KLINIEK SINT-JOZEF
CENTRUM VOOR PSYCHIATRIE EN PSYCHOTHERAPIE PITTEM
Boterstraat 6, 8740 Pittem | T. 051 46 70 41
F. 051 46 70 46 | info@sintjozefpittem.be
www.sintjozefpittem.be

PRIVACYBELEID KLINIEK SINT-JOZEF PITTEM

VERSIE: juni 2019

INHOUD

1. INLEIDING

Kliniek Sint-Jozef Pittem hecht veel belang aan het beschermen van de persoonlijke levenssfeer van zowel patiënten en hun context als medewerkers, artsen en andere betrokkenen.

In deze beleidstekst licht Kliniek Sint-Jozef toe hoe ze omgaat met het verwerken en beschermen van persoonsgegevens. Met persoonsgegevens bedoelen wij alle persoonlijke informatie die wordt verstrekt in het kader van de ziekenhuisopdracht.

Het verwerken van gegevens gaat zeer ruim en omvat zowel papieren als digitale verwerking. Kliniek Sint-Jozef verwerkt gegevens omwille van verschillende doeleinden die verder in deze tekst worden toegelicht.

Het opstellen van dit privacybeleid kadert binnen de GDPR-wetgeving[1] die gebruikers meer transparantie en controle wil geven over wat diensten en organisaties met verschafte gegevens doen. Daarnaast is deze tekst vanuit strategisch oogpunt belangrijk. Kliniek Sint-Jozef omschrijft in haar missie en visie waarden als transparantie, veiligheid, kwaliteit en participatie. Een eenduidig en duidelijk beleid omtrent gegevensbescherming is hier dan ook op zijn plaats.

De concrete toepassing van dit beleid staat omschreven in onze verschillende privacyverklaringen, respectievelijk voor patiënten, medewerkers en derden.

2. BEGRIPPEN

2.1. Persoonsgegevens

Onder persoonsgegevens wordt verstaan alle informatie over een geïdentificeerde of direct of indirect identificeerbare natuurlijke persoon.

De directe of indirecte identificatie van een natuurlijk persoon kan gebeuren dankzij verschillende elementen:

- Een identificatie (naam, locatiegegevens, rekeningnummer, e-mail, telefoon, cv, nummerplaat wagen, IP-adres, identiteitskaart- en rijksregisternummer, enz.)
- Een of meer elementen die kenmerkend zijn voor de fysieke, sociale, culturele, economische identiteit (foto, taal, leeftijd, leefgewoontes, bankgegevens, diploma, antwoorden op een vragenlijst, enz.)

2.2. Verwerking van persoonsgegevens

Binnen Kliniek Sint-Jozef geldt de bescherming van persoonsgegevens voor alle vormen van verwerking van die persoonsgegevens zoals die hierna worden gedefinieerd.

Een verwerking met betrekking tot persoonsgegevens is een bewerking of een geheel van bewerkingen, al dan niet uitgevoerd via geautomatiseerde procedés, met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, structureren, raadplegen, wijzigen, gebruiken, opslaan, verstrekken door middel van

[1] GDPR staat voor 'General Data Protection Regulation' of in het Nederlands Algemene Verordening Gegevensbescherming AVG. Deze Europese regelgeving is sinds 25 mei 2018.

doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van persoonsgegevens.

Elke hierboven vermelde bewerking m.b.t. persoonsgegevens geniet bescherming en moet gebeuren mits naleving van strikte richtlijnen.

2.3. Bijkomende definities

- *Persoonsgegevens over de gezondheid*: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
- *Anonieme gegevens*: alle gegevens die niet (meer) met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en die dus geen persoonsgegevens (meer) zijn.
- *Gepseudonimiseerde persoonsgegevens*: persoonsgegevens die op zodanige wijze verwerkt worden dat ze niet meer aan een specifieke natuurlijke persoon kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. Het gaat dus niet om anonieme gegevens, aangezien de natuurlijke persoon na pseudonimisering nog wel identificeerbaar is.
- *Bestand*: elk gestructureerd geheel van persoonsgegevens, samengesteld en bewaard op een logische, gestructureerde wijze die een systematische raadpleging toelaat, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is of verspreid op een functioneel of geografisch bepaalde wijze.
- *Verwerkingsverantwoordelijke*: de natuurlijke persoon, de rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt.
- *Bewerker*: de persoon die onder gezag van de verwerkingsverantwoordelijke gemachtigd is om de gegevens te verwerken.
- *Verwerker*: de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder onder het rechtstreekse gezag van de verwerkingsverantwoordelijke te staan.
- *Ontvanger*: de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan aan wie/waaraan persoonsgegevens worden verstrekt.
- *Patiënt*: de natuurlijke persoon, opgenomen of behandeld in het ziekenhuis.
- *Toestemming van de patiënt*: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting, waarmee de patiënt of zijn wettelijke vertegenwoordiger door middel van een verklaring of ondubbelzinnige actieve handeling aanvaardt dat persoonsgegevens betreffende die patiënt worden verwerkt.

