Privacyreglement

- Patiënten, bezoekers en leveranciers

Voorwoord

Iedereen heeft recht op bescherming van zijn persoonlijke levenssfeer. Om die bescherming te waarborgen geeft de Algemene Verordening Gegevensbescherming (AVG) aan hoe we moeten omgaan met persoonsgegevens, wat de rechten zijn van degene van wie persoonsgegevens worden verwerkt en wat de plichten zijn van degene die met de gegevens werkt.

Met dit reglement willen we inzicht geven in de manier waarop wij binnen het Albert Schweitzer ziekenhuis omgaan met gegevensverwerking voor patiënten, bezoekers en leveranciers.

Waar het gaat om de patiënten is, naast de AVG, ook de Wet op de geneeskundige behandelingsovereenkomst (WGBO) van belang. Deze wet geeft uitwerking aan de positie van de patiënt bij uitwisseling van gegevens en aan het met de privacy samenhangende beroepsgeheim. In dit reglement zijn de algemene privacy bepalingen rondom gegevensverwerking opgenomen en de rechten en plichten van partijen.

Dit privacyreglement is vastgesteld door de Raad van Bestuur van het Albert Schweitzer ziekenhuis op 25 november 2021, gehoord hebbende het advies van het Medisch Specialisten Bestuur (11 november 2021), de Cliëntenraad (10 november 2021) en met inachtneming van de instemming van de Ondernemingsraad (9 november 2021).

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Privacy speelt een belangrijke rol in de relatie tussen de patiënt, bezoeker of leverancier aan de ene kant en het Albert Schweitzer ziekenhuis aan de andere kant. Het Albert Schweitzer ziekenhuis beschikt over en verwerkt iedere dag een grote hoeveelheid medische dossiers van patiënten. Het is van het grootste belang dat zorgvuldig met deze vertrouwelijke informatie wordt omgegaan en dat de privacy van de patiënten te allen tijde gewaarborgd blijft. Het respecteren en beschermen van de privacy en persoonsgegevens van de patiënt maakt ook onlosmakelijk onderdeel uit van het leveren van goede zorg.

1.2 Doelstelling en toepassingsgebied

Dit reglement stelt algemene regels op, die betrekking hebben op de manier hoe het Albert Schweitzer ziekenhuis dagelijks omgaat met persoonsgegevens en de privacy van zijn patiënten, bezoekers en leveranciers, en wat er wettelijk wel en niet verantwoord is. Dit reglement is van toepassing op het Albert Schweitzer ziekenhuis, statutair gevestigd te Dordrecht met als werkgebied Dordrecht, Zwijndrecht, Sliedrecht en omstreken, en heeft betrekking op alle door of vanwege het Albert Schweitzer ziekenhuis geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het beleid zal beheerd en geactualiseerd worden door juridische zaken en wordt jaarlijks geëvalueerd. Een actuele versie is beschikbaar is in het documentbeheersysteem en op de internet site van het ziekenhuis.

1.3 Opbouw

Het reglement is als volgt opgebouwd: na de introductie (Hoofdstuk 1) volgen in Hoofdstukken 2 en 3 een uiteenzetting van de algemene beginselen van de bescherming van persoonsgegevens, rechtmatigheid, bijzondere categorieën persoonsgegevens en rechten van betrokkenen. Vervolgens gaat Hoofdstuk 4 over verwerking van data door het Albert Schweitzer ziekenhuis en hoofdstuk 5 over het verwerkingsregister en verwerkers. Tenslotte gaat hoofdstuk 6 over informatiebeveiliging en overige maatregelen en hoofdstuk 7 over de functionaris gegevensbescherming.

Dit document is opgesteld in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene verordening gegevensbescherming en overige relevante wet- en regelgeving.

1.4 Begripsbepalingen

Autoriteit Persoonsgegevens (AP): de toezichthouder die tot taak heeft toe te zien op de verwerking van persoonlijke gegevens krachtens de AVG;

AVG: Algemene Verordening Gegevensbescherming**;**

Beveiliging. Het samenhangend stelsel van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;

Betrokkene: diegene op wie een persoonsgegeven betrekking heeft;

Curator: een door de rechter benoemde vertegenwoordiger van een patiënt. De curator neemt beslissingen over geld en goederen (financiële zaken) en over de verzorging, verpleging, behandeling en begeleiding van de betrokkene (persoonlijke verzorging).

Datalek: Melding van een inbreuk op de beveiliging van persoonsgegevens.

Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de verwerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de verwerker gemachtigd is om persoonsgegevens te verwerken;

Functionaris voor de gegevensbescherming (FG): De FG adviseert en houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG) binnen het Albert Schweitzer ziekenhuis.

Hulpverlener: De natuurlijke persoon of rechtspersoon die zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbend op de persoon van de opdrachtgever of van een bepaalde derde; i.c. het Albert Schweitzer ziekenhuis;

Identificeerbare gegevens: gegevens die zonder onevenredige tijd en moeite aan de betrokkene zijn te koppelen;

Individuele hulpverlener*:* De natuurlijke persoon die in de uitoefening van een geneeskundig beroep uitvoering geeft aan de geneeskundige behandelingsovereenkomst, gesloten tussen de hulpverlener en de patiënt; i.c. de behandelaar;

Information security officer (ISO): De information security officer coördineert het stelsel van technische en organisatorische maatregelen op de wijze als beschreven in het informatiebeveiligingsbeleid van het Albert Schweitzer ziekenhuis

Medewerker: alle personen die op basis van een arbeidsovereenkomst, uitzendovereenkomst, detacheringsovereenkomst, gastvrijheidsovereenkomst, stageovereenkomst, of vrijwilligersovereenkomst of als co-assistent werkzaamheden verrichten voor het Albert Schweitzer ziekenhuis. Waaronder interne medewerkers, externe medewerkers (inhuur, gedetacheerd, pay-roll), sollicitanten, studenten, co-assistenten en stagiairs

Mentor: een door de kantonrechter benoemde vertegenwoordiger van een patiënt, die als gevolg van zijn geestelijke - en/of lichamelijke toestand tijdelijk of duurzaam niet in staat is of bemoeilijkt wordt zijn belangen van niet vermogensrechtelijke aard behoorlijk waar te nemen. De mentor verricht rechtshandelingen betreffende de verzorging, behandeling en begeleiding van de betrokkene.

Overige wet- en regelgeving Medische Informatica - Informatiebeveiliging in de zorg NEN7510.

Patiënt*:* Persoon die met de hulpverlener een behandelingsovereenkomst heeft gesloten of ten behoeve van wie een behandelingsovereenkomst is gesloten;

Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Verantwoordelijke: het bestuur van het Albert Schweitzer ziekenhuis;

Verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van gegevens;

Vertegenwoordiger*:* Degene, die optreedt namens een patiënt;

Verwerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

Verzamelen van persoonsgegevens: het verkrijgen van persoonsgegevens;

WGBO: Wet Geneeskundige Behandelingsovereenkomst; De overeenkomst waarbij een natuurlijk persoon of rechtspersoon, de hulpverlener, zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde;

Zorggegevens: persoonsgegevens die direct of indirect betrekking hebben op de lichamelijke of de geestelijke gesteldheid van betrokkene, verzameld door een behandelaar (beroepsbeoefenaar) op het gebied van de gezondheidszorg in het kader van zijn beroepsuitoefening.

2 Beginselen, rechtmatigheid en rechten van betrokkenen

2.1 Algemene beginselen van de bescherming van persoonsgegevens

Alle verwerkingsprocessen die worden uitgevoerd door, binnen of namens het Albert Schweitzer ziekenhuis waarbij persoonsgegevens betrokken zijn, moeten aansluiten op de beginselen van de bescherming van persoonsgegevens. De volgende beginselen worden in alle verwerkingsprocessen meegenomen:

2.1.1 Rechtmatigheid, behoorlijkheid en transparantie

Persoonsgegevens moeten op een zodanige wijze verwerkt worden dat deze ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Volgens dit beginsel moeten alle verwerkingen van persoonsgegevens in de eerste plaats rechtmatig en behoorlijk zijn. Dit houdt in dat alle processen waarbij persoonsgegevens verwerkt worden in overeenstemming met de wet moeten zijn (dit heeft betrekking op de AVG zelf alsook op nationaal recht). In de tweede plaats moeten alle verwerkingen transparant zijn. Dit houdt vooral in dat de betrokkene zich van de verwerking bewust is. Processen waarbij persoonsgegevens op een onredelijke of onrechtmatige manier verwerkt worden, bijvoorbeeld indien de betrokkene niet over het verwerken geïnformeerd werd, zijn dus in principe in strijd met dit beginsel.

