegevens worden er verwerkt op deze afdeling en in dit systeem?*

Als iemand belt slaan ze summiere informatie op. Er wordt dan de naam en het e-mailadres genoteerd van een persoon. E-mails die binnen komen via de website worden opgeslagen. Deze worden opgeslagen op naam en e-mailadres. De informatie die in de mails staat bevat vaak ook persoonsgegevens, waaronder vaak bijzondere persoonsgegevens. Het gaat dan om kinderen die ziek worden oid. Deze mails worden in zijn geheel opgeslagen in het systeem.

2. *Wat is het doel waarvoor de gegevens worden opgeslagen? 7Wbp*

Het doel van het opslaan van de gegevens is het in beeld houden van de meldingen, worden ze juist doorgezet en behandeld?

3. *Wat is de grond waarop jullie gegevens verwerken? 8 Wbp, wordt er bijvoorbeeld toestemming gevraagd?*

Er wordt geen toestemming gevraagd voor het opslaan van persoonsgegevens. Mensen sturen deze zelf dus gaan ze er vanuit dat mensen ermee akkoord gaan dat deze persoonsgegevens worden verwerkt. Als het om specifieke patiëntgegevens gaat worden ze bijvoorbeeld verwerkt in het kinddossier.

4. *Hoe beschermen jullie en/of het systeem de verwerkte gegevens?*

Mensen moeten toestemming hebben om in het systeem te kunnen. Die toestemming moeten zij krijgen van Lianne de Rooij, zij moet deze personen dan machtigen om bij deze gegevens te kunnen.

5. *Wie heeft er toegang tot de verwerkte gegevens?*

Front office mensen kunnen bij alle vragen komen en dus ook alle gegevens die daar in zitten. Zij hebben de rechten gekregen om deze gegevens te verwerken en sturen ze door naar de juiste persoon.

6. *Wie hoort er toegang te hebben tot de verwerkte gegevens?*

Zoals het nu geregeld is hebben de juiste mensen toegang tot de verschillende gegevens volgens de beheerder.

7. *Komen alle gegevens van een persoon direct naar boven bij het zoeken naar persoonsgegevens, of alleen het noodzakelijke?*

Naam en e-mail komen direct naar boven. Verder moet er geklikt worden op het document om de inhoud van de mail en dus eventueel verdere persoonsgegevens naar boven te halen. Er komt dus geen onnodige informatie naar boven op het moment dat je zoekt naar een persoon.

8. *Delen jullie (bijzondere) persoonsgegevens?*

zo ja, Met wie?

Hebben jullie intern afspraken over het al dan niet delen van deze informatie?

Ja, soms is er sprake van gegevens betreffende de gezondheid. In dat geval kunnen in de eerste plaats de front office medewerkers erbij. Zij zorgen dat de gegevens terecht komen bij de juiste arts of verpleegkundige. Daarmee worden de gegevens dus in de eerste plaats gedeeld, maar dit is intern. Extern worden gegevens gedeeld met het consultatiebureau. Hiervoor werd ik doorverwezen naar Elleke Suijk. Zij zou mij inhoudelijk meer kunnen vertellen.

9. *Hebben jullie in beeld wanneer sprake is van een datalek en waar meld je dat in zo'n situatie?*

Binnen KCC ICA is hier beleid over gemaakt. Zij weten wanneer sprake is van een datalek en hoe hierop te reageren. Of dit binnen KCC ook het geval is, is niet duidelijk. Ook hierover kan ik Elleke beter vragen stellen.

10. *Zien jullie zelf risico's in de manier waarop nu persoonsgegevens worden verwerkt?*

Nee, op dit moment is het volgens de functioneel beheerder goed geregeld.

11. *Hoelang worden gegevens bewaard, en is hier ook een reden voor?*

Gegevens worden nooit verwijderd. Hier is op dit moment geen reden voor.

12. *Is er ook iets afgesproken over de manier en het tijdstip van vernietiging van de gegevens?*

Nee, er is contact geweest met de beheerder van het systeem. Er is op dit moment geen mogelijkheid om gegevens te verwijderen of te archiveren. Mevrouw De Rooij gaf aan hier achter aan te gaan en contact op te nemen met haar manager.