3. DE UITVOERING VAN HET BELEID VOOR GEGEVENSBESCHERMING

Het privacybeleid van Kliniek Sint-Jozef is er gekomen naar aanleiding van de GDPR-wetgeving en werd ter goedkeuring voorgelegd aan de directie en de Raad van Bestuur van Kliniek Sint-Jozef. Deze tekst zal periodiek of bij belangrijke wijzigingen aangepast en opnieuw gevalideerd worden. Daarbij toetsen we de nieuwe regelgevende kaders af met deze beleidstekst.

4. TOEPASSINSGEBIEDEN VAN HET BELEID VOOR GEGEVENSBESCHERMING

4.1. Materieel toepassingsgebied

Deze beleidstekst is van toepassing op alle persoonsgegevens die Kliniek Sint-Jozef Pittem verwerkt. We verstaan hieronder niet alleen de gegevens van patiënten, maar ook die van context, medewerkers, artsen en andere betrokkenen.

4.2. Functioneel toepassingsgebied

Het beleid is van toepassing op alle verwerkingsdoelen. Doelen waarvoor Kliniek Sint-Jozef persoonsgegevens verwerkt zijn (niet-limitatief):

- zorg voor de patiënt (inclusief het uitnodigen van contactpersonen voor gesprekken, infosessies of activiteiten)
- facturatie
- personeelsdossier (loonverwerking, verzekering, sociale administratie, evaluaties, opleidingen, …)
- kwaliteitscontroles
- tevredenheidsenquêtes en andere acties i.v.m. de kwaliteit van de zorg
- wetenschappelijk onderzoek/onderzoeksprojecten
- rapportering (bijv. aan de overheid)
- initiatieven met een maatschappelijke relevantie (bijv. opendeurdag, activiteiten, …)

Kliniek Sint-Jozef verwerkt persoonsgegevens op geen enkele wijze voor louter commerciële doeleinden.

4.3. Organisatorisch toepassingsgebied

Met deze beleidstekst richt Kliniek Sint-Jozef zich tot iedereen die in haar opdracht persoonsgegevens verwerkt. Zowel de Raad van Bestuur, de directie, de artsen als de medewerkers, stagiairs en vrijwilligers worden verondersteld dit beleid mee uit te dragen. Daarom verspreidt Kliniek Sint-Jozef deze tekst via verschillende kanalen, o.a. via publicatie op het intranet en de website.

Het privacybeleid is ook van toepassing voor externe partners met wie Kliniek Sint-Jozef samenwerkt. Bij het afsluiten van contracten met bijvoorbeeld leveranciers heeft Kliniek Sint-Jozef specifieke aandacht voor de bescherming van persoonlijke gegevens.

Ook in de samenwerking binnen onze zorgnetwerken, met (openbare) diensten en bij de inzet van (sociale) media vormt dit beleid het uitgangspunt.

5. BELEIDSDOELSTELLINGEN VOOR GEGEVENSBESCHERMING

5.1. Krachtlijnen

Zoals in de inleiding aangegeven draagt Kliniek Sint-Jozef een aantal waarden hoog in het vaandel. Deze lijn wil Kliniek Sint-Jozef doortrekken bij het uitvoeren van haar privacybeleid.

Het bieden van kwalitatieve zorg vormt de kernopdracht van Kliniek Sint-Jozef. Het correct verwerken van persoonsgegevens is een noodzakelijk middel om deze kwaliteit te kunnen bieden. Kliniek Sint-Jozef wil hierbij maximale aandacht hebben voor de rechten en vrijheden van elke persoon die hier op een of andere manier bij betrokken is.

Met dit beleid vestigt Kliniek Sint-Jozef specifieke aandacht op volgende doelstellingen:

1. We zijn **transparant** over de persoonsgegevens die worden verwerkt en het doel waarvoor deze verwerking gebeurt. De communicatie hierover is eerlijk, toegankelijk en in begrijpelijke taal.
2. We beperken ons tot het verwerken van de **noodzakelijke gegevens** die ons in staat stellen om onze kernopdracht te vervullen, namelijk het bieden van kwalitatieve zorg. We maken gebruik van deze gegevens op een **rechtmatige** manier. Dat betekent bijvoorbeeld dat verwerking gebeurt in overeenstemming met de geldende wetgeving en de statutaire doelen van Kliniek Sint-Jozef Pittem.
3. Ook bij de gegevensverwerking behouden we de **integriteit** die we als zorginstelling aan de dag willen leggen.
4. We **bewaren** gegevens **niet langer dan noodzakelijk**. Bij het bepalen van deze noodzakelijkheid hanteren we onze wettelijke verplichtingen, de doelmatigheid en de rechten en vrijheden van de betrokkenen.
5. We bewaken actief dat de **rechten** van elke betrokkene (bijvoorbeeld het recht op inzage, het recht op afschrift, het recht op zorg) bij het verwerken van persoonsgegevens behouden blijven. We doen de nodige inspanningen om verschillende (wettelijke) kaders samen te brengen en van daaruit verschillende belangen tegenover elkaar af te wegen.
6. We doen alle mogelijke inspanningen om **inbreuken te voorkomen**, onder meer via sensibilisering omtrent informatieveiligheid en veilige, gebruiksvriendelijke tools. Eventuele inbreuken worden gerapporteerd via de geijkte kanalen. Via intern toezicht en periodieke controles bewaken we onze verantwoordingsplicht.
7. Gegevens moeten **juist** zijn en continu worden geactualiseerd.

5.2. Rechtmatigheid van de verwerking

Kliniek Sint-Jozef is wettelijk verplicht om aan de persoon wiens persoonsgegevens zij verwerkt de rechtsgrond van die verwerking mee te delen.
Deze mededeling gebeurt door vermelding van de rechtsgrond in de privacyverklaring(en) van Kliniek Sint-Jozef. De beschikbare rechtsgronden worden beperkt door de GDPR en Kliniek Sint-Jozef moet voor elke verwerkingsactiviteit de toepasselijke rechtsgrond kunnen aanduiden.

De toepasselijke rechtsgronden kunnen de volgende zijn:

1. *Noodzakelijkheid voor de uitvoering van de overeenkomst*
   De verwerking van de gegevens door Kliniek Sint-Jozef is noodzakelijk voor de uitvoering van een overeenkomst. Bij Kliniek Sint-Jozef gaat dat bijvoorbeeld om de opnameverklaring voor patiënten, contracten met leveranciers, arbeidsovereenkomsten met werknemers, …

2. Wettelijk verplicht

De verwerking is noodzakelijk voor de uitvoering van wettelijke verplichtingen. Het gaat hier bijvoorbeeld over verwerkingen die Kliniek Sint-Jozef doet omdat zij daartoe verplicht is krachtens de FOD Volksgezondheid of over gegevens die Kliniek Sint-Jozef, als werkgever, moet meedelen aan de FOD sociale zekerheid.

3. Gerechtvaardigd belang

De verwerking van persoonsgegevens kan noodzakelijk zijn voor de behartiging van het gerechtvaardigd belang van Kliniek Sint-Jozef.
Om te bepalen of Kliniek Sint-Jozef een dergelijk gerechtvaardigd belang heeft, is een nauwgezette juridische evaluatie nodig. Hierbij wordt bepaald of een betrokken persoon er zich redelijkerwijs mag aan verwachten, op het moment van en met het oog op de gegevensinzameling, dat zijn gegevens voor een ander welbepaald doeleinde, verenigbaar met het initiële doeleinde van de gegevensinzameling wordt gebruikt.

Het is belangrijk op te merken dat het rechtmatige belang specifiek is, en met omzichtigheid dient te worden gebruikt. Iedere beslissing om dit doeleinde te gebruiken dient geval per geval te gebeuren, en kan in geen geval veralgemeend worden of systematisch gebruikt worden.

4. Toestemming

Kliniek Sint-Jozef mag de persoonsgegevens van een betrokkene verwerken indien ze hiervoor van de betrokkene de toestemming heeft gekregen.

De verkregen toestemming moet vrij zijn en vereist een duidelijke positieve actie van de betrokken persoon. Het stilzwijgen, vooraf aangevinkte vakjes of het ontbreken van reactie vormen dus geen geldige toestemming (bijv. een 'verborgen' toestemming om reclame te ontvangen in een wedstrijdreglement is niet vrij genoeg).

De toestemming moet bovendien controleerbaar zijn en door Kliniek Sint-Jozef kunnen worden aangetoond: er is dus een bewijs nodig van het moment en de wijze waarop de toestemming werd gegeven.

Ingeval er meerdere vragen worden gesteld, moet de vraag om toestemming zodanig worden gesteld dat zij duidelijk wordt onderscheiden van andere vragen.
Kliniek Sint-Jozef zal bijvoorbeeld de toestemming vragen voor de verdere verspreiding van foto's of beeldmateriaal.

Een persoon heeft het recht om zijn toestemming op elk moment in te trekken.

