Raphaëlstichting	Vastgesteld door: Bestuur/MT dd 13-7-17 Versiedatum: 13-07-17, aanvulling 19-6-18 Evaluatiedatum: 13-07-20 HKZ-Nr.: 1.3.1. VG 2008 Proceseigenaar: Coördinator kwaliteit

Privacy en informatiebeveiliging
RICHTLIJNEN OMTRENT DE OMGANG
MET PERSONEN, PERSOONSGEGEVENS, PRIVACY EN DATALEK

Inhoudsopgave

1. Inleiding

Informatie en informatievoorziening zijn van groot belang in het werken binnen de zorg en dus ook voor de werkzaamheden van de Raphaëlstichting. De Raphaëlstichting wil binnen de geldende wet- en regelgeving de privacy beschermen en de vertrouwelijkheid van de gegevens borgen conform de wet- en regelgeving. Dit betekent dat we de privacy in ons gedrag respecteren op alle gebieden (lichamelijk, communicatie, informatie en territorium). Dat is enerzijds door ons gedrag (kloppen voordat we de kamer binnen gaan, geen post open maken van cliënten, niet zomaar aan iemands lichaam komen etc). Anderzijds betekent dat ook dat de informatie in onze systemen alleen toegankelijk is voor degenenen die daartoe bevoegd en overeenkomstig voor geautoriseerd zijn.

In hoofdstuk 2 worden kort de wet- en regelgeving en de definities gegeven.
In hoofdstuk 3 worden de algemeen geldende privacy afspraken / richtlijnen binnen de Raphaëlstichting weergegeven.
In hoofdstuk 4 worden de richtlijnen voor gegevensverwerking binnen de Raphaëlstichting weergegeven.
In hoofdstuk 5 wordt de werkwijze t.a.v. het omgaan met bedrijfsmiddelen beschreven.
In hoofdstuk 6 staan de verwijzingen naar gerelateerde documenten.

2. Wet- en regelgeving/ Definities

Wet- en regelgeving
In het kader van de Wetgeving is er beleid voor de Raphaëlstichting opgemaakt en is er voor alle verwerkingen van persoonsgegevens een gegevensverzameling gemaakt welke door de gebruikers volgens die richtlijnen moet worden gehanteerd naar besluit van het Bestuur en de COR.
Alle medewerkers, vrijwilligers en stagiaires van de Raphaëlstichting respecteren de privacy van cliënten [1] en medewerkers[2]. In deze notitie wordt nader omschreven wat de afspraken/ richtlijnen zijn en hoe de werkwijze t.a.v. het omgaan met gegevensverzamelingen is. Daarnaast zijn de gegevensverzamelingen voor medewerkers en voor cliënten apart geïnventariseerd in twee aparte notities.
1. Datalek: Met ingang van 1 januari 2016 geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerke n, datalekken onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.
2. Privacy en informatiebeveiliging: Op 25 mei 2018 treedt de'Algemene verordening Gegevensbescherming' in werking (Europese wetgeving). Deze heeft de wet 'bescherming persoonsgegevens'(Wbp) vervangen.
3. Electronische verwerking van gegevens van cliënten: Op 4 oktober 2016 heeft de eerste kamer ingestemd met het wetsvoorstel 'Cliëntenrechten bij elektronische verwerking van gegevens'. De wet is op 1-7-17 in werking. Een aantal bepalingen treedt pas na drie jaar in werking. (zie voetnoot [3]). Tegelijkertijd zal het "besluit electronische gegevensverwerking door zorgaanbieders in werking treden. Zorgaanbieders moeten dan ook voldoen aan de NEN 7513 (logging). Voldoen aan de NEN 7510,7511 en 7512 was al nodig wanneer het Burger service nummer (bsn-nummer) wordt verwerkt. Tevens regelt dit besluit dat er een functionaris gegevensbescherming moet zijn.

Definities
AP: Autoriteit Persoonsgegevens (voorheen College bescherming persoonsgegevens)

Datalek: Er is alleen sprake van een datalek als zich een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident kan gedacht worden aan het verlies van een USB-stick, diefstal van een laptop, inbraak door een hacker, het open laten staan van de computer met privacy gevoelige informatie.

Persoonsgegevens:

De privacywetgeving geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van

1 *Overal waar in deze notitie cliënt staat kan ook bewoner of cliënt van bv dagbesteding worden bedoeld.*
2 *Waar in deze notitie gesproken wordt over medewerker, wordt ook vrijwilliger/ stagiaire of contractant bedoeld*
3*Een aantal bepalingen uit dit wetsvoorstel treden pas na drie jaar in werking. Dit betreft de eis van gespecificeerde toestemming (artikel 15a, tweede lid), de registratie van de gespecificeerde toestemming (artikel 15c, tweede lid), het recht op elektronische inzage en afschrift (artikel 15d) en het recht op een elektronisch afschrift van de logging (artikel 15e). Daarnaast zal de minister de verplichting om toestemming te vragen voor het raadplegen van gegevens (artikel 15b), helemaal niet in werking laten treden.*

overleden personen of van organisaties geen persoonsgegevens zijn.

Een gegeven is een persoonsgegeven zodra het informatie verschaft over iemand waardoor de privacy in het geding kan komen. Persoonsgegevens zijn privacygevoelig omdat deze gegevens betreffen van de cliënt die direct of indirect betrekking hebben op de privé-situatie, lichamelijke, geestelijke en sociale gesteldheid.

Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook geboortedatum, geslacht, telefoonnummers en postcodes met huisnummers zijn persoonsgegevens.

Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

Bijzondere persoonsgegevens zijn:
•Godsdienst of levensovertuiging;
•Ras;
•Politieke voorkeur/ gezindheid;
• Burgerservicenummer (Bsn-nummer);
•Seksuele leven;
•Gegevens over iemands gezondheid;
•Lidmaatschap van een vakvereniging/ vakbond;
•Strafrechtelijk verleden;
•Gezondheid;
•Persoonsgegevens over onrechtmatig of hinderlijk handelen waarvoor een verbod is opgelegd.

Medische gegevens: gegevens over de behandeling van een patiënt.

Zorggegevens: gegevens over de zorgverlening aan een cliënt.