13. *Hebben jullie procedures als het gaat om het inzagerecht van betrokkene?*

Nee. Bij het KCC gaat het dan ook steeds om gegevens die patiënten zelf per mail of telefoon overdragen aan de GGD.

14. *Worden er alleen gegevens van klant opgeslagen of ook van bijvoorbeeld familie? Is dit dan ook daadwerkelijk nodig?*

De gegevens die worden opgeslagen zijn de gegevens die in de mails staan. Als daarin gegevens over familie staan worden die dus ook opgeslagen. Dit is nodig om de klant te helpen met zijn vraag. Er kan op dit moment niet geselecteerd worden welke gegevens wel en welke niet worden opgeslagen.

18 oktober 2016, Topdesk KCC, Elleke de Suijk

4. Hoe beschermen jullie en/of het systeem de verwerkte gegevens?

In principe worden geen gegevens doorgegeven. Ze controleren altijd de telefoonnummers zoals dat bij hen bekend is. Als ze het niet vertrouwen verwijzen ze mensen door naar het consultatiebureau. Zij hebben vaak beter in beeld hoe een gezin in elkaar zit. Op dat moment wordt er dus geen enkel informatie verstrekt, niet over adresgegevens, niet over afspraken etc. Er zijn ook dossiers waarin geheime adressen staan. In zo'n geval verwijzen ze direct door naar het consultatiebureau en doen ze zelf geen inhoudelijke uitspraken.

5. Wie heeft er toegang tot de verwerkte gegevens?

Op elkaars accounts werken gebeurt nog bij Reizigers. In principe kunnen de klantcontact medewerkers dan enkel in de afspraak systemen. Ze kunnen dan de NAW-gegevens, afspraken en welke reis er gemaakt wordt zien. Ze kunnen niet zien welke vaccinaties zijn gegeven. Dit is vooral in theorie zo, want in praktijk kun je dit wel zien door facturen die in de dossiers komen.

8. Delen jullie (bijzondere) persoonsgegevens?
zo ja, Met wie?
Hebben jullie intern afspraken over het al dan niet delen van deze informatie?

Aan artsen de groeigegevens, maar bijna altijd op verzoek van de ouders. Ouders kunnen zelf ook bij deze gegevens. Ze kunnen bij het volledige patiëntendossier via "mijn kind in beeld". Daarnaast worden gegevens gedeeld met het consultatiebureau.

9. Hebben jullie in beeld wanneer sprake is van een datalek en waar meld je dat in zo'n situatie?

Nee

10. Zien jullie zelf risico's in de manier waarop nu persoonsgegevens worden verwerkt?

Nee, zolang iedereen doet wat hij moet doen niet. Hierbij wordt wel erkend dat sommige mensen onzorgvuldig omgaan met het vergrendelen van schermen als ze vertrekken.

13. Hebben jullie procedures als het gaat om het inzagerecht van betrokkene?

Via internet kunnen klanten een formulier invullen dat heet "aanvraag persoonsgegevens". Hierop kunnen zij invullen welke gegevens ze willen ontvangen. Ze kunnen het volledige medische dossier opvragen.

17 oktober 2016, Tubis, Ton Froklage

Tubis is een landelijke database van de GGD voor TBC. Tubis wordt volgend jaar vervangen door een nieuw systeem. In principe ziet de medewerker van de GGD de gegevens van eigen klanten, maar je kunt ook de gegevens van klanten van andere GGD's opvragen. Daarnaast kun je een dossier tijdelijk overnemen waardoor je er toegang toe hebt. Het is dan niet de bedoeling dat je wijzigingen aanbrengt.

Klanten die voor 2011 voor het eerst zijn geweest zijn geïnformeerd over de verwerking van persoonsgegevens. Voor de klanten van na 2011 wordt geen toestemming meer gevraagd. Klanten zijn geïnformeerd middels plaatjes en folders. Als ze geen onderdeel willen zijn van de landelijke database kunnen ze dit aangeven en wordt het dossier geheim gemaakt.

1. *Welke persoonsgegevens worden er verwerkt op deze afdeling en in dit systeem?*

Naw- gegevens, Verzekeringsgegevens, huisartsonderzoek, patiëntendossier met daarin medische gegevens.