5.3. Rechten van de personen wiens persoonsgegevens worden verwerkt

De GDPR geeft veel rechten aan de personen van wie Kliniek Sint-Jozef de gegevens verwerkt.
De betrokken personen kunnen zich beroepen op deze rechten zodra persoonsgegevens door hen worden verwerkt, bijvoorbeeld vanaf de ondertekening van de opnameverklaring door de patiënt.
Het gaat hierbij over de volgende rechten:

1. Recht op informatie

Kliniek Sint-Jozef moet in alle transparantie gedetailleerde informatie verstrekken aan de betrokken personen over de wijze waarop de gegevens worden verwerkt en welke gegevens worden verwerkt.

Die informatie moet worden geleverd hetzij op het ogenblik van de inzameling (als die gegevens rechtstreeks bij de desbetreffende persoon worden verkregen), hetzij binnen een redelijke termijn (voor onrechtstreeks verkregen gegevens).

De volgende informatie moet minimum meegedeeld worden:
- De gegevens van Kliniek Sint-Jozef
- De gegevens van de Functionaris voor gegevensbescherming (DPO – Data Protection Officer)
- Het doeleinde van de verwerking
- De juridische basis van de verwerking (met inbegrip van het rechtmatige belang van Kliniek Sint-Jozef als dat het geval is)
- De bestemmelingen van de gegevens
- Of de intentie bestaat de gegevens al dan niet te transfereren naar het buitenland
- De bewaringsrichtlijnen
- De vermelding van de rechten van de persoon
- Het recht op intrekking van de toestemming
- Het recht tot indiening van een klacht bij de gegevensbeschermingsautoriteit

2. Recht op verbetering

Op verzoek van de betrokken persoon moeten onjuiste of onvolledige gegevens worden verbeterd, derden moeten hierover eveneens worden geïnformeerd als hen die gegevens werden meegedeeld, de betrokken persoon worden ingelicht over die derden aan wie de gegevens werden bekendgemaakt.
De betrokken persoon dient een antwoord te worden gegeven binnen een termijn van één maand. Voormelde termijn kan verlengd worden met twee maanden indien het om een complexe zaak gaat of indien er een aanzienlijk aantal vragen zijn.

3. Recht om vergeten te worden

De betrokken persoon mag vragen om definitief door Kliniek Sint-Jozef te worden “vergeten”. Dit is echter geen absoluut recht en er zijn voorwaarden aan verbonden. Alvorens tot enige actie over te gaan, moet elke aanvraag door Kliniek Sint-Jozef worden geanalyseerd.

4. Recht op overdraagbaarheid

De betrokken persoon kan Kliniek Sint-Jozef vragen om zijn persoonsgegevens, op een beveiligde manier, over te dragen van een informatica-omgeving naar een andere, wanneer die gegevens op basis van een toestemming of van de uitvoering van een overeenkomst worden geleverd. Kliniek Sint-Jozef moet de gegevens op gestructureerde, gangbare en leesbare wijze leveren, binnen een termijn van één maand, die eventueel kan worden verlengd.

5. Recht van inzage

Elke persoon wiens persoonsgegevens door Kliniek Sint-Jozef worden verwerkt mag vragen om gratis zijn eigen gegevens te ontvangen, en dit op beknopte, transparante, begrijpelijke, makkelijk toegankelijke wijze en in een heldere en makkelijke taal. Deze gegevens moeten binnen een termijn van één maand bezorgd worden, eventueel kan deze termijn worden verlengd.

6. Recht van bezwaar

Iedere persoon over wiens gegevens Kliniek Sint-Jozef beschikt, mag bezwaar aantekenen tegen verwerkingen die gebaseerd zijn op een gerechtvaardigd belang. Kliniek Sint-Jozef moet dan geval per geval onderzoeken of er zal worden ingegaan op dit verzoek. Het recht van bezwaar is derhalve niet absoluut, behalve ingeval van een bezwaar tegen "direct marketing", dat altijd dient te worden ingewilligd.

7. Recht op beperking van de verwerking

De betrokken persoon heeft, in bepaalde gevallen, recht om van Kliniek Sint-Jozef te verkrijgen dat de verwerking van zijn persoonlijke gegevens worden beperkt. Iedere aanvraag van dien aard moet door Kliniek Sint-Jozef worden geanalyseerd vooraleer tot enige actie wordt overgegaan.

