# Checklist Privacy & Informatie-beveiliging eerstelijn Babyconnect

Voor aansluiting op het VIPP-programma **Babyconnect** dienen eerstelijns verloskundigenpraktijken en kraamzorgorganisaties zorgvuldig om te gaan met de persoonsgegevens van cliënten en hiervoor maatregelen te treffen. Onderstaande checklist bevat alle punten die als praktijk moeten worden geregeld voordat gegevensuitwisseling veilig kan plaatsvinden volgens de regionale contractenset.

## Algemeen geldende wet- en regelgeving

- Zorgverleners zijn wettelijk verplicht om gezondheidsgegevens van hun cliënten vast te leggen in een dossier. Dat is nodig voor een goede behandeling of verzorging. Cliënten kunnen dus niet altijd voorkomen dat hun gezondheidsgegevens worden opgenomen in een (medisch) dossier.
- De dossierplicht bij een geneeskundige behandeling staat in de Wet op de geneeskundige behandelingsovereenkomst (WGBO artikel 7:454 lid 1 BW). Omdat het wettelijk verplicht is om gezondheids-gegevens op te nemen in een dossier, hoeft de cliënt hiervoor geen toestemming te geven.
- In de Algemene verordening gegevensbescherming (AVG) staat dat zorgverleners maatregelen moeten nemen om gezondheids-gegevens goed te beveiligen (artikel 32 AVG). In de norm NEN 7510 staat hoe zorgverleners dat moeten doen. Voor verloskundigen is een toolkit beschikbaar die hen helpt de eerste stappen te zetten om te voldoen aan de NEN-normering.

## Checklist

We gaan ervan uit dat je als zorgverlener zorgvuldig omgaat met de persoonsgegevens van jouw cliënten en dat je hiervoor reeds maatregelen hebt getroffen. We willen daarnaast nog enkele punten benadrukken die belangrijk zijn om geregeld te hebben als praktijk, voordat veilige gegevensuitwisseling kan verlopen volgens de regionale contractenset voor gegevensuitwisseling in de geboortezorg.

Babyconnect

**Bij het tekenen van de regionale samenwerkingsovereenkomst, de DPIA* en de VWO** geef je als praktijk aan het volgende geregeld te hebben:**

1 Binnen de praktijk/organisatie is een procedure opgesteld met afspraken over het informeren over, en uitvragen van, toestemming van de cliënt:

- Is de cliënt goed geïnformeerd over de uitwisseling van diens gegevens?
- Wanneer wordt toestemming voor de uitwisseling gevraagd?
- Hoe en waar wordt de verkregen toestemming vastgelegd?

Wist je dat?

*Gebruik je een elektronisch uitwisselingssysteem zodat andere zorgverleners (buiten de praktijk of zorginstelling) gegevens van cliënten kunnen raadplegen? Dan mag je gegevens alleen uitwisselen via dit systeem als de cliënt hierover geïnformeerd is en hiervoor uitdrukkelijke toestemming heeft gegeven.*
*Er bestaan soms meerdere regionale elektronische uitwisselingssystemen voor zorgverleners om gegevens te delen. Daardoor kan het gebeuren dat een cliënt op meerdere plekken en van meerdere hulpverleners de vraag krijgt om toestemming te geven. Een landelijke toestemmingsvoorziening (MITZ) is hiervoor in de maak, deze is echter nog niet beschikbaar.*

2 De toegang van medewerkers is vastgelegd in een autorisatiebeleid waarin staat wie toegang/recht heeft tot het bekijken van een dossier.

Dit betekent dat je schriftelijk vastlegt welke rol verschillende medewerkers in jouw praktijk hebben en welke toegang zij hebben tot het cliëntendossier. Denk aan verloskundigen/kraamverzorgenden (in opleiding), waarnemers, assistenten, etc. Toegang vindt daarbij alléén plaats als er sprake is van betrokkenheid bij de behandeling van de cliënt.