2. *Wat is het doel waarvoor de gegevens worden opgeslagen? 7Wbp*

Gezondheid

3. *Wat is de grond waarop jullie gegevens verwerken? 8 Wbp, wordt er bijvoorbeeld toestemming gevraagd?*

-

4. *Hoe beschermen jullie en/of het systeem de verwerkte gegevens?*

Inloggen met ww+gebruikersnaam

5. *Wie heeft er toegang tot de verwerkte gegevens?*

Artsen, verpleegkundige en medisch technisch personeel

6. *Wie hoort er toegang te hebben tot de verwerkte gegevens?*

Beter afschermen dan dit is voor de praktijk niet mogelijk. Iedereen moet bij alle gegevens van de patiënt kunnen.

7. *Komen alle gegevens van een persoon direct naar boven bij het zoeken naar persoonsgegevens, of alleen het noodzakelijke?*

Alleen het noodzakelijke.

8. *Delen jullie (bijzondere) persoonsgegevens?*

zo ja, Met wie?

Hebben jullie intern afspraken over het al dan niet delen van deze informatie?

In principe niet, maar wel naar cliënt of bijvoorbeeld naar huisartsen op verzoek van de cliënt. En er worden screenings gedaan voor het GCA (COA) bij asielzoekers. Daarnaast gaan er brieven naar huisartsen.

9. *Hebben jullie in beeld wanneer sprake is van een datalek en waar meld je dat in zo'n situatie?*

Nee. Hij is van mening dat er geen sprake kan zijn van een datalek, omdat het allemaal goed is geregeld. Er is dus ook geen duidelijkheid over hoe te handelen in geval van een datalek.

10. *Zien jullie zelf risico's in de manier waarop nu persoonsgegevens worden verwerkt?*

Nee. En in april komt er een nieuw programma.

11. *Hoelang worden gegevens bewaard, en is hier ook een reden voor?*

Ze hanteren de bewaartermijn van een richtlijn. Papieren dossiers zijn onlangs nog gesaneerd. Nu wordt alles bewaard, want dat is digitaal. Er is in dit systeem geen optie om meerdere dossiers tegelijk te verwijderen. Er is geen tijd en mankracht om de dossier handmatig en een voor een te verwijderen. Wellicht dat er in het nieuwe systeem wel een optie voor is, maar op dit moment wordt alles dus gewoon bewaard.

12. *Is er ook iets afgesproken over de manier en het tijdstip van vernietiging van de gegevens?*

Digitaal niet.

13. *Hebben jullie procedures als het gaat om het inzagerecht van betrokkene?*

Ja daar hebben ze richtlijnen voor. Bij de balie ligt er ook een folder over zodat mensen die in kunnen zien.

14. *Worden er alleen gegevens van klant opgeslagen of ook van bijvoorbeeld familie? Is dit dan ook daadwerkelijk nodig?*

Alleen van klant.

(Er is een bewerkersovereenkomst)

28 september 2016, Orion forensisch, Willeke Vanhooren,

Dienstverlening in opdracht van gemeente en politie. Verplichte DNA onderzoeken in de politiecel. Het zijn onafhankelijke artsen en zij zijn vraagbaken voor individuele (huis)artsen. Ze zijn 24/7 beschikbaar. Er hebben dus altijd artsen dienst.

1. *Welke persoonsgegevens worden er verwerkt op deze afdeling en in dit systeem?*

NAW-gegevens worden opgeslagen. Daarnaast hebben ze een medisch dossier van patiënten. Dit dossier stellen zij zelf op. Ze hebben dus geen toegang tot patiënt gegevens van buiten de GGD

2. *Wat is het doel waarvoor de gegevens worden opgeslagen? 7Wbp*

Patiënten zo goed mogelijk kunnen helpen.

3. *Wat is de grond waarop jullie gegevens verwerken? 8 Wbp, wordt er bijvoorbeeld toestemming gevraagd?*

Er is een wettelijke grondslag op basis waarvan zij gegevens bewaren. De grond van de verwerking hangt hiermee samen.

4. *Hoe beschermen jullie en/of het systeem de verwerkte gegevens?*

Je kunt alleen in Orion forensisch door in te loggen met een inlognaam, wachtwoord en een verificatie middels sms bericht naar het telefoonnummer dat bij het systeem bekend is.