3. Algemene Privacy Richtlijnen Raphaëlstichting

3.1. Algemeen Privacy respecteren (werken of niet werken met persoonsgegevens)

Algemeen geldt het volgende:

- We delen geen privacy gevoelige informatie over of van de Raphaëlstichting, haar medewerkers en haar cliënten met derden.
- We verwerken geen persoonlijke gegevens zonder omschreven doel, dat niet strijdig is met wet- en regelgeving.
- Indien er gebruik gemaakt wordt van de fax, printer dan wel e-mail mogen gegevens niet onbeheerd ter inzage liggen voor onbevoegde anderen.
- Indien een computer onbeheerd achtergelaten wordt, dient er gebruik gemaakt te worden van de beveiligingscode. Bij verlaten van de werkplek wordt de computer dus gelocked (clear screen).
- Kasten, bureaus en kamers waarin zich privacy gevoelige informatie bevindt, dienen bij afwezigheid afgesloten te zijn. Aan het einde van de werkdag worden gegevensdragers (papier en digitaal) opgeborgen (clean desk).
- Gasten / bezoekers of mensen zonder duidelijke bedoeling aanspreken “Kan ik u misschien helpen / heeft u een afpsraak?”.
- Bij het testen van applicaties worden nooit gegevens van bestaande mensen gebruikt (tenzij geanonimiseerd).
- We bespreken in openbare ruimtes geen cliënten of personen (ook niet in een telefoongesprek). Stoom afblazen mag, maar wel met de deur dicht!
- We respecteren intellectuele eigendomsrechten van gebruikte software (geen illegale software).
- We printen geen documenten met vertrouwelijke gegevens tenzij absoluut noodzakelijk.
- Privacygevoelige documenten die niet meer nodig zijn worden versnipperd. We gebruiken een papierversnipperaar bij verwijdering vertrouwelijke documenten.
- Documenten die persoonsgegevens bevatten mogen alleen worden gemaild indien vergrendeld/ beveiligd met een wachtwoord. Het wachtwoord wordt telefonisch door gegeven.
- Bij het versturen van emails buiten de instelling, de email-adressen bij voorkeur opnemen in de bcc. Bij voorkeur geen privé email-adressen gebruiken.
- Bij voorkeur geen gedeelde accounts gebruiken. Als er wel met een gedeelde accout wordt gewerkt

gebruikt en er wordt een download gemaakt, dan eraan denken om de map downloads leeg te maken voor het afsluiten van de computer.
- Nieuwe personeelsleden die persoonsgegevens verwerken dienen een verklaring omtrent het gedrag overleggen. Dit geldt ook voor medewerkers van externe partijen die toegang hebben tot de persoonsgegevens van de RS.
- Er wordt een bewerkersovereenkomst ondertekend met derden die persoonsgegevens van de RS bewerken.

3.2. Richtlijnen voor het omgaan met persoonsgegevens cliënten

Persoonsgegevens zijn privacygevoelig omdat deze gegevens betreffen van de cliënt die direct of indirect betrekking hebben op de privé-situatie, lichamelijke, geestelijke en sociale gesteldheid.
Met betrekking tot bovenstaande gelden afspraken met betrekking tot het omgaan met de persoonsgegevens van de cliënt:
- Iedere medewerker heeft een beroepsgeheim, welke dient te worden nageleefd (zie CAO).
- Dossiers mogen in principe niet worden meegenomen buiten de (woon)groepen of kantoren tenzij de werkzaamheden dit noodzakelijk maken. Tijdens vervoer en meenemen in de thuis-/cliëntsituatie van persoonsgegevens zorgt de medewerker ervoor dat de gegevens niet zichtbaar dan wel toegankelijk zijn voor derden.
- Het dossier mag worden ingezien door de cliënt en zijn (wettelijke) vertegenwoordiger. Wordt aan (wettelijke) vertegenwoordigers van cliënten inzage verleend dan is hierbij de persoonlijk begeleider aanwezig zodat uitleg of informatie kan worden gegeven.
- Dossiers mogen alleen worden ingezien door medewerkers die bij de zorgverlening zijn betrokken. Met andere woorden, alleen teamleden, werkzaam in de betreffende woonvorm of team, medewerkers belast met behandeling. Voor anderen (stagiaires) moet toestemming aan de cliënt worden gevraagd.
- In het kader van de privacywetgeving is het dossier verder alleen in te zien voor medewerkers belast met interne audits of een controletaak in het kader van de regeling administratieve organisatie/interne controle AO/IC tenzij de cliënt geen machtiging hiertoe heeft verleend. Deze inzage gebeurt dan vanuit gerichte vraagstelling. Indien derden (bv accountants, externe auditoren, Inspectie, zorgkantoor) inzage willen in de dossiers dient hiervoor het machtigingsformulier te zijn ondertekend.
- De centrale cliëntenadministratie heeft, voor zover dit voor het verrichten van de werkzaamheden noodzakelijk is, toegang tot het administratieve deel van de dossiers.
- Vrijwilligers en stagiaires hebben in principe geen inzage tenzij er toestemming is van de cliënt.
- Bewaartermijnen moeten in acht worden genomen: Zie onder bewaartermijnen en verantwoordelijke functionarissen hieronder.

<u>Rechten van de cliënt/ wettelijk vertegenwoordiger</u>
Hij/zij geeft:
-nadrukkelijke toestemming voor verwerking, opvragen, vertrekken of doorgeven van persoonsgegevens.
Hij/zij heeft:
-het recht op informatie: te weten op welke wijze persoonsgegevens worden geregistreerd. Het recht te weten of gegevens bij derden worden opgevraagd, het recht te weten welke gegevens door derden worden verstrekt, het recht te weten of gegevens worden doorgegeven aan derden;
-het recht te weten wat er geregistreerd staat over haar/hem (inzagerecht/ AVG art 15);
-het recht op rectificatie en aanvulling gegevens te verbeteren en/of te verwijderen (AVG art 16) (correctierecht) (zie ook hoofdstuk 4.1);
-Het recht om bezwaar te maken tegen de gegevensverwerking;
-Het recht op beperking van de verwerking (art 18 AVG): Het recht om minder gegevens te laten verwerken. Bv gegevens zijn mogelijk onjuist, verwerking is onrechtmatig, gegevens zijn niet meer nodig, betrokkene maakt bezwaar).
-het recht op vergetelheid (art 17 AVG); Dit recht houdt in dat organisaties in een aantal gevallen persoonsgegevens moeten wissen als een betrokkene (diegene van wie de organisatie gegevens verwerkt) erom vraagt.
De WGBO gaat in beginsel uit van een bewaartermijn van 15 jaar na beëindiging van de behandeling.
Op verzoek van een wilsbekwame cliënt kan eerder tot vernietiging worden overgegaan. Langer bewaren is toegestaan vanuit goed hulpverlenerschap/zorgverlenerschap maar alleen bij:
-langlopende behandeling; als er de verwachting is dat een cliënt na beëindiging van de behandeling

later weer onder behandeling stelt en wanneer de huidige behandeling belangrijke informatie bevat voor mogelijk opvolgende behandelingen zoals erfelijkheidsinformatie.