2.1.2 Doelbinding

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

Het principe van doelbinding eist dat de doelen van het verwerken voorafgaand aan het verwerken specifiek vastgelegd zijn. Vooral mogen de doeleinden niet te vaag of te breed geformuleerd zijn, en mogen ze na het verzamelen niet meer gewijzigd worden.

Voor het Albert Schweitzer ziekenhuis geldt dat de kaders waarbinnen de doelstelling van de verwerking van persoonsgegevens dient te blijven, zijn:

- zorgverlening en ondersteuning van patiëntenzorg;
- de behandeling en afhandeling van klachten en incidenten;
- het scheppen van voorwaarden voor wetenschappelijk onderzoek, statistiek en onderwijs;
- ondersteuning van de bedrijfsvoering.

2.1.3 Minimale gegevensverwerking

In de derde plaats vraagt het beginsel van minimale gegevensverwerking, dat gegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

Dit beginsel houdt in dat persoonsgegevens alleen verwerkt mogen worden indien het noodzakelijk is dat zij verwerkt worden. Persoonsgegevens die niet noodzakelijk zijn, mogen in beginsel niet verzameld worden. Indien een aantal verschillende verwerkingsprocessen uitgevoerd worden, is het beginsel van minimale gegevensverwerking op elke verwerking van toepassing.

Verder houdt het beginsel van minimale gegevensverwerking in, dat alleen medewerkers, die ter uitoefening van hun taken toegang tot bepaalde persoonsgegevens moeten hebben, deze categorieën persoonsgegevens mogen inzien.

2.1.4 Juistheid

Verder moeten gegevens in beginsel juist zijn en zo nodig geactualiseerd worden. Alle redelijke maatregelen moeten worden genomen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

Het beginsel van juistheid houdt vooral in dat alle gegevens over een persoon juist moeten zijn. Indien gegevens onjuist blijken te zijn, moeten deze gegevens zo snel mogelijk verbeterd of aangevuld worden. Dit geldt zowel voor gegevens die bij het verzamelen van gegevens al onjuist waren alsook indien de feitelijke situatie verandert en gegevens daardoor aangepast moeten woorden.

2.1.5 Integriteit en vertrouwelijkheid

Het beginsel van integriteit en vertrouwelijkheid bepaalt, dat er passende technische of organisatorische maatregelen worden genomen. Naast een passende beveiliging moeten de persoonsgegevens onder meer

beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.

Dit betekent dat het Albert Schweitzer ziekenhuis en mogelijk ingeschakelde verwerkers zorgvuldig met persoonsgegevens omgaan. Zorgvuldigheid betekent in de eerste instantie dat medewerkers, die met persoonsgegevens werken, vertrouwelijk met gegevens omgaan, en in de tweede plaats, dat het Albert Schweitzer ziekenhuis technische en organisatorische maatregelen treft, die gegevens verder beveiligen en afschermen.

2.1.6 Verantwoordingsplicht

Het Albert Schweitzer ziekenhuis is verantwoordelijk voor de naleving van de beginselen en kan deze aantonen. Het Albert Schweitzer ziekenhuis moet aantonen, dat de beginselen van gegevensverwerking juist en correct worden nagekomen. Indien het Albert Schweitzer ziekenhuis haar verplichtingen niet (goed) nakomt, is zij aansprakelijk.

2.2 Rechtmatigheid

Het Albert Schweitzer ziekenhuis moet kunnen aantonen dat elk verwerkingsproces op een wettelijke grondslag is gebaseerd. Verwerking van persoonsgegevens is daardoor alleen rechtmatig indien het Albert Schweitzer ziekenhuis kan aantonen dat een van de voorwaarden uit artikel 6 AVG van toepassing is. Dit betekent dat de verwerking van persoonsgegevens door het Albert Schweitzer ziekenhuis alleen is toegestaan als de verwerking is gebaseerd op een van de volgende gronden:

2.2.1 Toestemming

In het geval van toestemming is verwerking van persoonsgegevens alleen rechtmatig indien de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doelen. Toestemming is alleen geldig indien hij geïnformeerd, vrijwillig en specifiek gegeven werd.

Toestemming kan te allen tijde door de betrokkene ingetrokken worden. Intrekken van toestemming heeft geen negatieve gevolgen op de rechtmatigheid van de verwerkingen, die vóór het intrekken van toestemming plaats hebben gevonden. Het verwerken van persoonsgegevens moet uiteraard onverwijld beëindigd worden zodra toestemming is ingetrokken, tenzij de verwerkingen op een ander rechtsgrond gesteund kunnen worden.

2.2.2 Uitvoering van een overeenkomst

Persoonsgegevens mogen ook verwerkt worden indien verwerking noodzakelijk is om een overeenkomst uit te voeren, of om op verzoek van de betrokkene een overeenkomst tot stand te kunnen brengen. Dit is bijvoorbeeld van toepassing op de geneeskundige behandelingsovereenkomst met de patiënt, waarvoor een grote hoeveelheid persoonsgegevens verwerkt moeten worden, zowel vóór het tot stand komen van de overeenkomst als ook tijdens de behandeling. Verder is deze rechtsgrond van toepassing op verwerkingsprocessen die in verband staan met het uitvoeren van overeenkomsten tussen Albert Schweitzer ziekenhuis en haar klanten.

Het Albert Schweitzer ziekenhuis kan alleen een beroep op deze rechtsgrond doen indien de gevraagde gegevens daadwerkelijk noodzakelijk zijn voor de uitvoering van de overeenkomst. In de regel zal deze grondslag voor het Albert Schweitzer ziekenhuis in de relatie met de patiënt de belangrijkste grondslag vormen. De geneeskundige behandelingsovereenkomst (en de uitvoering hiervan) vormt de basis voor de relatie arts en/of verpleegkundige enerzijds en de patiënt anderzijds.

2.2.3 Wettelijke verplichting

Uiteraard mag het Albert Schweitzer ziekenhuis gegevens verwerken indien zij wettelijk verplicht is om de verwerkingen uit te voeren. Er bestaat een aantal wettelijke verplichtingen die van toepassing kunnen zijn. Albert Schweitzer ziekenhuis is vooral verplicht om gegevens te verwerken om aan haar verplichtingen als werkgever te voldoen en vanwege fiscale verplichtingen.

2.2.4 Vitale belangen

Persoonsgegevens mogen verder verwerkt worden indien de verwerking noodzakelijk is om vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen. Deze voorwaarde is vooral bij medische noodgevallen van toepassing, bijvoorbeeld in het geval van een noodsituatie, zoals in het geval de

patiënt buiten kennis is, men niet eerst toestemming nodig heeft van de patiënt op de spoedeisende hulp om identiteitsgegevens door te geven aan de behandeld arts. Ook kan deze grondslag van toepassing zijn indien er sprake is van een epidemie met (mogelijk) grote maatschappelijke gevolgen.

2.2.5 Taak van algemeen belang

Verwerking van gegevens is ook toegestaan indien het Albert Schweitzer ziekenhuis persoonsgegevens verwerkt in verband met de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan haar is opgedragen. Deze voorwaarde is alleen van toepassing indien de persoonsgegevens daadwerkelijk noodzakelijk zijn voor de verwerking in verband met de uitoefening van een publiekrechtelijke taak.

2.2.6 Gerechtvaardigde belangen

Persoonsgegevens mogen verder verwerkt worden indien het Albert Schweitzer ziekenhuis een gerechtvaardigd belang kan aantonen, dat wil zeggen indien de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van het Albert Schweitzer ziekenhuis of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen dan de belangen van het ziekenhuis.