5. *Wie heeft er toegang tot de verwerkte gegevens?*

Iedereen die toegang heeft tot Orion Forensisch kan bij alle gegevens van alle personen.

6. *Wie hoort er toegang te hebben tot de verwerkte gegevens?*

Artsen moeten in alle dossiers kunnen, omdat ze elkaars adviezen moeten kunnen inzien. Ze werken in 24 uurs diensten en er wordt dus veel afgewisseld. Secretaresses moeten kunnen zoeken op naam en moeten het medicijn gebruik dat bekend is in het systeem kunnen raadplegen. Zij moeten dit gebruik door kunnen geven aan de politie, zodat de politie zorg kan dragen voor het tijdig geven van medicijnen aan personen in de cel. Secretaresses kunnen nu alles zien. Zij zouden bijvoorbeeld de verslagen van de artsen over de gezondheidstoestand van patiënten niet hoeven te zien. Dit zou dus scherper geregeld kunnen worden.

7. *Komen alle gegevens van een persoon direct naar boven bij het zoeken naar persoonsgegevens, of alleen het noodzakelijke?*

Alleen NAW-gegevens. Vervolgens moet je doorklikken naar het dossier om de rest van de gegevens van een persoon naar boven te halen.

8. *Delen jullie (bijzondere) persoonsgegevens?*

zo ja, Met wie?

Hebben jullie intern afspraken over het al dan niet delen van deze informatie?

Er wordt veel gewerkt met gegevens betreffende de gezondheid. Het medicijngebruik wordt gedeeld met derden, voornamelijk met de politie. Dit gebeurt middels een overdrachtsformulier. Politie zorgt dan voor tijdige medicatie voor de arrestanten. Intern worden de gegevens regelmatig gedeeld bij casuïstiekbespreking. Dit gebeurt anoniem. Hierbij valt dus niet te spreken over persoonsgegevens. Het is immers niet tot een persoon te herleiden.

9. *Hebben jullie in beeld wanneer sprake is van een datalek en waar meld je dat in zo'n situatie?*

Ze geeft hierbij aan dat er sprake is van een datalek wanneer bijvoorbeeld een externe arts zijn telefoon kwijt raakt. Ze zou dit dan melden bij de servicedesk.

10. *Zien jullie zelf risico's in de manier waarop nu persoonsgegevens worden verwerkt?*

Het duurt op dit moment erg lang voor artsen de dossiers afhandelen. Tot die tijd kan iedereen met toegang in dat dossier om dingen te wijzigen of zelfs te verwijderen. Dit zou anders moeten.
Co-assistenten hebben vaak geen VOG of geheimhoudingsverklaring hoeven tekenen, terwijl zij nog geen arts zijn (zitten nog in de masterfase van hun opleiding). Zij hebben beroepsmatig dus nog geen geheimhoudingsplicht en dit wordt vanuit de GGD ook niet altijd geregeld.
Wanneer nog meer sprake is van een datalek heeft ze niet zuiver. Zo geeft ze bijvoorbeeld aan dat ze zich kan voorstellen dat wanneer zij hun schermen niet vergrendelen, er ook sprake is van een datalek. Het gaat om zeer gevoelige informatie. Als je ingelogd staat kan iedereen in het gebouw bij die informatie.

11. *Hoelang worden gegevens bewaard, en is hier ook een reden voor?*

Ze hebben nog een papieren archief waarin gegevens 15 jaar worden bewaard. Het digitale systeem is nog jong. Daarover is nog niets geregeld, maar ze denkt dat dit ook 15 jaar zal zijn. Dit is ook wettelijk verplicht.

12. *Is er ook iets afgesproken over de manier en het tijdstip van vernietiging van de gegevens?*

Na die 15 jaar worden de gegevens vernietigd. De papieren dossiers worden in de daarvoor bestemde beveiligde container gedaan. Hoe ze dit digitaal gaan doen is nog niet bekend.

13. *Hebben jullie procedures als het gaat om het inzagerecht van betrokkene?*

Ja, hiervoor zijn aanvraagformulieren. De betrokkene kan dan aanvinken of er inzage of een kopie gewenst is. Hiertoe krijgt de betrokkene dan de mogelijkheid.