3 Er wordt altijd ingelogd met 2 factor authenticatie in het bronsysteem.

Dit betekent dat er met twee manieren ingelogd moet worden, bijvoorbeeld een wachtwoord gevolgd door een sms of een wachtwoord met een Authenticator App. Nb: dit geldt enkel voor het bronsysteem. Bij HINQ kan vanuit het bronsysteem met ‘Single Sign On’ worden ingelogd.

Wist je dat?

*In eerste instantie is het dossier met gezondheidsgegevens van de cliënt toegankelijk voor de behandelend zorgverlener. Daarnaast kunnen andere zorgverleners toegang krijgen tot het dossier, als zij betrokken zijn bij de behandeling van deze cliënt. Zo kun je samenwerken met een assistent of een collega om advies vragen. Zorgverleners die toegang hebben tot het dossier, hebben een geheimhoudingsplicht. De medewerkers die toegang krijgen moeten echter wel betrokken zijn bij de behandeling van desbetreffende cliënt en de toegang moet noodzakelijk zijn voor hun werkzaamheden.*

**Data protection impact assessment, waarmee vooraf de privacy-risico's van een gegevensverwerking in kaart worden gebracht.*

*** Verwerkersovereenkomst, waarmee beide partijen (leverancier en zorgaanbieder) verklaren dat zij op de juiste wijze persoonsgegevens verwerken.*

4 Alle activiteiten binnen het bronsysteem en binnen de viewer worden geregistreerd via het persoonlijke account. Middels deze 'logging' worden de activiteiten van een gebruiker vastgelegd en zijn deze opvraagbaar.

Wist je dat?

*De zorgverlener heeft de plicht om deze logging files te controleren. Dit mag steekproefsgewijs gebeuren met een vaste frequentie. Een cliënt heeft een wettelijk recht om deze logging files op te vragen en zo te weten wie er in het dossier hebben gekeken.*

5 Zorg dat alle medewerkers *aantoonbaar* bekend zijn met het beleid en de procedures t.a.v. de omgang met cliëntgegevens:

- Bestaande medewerkers hebben de e-learnings*** gevolgd.
- Nieuwe medewerkers volgen de e-learnings.

Zorgverleners horen zich bewust te zijn van de risico's waar het gevoelige persoonsgegevens van cliënten betreft. Dit wordt ook wel privacy-bewustzijn genoemd. De AVG vereist van zorgverleners dat zij bekend zijn met deze regels en procedures. Met het voltooien van de e-learnings wordt dit bewustzijn gewaarborgd onder zorgverleners, waarbij thema's aan bod komen als:

- Hoe ga je als zorgverleners om met cliëntgegevens? O.a.: Vergrendel je scherm als je wegloopt en laat niet zomaar documenten slingeren maar berg deze op in een afsluitbare kast.
- Geef nooit zomaar cliëntgegevens door als er om wordt gevraagd zonder te verifiëren of de vrager hier recht op heeft en laat deze zich legitimeren.

**Samengevat: Checklist 'Klaar voor gegevensuitwisseling'**

In het kader van digitale gegevensuitwisseling in de geboortezorg, dient elke eerstelijns- praktijk en kraamzorgorganisatie minimaal de volgende zaken te hebben geregeld:

- [ ] Binnen de praktijk is een procedure opgesteld met afspraken over het informeren over, en uitvragen van, toestemming van de cliënt
- [ ] De toegang van medewerkers is vastgelegd in een autorisatiebeleid waarin staat wie toegang/recht heeft tot het bekijken van een dossier
- [ ] Er wordt altijd ingelogd met 2 factor authenticatie in het bronsysteem.
- [ ] Alle activiteiten binnen het bronsysteem en binnen de viewer wordt geregistreerd via de persoonlijke account. Middels deze 'logging' worden de activiteiten van een gebruiker vastgelegd en zijn deze opvraagbaar.
- [ ] Zorg dat alle medewerkers aantoonbaar bekend zijn met het beleid en de procedures t.a.v. de omgang met cliëntgegevens.

*** *E-learnings die zijn aangeboden vanuit het landelijk programmabureau Babyconnect*

Babyconnect