Gerechtvaardigde belangen kunnen onder andere bedrijfsbelangen of andere economische belangen betreffen, indien het belang voldoende zwaar weegt. De feitelijke aanwezigheid van een belang is echter niet voldoende. Deze voorwaarde kan alleen toegepast worden indien maatregelen getroffen zijn voor de veiligheid van data, en indien de proportionaliteit en subsidiariteit van de verwerking gewaarborgd is.

Proportionaliteit betreft de vraag naar de effectiviteit en evenredigheid. Als met de verwerking van gegevens niet het gestelde doel kan worden bereikt, dan is die verwerking niet proportioneel (effectiviteit). Het doel dat wordt nagestreefd moet in verhouding staan tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt (evenredigheid). Subsidiariteit betreft de vraag of het genoemde doel niet op een andere minder ingrijpende wijze (bijv. door geen of minder persoonsgegevens te verwerken) kan worden bereikt. De belangen van de verwerkingsverantwoordelijke en de betrokkene moeten dus voorzichtig afgewogen worden. De afweging van belangen dient gemotiveerd en gedocumenteerd te worden.

2.3 Bijzondere categorieën van persoonsgegevens

2.3.1 Verwerkingsverbod

Het is belangrijk dat opgemerkt wordt dat persoonsgegevens in verschillende categorieën vallen. De hierboven beschreven voorwaarden voor rechtmatigheid zijn op het grootste deel van persoonsgegevens van toepassing. Echter een aantal categorieën persoonsgegevens is uitgezonderd.

Artikel 9 (1) AVG bepaalt dat de verwerking van de volgende persoonsgegevens verboden is:

- Persoonsgegevens waaruit ras of etnische afkomst blijken;
- Persoonsgegevens waaruit politieke, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken;
- Verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gegevens over gezondheid (medische gegevens), of met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Bijzondere categorieën persoonsgegevens zijn bijzonder gevoelig. Deze categorieën persoonsgegevens hebben een bijzondere bescherming, omdat het bekend worden van deze gegevens mogelijk negatieve gevolgen voor de betrokkene kan hebben. Om de betrokkene te beschermen verwerkt het Albert Schweitzer ziekenhuis deze categorieën data in principe niet, met uitzondering van medische patiëntgegevens. Aangezien het verwerken van deze medische persoonsgegevens noodzakelijk is voor het uitvoeren van de geneeskundige behandelingsovereenkomst met de patiënt. Verder zal het Albert Schweitzer ziekenhuis bijzondere persoonsgegevens ook verwerken indien dit noodzakelijk is om aan een wettelijke plicht te voldoen.

Naast bijzondere gegevens kennen we ook gevoelige gegevens. Dit zijn vooral gegevens die gelet op de inhoud of naar hun aard als gevoelig worden aangemerkt, omdat dit bijvoorbeeld iets zegt over de financiële situatie van een persoon, of het minderjarigen betreft.

2.3.2 Uitzonderingen op het verbod van verwerking

In beginsel mogen bijzondere categorieën persoonsgegevens dus niet verwerkt worden. Er bestaat echter een aantal uitzonderingen op dit beginsel.

Artikel 9 (2) AVG benoemt tien uitzonderingen, waarvan een aantal ook voor het Albert Schweitzer ziekenhuis van belang kan zijn.

- De betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor één of meer welbepaalde doeleinden. Hieronder valt in dit geval ook het uitvoeren van de geneeskundige behandelingsovereenkomst met welke overeenkomst en uitvoering de patiënt heeft ingestemd;
- De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;
- De verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- De verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang;
- De verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Dit mag echter alleen als het onderzoek een algemeen belang dient, het vragen van uitdrukkelijke toestemming onmogelijk blijkt en voldoende waarborgen zijn getroffen om zo min mogelijk risico's voor de persoonlijke levenssfeer van de betrokkene te creëren.

Indien één van deze uitzonderingen van toepassing is, mogen bijzondere persoonsgegevens bij uitzondering verwerkt worden.

3 Rechten van betrokkenen

Betrokkenen hebben onder andere het recht hun persoonsgegevens in te zien, te wijzigen of te laten verwijderen. Vanuit de Wet op de geneeskundige behandelingsovereenkomst (Wgbo) is dit niet een nieuw recht. De patiënt heeft immers onder de Wgbo al het recht om inzage te verlangen in zijn of haar medisch dossier. Onder de AVG zijn de rechten van betrokkenen, en met name het inzagerecht, zeer ruim: zo hoeft de patiënt niet verplicht aan te geven waarom hij of zij gegevens wil inzien. Ook is de betrokkene niet verplicht om een specifiek verzoek in te dienen: de patiënt mag vragen om al zijn persoonsgegevens die van hem zijn opgeslagen in te zien.

Het is belangrijk dat er rekening mee gehouden wordt dat dergelijk algemeen geformuleerde verzoeken veel tijd in beslag kunnen nemen om af te handelen. De termijn waarin aan een dergelijk verzoek voldaan moet zijn, is vier weken.

Een betrokkene moet zich altijd identificeren om een recht uit te kunnen oefenen. Doet hij of zij dat niet, dan hoeft het verzoek niet in behandeling genomen te worden om misbruik te voorkomen.

3.1 Recht op Informatie

Het Albert Schweitzer ziekenhuis is verplicht aan de betrokkene bepaalde informatie te verstrekken om de transparantie van verwerkingen te waarborgen.

Informatie die in ieder geval aan de betrokkene verstrekt moet worden:

- De contactgegevens van het Albert Schweitzer ziekenhuis en van haar vertegenwoordiger;
- De contactgegevens van de functionaris voor gegevensbescherming;
- De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking;
- In voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- Of persoonsgegevens doorgegeven worden aan een land buiten de Europese Unie of aan een internationale organisatie:
    - Indien gegevens naar een derde land doorgegeven worden, moet ook vermeld zijn of er een adequaatheidsbesluit is genomen door de Europese Commissie;
    - Indien gegevens naar een derde land of naar een internationale organisatie doorgegeven worden waar de privacy van betrokkenen door passende of geschikte waarborgen beschermd wordt (artikel 46, 47 of 49 (1) AVG) moet de betrokkene geïnformeerd worden uit welke waarborgen de maatregelen bestaan, en hoe ze toegankelijk zijn;

- De periode gedurende welke de persoonsgegevens zullen worden opgeslagen of, indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
- Dat de betrokkene het recht heeft om het Albert Schweitzer ziekenhuis te verzoeken om inzage, overdraagbaarheid van gegevens (dataportabiliteit), rectificatie of verwijdering van persoonsgegevens, beperking van en bezwaar tegen verwerking;
- Het recht toestemming te allen tijde weer in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van verwerkingen op basis van de toestemming vóór de intrekking daarvan;
- Dat de betrokkene het recht heeft een klacht in te dienen bij de Autoriteit Persoonsgegevens (de toezichthouder);
- Het bestaan van geautomatiseerde besluitvorming, waaronder profilering, en tenminste in het geval van profilering, nuttige informatie over de onderliggende logica, het belang en de verwachte gevolgen van de verwerking voor de betrokkene.

In het geval dat informatie direct van de betrokkene verzameld wordt, geeft het Albert Schweitzer ziekenhuis de volgende aanvullende informatie aan de betrokkene:

- Of de verwerking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten; en
- Of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.

De informatie moet bij het verzamelen van persoonsgegevens aan de betrokkene verstrekt worden. Het Albert Schweitzer ziekenhuis deelt de informatie ook aan de betrokkene mee wanneer het ziekenhuis het plan vormt om persoonsgegevens voor een ander doel te gebruiken dan waarvoor zij oorspronkelijk zijn verzameld. Het Albert Schweitzer ziekenhuis licht de betrokkene in vóórdat de verwerking begint.

Indien de informatie niet direct van de betrokkene is verkregen maar uit een ander bron afkomstig is, ligt de situatie iets anders. In een dergelijk geval moet de bovengenoemde informatie ook aan betrokkene verstrekt worden, met de aanvulling om welke categorieën van persoonsgegevens het gaat.

Verder dient rekening te worden gehouden met de volgende punten:

- De bovengenoemde informatie wordt binnen een redelijke termijn verstrekt, maar uiterlijk binnen een maand (4 weken) na de verkrijging van persoonsgegevens;
- Indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene;
- Indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de gegevens voor het eerst worden verstrekt.