-als er een concrete klachtprocedure loopt tegen de hulp/zorgverlener.

Vanuit verantwoording van financiële administratie geldt (o.a. Belastingwetgeving; 7 jaar bewaartermijn) dat een zorgaanbieder/hulpverlener verplicht is om herleidbaar (mogelijk tot Ondersteuningsplan) de behandeling te kunnen aantonen. Dit betekent dat er altijd gegevens van clienten verplicht aanwezig (moeten) blijven.

-Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.Sommige organisaties nemen een besluit op basis van automatisch verwerkte gegevens. Dit gebeurt bijvoorbeeld bij profilering. De Algemene verordening gegevensbescherming (AVG) geeft mensen recht op een menselijke blik bij besluiten die over hen gaan.
Voorbeelden zijn de automatische weigering van een online ingediende kredietaanvraag of verwerking van sollicitaties via internet zonder menselijke tussenkomst.

-Het recht op dataportabiliteit (art 20 AVG). Het recht om persoonsgegevens over te dragen (NIEUW). Het houdt in dat mensen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft.
Zo kunnen zij hun gegevens bijvoorbeeld makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst. Ook kunnen mensen vragen om gegevens rechtstreeks over te dragen aan een andere organisatie.

Hij/zij is:
-op de hoogte van de mogelijkheid van informatieoverdracht aan derden waarbij geen toestemming is vereist van betreffende cliënt.

<u>Bewaartermijnen en verantwoordelijk functionarissen</u>

- In beginsel worden stukken niet langer bewaard dan nodig is. De vraag is steeds of de persoonsgegevens nog ter zake zijn.
- We verwijderen en vernietigen dus de informatie over cliënten die naar het redelijk inzicht van de eindverantwoordelijke voor de betreffende registratie/het betreffende dossier overbodig of achterhaald is.
- Verwijdering blijft achterwege wanneer redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede wanneer bewaring op grond van wettelijk voorschrift vereist is of wanneer daarover tussen de betrokkene en de verantwoordelijke overeenstemming bestaat.
- De verantwoordelijke stelt vast hoe lang de opgenomen persoonsgegevens bewaard moeten blijven.
  - Medische- en zorggegevens worden vijftien jaar bewaard. De bewaartermijn voor *medische gegevens* is in beginsel 15 jaren (WGBO 1-4-2005), te rekenen vanaf het tijdstip waarop zij zijn vervaardigd, of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener c.q. de verantwoordelijke voortvloeit. Dossiers van cliënten die uit zorg zijn gegaan - inclusief het ondersteuningsplan - moeten minimaal 15 jaar na het uit zorg gaan bewaard blijven.
  - *Gegevens in het kader van de Wet BOPZ* dienen vijf jaar na dato van vervaardiging of beëindiging van behandeling te worden bewaard of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.
  - *Gegevens van niet-medische aard worden vijf jaar bewaard. Gegevens van niet medische aard* worden niet langer bewaard dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij zijn verzameld of verwerkt, tenzij ze geanonimiseerd zijn of voor zover ze uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden bewaard.
- Als een instelling buiten de Raphaëlstichting *alle* zorg voor een cliënt (definitief) overneemt, dragen we - na verkregen toestemming van de cliënt/diens wettelijke vertegenwoordiger – een kopie van het het (geschoonde) dossier over aan deze instelling. Het originele dossier wordt bewaard tot de wettelijke bewaartermijn verstreken is. De instellingsleider treft voor de bewaring in een archief de nodige voorzieningen.
- Ten slotte: informatie uit een dossier kan van groot belang zijn voor het bewaren van de levensgeschiedenis van een cliënt. Het is de taak van de persoonlijk begeleider om dergelijk materiaal veilig te stellen, ook als daar geen zorgverlenend doel meer mee wordt gediend. Bedenk dat ook als het dossier dun is, dat niet betekent dat ook het leven van de cliënt dun is geweest!

Verantwoordelijkheden betrokken functionarissen

- (Huis)artsen zijn verantwoordelijk voor het hanteren van de bewaartermijn van de medische dossiers.
- BOPZ-artsen en BOPZ verantwoordelijken zijn verantwoordelijk voor het hanteren van de bewaartermijnen van de BOPZ-gegevens.
- Instellingsleiders zijn verantwoordelijk voor het hanteren van de bewaartermijnen van de dossiers van cliënten en cliënten die uit zorg zijn gegaan. Na het verstrijken van de bewaartermijn zorgt de instellingsleider voor vernietiging van de gegevens uit het dossier die niet langer bewaard behoeven te worden.

Informatie persoonsgegevens voor uitstapjes
Soms is het met het oog op de veiligheid en gezondheid van cliënten noodzakelijk om bij buitenactiviteiten persoonsgegevens bij de hand te hebben. Denk bijvoorbeeld aan instructies hoe te handelen bij een epileptisch insult, informatie over allergieën, medicatiegebruik, etc. We zullen dan steeds een afweging moeten maken tussen het risico dat voortvloeit uit het meeslepen van informatie en het nadeel dat voor de cliënt kan ontstaan als die calamiteiteninformatie niet steeds onder handbereik is. Uiteraard is extra alertheid geboden als dergelijke gegevens meegaan naar bijvoorbeeld het zwembad, op vakantie, bij uitstapjes, etc.