14. *Worden er alleen gegevens van klant opgeslagen of ook van bijvoorbeeld familie? Is dit dan ook daadwerkelijk nodig?*

In principe alleen gegevens van de betrokkene. Mocht het gaan om erfelijke ziektes van bijvoorbeeld de ouders, dan worden deze ook vastgelegd. Hierbij worden dan niet de gegevens van de ouders zelf vastgelegd.

Bijlage VI. Geheimhoudingsverklaring van de GGD

Hart voor Brabant

Gezondheid telt!

Verklaring geheimhouding

Bij deze beloof ik dat ik de gegevens, waarvan ik door of uit hoofde van mijn functie bij de GGD Hart voor Brabant kennis draag, en die mij als geheim zijn toevertrouwd, of waarvan ik het vertrouwelijk karakter moet begrijpen, niet zal openbaren of zal gebruiken voor een ander doel dan waarvoor ze mij ter kennis zijn gekomen tenzij ik daartoe beroepshalve verplicht ben.

Tot de gegevens die mij als geheim zijn toevertrouwd of waarvan ik het vertrouwelijk karakter moet begrijpen, behoren in ieder geval alle persoonlijke gegevens betreffende patiënten/cliënten van de GGD Hart voor Brabant.

Tevens beloof ik alles in het werk te stellen om de gegevens waarvoor ik verantwoordelijkheid draag, steeds ook bij afwezigheid voldoende te beschermen en veilig op te bergen.

Naam, voorletters : ……

Adres : ……

Postcode/woonplaats : ……

Functie/team : ……

Plaats ……Datum ……

Handtekening:

.....

Bijlage VII. Register verwerking persoonsgegevens

Hart voor Brabant

Gezondheid telt!

Register verwerking persoonsgegevens

De GGD moet een registratie bijhouden waarom hij (bijzondere) persoonsgegevens verzamelt (het doel), welke gegevens dat zijn en van wie en wie toegang heeft tot deze gegevens. In deze tabel kunt u lezen welke gegevens de GGD verzamelt.

Jeugdgezondheidszorg					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Bevorderen van de gezondheid en de ontwikkeling van de jeugdige. Adviseren partners en gemeenten bij hun beleid. Informeren en onder-steunen van onder-zoek en onderwijs.	Jeugdigen van 0-19 jaar en hun ouders	NAW-gegevens (NAW = naam, adres, woonplaats) Burgerservicenummer	Gezondheid Seksuele leven Ras	Medewerkers jeugd-gezondheidszorg Jeugdarts, jeugd-verpleegkundige, teamassistente en applicatiebeheerder: raadplegen, invoeren en muteren	--

Bemoeizorg (openbare geestelijke gezondheidszorg)					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Toeleiden van mensen naar de reguliere zorg	Individuele burgers	NAW-gegevens Sociaal-medische gegevens, waaronder de woon- en gezinssituatie Financiële gegevens (inkomen)	Gezondheid Strafrechtelijke gegevens	Medewerkers openbare geestelijke gezondheidszorg	De GGD wisselt alleen gegevens uit in overleg met de klant.
Mogelijkheid om nadere informatie over de patiënt te vragen	Melders van overlastsituaties	NAW-gegevens	Geen	Verpleegkundige: raadplegen, muteren en verwijderen.	Andere (behande-lende) instellingen, maar alleen in overleg met de betrokkene.

Infectieziektebestrijding					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Verwerken van meldingen van infectieziekten en registreren van vaccinaties	Patiënten	NAW-gegevens Burgerservicenummer Geboortedatum Nationaliteit Land van herkomst Gegevens uit bron- en contactonderzoeken Verzekeringsgegevens	Gezondheid Seksuele leven	Medewerkers infectie-ziektebestrijding Epidemioloog: raad-plegen Applicatiebeheerder: raadplegen, invoeren en muteren. Arts, verpleegkundige, gezondheidskundige, secretaresse: raad-plegen, muteren en verwijderen	Hulpverleners en derden, alleen na toestemming patiënt
	Mensen die in contact zijn gekomen met patiënten of een bron van besmetting	NAW-gegevens Burgerservicenummer Geboortedatum Nationaliteit Land van herkomst	Gezondheid		Hulpverleners en derden, alleen na toestemming klant
	Artsen Medische/veterinaire beroepsbeoefenaars	NAW-gegevens	Geen		Hulpverleners en derden, alleen na toestemming klant