Indien het Albert Schweitzer ziekenhuis van plan is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt zij vóór de verdere verwerking informatie over dat andere doel en alle relevante verdere informatie.

De informatieplicht is niet van toepassing indien en voor zover

- De betrokkene reeds over de informatie beschikt;
- Het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder:
    - Bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de toepasselijke voorwaarden en waarborgen, of
    - Voor zover de verplichting om informatie te verstrekken de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

In dergelijke gevallen neemt het Albert Schweitzer ziekenhuis passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie.

.

- Het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven door een wet die op het Albert Schweitzer ziekenhuis van toepassing is en passende maatregelen van toepassing zijn om de gerechtvaardigde belangen van de betrokkene te beschermen;
- De persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Europees of nationaal recht, waaronder een statutaire geheimhoudingsplicht.

3.2 Recht op Inzage

De betrokkene heeft op grond van zowel de AVG als de Wgbo een recht op inzage. Beide rechten worden in deze paragraaf besproken. Door de desbetreffende verantwoordelijken dienen de volgende rechten te worden gerespecteerd.

- Recht op inzage op grond van de AVG ten aanzien van het verkrijgen van een overzicht van persoonsgegevens, dit betreft ook niet-medische persoonsgegevens of -dossiers (paragraaf 3.2.1);
- Recht op inzage op grond van de Wgbo ten aanzien van het verkrijgen van inzage in het medisch dossier (paragraaf 3.2.2).

3.2.1 Recht op inzage op grond van de AVG

De betrokkene kan een verzoek indienen om te weten of persoonsgegevens betreffende hem of haar verwerkt worden en om de persoonsgegevens die bij het Albert Schweitzer ziekenhuis over hem of haar opgeslagen zijn in te zien. Het Albert Schweitzer ziekenhuis is verplicht tot inzage van die persoonsgegevens en zal de volgende informatie moeten verstrekken:

- De verwerkingsdoeleinden;
- De betrokken categorieën van persoonsgegevens;
- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- Indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- Dat de betrokkene het recht heeft het Albert Schweitzer ziekenhuis te verzoeken dat persoonsgegevens worden gewijzigd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
- Dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;
- Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
- Het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor betrokkene;
- Indien persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie er passende waarborgen zijn genomen gelet op de doorgifte van de persoonsgegevens.

Het Albert Schweitzer ziekenhuis is op verzoek van de betrokkene verplicht om een kopie van de persoonsgegevens die worden verwerkt te verstrekken. Een volledig overzicht kan op verschillende manieren worden gegeven. Uitgangspunt is dat er (digitale) kopieën van het dossier worden verstrekt. In sommige gevallen kan het ook een optie zijn om de patiënt de gegevens op locatie te laten inzien. Dit mag echter alleen in overleg met de betrokkene.

Houd er in elk geval rekening mee dat de volgende informatie niet wordt overhandigd bij een inzageverzoek, ook niet als daar uitdrukkelijk om wordt gevraagd:

- Persoonlijke en vertrouwelijke werkaantekeningen en notities. Te denken valt aan interne e-mails voor overleg. Maken de gegevens uit deze e-mails onderdeel uit van het dossier, dan moeten deze gegevens wel worden overhandigd;
- Documenten waarin persoonsgegevens van derden zijn opgenomen. Afschriften van deze documenten mogen alleen worden overhandigd als deze andere persoonsgegevens voldoende zijn afgeschermd. Bijvoorbeeld geanonimiseerd of onleesbaar gemaakt;
- Persoonsgegevens die worden gebruikt in het kader van de voorkoming, opsporing en vervolging van strafbare feiten.
- Correspondentie inzake incidenten, klachten en aansprakelijkstellingen.

3.2.2 Recht op inzage op grond van de Wgbo

Op grond van de Wgbo heeft de patiënt het recht op inzage en/of kopie van de gegevens die in het kader van de behandeling zijn vastgelegd. Onder het medisch dossier wordt verstaan het geheel aan informatie, vastgelegd in het kader van de behandeling van de patiënt. Dit betreft voor het papieren dossier alle in het

dossier opgenomen gegevens. Dus inclusief de geschreven delen van zowel de behandelend arts als de verpleging. Dit betreft eveneens alle elektronisch vastgelegde gegevens.

Persoonlijke werkaantekeningen vallen **niet** onder het inzagerecht en dienen daarom niet in het dossier te zijn opgenomen. Inzage in gegevens wordt niet verstrekt indien dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander dan de patiënt, zoals gegevens over anderen of gegevens over de patiënt verstrekt door anderen (bijvoorbeeld familieleden).

Informeel verzoek tot inzage

Dit verzoek kan tijdens het consult met de behandelend arts worden afgehandeld.

Een formeel verzoek tot kopie dossier

Het verzoek tot inzage wordt afgehandeld door de behandelaar zelf of door de medewerkers van het medisch archief. Een kopie van het dossier kan worden aangevraagd door een aanvraagformulier (te vinden op de website van het ziekenhuis) te sturen aan het medisch archief. In het formulier moet worden aangeven welk deel van het dossier men wenst te ontvangen:

- Verpleegkundig;
- Medisch;
- Klinisch;
- Poliklinisch;
- Welk specialisme en
- Welke periode.

Een formeel verzoek om een kopie van een medisch dossier dient schriftelijk te worden gedaan, voorzien van een kopie legitimatiebewijs. Na toestemming te hebben verkregen van de behandelaar worden alle gegevens uit het medisch dossier gekopieerd. Het duplicaat kan worden afgehaald door de aanvrager. De verstrekking wordt schriftelijk bevestigd. Als een derde namens de patiënte een kopie van het dossier opvraagt of ophaalt, dan moet ook hiervoor schriftelijk toestemming worden gegeven. Er dient zowel een kopie van het eigen legitimatiebewijs als een kopie van het legitimatiebewijs van de gemachtigde bijgevoegd te worden. De gemachtigde dient zich bij het ophalen van de kopie van het dossier te legitimeren. Zie voor meer informatie over ‘vertegenwoordiging’ van of bij een inzageverzoek *paragraaf 4.2.4*.

3.3 Recht op correctie, verwijdering en vergeten te worden

Na een inzageverzoek kan blijken dat persoonsgegevens onjuist zijn. In dat geval heeft betrokkene het recht om de onjuiste persoonsgegevens te laten corrigeren. Verder heeft betrokkene het recht om onvolledige informatie aan te vullen.

Naast een recht op correctie heeft de betrokkene het recht om van het Albert Schweitzer ziekenhuis zonder onredelijke vertraging te verlangen dat persoonsgegevens worden gewist. Het Albert Schweitzer ziekenhuis is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- De betrokkene trekt toestemming in voor het verwerken en dit is de enige grondslag waarop de verwerking berust of kan berusten;
- De betrokkene heeft gegrond bezwaar gemaakt tegen de verwerking;
- De persoonsgegevens zijn onrechtmatig verwerkt;
- De persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op het Albert Schweitzer ziekenhuis rust.

Naast het recht op verwijdering heeft de betrokkene onder bepaalde omstandigheden ook het recht om vergeten te worden. Dit recht ligt in het verlengde van het recht op verwijdering van gegevens. Het gaat dan om situaties waarbij het ziekenhuis als verwerkingsverantwoordelijke persoonsgegevens van de betrokkene openbaar heeft gemaakt (bijvoorbeeld door ze online te zetten) en de betrokkene gevraagd heeft deze gegevens te wissen. Naast het wissen van de gegevens uit de eigen systemen moet het ziekenhuis redelijke technische en organisatorische maatregelen nemen om andere verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene vergeten wil worden. Dit

betekent dat ieder koppeling naar en kopie van de gegevens gewist moet worden. Daarbij geldt: hoe belangrijker de wijziging, hoe meer moeite er moet worden gedaan om die andere partijen in te lichten.