3.3. Privacy afspraken/ richtlijnen medewerkers

Gegevens van sollicitanten
De toekomstige werkgever mag alleen vragen stellen aan een sollicitant over aspecten die voor de functie en/of voor de functievervulling relevant zijn, zoals vakbekwaamheid (opleiding, kennis en ervaring). De van de sollicitanten verkregen informatie dient de werkgever vertrouwelijk en zorgvuldig te behandelen. Als de werkgever inlichtingen of strafrechtelijke gegevens over de sollicitant wil inwinnen bij derden, moet hij hiertoe vooraf toestemming voor vragen. De beoogde informatie moet direct verband houden met de te vervullen vacature en mag geen onevenredige inbreuk maken op de persoonlijke levenssfeer van de sollicitant. Resultaten van een psychologische test of de uitslag van een medische keuring mogen alleen na toestemming van de sollicitant aan de werkgever, de opdrachtgever, verstrekt worden.
<u>Bewaartermijn</u>
Op de gegevensverzamelingen is de bewaartermijn telkens vermeld. Hieronder wordt de algemene richtlijn genoemd:

- Vijf jaar na einde dienstverband moeten de persoonsgegevens worden verwijderd tenzij langer bewaren noodzakelijk is ter voldoening aan een wettelijke bewaarplicht.

- Zeven jaar voor zogenoemde fiscale basisgegevens:
  - het grootboek
  - de debiteuren- en crediteurenadministratie
  - de in- en verkoopadministratie
  - de voorraadadministratie
  - de loonadministratie

- Loonbelastingverklaringen, kopieën van het identiteitsbewijs en bijlagen studenten- en scholierenregeling moeten tenminste vijf volle kalenderjaren na het einde van de dienstbetrekking bewaard worden. Deze termijn geldt ook voor loonbelastingverklaringen die zijn vervangen door nieuwe.
- Zaken met betrekking tot werknemersverzekeringen, UWV, dienen minimaal 10 jaar bewaard te worden.
- PFZW-(Pensioenfonds Zorg en Welzijn) zaken dient 7 jaar bewaard te worden.

<u>Verwijderen gegevens sollicitanten</u>
Al deze gegevens moeten uiterlijk vier weken nadat de sollicitatieprocedure is beëindigd, verwijderd worden. Wel kan de sollicitant toestemming geven om de gegevens tot maximaal een jaar te bewaren, bijvoorbeeld omdat er op een later tijdstip een functie beschikbaar komt.

***Gegevens van m*edewerkers**
Afspraken met betrekking tot het omgaan met de persoonsgegevens van de medewerker:

- Personeelsdossiers mogen alleen worden ingezien door de betrokken medewerker zelf, medewerkers van de M&O afdeling van de instelling of direct leidinggevenden. Voor anderen moet toestemming aan de medewerker worden gevraagd.

- De medewerker heeft recht op informatie over, inzage in, aanvulling, verbetering, verwijdering en afscherming van zijn persoonsgegevens. Daarnaast kan de medewerker klagen bij de werkgever als de medewerker meent dat de werkgever de persoonsgegevens ten onrechte aan een ander heeft verstrekt.
- Voor het verstrekken van personeelsgegevens aan een andere organisatie voor direct marketing doeleinden is toestemming van de medewerkers nodig. Het ligt immers niet voor de hand om personeelsgegevens voor dit doeleinde te gebruiken. Soms vraagt een organisatie een werkgever reclamepost te verzenden aan de medewerkers, bijvoorbeeld voor het afsluiten van een voordelige ziektekostenverzekering. Een werkgever kan dit namens een organisatie doen waardoor hij geen personeelsgegevens hoeft te verstrekken. In dat geval is het verstandig om de medewerkers vooraf op de hoogte te stellen en de mogelijkheid te bieden om bezwaar te maken. Zo zorgt de werkgever ervoor dat alleen geïnteresseerde medewerkers reclamepost ontvangen. Als een werkgever van plan is om vaker reclamepost te verzenden, dan heeft hij hiervoor toestemming van de ondernemingsraad (OR) nodig.

<u>Verstrekken persoonsgegevens medewerkers mag bij:</u>
Uitvoeren van een overeenkomst
Gegevens kunnen worden verstrekt aan derden indien dit noodzakelijk is voor de uitvoering van een overeenkomst (uw arbeidscontract) die u met uw medewerker heeft of gaat sluiten. In dit geval wordt ervan uitgegaan dat de medewerker bij het sluiten van de overeenkomst zich ervan bewust bent dat er bepaalde gegevens moeten worden verstrekt.

Wettelijke verplichting
U kan verplicht zijn om bepaalde persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van een wettelijke plicht. U bent bijvoorbeeld op grond van artikel 47 van de Algemene wet inzake rijksbelastingen verplicht om de fiscus te voorzien van alle gegevens die van belang kunnen zijn voor de belastingheffing. Ook bent u op grond van een bevel van de rechter-commissaris in strafzaken verplicht bepaalde persoonsgegevens van een verdachte medewerker te verstrekken.

Toestemming
De toestemming van de medewerker is ook een grondslag waarop u de personeelsgegevens mag verstrekken aan een andere organisatie. Deze toestemming kan echter op elk moment door de medewerker worden ingetrokken. Daarmee vervalt de grondslag van de verstrekking en is de verstrekking onrechtmatig. Instemming van de ondernemingsraad voor een bepaalde verstrekking vervangt de individuele toestemming niet. Als u toestemming vraagt, moet u de medewerker duidelijk uitleggen waar u toestemming voor vraagt en wat de gevolgen zijn van het geven van toestemming. Voorbeelden van gevallen waarin u toestemming moet vragen: het publiceren van de geïndividualiseerde productiecijfers op het (interne) netwerk of prikbord en het publiceren van een smoelenboek met de foto's van de medewerkers.
U mag personeelsgegevens gebruiken voor een ander doel dan waarvoor ze zijn verkregen. Dit mag alleen als dat verenigbaar is met het oorspronkelijke doel. Of dat het geval is, hangt af van de concrete omstandigheden. Als de medewerker toestemming heeft gegeven, zal verstrekking vrijwel steeds verenigbaar zijn met het doel van verkrijging. Als de medewerker goede redenen heeft om uw gegevens geheim te willen houden, dient u dit te respecteren.

<u>Rol van de ondernemingsraad</u>
Artikel 27 van de Wet op de ondernemingsraden geeft een opsomming wanneer de OR instemmingsrecht heeft. De OR heeft bijvoorbeeld instemmingsrecht bij het gebruik van personeelsvolgsystemen of bij voorgenomen verstrekkingen van personeelsgegevens. De autoriteit Persoonsgegevens heeft een lijst opgesteld met een aantal toetspunten voor de OR.

