Informatiebeveiliging en privacy

informatie voor klanten van Orfeus - mei 2018

Waarom deze informatie

Er is nieuwe wetgeving van kracht die aanvullende eisen stelt aan de elektronische verwerking van gegevens en aan privacybescherming. Op dit moment staat de AVG (Algemene Verordening Gegevensbescherming) volop in de belangstelling; deze verordening vervangt op 25 mei 2018 de Wbp. Al eerder van kracht werden de Wet cliëntenrechten bij elektronische verwerking van gegevens (1-7-2017) en het Besluit elektronische gegevensverwerking in de zorg (1-1-2018).

Met deze notitie informeren we onze eerstelijns klanten - verloskundigenpraktijken - over de maatregelen die Orfeus als ICT-dienstverlener heeft genomen. Klanten van Orfeus kunnen deze informatie gebruiken in hun eigen privacybeleid of privacyverklaring en als verantwoording richting Autoriteit Persoonsgegevens.

Informatiebeveiliging Orfeus

Informatiebeveiliging gaat over het behouden van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Informatiebeveiliging is belangrijk, zeker in de zorgsector waar medische en patiëntgegevens worden beheerd en uitgewisseld. Beveiliging van de informatievoorziening is daarmee een belangrijk aandachtspunt in het beleid en de werkwijze van Orfeus.

NEN7510 is de landelijke norm voor informatiebeveiliging in de zorg. Orfeus is in 2017 gecertificeerd op basis van NEN7510. Dit houdt in dat Orfeus passende technische en organisatorische maatregelen heeft genomen om de risico's die de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie in Orfeus Online kunnen aantasten, terug te dringen. De certificering houdt ook in dat Orfeus elk jaar aan een controle-audit wordt onderworpen en na 3 jaar wordt beoordeeld voor hercertificering.

Orfeus hecht niet alleen aan haar eigen informatiebeveiliging, maar ook aan die van andere partijen. De servers waar Orfeus Online op draait zijn ondergebracht bij een gecertificeerd datacentrum (NEN7510, ISO27001). Voor eventuele samenwerking met andere leveranciers heeft Orfeus als beleid dat zij alleen in zee gaat met gecertificeerde partijen. De gegevensuitwisseling tussen klanten en instanties als Perined, RIVM, Peridos, Zorgmail en Vecozo, gaat op basis van overeenkomsten die verloskundigenpraktijken met deze instanties hebben gesloten. Orfeus faciliteert vervolgens deze informatie-uitwisseling en zorgt dat deze voldoet aan door partijen gestelde transport beveiligingseisen en authenticatie.

Orfeus en de AVG

Orfeus heeft voor klanten een verwerkersovereenkomst beschikbaar die AVG-proof is, op maat gemaakt en gecheckt door juridisch adviesbureau ICTRecht. De verwerkersovereenkomst vervangt de huidige bewerkersovereenkomst die Orfeus met klanten heeft, maar die zijn geldigheid verliest op 25 mei 2018. Overigens ligt verantwoordelijkheid om de nieuwe verwerkersovereenkomst te lezen en te ondertekenen bij de verloskundigenpraktijk.

In de verwerkersovereenkomst zijn de verantwoordelijkheden en verplichtingen van verwerker en verwerkingsverantwoordelijke conform de eisen van de AVG vastgelegd. In het verlengde van deze service, heeft Orfeus twee tabellen gemaakt met informatie die verloskundigen kunnen gebruiken voor hun eigen AVG-dossier en privacyverklaring:

1. het door Orfeus opgestelde register van verwerkingen dat voor onze klanten relevant is (NB: als verwerkingsverantwoordelijke heb je ook een eigen plicht om een register van verwerkingen op te stellen);
2. de faciliteiten die Orfeus standaard beschikbaar heeft om verzoeken van betrokkenen (cliënten) op basis van de AVG in te kunnen willigen (NB: het is aan de verwerkingsverantwoordelijke om over verzoeken van cliënten te besluiten en de gewenste actie uit te voeren).