5.4. Gegevensinbreuken

Een inbreuk in verband met persoonsgegevens is de vernietiging, het verlies, de vervalsing of de openbaarmaking van persoonsgegevens die niet zijn toegestaan. Enkele voorbeelden van mogelijke gegevensinbreuken zijn:

- Het verstrekken van een wachtwoord aan een derde
- Een kwijtgeraakte USB-stick waarop zich persoonsgegevens bevinden
- Een gestolen werklaptop
- Een vastgestelde inbraak door een hacker
- Een kwetsbaarheid in een applicatie waardoor persoonsgegevens gelekt worden
- Een niet-toegelaten wijziging van persoonsgegevens in een database
- …

Telkens dient te worden nagegaan of er effectief sprake is van een gegevensinbreuk en wat de ernst ervan is. Kliniek Sint-Jozef heeft een specifieke procedure uitgewerkt in geval van inbreuken m.b.t. persoonsgegevens.

Overeenkomstig de GDPR voorziet die procedure, onder andere, in de verplichting om de betrokken personen en de gegevensbeschermingsautoriteit op de hoogte te brengen.

6. DE BELEIDSTAKEN EN BIJHORENDE ORGANISATIEPROCESSEN

Om de bovengenoemde beleidsdoelstellingen te bereiken zijn een aantal taken vastgelegd. Deze taken zijn in lijn met alle wettelijke verplichtingen die Kliniek Sint-Jozef Pittem dient na te streven. De algemene verantwoordelijkheid voor het uitvoeren van deze taken berust bij het directiecomité van Kliniek Sint-Jozef Pittem. De delegatie van de taken en specifieke taken zijn opgenomen in hoofdstuk 7.

1. Kliniek Sint-Jozef houdt permanent een **dataverwerkingsregister** bij. Dat is een lijst van alle verwerkingsactiviteiten waarbij persoonsgegevens van de categorieën van betrokkenen (patiënten, medewerkers, …) worden verwerkt. De lijst omvat:
    - een overzicht van de verwerkingsdoelen
    - categorieën van persoonsgegevens
    - wijze van verzamelen van persoonsgegevens
    - wijze van opslag van persoonsgegevens (intern/extern)
    - welke persoonsgegevens welk verwerkingsdoel dienen
    - welke persoonsgegevens worden uitgewisseld indien van toepassing

- met wie eventuele gegevensuitwisseling gebeurt
- aanduiding van de verwerkingsgrond
- bewaartermijnen
- technische en organisatorische maatregelen

Het verwerkingsregister wordt bijgewerkt in het geval van bijkomende verwerkingsdoelen of belangrijke wijzigingen (bijvoorbeeld veranderde wetgeving en nieuwe processen). We toetsen dit ook telkens af aan de wettelijke en statutaire taken van Kliniek Sint-Jozef. We zien erop toe dat een nieuw doel verenigbaar blijft met het oorspronkelijke doel.

Kliniek Sint-Jozef houdt het register digitaal bij en het is opvraagbaar volgens de wettelijke bepalingen (door de Gegevensbeschermingsautoriteit).

2. Kliniek Sint-Jozef Pittem stelt een lijst op van **criteria** die ze gebruikt om na te gaan of een verwerking een **verhoogd risico** inhoudt voor de betrokkene. Indien nodig voert Kliniek Sint-Jozef voorafgaand een **gegevensbeschermingseffectenbeoordeling** uit. Op basis van deze analyse neemt Kliniek Sint-Jozef maatregelen die ervoor zorgen dat bij verwerking de kans op inbreuken verkleind wordt. Kliniek Sint-Jozef beschikt ook over een procedure inzake het afhandelen van een inbreuk.

3. Kliniek Sint-Jozef beheert de **contractuele bepalingen met verwerkers**. Deze bepalingen bevatten onder meer de instructies die horen bij de verwerking, de verplichtingen waaraan de verwerker moet voldoen in het kader van het naleven van wet- en regelgeving (o.a. informatieveiligheid). Kliniek Sint-Jozef houdt actief toezicht op deze contractuele bepalingen. Wanneer de verwerking plaatsvindt onder gemeenschappelijke verantwoordelijkheid, maakt Kliniek Sint-Jozef duidelijke afspraken met het oog op de rechten van betrokkene en de informatieplicht tegenover betrokkene. De verantwoordelijkheden worden duidelijk gedocumenteerd en gecommuniceerd naar de betrokkene.

4. In de **interne organisatieprocessen** neemt Kliniek Sint-Jozef zowel het **informeren** van de betrokkene over gegevensverwerking als de **rechten** van de betrokkene m.b.t. gegevensverwerking op.