3.4.Overige aspecten

- Privacybescherming schuilt niet alleen in regelingen en werkinstructies, maar ook in privacybewustzijn van mensen die met gevoelige informatie werken.
- Praat niet bij de koffietafel of soortgelijke gelegenheden over cliënten, vertegenwoordigers of problemen die u met hen ervaart. Stoom afblazen mag, maar wel met de deur dicht!
- Niet alles waar een naam van een medewerker of cliënt in wordt genoemd is per definitie privacygevoelig.
- Het zorgvuldig (doen) vernietigen van (kopieën) van vertrouwelijke stukken blijft een aandachtspunt. Bij het gewone oud papier zitten soms stukken die met recht als privacygevoelig aan te merken zijn. Privacygevoelige informatie dient versnipperd te worden.

Ten slotte
De geest van deze procedure is daarom minstens zo belangrijk als de letter.

- Privacybescherming schuilt niet alleen in regelingen en werkinstructies, maar ook in privacybewustzijn van mensen die met gevoelige informatie werken.
- Het zorgvuldig (doen) vernietigen van (kopieën) van vertrouwelijke stukken blijft een aandachtspunt. Bij het gewone oud papier zitten soms stukken die met recht als privacygevoelig aan te merken zijn. Privacygevoelige informatie dient versnipperd te worden.
- We proberen binnen de kaders van de wet een hanteerbaar evenwicht te bewaren tussen:
  * 'wie wat bewaart die heeft wat' en 'opgeruimd staat netjes'
  * 'need to know' en 'respect voor privacy'.
- Veilige werkplek (clean desk en clear screen)
  - Bij verlaten van de werkplek wordt de computer gelocked (clear screen)
  - Aan het einde van de werkdag worden gegevensdragers (papier en digitaal) opgeborgen (clean desk).

4. Richtlijnen gegevensverwerking Raphaëlstichting

4 1. Richtlijnen gegevensverwerking

Met verwerken wordt bedoeld alle handelingen met persoonsgegevens vanaf het verzamelen tot aan het vernietigen. Dat wil zeggen elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens; hieronder vallen in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken van persoonsgegevens door middel van doorzending, verspreiding of enige andere vorm van het terbeschikkingstelling, alsmede het met elkaar in verband brengen, afschermen, uitwissen of vernietigen van de gegevens.

Reikwijdte

Deze richtlijnen hebben betrekking op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet-geautomatiseerde verwerking van persoonsgegevens, die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Voorwaarden voor het verwerken zijn:
a. Zorgvuldige verwerking
b. Verwerker dient na te gaan of er sprake is van informatieplicht
c. Inzagerecht/ correctierecht
d. Recht van verzet
e. Bewaartermijn
f. Verstrekken alleen onder bepaalde voorwaarden zoals bv wetgeving
g. Afdoende beveiligd
Deze voorwaarden worden hieronder verder uitgewerkt.

a. Zorgvuldig
Een gegevensverwerking dient in overeenstemming met de wet, behoorlijk en zorgvuldig te geschieden. De persoonsgegevens moeten verzameld zijn voor welbepaalde uitdrukkelijk in de gegevensverzamelingen omschreven en gerechtvaardigde doeleinden. Vervolgens moet de verwerking een rechtmatige grondslag hebben en mag niet onverenigbaar zijn met het doel waarvoor de instelling de gegevens heeft verzameld. In het onderzoek dat hieraan is vooraf gegaan zijn de grondslagen van de verwerkingen onderzocht en goed bevonden. Ook zal men moeten controleren of de verwerking niet bovenmatig is ten opzichte van het te dienen doel.

b. Verwerker dient na te gaan of er sprake is van informatieplicht
Een persoon wiens gegevens worden verwerkt, moet kunnen nagaan wat er met die gegevens gebeurt. De betrokkene moet door de instelling worden geïnformeerd over welke gegevens er over hem/haar worden verzameld, wat het doel is, hoe met de gegevens wordt om gegaan en aan wie de gegevens buiten de instelling worden verstrekt.

De informatieverstrekking, kan zowel mondeling als schriftelijk geschieden, maar moet in ieder geval vermelden:

- Wie de instelling is die de gegevens verwerkt;
- Voor welk doel of doeleinden de instelling de gegevens verzamelt en verwerkt.

De instelling moet hiernaast nadere informatie verschaffen als dat tegenover de betrokkene nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen. De instelling moet daarbij rekening houden met de aard van de gegevens, de omstandigheden waaronder de instelling deze heeft verkregen en het gebruik dat de instelling ervan gaat maken. Hoe gevoeliger de gegevens die de instelling verwerkt voor de betrokkene liggen, hoe meer reden er is om de betrokkene gedetailleerd te informeren over de gegevensverwerking.

Via betrokkene
Als de instelling de gegevens bij de betrokkene zelf verkrijgt, moet de instelling de betrokkene vòòr de verkrijging informeren. Van verkrijging bij de betrokkene zelf is bijvoorbeeld sprake wanneer hij of zij op een formulier persoonsgegevens invult en dit formulier aan de instelling toezendt. De instelling kan de informatie, wie de instelling is en voor welk doel, dan bijvoorbeeld op het formulier opnemen.

Buiten de betrokkene om
Bij verkrijging buiten de betrokkene om moet de instelling hem of haar informeren op het moment dat de instelling de gegevens vastlegtof als de instelling de gegevens uitsluitend verzamelt om deze aan een derde te verstrekken, uiterlijk op het moment van eerste verstrekking aan die derde.

Hoe?
De instelling moet de informatie op zodanige wijze verstrekken dat de betrokkene er daadwerkelijk de beschikking over krijgt. Een algemene verwijzing naar elders verkrijgbare informatie is dus niet voldoende. Wanneer de instelling de gegevens van de betrokkene zelf verkrijgt, kan de instelling bijvoorbeeld de informatie opnemen op het formulier waarop de betrokkene de gegevens verstrekt.
Als de instelling de gegevens via een andere weg verkrijgt moet de instelling bij een beperkt aantal betrokkenen allen informeren. Gaat het om een hele groep, dan mag de instelling volstaan met een algemenere vorm van informatieverstrekking.
De instelling hoeft niet te informeren als er sprake is van wettelijke plicht of als er zeer tijdrovende inspanning geleverd moet worden om het adres van de betrokkene te achterhalen.
Er bestaat geen informatieplicht als de betrokkene al op de hoogte is van de identiteit van degene die de gegevens verzamelt en de doelen van de verwerking.

c. Inzagerecht/ correctierecht
Wanneer inzage?
Iedereen mag met redelijke tussenpozen (schriftelijk) bij de verantwoordelijke medewerker vragen of, en zo ja, welke persoonsgegevens de instelling ten aanzien van hem verwerkt. De verantwoordelijke medewerker dient aan dit verzoek tot inzage en/of het gevraagde afschrift zo spoedig mogelijk doch uiterlijk binnen 4 weken te voldoen. Als de betrokkene de instelling buitensporig vaak met een dergelijk verzoek benadert, hoef de instelling daaraan geen gehoor te geven.