Al eerder heeft Orfeus op haar website de FAQ rondom de AVG geplaatst en via het prikbord van de gebruikers een link daar naartoe geplaatst.

Overige relevante wetgeving

Naast de AVG zijn voor zorgverleners en hun ICT-dienstverleners ook de Wet cliëntenrechten bij elektronische verwerking van gegevens (per 1-7-2017, deels per 1-7-2020) en het Besluit elektronische gegevensverwerking in de zorg (per 1-1-2018) van belang. Op de KNOV-site is hier al eerder informatie over geplaatst. Deze Wet en het Besluit stellen extra eisen aan de informatiebeveiliging en geven extra rechten aan cliënten/patiënten. De nieuwe wetgeving is vooral gericht op elektronische uitwisselingssystemen. Via een uitwisselingssystemen kunnen verschillende soorten

zorgverleners zonder verwijzing of overdracht informatie ophalen uit een medisch dossier (men noemt dit pull-verkeer). Dit is het geval bij inzageportalen, ziekenhuissystemen, het LSP etc. Orfeus 1e lijn is in de eerste plaats een zorginformatiesysteem, voor intern gebruik, waarbij alleen bij verwijzing of overdracht informatie wordt uitgewisseld met andere zorgverleners (men noemt dit push-verkeer). Echter, de ontwikkelingen in de markt en de wens om binnen verloskundige samenwerkingsverbanden (VSV's), tussen 1e en 2e lijn en met zwangeren informatie en dossiers uit te wisselen, bewegen zich steeds meer in de richting van elektronische uitwisselingssystemen, met alle extra eisen van dien. Het is goed om hier ook als klant alert op te zijn.

Richtlijnen informatiebeveiliging klanten

Informatiebeveiliging is een gezamenlijke verantwoordelijkheid van Orfeus, als ICT-dienstverlener, en van verloskundigen, als gebruikers van Orfeus. Wij vragen onze klanten om gebruik te maken van de faciliteiten die Orfeus hiervoor beschikbaar stelt en om bekend veronderstelde beveiligingsrichtlijnen na te leven. De belangrijkste adviezen en tips nog eens op een rij:

- Verander een nieuw of gereset wachtwoord, dat praktijk(beheerder) ontvangt van de Orfeus helpdesk, liefst direct of anders zo spoedig mogelijk.
- Wijzig het wachtwoord regelmatig, tenminste 1x per jaar (wanneer meerdere gebruikers een zelfde account gebruiken moet het nieuwe wachtwoord natuurlijk wel worden doorgegeven aan de andere gebruikers).
- Gebruik MFA (Multi Factor Authentication) voor de persoonlijke logins; Orfeus faciliteert dit, maar de praktijk(beheerder) moet MFA zelf aanzetten.
- Leen de combinatie van gebruikersnaam, wachtwoord en token nooit uit; deze zijn strikt persoonlijk.
- Sla zo min mogelijk vertrouwelijke informatie op je telefoon, tablet, laptop of andere media op; doe dit in ieder geval altijd versleuteld en verwijder de informatie weer zo snel mogelijk.
- Laat je ICT middelen die je gebruikt om toegang te krijgen tot Orfeus Online nooit onbeheerd achter, voorzie ze van een toegangscode en zo mogelijk encryptie.
- Steek nooit zomaar onbekende USB-sticks in je PC, deze kan virussen bevatten.
- Deel geen vertrouwelijke informatie via onbeveiligde media zoals e-mail, Whatsapp, of filesharing applicaties als Dropbox, Google Drive etc.
- Download alleen bestanden van betrouwbare herkomst.
- Wees bedacht op verdachte (of phishing mails). Klik nooit op een link en open nooit een bijlage in een dergelijke verdachte mail.
- Gebruik Zorgmail voor het communiceren van vertrouwelijke informatie met andere zorgverleners.
- Gebruik de Orfeus Zwanger app voor het delen van vertrouwelijke informatie met je cliënten.