5. Kliniek Sint-Jozef zorgt voor (preventieve) maatregelen waarmee ze **inbreuken** kan vaststellen, melden en afhandelen. Dit gaat bijvoorbeeld over het bijhouden van een register van inbreuken, de interne communicatie en afhandeling, de communicatie naar betrokkene en de Gegevensbeschermingsautoriteit, …

6. Kliniek Sint-Jozef Pittem voorziet **duidelijke instructies en richtlijnen** in overeenstemming met de verantwoordelijkheid die haar medewerkers hebben ten aanzien van persoonsgegevens en de verwerking ervan. Kliniek Sint-Jozef communiceert deze instructies via een gedragscode, procedures, sensibilisering en opleiding (folder, intranet, nieuwsbrief, …) en functiebeschrijvingen. Kliniek Sint-Jozef neemt de verplichting tot naleving op in het arbeidsreglement. Overtredingen worden afgehandeld in lijn met het beleid inzake sancties.

7. TOEPASSING VAN HET BELEID GEGEVENSBESCHERMING OP DE REGIONALE NETWERKEN

Kliniek Sint-Jozef wil dit privacybeleid actief uitdragen naar haar partners in de zorgnetwerken waar ze deel van uitmaakt.
Kliniek Sint-Jozef ziet hierbij toe op de impact van de samenwerking en de verantwoordelijkheid over de gegevensverwerking en overlegt binnen het netwerk over de toe te passen beleidsprincipes en hoe we die realiseren.

8. DE ORGANISATIE VAN GEGEVENSBESCHERMING

De algemene verantwoordelijkheid voor het uitvoeren van de beleidstaken met betrekking tot gegevensverwerking berust bij het **directiecomité** van Kliniek Sint-Jozef. Bepaalde taken worden gedelegeerd. Het directiecomité ziet toe op een correcte uitvoering ervan. We omschrijven hieronder de belangrijkste taken.

Verantwoordelijkheid over persoonsgegevens

De verantwoordelijkheid voor het uitvoeren van de beleidstaken in het kader van gegevensbescherming ligt bij het directiecomité van Kliniek Sint-Jozef. Het directiecomité is verantwoordelijk voor het bekrachtigen van de beleidsdoelen en de hierbij horende taken. In de uitvoering van deze verantwoordelijkheden kan het directiecomité beroep doen op de adviezen van de functionaris voor de gegevensbescherming of data protection officer (DPO). Elke beoordeling van risico's vindt plaats onder verantwoordelijkheid van het directiecomité, alsook de uitvoering van de bijhorende maatregelen. Het directiecomité is daarnaast ook eindverantwoordelijk voor alle verplichtingen uit hoofde van de wet- en regelgeving, waaronder de bepalingen in de verordening 2016/679. Hiervoor delegeert het directiecomité een aantal taken, zoals hieronder opgesomd.

Toezicht gegevens medisch dossier patiënten

Als psychiatrisch ziekenhuis definieert Kliniek Sint-Jozef het geheel aan gegevens dat wordt bijgehouden in het multidisciplinair elektronisch patiëntendossier als 'medisch dossier'. Het betreft hier dus niet enkel gezondheidsgegevens, maar ook sociale gegevens en administratieve gegevens.

Het beleid voor gegevensbescherming doet op geen enkele wijze afbreuk aan de wettelijke verplichtingen die de hoofdgeneesheer/verpleegkundig paramedisch directeur hebben met het oog op de toepassing van de wetgeving over gegevensbescherming.
De hoofdgeneesheer (en voor verpleegkundige gegevens in nauwe samenspraak met de directeur patiëntenzorg) heeft vanuit deze opdracht de verantwoordelijkheid inzake de gegevensbescherming van gegevens in het medisch dossier. Bij belangrijke wijzigingen, zowel op technologisch vlak als op niveau van de verwerking zelf (zoals het invoeren van geautomatiseerde beslissingen of de inschalingen van zorgzwaartemetingen), assisteren de hoofdgeneesheer en de directeur patiëntenzorg in het uitvoeren van de gegevens-beschermingseffectenbeoordeling.
In de uitvoering van het beleid voor gegevensbescherming krijgt de hoofdgeneesheer de taak toegewezen om te oordelen over het ontwerp van een model van gegevensclassificatie, in relatie met de bijhorende organisatieprocessen. Op basis van de vooropgestelde classificatie legt de stuurgroep gegevensbescherming criteria vast voor het uitvoeren van een

gegevensbeschermingseffectenbeoordeling, het melden van inbreuken, specifieke technische en/of organisatorische maatregelen, ….

Voor de toepassing van de rechten van de betrokkene (in het bijzonder deze van de patiënt) voor gezondheidsgegevens die buiten het patiëntendossier worden verwerkt, assisteert de hoofdgeneesheer bij het uitwerken van de beleidslijnen.

De hoofdgeneesheer stimuleert de correcte omgang met patiëntengegevens bij de (para)medische diensten van Kliniek Sint-Jozef. De hoofdgeneesheer neemt bovendien alle relevante aspecten van gegevensbescherming mee in de evaluatie van (kandidaat) artsen en hun opleidingstraject tijdens dienstverband.