Het antwoord moet schriftelijk zijn, tenzij een gewichtig belang van de betrokkene vergt dat de instelling een andere vorm kiest, bijvoorbeeld mondeling. Een mogelijk beperkende grond voor inzage of afschrift kunnen gewichtige belangen zijn van anderen dan de verzoeker.
Voor de verstrekking van een afschrift mag een redelijke vergoeding in rekening worden gebracht.

Wanneer corrigeren?
De betrokkene mag de instelling verzoeken zijn gegevens te corrigeren. De instelling is alleen verplicht te corrigeren als:
- de gegevens feitelijk onjuist zijn onvolledig of niet ter zake dienend zijn voor het doel (zie gegevensverzameling) waarvoor de instelling ze verwerkt;
- de gegevens op een andere wijze, in strijd met de privacywetgeving of een andere wet,zijn verwerkt.

Correctie houdt in verbeteren, aanvullen, verwijderen, afschermen of op een andere manier er voor zorgen dat de instelling de onjuiste gegevens niet langer gebruikt.

De instelling moet binnen vier weken schriftelijk aangeven of en in hoeverre de instelling aan het correctieverzoek zal voldoen.
In geval van correctie van de gegevens moet de instelling derden aan wie de instelling de onjuiste gegevens van de betrokkene eerder heeft verstrekt, van de wijzigingen op de hoogte stellen. Dit hoeft de instelling niet te doen als het onmogelijk is om die derden op te sporen of als de instelling daartoe een onevenredige inspanning zou moeten leveren.

d. Recht van verzet/ recht om te verwijderen (vergetelheid)
De betrokkene kan in een aantal gevallen bezwaar maken tegen een gegevensverwerking. De privacywetgeving noemt dit het recht van verzet.
De betrokkene kan tegen een verwerking verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden. De instelling moet als verantwoordelijke binnen vier weken na ontvangst van het verzet beoordelen of het verzet terecht is. Is dat het geval, dan moet de instelling de verwerking onmiddellijk beëindigen.
Dit kan niet in de volgende situaties:
-is de gegevensverwerking noodzakelijk voor de goede vervulling van een door de instelling of door een ander bestuursorgaan verrichte publiekrechtelijke taak, of;
- voor een gerechtvaardigd belang van de instelling (de verantwoordelijke) of een derde.
De betrokkene heeft ook recht op verzet als het verwerken van zijn persoonsgegevens geschiedt voor direct marketingdoeleinden. In dit geval moet de instelling de desbetreffende verwerking onmiddellijk beëindigen.

Wanneer niet verwijderen?
Aan het verzoek tot vernietiging kan niet voldaan kan worden als op basis van de professionele inschatting er een verwachting is dat een cliënt na beëindiging van de behandeling later weer onder behandeling komt. Dit moet dan wel goed gemotiveerd worden / zijn. Anders geldt m.i. artikel 455 (WGBO/burgerlijk wetboek).
Bewaren vanuit goed hulp/zorgverlener geldt alleen maar bij:

· Langlopende behandeling; als er de verwachting is dat een cliënt na beëindiging van de behandeling later weer onder behandeling stelt en wanneer de huidige behandeling belangrijke informatie bevat voor mogelijk opvolgende behandelingen zoals erfelijkheidsinformatie.
· Als er een concrete klachtprocedure loopt tegen de hulp/zorgverlener.

e. Bewaartermijn
De instelling mag persoonsgegevens niet langer bewaren dan noodzakelijk is voor het doel waarvoor de instelling de gegevens verzamelt of (verder) verwerkt. Hoelang de instelling de gegevens feitelijk mag bewaren, hangt af van het doel waarvoor de instelling de gegevens heeft verzameld en verder verwerkt. Dit kan per situatie verschillen: er is niet een vaste bewaartermijn.
De WGBO gaat in beginsel uit van een bewaartermijn van 15 jaar na beëindiging van de behandeling.
De instelling mag persoonsgegevens langer bewaren als dat gebeurt voor historische, statistische of wetenschappelijke doeleinden.

f. Verstrekken alleen onder bepaalde voorwaarden
Belangrijkste grondslagen voor het verstrekken van persoonsgegevens.
De instelling mag de gegevens verstrekken aan derden met name als het noodzakelijk is voor de uitvoering van een overeenkomst die de instelling met derden heeft of gaat afsluiten of als de instelling de gegevens moet verstrekken op grond van een wettelijk voorschrift of als de medewerker/ cliënt(vertegenwoordiger) ondubbelzinnige toestemming heeft gegeven.
Aan welke partijen kunnen telefoonnummers en/of adressen verstrekt worden?
Er is een verschil tussen het structureel of incidenteel verstrekken van gegevens. De partijen waar persoonsgegevens aan kunnen worden verstrekt, zijn op de gegevensverzamelingen genoemd. Partijen die niet zijn genoemd en incidenteel informatie opvragen, kunnen op de volgende manieren bediend worden:

- De instelling kan aan betrokkene het telefoonnummer of adres van de opvrager van persoonsgegevens geven zodat deze zelf de opvrager kan benaderen.
- In de gegevensverzamelingen wordt voorts aangegeven wie toestemming voor gebruik heeft. Voor een instantie of persoon zonder toestemming voor gebruik dient hiervoor toestemming gevraagd te worden. In noodgevallen kan door de beheerder toestemming worden gegeven, ook bij een twijfelgeval.
- Wanneer de persoonsgegevens, inclusief gegevens met betrekking tot iemands gezondheid, door derden bv de gemeente worden opgevraagd in het kader van de taken ten aanzien van de maatschappelijke ondersteuning (waaronder bijvoorbeeld het onderzoek naar de noodzaak van de (maatwerk)voorziening of in verband met een heroverweging van die noodzaak), is hiervoor eerst ondubbelzinnige toestemming van de cliënt of diens vertegenwoordiger vereist. Ondubbelzinnige toestemming houdt in expliciete toestemming voor het verstrekken van concreet benoemde gegevens. Als de gemeente rechtmatig om de gegevens vraagt, bestaat dat risico niet, omdat de wet voorschrijft dat de zorgaanbieder in dat geval verplicht is om mee te werken.

g. Beveiliging
De gegevensverzameling dient afdoende te zijn beveiligd.