Het recht op verwijdering en het recht om vergeten te worden zijn niet absoluut, maar moeten gewogen worden tegen andere rechten en belangen. Het Albert Schweitzer ziekenhuis is niet verplicht om gegevens te wissen en te verwijderen wanneer verwerking nodig is:

- Voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie,
- Voor het nakomen van een wettelijke verwerkingsverplichting of voor het vervullen van een taak van algemeen belang of het uitoefenen van openbaar gezag dat aan het Albert Schweitzer ziekenhuis is verleend
- Met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden,
- Voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

3.4 Recht op beperking van de verwerking

De betrokkene heeft een recht op beperking van de verwerking onder de volgende omstandigheden:

- De juistheid van de persoonsgegevens wordt door de betrokkene betwist;
- De verwerking is onrechtmatig en de betrokkene kiest voor beperking van het gebruik van persoonsgegevens in plaats van voor het wissen ervan;
- Het Albert Schweitzer ziekenhuis heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van het Albert Schweitzer ziekenhuis zwaarder wegen dan die van de betrokkene.

Het gevolg van een beperking van de verwerking is dat het Albert Schweitzer ziekenhuis persoonsgegevens slechts mag verwerken:

- indien betrokkene toestemming geeft; of
- indien het nodig is voor een rechtsvordering; of
- ter bescherming van de rechten van een andere persoon; of
- om gewichtige redenen van algemeen belang.

Het Albert Schweitzer ziekenhuis moet verder iedere ontvanger van persoonsgegevens op de hoogte brengen van de vereiste beperking van verwerking. Indien de beperking van de verwerking weer wordt opgeheven, wordt de betrokkene vóór de opheffing door het Albert Schweitzer ziekenhuis op de hoogte gebracht.

3.5 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij of zij aan het Albert Schweitzer ziekenhuis heeft verstrekt, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen, en het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door het Albert Schweitzer ziekenhuis, indien

- de verwerking berust op toestemming én
  de verwerking via geautomatiseerde processen wordt verricht.

Indien het technisch mogelijk is, kan de betrokkene verzoeken dat gegevens rechtstreeks van het Albert Schweitzer ziekenhuis naar een nieuwe verwerkingsverantwoordelijke worden doorgezonden.

3.6 Recht van bezwaar

Indien persoonsgegevens verwerkt worden op basis van algemeen belang of gerechtvaardigde belangen van het Albert Schweitzer ziekenhuis of van een derde, heeft de betrokkene het recht om vanwege met zijn of haar specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens. Het Albert Schweitzer ziekenhuis staakt de verwerking van de persoonsgegevens tenzij zij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met een rechtsvordering.

De betrokkene heeft altijd het recht om bezwaar te maken tegen verwerking van persoonsgegevens ten behoeve van direct marketing.

3.7 Geautomatiseerde individuele besluitvorming

De betrokkene heeft het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

Dit recht is niet van toepassing indien het besluit:

- noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en het Albert Schweitzer ziekenhuis; of
- wettelijk is toegestaan; of
- berust op de uitdrukkelijke toestemming van de betrokkene

In het geval dat het besluit noodzakelijk is of op toestemming berust, treft het Albert Schweitzer ziekenhuis passende maatregelen ter bescherming van de rechten en vrijheden van de betrokkene, waaronder ten minste:

- het recht op menselijke tussenkomst;
- het recht om zijn standpunt kenbaar te maken; en
- het recht om het besluit aan te vechten.

Verder mogen deze besluiten niet op bijzondere categorieën van persoonsgegevens gebaseerd zijn, tenzij er passende maatregelen ter bescherming van de belangen van betrokkenen getroffen zijn én:

- de betrokkene uitdrukkelijk toestemming heeft gegeven of
- de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang.

3.8 Klachten

Indien de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of andere redenen heeft tot klagen met betrekking tot de verwerking van persoonsgegevens, kan hij een klacht indienen op de wijze zoals beschreven in het klachtenreglement van het Albert Schweitzer ziekenhuis.

De betrokkene kan ook de Autoriteit Persoonsgegevens verzoeken een onderzoek in te stellen of de wijze van gegevensverwerking door de verantwoordelijke in overeenstemming is met de AVG.

4 Verwerking van data door het Albert Schweitzer ziekenhuis

Het Albert Schweitzer ziekenhuis verwerkt persoonsgegevens in verschillende situaties. Zij verwerkt hoofdzakelijk gegevens van patiënten om haar diensten aan te kunnen bieden, gegevens van medewerkers in haar hoedanigheid van werkgever, en data van derden, zoals potentiële klanten, sollicitanten, en leveranciers van diensten en goederen.

4.1 Wijze van verwerking

4.1.1 Algemene beginselen

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit en proportionaliteit (zie uitleg in par. 2.2.6). Wanneer met geen of minder persoonsgegevens hetzelfde doel bereikt kan worden, moet daar altijd voor gekozen worden.

Zoals in de voorafgaande hoofdstukken besproken, moeten persoonsgegevens juist, ter zake dienend, actueel en niet bovenmatig veel zijn in het licht van het doel van de verwerking. Dit betekent dat alleen die persoonsgegevens mogen worden gebruikt die strikt noodzakelijk zijn voor het doel van de verwerking. Wanneer het bijvoorbeeld voldoende is om iemands contactgegevens te gebruiken, is het niet nodig om ook een pasfoto en BSN te vragen. In ieder geval gelden voor het gebruik van het BSN strenge regels. Alleen indien de wet voorschrijft dat het gebruik van een BSN is toegestaan, dan mag een BSN worden verwerkt. Denk hierbij aan de verplichting tot gebruik van het BSN op basis van de Wet gebruik burgerservicenummer in de zorg (Wbsn-z). Wanneer ook met anonieme gegevens volstaan kan worden, mogen geen herleidbare persoonsgegevens gebruikt worden.

4.1.2 Doelen

Bij alle processen waarvoor of waarbij het Albert Schweitzer ziekenhuis persoonsgegevens verwerkt, houdt zij zich aan de wettelijke bepalingen en leeft zij de beginselen inzake verwerking van persoonsgegevens na. Algemeen uitgangspunt is dat persoonsgegevens alleen verzameld en verwerkt worden als daarvoor een doel bestaat. Dit doel moet welbepaald, duidelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagegaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel.

Het Albert Schweitzer ziekenhuis verwerkt persoonsgegevens onder meer in het kader van:

- Het uitvoeren van de geneeskundige behandelingsovereenkomst conform de Wgbo, zorgverlening en ondersteuning van patiëntenzorg;
- De behandeling en afhandeling van klachten en incidenten;
- Het verrichten van wetenschappelijk onderzoek, statistiek en onderwijs;
- Ondersteuning van de bedrijfsvoering
- Het aangaan en uitvoeren van arbeidsovereenkomsten met medewerkers;
- Het voldoen aan wettelijke verplichtingen.

Het Albert Schweitzer ziekenhuis verwerkt persoonsgegevens niet voor doelen die niet toereikend bepaald, uitdrukkelijk omschreven of gerechtvaardigd zijn.

4.1.3 Training en Awareness

Om privacybewust te worden, te zijn, en te blijven, zorgt het Albert Schweitzer ziekenhuis voor kennissessies op het gebied van privacy en omgaan met persoonsgegevens. Tevens is er een intranetsite en bestaan er diverse specifieke beleidsregels op onderwerp, procedures, werkwijzen om iedere medewerker in zijn werkzaamheden handvatten te bieden bij het verwerken van de persoonsgegevens waarmee zij werken.

4.1.4 Geheimhoudingsplicht en het verstrekken van persoonsgegevens

De behandelaar, medebehandelaars, de beheerder, de verwerker en de verantwoordelijke zijn verplicht te zwijgen tegen anderen over alle informatie die zij over betrokkene hebben. Na overlijden van de betrokkene blijft deze zwijgplicht bestaan.

De zwijgplicht kan slechts worden doorbroken:

- Op grond van een wettelijk voorschrift;
- Indien de betrokkene toestemming heeft gegeven;

- Wanneer de behandelaar zich gesteld ziet voor een conflict van plichten. In een dergelijke situatie dient de behandelaar het individuele belang van de betrokkene af te wegen tegen het algemeen belang.