De applicatieverantwoordelijke past het beleid toe inzake verwerking van gegevens uit het medisch dossier. Hij stelt, onder de verantwoordelijkheid van de hoofdgeneesheer, het register van verwerkingsactiviteiten op van de artsen, de (para)medische disciplines en het medisch secretariaat. Hij duidt hierbij duidelijk aan welke persoonsgegevens worden ingezameld op basis van een toestemming. Het medisch secretariaat en de dienst maatschappelijk werk richten op vraag van de stuurgroep gegevensbescherming de nodige processen in met het oog op het verstrekken van informatie aan de patiënt en vragen met betrekking tot de rechten van de patiënt. Specifieke aandacht gaat uit naar het registreren van toestemmingen in het kader van eHealth, de registratie van verwijzers en de huisarts en de identificatie van de patiënt, waaronder de gegevensstromen met het rijksregister.

Toezicht financiële gegevens patiënten

De financieel-administratief directeur van Kliniek Sint-Jozef stelt het register op van verwerkingsactiviteiten binnen de dienst boekhouding. De dienst boekhouding, onder verantwoordelijkheid van haar directeur, kijkt toe op de uitwisseling van persoonsgegevens met de overheid, de mutualiteiten, …

Toezicht latere verwerking gegevens patiënten

De hoofdgeneesheer houdt toezicht op de verantwoordelijkheid voor de latere verwerking van gezondheidsgegevens. Hij voert hierbij de verplichtingen uit met het oog op gegevensbescherming, zoals het toezicht op de volledigheid van het verwerkingsregister, de overeenkomsten met verwerkers en de analyse van de risico's. Ook de rechten van de betrokkene, en eventuele toestemmingen, vallen onder zijn beheer. Daarnaast houdt de hoofdgeneesheer toezicht op de latere verwerking van gezondheidsgegevens die gestoeld is op de wettelijke basis. Informatieveiligheid is hierbij een expliciet onderdeel van het toezicht. In geval van een latere verwerking van gezondheidsgegevens waarvoor het advies van een ethisch comité is vereist, worden de modaliteiten voor gegevensbescherming afgetoetst.

Voor de latere verwerking van niet-medische persoonsgegevens is het diensthoofd van de dienst die de verwerking uitvoert, verantwoordelijk voor het toezicht. Wanneer deze latere verwerking plaatsvindt uit hoofde van een overheidsverplichting, dan gebeurt het toezicht eveneens door de dienst die hiermee belast is, in coördinatie met de stuurgroep gegevensbescherming en op advies van de functionaris of DPO.

De latere verwerking voor kwaliteitsdoeleinden en beleidsrapporteringen, vallen onder verantwoordelijkheid van de dienst aan wie de rapportering plaatsvindt in samenspraak met de betreffende applicatieverantwoordelijke. Het toezicht op de

verwerker wordt georganiseerd door deze applicatieverantwoordelijke, met ondersteuning van de DPO.

De latere verwerking van gezondheidsgegevens uit het patiëntendossiers voor kwaliteitsdoeleinden ten behoeve van inspectiediensten, valt onder de verantwoordelijkheid van de hoofdgeneesheer.

Toezicht persoonsgegevens medewerkers en artsen

De personeelsdienst, onder verantwoordelijkheid van de financieel-administratief directeur, krijgt in het beleid voor gegevensbescherming de taak om de gegevensbescherming te bewaken van persoonsgegevens van alle medewerkers (al dan niet in dienst), met uitzondering van de artsen. Het is de taak van de personeelsdienst om bij de implementatie van (nieuwe) verwerkingsprocessen waarbij de persoonsgegevens van medewerkers worden verwerkt, het beschreven beleid te vertalen en toe te passen. Daar waar nieuwe organisatieprocessen worden ingevoerd of bestaande organisatieprocessen worden gedigitaliseerd, zorgt de financieel-administratief directeur voor de analyse van de verwerkingsgrond, de eventuele bijhorende besprekingen met de personeelsvertegenwoordiging (bijvoorbeeld in het kader van transparantie en de evaluatie van gerechtvaardigde belangen) en de bijhorende gegevensbeschermingseffectenbeoordeling. De financieel-administratief directeur levert daarenboven een actieve bijdrage bij het onderhouden van het register van verwerkingsactiviteiten voor personeelsgegevens.

Voor de verwerking van persoonsgegevens van artsen wordt de corresponderende taak toebedeeld aan de coördinator van het medisch secretariaat onder verantwoordelijkheid van de hoofdgeneesheer.