4.2. Informatiebeveiliging

De instelling moet passende technische en organisatorische maatregelen nemen om het verlies van gegevens of onrechtmatige verwerking tegen te gaan.
-De technische en organisatorische maatregelen die de instelling neemt, moeten een passend beveiligingsniveau garanderen en de risico's van de verwerking en de aard van de te beschermen gegevensverwerking moet rekening houden met de stand van de techniek en de kosten van de maatregelen. De technische en organisatorische maatregelen moeten er mede op gericht zijn onnodige verzameling of verdere verwerking te voorkomen. Dit is uitbesteed aan een externe partij.
-Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt. Daarvoor is beleid vast gesteld dat aangeeft welke eisen er worden gesteld aan de informatiebeveiliging in het algemeen en aan de beveiliging van persoonsgegevens in het bijzonder. Binnen de organisatie is de werkgroep informatiebeveiliging en de security officer belast met de implementatie van dit beleid. Ook wordt gecontroleerd middels (interne) audits of de maatregelen door de medewerkers worden nageleefd.
Naast het beleid informatiebeveiliging voor de lange termijn is er ook een aantal procedures en werkinstructies/ richtlijnen voor de dagelijkse praktijk.
-De verantwoordelijkheden voor de informatiebeveiliging en gegevensverwerking zijn vastgelegd.
-Het bewustzijn van medewerkers op elk niveau binnen de organisatie over de noodzaak van beveiliging en van de zorgvuldige verwerking van persoonsgegevens, is de belangrijkste voorwaarde om een stelsel van algemene maatregelen en procedures voor beveiliging effectief te laten functioneren. Beveiliging heeft geen effect als deze alleen maar op papier bestaat. De beveiligingsmaatregelen zullen daadwerkelijk door de medewerkers moeten worden uitgevoerd en alle medewerkers moeten hun bijdrage daaraan leveren.

4.3. Melden van afwijkingen, (bijna-) overtredingen en incidenten: Werkwijze voor medewerkers (zie ook werkinstructie datalek):

-Medewerkers melden (vermoeden van) overschrijden informatiebeveiligingsrichtlijnen via het meldformulier ‘Datalek’ op Kristal onder formulieren.
-Meldplicht
Iedereen die een geval van fraude, misleiding of onrechtmatig gedrag ontdekt of vermoedt, is verplicht dit onmiddellijk te melden. Overtredingen of incidenten meld je direct bij de Security Officer. Zie procedure ‘Datalek’. De Security Officer zorgt voor de vastlegging, afwikkeling en evaluatie. Het bestuur is verantwoordelijk voor de communicatie met externe partijen bij incidenten en calamiteiten. Noodgevallen en wettelijke bepalingen daargelaten.

4.4. Werkwijze: hoe omgaan met gegevensverzamelingen

Gegevens worden verwerkt zoals in de dataclassificatie voor cliënten en voor medewerkers is vastgelegd.
De activiteiten voor het omgaan met gegevensverzamelingen zijn:
- Informeren nieuwe cliënten en nieuwe medewerkers over privacy en het zorgvuldig omgaan met persoonsgegevens.
- Controle of nieuwe gegevensverzamelingen voldoen aan de bepalingen van de privacywetgeving en indien nodig melden bij de AP.
- Het uitvoeren van een drie-jaarlijkse toets of alle gegevensverzamelingen binnen de organisatie voldoen aan de bepalingen van de privacywetgeving.

Deze (hoofd)activiteiten worden hierna verder uitgewerkt.

1. Nieuwe cliënten en nieuwe medewerkers worden bij de aanvang van de dienstverlening (in zorg komen)/start arbeidscontract gewezen op:

-het feit dat de persoonsgegevens worden verzameld en behandeld conform de privacywetgeving.

-het recht op inzage en correctie van zijn persoonsgegevens.

1a. Elke cliënt heeft in de zorgovereenkomst getekend voor het feit dat zijn/ haar persoonsgegevens toegankelijk zijn voor medewerkers van de Raphaëlstichting in het kader van de zorg – en dienstverlening

1b. Elke medewerker/ vrijwilliger/ stagiair heeft geheimhoudingsplicht geregeld via de CAO, beroepsgroep of het (arbeids)contract.

2. Tijdens de dienstverlening

-Medewerkers gaan zorgvuldig om met de privacy van zowel cliënten als medewerkers conform de bovengenoemde privacy afspraken/ richtlijnen.

-Het geven van inzage op en correctie van opgenomen persoonsgegevens van betrokkene gebeurt door de verantwoordelijke medewerker conform de WPB.

-Gegevens bewaren volgens bovengenoemde privacy afspraken/ richtlijnen.

3. Bij het aanmaken van nieuwe geautomatiseerde gegevens bestanden dienen de onderstaande stappen (a t/m h) te worden doorlopen

a)Zijn er nieuwe gegevens opgesteld/ingericht?

b)Is de reikwijdte van de nieuwe gegevensverzameling vastgesteld? (heeft de gegevensverzameling betrekking op persoonsgegevens).

c)Indien de reikwijdte van de verzameling gegevens is vastgesteld en betrekking heeft op persoonsgegevens: heeft er een controle plaatsgevonden of kan worden volstaan met een bestaande gegevensverzameling? Zo ja dan die bestaande gegevensverzameling gebruiken.

d)Indien er sprake is van een volstrekt nieuwe gegevensverzameling en een nieuwe opzet vereist is: zijn de persoonsgegevens vastgelegd en is het doel omschreven?

e)Indien er sprake is van in punt d. genoemde situatie: wordt in deze nieuwe gegevensverzameling gebruik gemaakt van privacygevoelige informatie?

f) indien er sprake is van de in punt e. genoemde situatie: is de nieuwe gegevensverzameling getoetst aan de eisen die de privacywetgeving stelt? (rechtmatige grondslag, doel en actoren).

g) Indien vereist wordt een gegevensverzameling aangemeld bij het AP.

h) Eenmaal per 3 jaar inventariseert de kwaliteitscoördinator of alle gegevensverzamelingen binnen de organisatie voldoen aan de bepalingen van de AP.