De schriftelijke toestemming van de betrokkene is vereist voor verstrekking van persoonsgegevens aan derden, tenzij zulks noodzakelijk is ter uitvoering van een wettelijk voorschrift of op grond van redenen genoemd in dit privacyreglement. Persoonsgegevens mogen slechts worden verstrekt met in acht nemen van de beveiliging.

Buiten de instelling kunnen persoonsgegevens worden verstrekt, voor zover voor hun taakuitoefening noodzakelijk, aan:

- degenen, die rechtstreeks betrokken zijn bij de actuele zorg- of hulpverlening aan de betrokkene, tenzij laatstgenoemde kenbaar heeft gemaakt daartegen bezwaar te hebben;
- instanties voor statistiek en beleid; gegevens worden in dat geval slechts in zodanige vorm verstrekt, dat zij redelijkerwijs niet door de ontvanger tot individuele personen identificeerbaar zijn en nadat ter zake over het gebruik van die gegevens afspraken zijn gemaakt;
- aan ziektekostenverzekeraars binnen de kaders als genoemd in paragraaf 4.2.2

4.2 Patiëntgegevens

De eerste belangrijke groep van betrokkenen van wie het Albert Schweitzer ziekenhuis persoonsgegevens verwerkt zijn patiënten. Persoonsgegevens, waaronder zorggegevens, van patiënten worden hoofdzakelijk door het Albert Schweitzer ziekenhuis verwerkt om haar verbintenissen op grond van de geneeskundige behandelingsovereenkomst na te kunnen komen. Verder zijn er verwerkingsprocessen die door het Albert Schweitzer ziekenhuis uitgevoerd worden om aan een wettelijke verplichting te voldoen.

Alle verwerkingsprocessen alsmede hun wettelijke grondslagen kunnen in een verwerkingsregister ingezien worden.

Te allen tijde houdt het Albert Schweitzer ziekenhuis rekening met de gerechtvaardigde belangen van betrokkenen en streeft er naar de algemene principes van de bescherming van persoonsgegevens na te leven.

Het uitvoeren van de geneeskundige behandelingsovereenkomst is altijd met veel verwerkingsprocessen verbonden. Uiteraard past het Albert Schweitzer ziekenhuis bijzondere veiligheids- en vertrouwelijkheids-regels op alle gegevens van patiënten toe en worden zij bijzonder beschermd.

4.2.1 Wet geneeskundige behandelingsovereenkomst

De basis – grondslag – voor het verwerken van persoonsgegevens van patiënten is voor het Albert Schweitzer ziekenhuis de uitvoering van de geneeskundige behandelingsovereenkomst op grond van de Wgbo. Deze Wgbo geeft uitwerking aan de positie van de patiënt bij uitwisseling van gegevens en aan het met de privacy samenhangende beroepsgeheim. Ook in de uitoefening van de geneeskundige behandelingsovereenkomst geldt dat alleen die persoonsgegevens mogen worden verwerkt die voor het doel, de behandeling, noodzakelijk zijn.

4.2.2 Zorggegevens van patiënten

Voor de verwerking van zorggegevens is uitdrukkelijke toestemming van de betrokkene vereist, tenzij het een geval betreft zoals genoemd in de volgende situaties of indien de verwerking noodzakelijk is ter uitvoering van een wettelijk voorschrift.

De uitdrukkelijke voorafgaande toestemming van de patiënt is niet vereist indien:

a) door de verantwoordelijke persoonsgegevens betreffende de gezondheid worden verstrekt aan:
   - Hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene; dan wel met het oog op het beheer van de organisatie van de verantwoordelijke;
   - Verzekeraars voor zover dat noodzakelijk is voor de beoordeling van het door de verzekeringsinstelling te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt, dan wel voor zover dat noodzakelijk is voor de uitvoering van de verzekeringsovereenkomst. Hierbij geldt dat persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid en seksuele leven uitsluitend mogen worden verwerkt voor zover dit noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid als genoemd onder a);

b) de persoonsgegevens alleen worden verstrekt aan personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht;
c) onverminderd eventuele wettelijke voorschriften slechts de volgende personen toegang hebben tot de gegevensverwerking:
   - De behandelaar die deze gegevens heeft verzameld of diens waarnemer of opvolger en de medebehandelaars voor zover dit nodig is voor de multidisciplinaire behandeling van de betrokkene;
   - Voorts hebben toegang tot de gegevensverwerking de beheerder en de bewerker, voor zover dit in het kader van beheer en bewerking noodzakelijk is. De verantwoordelijke heeft als zodanig geen toegang tot de persoonsgegevens tenzij dit noodzakelijk is in verband met zijn algemene verantwoordelijkheid als verantwoordelijke voor de verwerking van de persoonsgegevens;
d) persoonsgegevens zodanig zijn geanonimiseerd dat zij redelijkerwijs niet herleidbaar zijn. De verantwoordelijke kan besluiten deze geanonimiseerde gegevens te verstrekken ten behoeve van doeleinden die verenigbaar zijn met het doel van de gegevensverwerking;
e) gegevens betreffende erfelijke eigenschappen slechts mogen worden verwerkt wanneer de verwerking plaatsvindt met betrekking tot de betrokkene bij wie de erfelijke gegevens worden verkregen, tenzij:
   - Een zwaarwegend geneeskundig belang prevaleert;
   - De verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoeken.

4.2.3 Vertegenwoordiging van patiënten

Ten aanzien van de vertegenwoordiging van patiënten moet rekening worden gehouden met de volgende uitgangspunten:

Algemeen geldt dat de persoon, die in de plaats treedt van de betrokkene, de zorg van een goed vertegenwoordiger dient te betrachten. Hij is gehouden de betrokkene zoveel mogelijk bij de vervulling van zijn taken te betrekken. Indien een vertegenwoordiger optreedt namens de betrokkene, komt de verantwoordelijke zijn verplichtingen die voortvloeien uit de wet en dit reglement na jegens deze vertegenwoordiger, tenzij de nakoming niet verenigbaar is met de zorg van een goed verantwoordelijke.

Minderjarigen onder de 12 jaar.

Indien de betrokkene jonger is dan twaalf jaar treden de ouders die het ouderlijk gezag uitoefenen dan wel de voogd in de plaats van de betrokkene. Hetzelfde geldt voor de betrokkene die de leeftijd van twaalf jaar heeft bereikt en niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake.

Tot de leeftijd van 12 jaar kunnen ouders die het ouderlijk gezag uitoefenen zonder instemming van hun kind een kopie van het dossier verkrijgen. Indien de behandelend arts het verstrekken van de kopie niet verenigbaar vindt met de zorg van een goed hulpverlener, dan kan het verstrekken van een kopie worden geweigerd.

Wordt een inzage/kopie gevraagd door de ouders, dan dient bij het schriftelijke verzoek te worden verklaard dat zij het ouderlijk gezag over het kind uitoefenen. Indien het verzoek wordt gedaan door de voogd van het kind, dient een afschrift van de voogdijbeschikking in het dossier aanwezig te zijn. Is deze niet aanwezig, dan dient deze alsnog te worden verstrekt en in het dossier te worden opgenomen

Minderjarigen van 12 tot 16 jaar

Indien de betrokkene in de leeftijdscategorie van twaalf tot zestien jaar valt en in staat is tot een redelijke waardering van zijn belangen, treden naast de betrokkene zelf diens ouders op. Is een kind 12 jaar of ouder en nog jonger dan 16 jaar dan dient het kind naast de ouders in te stemmen met de behandeling, dan wel het verzoek tot inzage.

Personen van 16 jaar en ouder

Is het kind 16 jaar of ouder dan oefent alleen het kind, of de gemachtigde, zijn of haar rechten uit. Ditzelfde geldt voor het uitoefenen van de rechten van betrokkenen of het verkrijgen van een kopie van het medisch dossier.

Wilsonbekwamen

Indien de betrokkene ouder is dan zestien jaar en niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake of indien de betrokkene is overleden, dan treedt, in volgorde als hier weergegeven, als vertegenwoordiger voor hem op:

a) De curator of mentor indien de betrokkene onder curatele staat of ten behoeve van hem het mentorschap is ingesteld;
b) De persoonlijk gemachtigde indien de betrokkene deze schriftelijk heeft gemachtigd, tenzij deze persoon niet optreedt;
c) De echtgenoot of andere levensgezel van de betrokkene, tenzij deze persoon dat niet wenst of ontbreekt;
d) Een ouder, kind, broer, zus, grootouder of kleinkind van de betrokkene, tenzij deze persoon dat niet wenst of ontbreekt.