Forensische geneeskunde					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Dossiervorming van de verrichtingen tijdens de forensische diensten	Overledene	NAW-gegevens Identificatiegegevens	Gezondheid	Forensische artsen en administratie	Ambtenaar burgerlijke stand Huisartsen, specialisten, alleen na toestemming.
	Patiënten	NAW-gegevens	Gezondheid		Huisartsen, specialisten, alleen na toestemming patiënt/overledene
	Hulpverleners	NAW-gegevens	Geen		Alleen na toestemming hulpverlener

Medische milieukunde					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Verzamelen van gegevens over het gevaar voor de (volks)gezondheid door milieuproblemen om zo advies te kunnen geven.	Individuele burgers	NAW-gegevens Telefoonnummer Emailadres	Gezondheid	Medewerkers medische milieukunde Andere GGD-medewerkers, als dit nodig is.	Andere instellingen, mits de betrokkene schriftelijk toestemming geeft.

Reizigerszorg					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Adviseren, begeleiden behandelen van reizigers	Reizigers	NAW-gegevens Reisgegevens	Gezondheid	Medewerkers reizigerszorg Verpleegkundigen en arts: raadplegen, invoeren en muteren Applicatiebeheerder: raadplegen, muteren en verwijderen	Huisarts, alleen na toestemming klant

Seksuele gezondheid					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Voorkomen en bestrijden van seksueel overdraag-bare aandoeningen (soa). Verzamelen van gegevens over voorkomen van soa Beantwoorden van vragen, geven van adviezen en behandelen.	Cliënten uit risicogroepen	Opleidingsniveau Geboorteland ouders Geboorteland Als cliënten akkoord gaan: NAW-gegevens	Seksuele leven	Medewerkers seksuele gezondheid Arts, verpleeg-kundige, assistent en applicatiebeheerder: raadplegen, muteren en verwijderen	--

Tuberculosebestrijding					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Opsporen, behandelen en bestrijden van tuberculose	Patiënten	NAW-gegevens Geboortedatum Geslacht Nationaliteit Behandelend arts	Gezondheid	Medewerkers tuber-culosebestrijding	Medewerkers andere GGD'en Huisartsen, medisch specialisten
	Personen die in contact kwamen met de patiënten	NAW-gegevens Geboortedatum Geslacht Nationaliteit Behandelend arts	Gezondheid		Medewerkers andere GGD'en Huisartsen, medisch specialisten
	Risicogroepen zoals GGD-medewerkers en verslaafden	NAW-gegevens Geboortedatum Geslacht Nationaliteit Behandelend arts	Gezondheid		Medewerkers andere GGD'en Huisartsen, medisch specialisten, arbo-artsen

Inspecties kinderopvang					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Uitvoeren inspecties kindercentra	Medewerkers kindercentra	Naam Diploma's Datum in dienst Datum Verklaring omtrent het gedrag	Geen	Inspecteurs en secretarieel medewerkers	Bij een calamiteit kan het zijn dat de GGD gegevens uitwisselt met DUO of de gemeente
	Gastouders, inwonende volwassen huisgenoten en eigen minderjarige kinderen die de gastouder in eigen huis verzorgt	NAW-gegevens Burgerservicenummer Geslacht Geboortedatum Datum (ontbinding) huwelijk of geregis-treerd partnerschap	Geen		Bij een calamiteit kan het zijn dat de GGD gegevens uitwisselt met DUO of de gemeente
	Kinderen die de gast-ouderbureaus bemiddelen	NAW-gegevens Burgerservicenummer	Geen		Bij een calamiteit kan het zijn dat de GGD gegevens uitwisselt met DUO of de gemeente

Centrum Jeugd & Gezin					
Het doel van de verwerking	**Van wie verwerkt de GGD gegevens?**	**Welke persoonsgegevens?**	**Bijzondere persoonsgegevens**	**Wie (van de GGD) werkt hiermee?**	**Aan wie verstrekt de GGD de persoons-gegevens?**
Uitvoeren trainingscentrum Jeugd en Gezin	Jeugdigen van 0-19 jaar en hun ouders	NAW-gegevens Reden van aanmelding voor een training.	Geen	Medewerkers CJG	Trainers van het trainingscentrum