4.5. Externe gegevensverzamelingen

Bij het ECD en andere applicaties worden de gegevensverzamelingen door een externe partij beheerd. Dat geldt ook voor de apotheek. Met deze partijen is een bewerkersovereenkomst afgesloten. Tevens dienen zij te voldoen aan de wet- en regelgeving en bij voorkeur NEN 7510 en ISAE 3402 gecertificeerd te zijn.

5. Bedrijfsmiddelen

Veiligheid en registratie door Raphaëlstichting
We loggen toegang tot kritische systemen voor beveiligingsdoeleinden. o.a. om aan te kunnen tonen wie wanneer welke toegang heeft gehad. Dit gebeurt alleen ter controle van bijvoorbeeld incidenten. Een verzoek tot inzage kan gedaan worden bij de Security Officer.

Veilig gebruik van bedrijfsmiddelen

- Toegangsbeveiliging middelen (laptops, telefoons, USB sticks e.d). Mocht gebruik van deze middelen gewenst zijn voor de uitvoering van de werkzaamheden dan in overleg met/na goedkeuring door helpdesk van I-care solutions (deze registreert het middel en zorgt voor veilige opslag en de verwijdering van (gegevens op) het middel Gebruik van USB sticks, cloudopslag of andere middelen, voorzover niet in eigendom of verstrekt door Raphaëlstichting is niet toegestaan.
- Gebruik geen USB sticks of andere verwijderbare media (SD cards, SSD's etc) voor opslag en transport van kritische informatie (tenzij in overleg met en middel goedgekeurd door helpdesk I-Care).
- Op telefoon en laptop staan intern vertrouwelijke gegevens van Raphaëlstichting wees je daarvan bewust en behandel deze ook zo (niet uitlenen, geen gebruik door kinderen, afsluiten en opbergen).
- Voorkom malware en virussen: Installeer geen onnodige niet werk gerelateerde software op de machines: check altijd met de helpdesk I-Care als je iets nieuws wilt installeren.

- Behandel de spullen van Raphaëlstichting als een goed huisvader en meldt diefstal en vermissing direct aan de Security Officer.
- Sluit de machine altijd helemaal af als je klaar ben met werken en je gaat verplaatsen (niet in de slaapstand maar echt uit).

Gebruik mail en internet

- Internet en Raphaëlstichting email voor niet-zakelijk verkeer is beperkt toegestaan, voorzover dit niet storend is voor de goede voortgang en kwantiteit van de dagelijkse werkzaamheden, dit ter beoordeling aan de directie.
- Geen bezoek aan websites waar mogelijk discriminerende, seksuele of criminele inhoud te vinden is.
- Wanneer een email wordt verstuurd naar meerdere personen, de namen van die personen in de bcc zetten. Om te voorkomen dat email adressen overal verspreid worden.
- Indien vertrouwelijke stukken gemaild worden (bv zorgplan naar vertegenwoordiger client of stukken met BSN-nummer) kan dit alleen wanneer het bestand is beveiligd met een wachtwoord. Het wachtwoord kan vervolgens doorgebeld of via de sms worden doorgegeven.

Gebruik Software

- We respecteren intellectuele eigendomsrechten en gebruiken geen illegale software of andere middelen zonder toestemming van de eigenaar.
- Ingeval van twijfel over de rechten of legaliteit van software: overleg met de Security Officer.

Wachtwoorden (gebruik veilige)

- Wachtwoorden schrijf je niet op, deel je niet met anderen (ook geen mensen die zich voordoen als ‘helpdesk, servicedesk’ etc.).
- Gebruikte wachtwoorden voor toegang tot Raphaëlstichting netwerk verschillen van je persoonlijke wachtwoord en zijn voldoende veilig (www.checkjewachtwoord.nl).
- Wachtwoordbeleid: Wachtwoordbeleid is in de maak (voor eind 2017) en gaat gehanteerd worden. Twee-weg authentificatie komt ook: dan heb je ook je telefoon nodig.

Toegangsbeheer (kantoortoegang)

- Medewerkers ontvangen een persoonlijke toegangspas/sleutel die strikt persoonlijke toegang verschaft (voorkom indringers, begeleidt meelopende bezoekers naar de receptie/gastheer of vrouw)
- Toegang is alleen toegestaan tijdens kantooruren of daarbuiten indien noodzakelijk voor werkzaamheden.
- Meldt verlies of diefstal van pas/sleutel direct.
- Je maakt geen kopieën van de sleutel/pas.
- Je levert de pas weer in bij de beëindiging van de werkzaamheden.

Toegang voor bezoekers van Raphaëlstichting

- Bezoekers worden ontvangen en naar de uitgang begeleid door de gastheer of vrouw.
- Bezoekers worden niet achtergelaten in ruimtes waar gegevens toegankelijk zijn (open kasten, niet afgesloten computers of verwijderbare media).

Social media (Zie PR-Gedragscode Social media-BEL.ALG-versie 01)
·Wees betrouwbaar op sociale media: respecteer privacy van anderen.
· Respecteer de privacy van bewoners, cliënten, deelnemers en je collega's en plaats nooit foto- of videomateriaal waar zij op staan op de sociale media waar je gebruik van maakt. Ook als je binnen je eigen persoonlijke netwerk werkgerelateerde berichten plaatst of reageert op berichten, besef dan dat je te allen tijde ook een medewerker, stagiaire of vrijwilliger van de Raphaëlstichting bent. Maak in een reactie altijd je rol binnen de Raphaëlstichting duidelijk.
· Reageer nooit anoniem of onder een schuilnaam.
· Betrouwbaarheid toon je door ook online respectvol met je collega’s, klanten of andere (zakelijke) relaties om te gaan.

Meldplicht:

- Afwijkingen en/ of incidenten geef de medewerker zo snel mogelijk door aan de security officer.

6. Verwijzingen

Zie ook de volgende documenten:
Informatiebeleidsplan Raphaëlstichting
Informatiebeveiligingsbeleid

Dossiervoering cliënten richtlijnen, werkinstructie
Privacy: Persoonsgegevens medewerkers: inventarisatie bestanden medewerkers.
Privacy: Persoonsgegevens cliënten: Inventarisatie bestanden cliënten
Privacy cliëntgegevens Werkinstructie zorgafdelingen VenV RSZ
Privacy-bewaarinstructie medisch dossier en zorgdossier RSZ.
Gedragscode Social media

Datalek procedure

Datalek Werkinstructie