Anderen dan de patiënt

Bij het opvragen van een kopie van een medisch dossier door een ander dan de patiënt zelf (advocaat, medisch adviseur, verzekeringsmaatschappij, politie en justitie) is een door de patiënt getekende machtiging noodzakelijk.

4.2.4 Persoonsgegevens van patiënten (niet-zorggegevens)

Persoonsgegevens, niet zijnde zorggegevens, mogen slechts rechtmatig worden verwerkt op grond van de grondslagen als opgenomen in paragraaf 2.2. Voorbeelden van persoonsgegevens die niet bestaan uit zorggegevens, zullen in de regel alleen worden verwerkt op basis van voorafgaande toestemming, het uitvoeren van een overeenkomst, het voldoen aan een wettelijke verplichting, of vanwege een gerechtvaardigd belang van het Albert Schweitzer ziekenhuis dat zwaarder weegt dan het persoonlijk belang van de betrokkene. Denk hierbij aan onder meer contactgegevens van de familieleden van de betrokkene die door de betrokkene als contactpersoon worden benoemd (toestemming). Het verwerken van de benodigde persoonsgegevens om bijvoorbeeld gebruik te kunnen maken van de faciliteiten van het Albert Schweitzer ziekenhuis (overeenkomst).

4.3 Statistisch en wetenschappelijk onderzoek

Het Albert Schweitzer ziekenhuis kan persoonsgegevens verder gebruiken om statistieken en analyses te kunnen maken. Verwerkingen van persoonsgegevens voor historische, statistische en wetenschappelijke (medische) doeleinden worden niet beschouwd als onverenigbaar met de doeleinden waarvoor de persoonsgegevens eerder zijn verzameld. In naleving van haar verplichtingen treft het Albert Schweitzer ziekenhuisvoorzieningen om te verzekeren dat de verdere verwerking van de persoonsgegevens uitsluitend plaatsvindt ten behoeve van deze specifieke doeleinden.

Persoonsgegevens ten behoeve van wetenschappelijk onderzoek en statistiek waarvoor goedkeuring van de toetsingscommissie voor wetenschappelijk onderzoek is vereist, kunnen alleen dan zonder toestemming van de betrokkene worden verstrekt, indien en voor zover dat voortvloeit uit het protocol dat door de toetsingscommissie is goedgekeurd.

4.4 Leveranciers

Als de administratie met betrekking tot leveranciers persoonsgegevens bevat, is de AVG van toepassing. Het is toegestaan om persoonsgegevens te verwerken en te gebruiken met het oog op een administratie van leveranciers als de verwerking plaatsvindt voor de administratie van leveringen en bestellingen, de levering van diensten, betalingen van diensten en bestellingen, incasso, intern management, audit of wettelijke verplichtingen.

Alleen relevante en noodzakelijke persoonlijke gegevens mogen worden verwerkt, gedocumenteerd of gebruikt in het geval dat het persoonsgegevens van een leverancier betreft.

4.5 Cameratoezicht en toegangscontrole

4.5.1 Cameratoezicht

Het gebeurt steeds vaker dat patiënten en bezoekers binnen instellingen strafbare feiten plegen of zich agressief gedragen. En dat zorgt in toenemende mate voor problemen. Het Albert Schweitzer ziekenhuis - een voor iedereen toegankelijk ziekenhuis - is ervoor verantwoordelijk dat de veiligheid van patiënten, bezoekers en medewerkers in alle redelijkheid wordt gewaarborgd. Met behulp van cameratoezicht wordt getracht de veiligheid in het ziekenhuis te verbeteren en te waarborgen.

Aan cameratoezicht waarbij beeld- en geluidsopnamen worden gemaakt, kleven meerdere juridische consequenties. Het vastleggen van gegevens (beelden) kan slechts binnen de kaders van de vooraf omschreven doelen en dient tot een minimum te worden beperkt.

Op het plaatsen van een videocamera voor cameratoezicht in het kader van veiligheid is de AVG van toepassing. De wet is van toepassing op het opnemen van beeld- en geluidsopnamen voor zover personen herkenbaar in beeld worden gebracht. Daaronder wordt ook verstaan het herkenbaar kunnen maken van personen aan de hand van details van de beeldopnamen.

Voor cameratoezicht in het kader van veiligheid geldt de grondslag ‘gerechtvaardigd bedrijfsbelang’. Het cameratoezicht moet noodzakelijk zijn om ‘de reguliere bedrijfsactiviteiten’ te verrichten. Een ziekenhuis heeft als reguliere bedrijfsactiviteit het verlenen van zorg. Dit kan alleen in een veilige omgeving. Daarmee heeft het ziekenhuis een juridische grondslag om camera’s op te stellen.

Het Albert Schweitzer ziekenhuis informeert eenieder over het feit dat er in de instelling uit veiligheidsoverwegingen video-opnamen worden gemaakt. In het Albert Schweitzer ziekenhuis hangen op diverse plaatsen borden en stickers met de tekst: “in deze instelling wordt over uw en onze veiligheid gewaakt door middel van video-opnamen”. Het Albert Schweitzer ziekenhuis voldoet aan de eis van informatieverstrekking door over het camerabeleid te communiceren met personeel, patiënten en bezoekers. Daarnaast is het beleid gepubliceerd in het documentbeheerssysteem van het ziekenhuis.

4.5.2 Toegang en gebruik van camerabeelden

De afdeling Beveiliging/Facilitaire dienst is verantwoordelijk voor het beheer van het videobeveiligingssysteem en heeft exclusieve controle over het vrijgeven van videobeelden die door dit systeem worden opgeslagen.

Gegevens mogen zo lang bewaard worden als noodzakelijk is voor het doel waarvoor zij zijn verzameld. In het algemeen geldt dat beeld- en geluidsopnamen niet langer dan vier weken bewaard mogen worden. Daarna dienen zij te worden vernietigd. Beelden van incidenten, die dienen als bewijsmateriaal worden eventueel langer bewaard. In het Albert Schweitzer ziekenhuis is sprake van een reactief beleid. De beeld- en geluidopnamen worden bekeken op het moment dat daartoe aanleiding is, bijvoorbeeld als er een incident is geweest. De bewaartermijn van opgeslagen beelden kan worden verlengd als er beelden van strafbare feiten zijn vastgelegd die gebruikt kunnen worden als bewijs of ondersteunend materiaal in een gerechtelijke procedure.

Veiliggestelde beelden kunnen in het kader van een strafrechtelijk onderzoek overgedragen worden aan politie en/of justitie. Het verstrekken van beelden aan politie en/of justitie gebeurt op initiatief van het Albert Schweitzer ziekenhuis indien het in het belang is van het ziekenhuis en verenigbaar is met de doelstellingen van de camerabewaking. In andere gevallen worden alleen beelden verstrekt indien politie en/of justitie beschikken over de vereiste ‘Vordering verstrekking historische gegevens’.

4.5.3 Toegangscontrole

Het Albert Schweitzer ziekenhuis gebruikt een geautomatiseerd toegangssysteem. Het uitgangspunt voor bevoegdheid tot de ruimtes is géén toegang, tenzij het openbare ruimtes betreft (binnen de geldende openingstijden). De toegang van personen tot ruimtes wordt bepaald door de rol(len) die zij in het zorg- respectievelijk bedrijfsproces vervullen. Toegang wordt beperkt tot datgene wat voor een rol (functieprofiel) noodzakelijk is.

Patiënten hebben toegang tot de openbare ruimtes en tot de ruimtes waar zij in het kader van hun zorg verblijven of een behandeling ondergaan. Voor bezoekers geldt dat zij toegang hebben tot de patiënten, medewerkers, zorgverleners die zij bezoeken voor zover die daar mee instemmen en voor zover dat bij ieders rol past.