Toezicht toepassing gegevensbescherming door medewerkers en artsen

Per departement (patiëntenzorg, administratie en facilitaire diensten) heeft de betreffende directeur de verantwoordelijkheid om de verplichtingen inzake het toepassen van dit beleid te vertalen naar het arbeidsreglement, de toepasselijke handvesten en functieprofielen (met uitzondering van de verplichtingen van de artsen), het sanctiebeleid en de controles en evaluaties. Voor de corresponderende verplichtingen voor artsen wordt deze verantwoordelijkheid bij de hoofdgeneesheer gelegd.

Algemeen toezicht gegevensbescherming bij verwerkers

Het algemeen toezicht op verwerkers van persoonsgegevens die in opdracht van Kliniek Sint-Jozef persoonsgegevens verwerken, wordt uitgevoerd door de veiligheidsconsulent voor wat betreft de informatieveiligheid en van het diensthoofd van de dienst waarvoor de verwerking wordt uitgevoerd, in samenspraak met de functionaris voor de gegevensbescherming of DPO. De aankoopdienst voert de instructies hierover uit onder toezicht van de directeur facilitaire diensten.

Gegevensbescherming bij zorginnovatie

Elk organisatieproces dat gedigitaliseerd wordt of voor elk (al dan niet nieuw) organisatieproces waarbij innoverende technologieën worden gebruikt wordt de functionaris voor de gegevensbescherming of DPO geconsulteerd. De verantwoordelijkheid hiervoor ligt bij de initiatiefnemer (de arts, de directeur patiëntenzorg, de applicatieverantwoordelijke). Voor wat betreft de artsen kijken

de hoofdgeneesheer en de medische raad, samen met de functionaris of DPO, toe op de correcte toepassing.

Uitoefenen van de rechten van de betrokkene

De ombudsfunctie wordt ingevuld volgens de bepalingen in de wet patiëntenrechten. In de uitvoering van de taak adviseert de functionaris voor de gegevensbescherming of DPO, op vraag van de Ombudsdienst, over antwoorden op vragen van de patiënt betreffende de verwerking van diens persoonsgegevens. Dit antwoord is niet bindend voor de Ombudsdienst, zodat de onafhankelijkheid van deze functie gevrijwaard blijft.

9. DE RELATIE TUSSEN GEGEVENSBESCHERMING EN INFORMATIEVEILIGHEID

Voor Kliniek Sint-Jozef worden de taken van de veiligheidsconsulent en van de functionaris voor de gegevensbescherming of DPO opgenomen door medewerkers van een externe firma (BDO).

De veiligheidsconsulent en de DPO adviseren en ondersteunen de stuurgroep gegevensbescherming van Kliniek Sint-Jozef.

10. DE STUURGROEP GEGEVENSBESCHERMING

De stuurgroep gegevensbescherming wordt gemonitord en inhoudelijk ondersteund door de externe DPO. Voorts bestaat de stuurgroep uit:

- financieel-administratief directeur
- stafmedewerker patiëntenzorg / applicatieverantwoordelijke elektronisch patiëntendossier
- systeembeheerder

De stuurgroep adviseert het directiecomité en de Raad van Bestuur inzake alle verantwoordelijkheden die de organisatie rond gegevensbescherming draagt:

- het bijsturen van het beleid rond gegevensbescherming
- het aanstellen van een functionaris voor de gegevensbescherming
- het bewaken van de onafhankelijkheid van de functionaris voor de gegevensbescherming
- het monitoren van de organisatieprocessen die in deze beleidstekst zijn beschreven met het oog op gegevensbescherming; het inrichten en in stand houden van deze processen; het toekennen van verantwoordelijkheden voor het uitvoeren van deze processen
- het formuleren van adviesvragen
- het bijsturen van het beleid en de uitvoering ervan op advies van de functionaris
- de beslissingen inzake risicobeheer bij het verwerken van persoonsgegevens; de tijdsbesteding van de functionaris is een onderdeel van dit risicobeheer
- de goedkeuring van de classificatieschema's bijvoorbeeld voor het bepalen wanneer een gegevensbeschermingseffectenbeoordeling dient plaats te vinden of voor het melden van inbreuken
- beslissingen over alle overwegingen, waaronder verwerkingen gebaseerd op gerechtvaardigd belang, verenigbaarheid van de doelen bij een latere verwerking, …
- het aanleggen van de nodige documentatie bij alle (voorstellen tot) beslissingen

- het formaliseren van deze beslissingen door het directiecomité
- de toepassing van de sancties bij overtredingen
- toezien op de toepassing van het beleid in horizontale en verticale zorgnetwerken

De samenstelling van de stuurgroep wordt voorgelegd aan de Raad van Bestuur en het directiecomité ter beslissing.