Patiënten kunnen gebruik maken van de door het Albert Schweitzer ziekenhuis aangeboden persoonlijke elektronische informatiediensten (o.a. patiëntportaal, afspraaknotificatie per e-mail/sms). De inrichting en het beoogde gebruik van deze informatiediensten is helder beschreven, dit inclusief beschrijving van de toepasselijke informatiebeveiliging.

5 Verwerkingsregister en verwerkers

5.1 Verwerkingenregister

Alle verwerkingen van persoonsgegevens die plaatsvinden bij het Albert Schweitzer ziekenhuis worden opgenomen in het verwerkingenregister. In het verwerkingenregister worden de volgende gegevens opgenomen:

- de naam en de contactgegevens van Albert Schweitzer ziekenhuis, eventuele gezamenlijke verwerkingsverantwoordelijken en de functionaris voor de gegevensbescherming;
- doelen van de verwerking;
- een beschrijving van de categorieën van betrokkenen en van persoonsgegevens;
- de ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie;
- bewaartermijnen van de persoonsgegevens;
- een beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het Albert Schweitzer ziekenhuis zorgt ervoor dat dit register actueel wordt gehouden. Nieuwe verwerkingen worden opgenomen in het register en wijzigingen in bestaande verwerkingen moeten ook worden doorgevoerd. De Autoriteit Persoonsgegevens kan inzage vragen in het register.

5.2 Gegevensbeschermingseffectbeoordeling (GEB)

Een Gegevensbeschermingseffectbeoordeling (GEB; Engels: DPIA; en in de praktijk vaak ook Privacy Impact Assessment (PIA) genoemd) is verplicht voor risicovolle verwerkingen van persoonsgegevens. Om te bepalen of sprake is van een risicovolle verwerking moeten de volgende factoren worden afgewogen: soort verwerking, of er nieuwe technologieën worden gebruikt bij de verwerking, aard, omvang, context en doel van de verwerking.

In ieder geval is volgens de AVG de uitvoering van een GEB verplicht in de volgende vier gevallen:

- een systematische en uitgebreide beoordeling van persoonlijke aspecten van personen, gebaseerd op geautomatiseerde verwerking, mits op basis daarvan besluiten kunnen worden genomen die (rechts)gevolgen hebben voor de persoon, zoals profiling;
- grootschalige verwerking van bijzondere persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten; of
- stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten (bijvoorbeeld door middel van cameratoezicht).
- de verwerkingen waarvan de Autoriteit Persoonsgegevens heeft aangegeven op haar website dat daarvoor een GEB verplicht is.

Dit is geen uitputtende lijst. Hoewel de AVG bovengenoemde drie situaties specifiek noemt, dient voor alle situaties met een mogelijk hoog risico voor betrokkenen een GEB te worden uitgevoerd. Er is sprake van een hoog risico wanneer de voorgenomen verwerking aan twee of meer van de volgende negen criteria voldoet:

1. evaluatie van personen of scoretoekenning;
2. geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
3. stelselmatige monitoring;
4. gevoelige gegevens of gegevens van zeer persoonlijke aard;
5. op grote schaal verwerkte gegevens;
6. matching of samenvoeging van datasets;
7. gegevens met betrekking tot kwetsbare betrokkenen
8. innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
9. blokkering van een recht, dienst of contract.

Indien een GEB uitgevoerd wordt, gaat het Albert Schweitzer ziekenhuis in op de verwerkingen en de bijbehorende doelen. De GEB zal ook een beoordeling bevatten van de noodzaak van de verwerking, de risico's van de verwerking en de beoogde maatregelen voor deze risico's. Ten slotte voert het Albert Schweitzer ziekenhuis een toetsing uit om te bepalen of de verwerking overeenkomstig de aanbevelingen en conclusies van de GEB wordt uitgevoerd. Voordat een proces dat verplicht aan een GEB moet worden onderworpen wordt doorgevoerd, moet de GEB eerst aan de FG van het Albert Schweitzer ziekenhuis worden voorgelegd voor advies.

5.3 Verwerkers

Het komt voor dat derde partijen persoonsgegevens verwerken in opdracht van het Albert Schweitzer ziekenhuis. De derde partijen zijn zogenaamde verwerkers. Deze derden voeren dan namens het Albert Schweitzer ziekenhuis een proces uit, waarbij het Albert Schweitzer ziekenhuis zelf of de derde via het Albert Schweitzer ziekenhuis persoonsgegevens verwerkt. Het Albert Schweitzer ziekenhuis schakelt alleen verwerkers in die voldoende garanties bieden tot het treffen van passende technische en organisatorische maatregelen.

Verder zorgt het Albert Schweitzer ziekenhuis ervoor dat met iedere verwerker een verwerkersovereenkomst wordt afgesloten die betrekking heeft op de zorgvuldige omgang met de persoonsgegevens door de verwerker.

5.4 Derde Landen

Persoonsgegevens mogen in principe niet worden geëxporteerd naar een land buiten de EU. Binnen de EU geldt het uitgangspunt van ‘free flow of information/ personal data’. Het exporteren van persoonsgegevens naar andere EU-lidstaten is onder dezelfde voorwaarden toegestaan als binnen Nederland.

Onder exporteren wordt o.a. verstaan: het buiten de EU/EER opslaan (bijvoorbeeld in de cloud) of het ter beschikking stellen van persoonsgegevens. Hieronder valt niet het via internet zichtbaar maken van persoonsgegevens aan personen buiten de EU.

Onder bepaalde omstandigheden mogen persoonsgegevens wel worden geëxporteerd naar buiten de EU/EER, zoals wanneer er in het exportland een passend beschermingsniveau is. De Europese Commissie kan besluiten dat een land een passend beschermingsniveau heeft d.m.v. een adequaatheidsbesluit (‘adequacy decision’) of wanneer door de Europese Commissie goedgekeurde standaardcontracten worden gebruikt. Neem altijd contact op met de afdeling Juridische Zaken wanneer hiervan sprake is.

6 Informatiebeveiliging en overige maatregelen

6.1 Informatiebeveiliging

Het Albert Schweitzer ziekenhuis beschermt persoonsgegevens continu en met passende beveiligingsmaatregelen. In het informatiebeveiligingsbeleid is nader uitgewerkt op welke wijze het Albert Schweitzer ziekenhuis haar informatiebeveiligingsbeleid heeft ingericht. Naast technische maatregelen zoals encryptie, zijn ook organisatorische maatregelen relevant. Een voorbeeld van een organisatorische maatregel (met een technische component) is het bepalen wie toegang heeft tot bepaalde persoonsgegevens (autorisaties). Het basisprincipe is dat hoe groter het risico van de verwerking is, hoe zwaarder de beveiligingseisen zijn.

Bij het bepalen van de organisatorische, procedurele en technische beveiligingsmaatregelen ter bescherming van persoonsgegevens houdt het Albert Schweitzer ziekenhuis rekening met de aard, omvang, context en het doel van verwerking van deze persoonsgegevens. Ook de waarschijnlijkheid van een incident en impact voor betrokkenen worden hierin meegenomen. Deze maatregelen worden periodiek geëvalueerd en geactualiseerd.

Bij de aanschaf of ontwikkeling van nieuwe producten, systemen of processen moet de bescherming en beveiliging van persoonsgegevens altijd als een van de factoren worden beschouwd waarmee vooraf al rekening moet worden gehouden bij het beoordelen van hun geschiktheid (privacy by design en default).

6.1.1 Privacy by Design

Beveiligingseisen en maatregelen zijn een centraal onderdeel van Privacy by Design (PbD). PbD betekent, dat voordat een begin wordt gemaakt met nieuwe verwerkingen, zoals bij een nieuw project, een samenwerkingsverband, of de aanschaf van software waarmee persoonsgegevens gemoeid zijn, wordt nagedacht over het risico met betrekking tot de privacy. Deze analyse wordt vertaald naar concrete beveiligingseisen en maatregelen die het Albert Schweitzer ziekenhuis neemt om persoonsgegevens adequaat te beschermen.

PbD is een methode die organisatiebreed wordt toegepast binnen het Albert Schweitzer ziekenhuis om de privacy van betrokkenen zo goed mogelijk te waarborgen. PbD betekent in ieder geval dat dataminimalisatie en pseudonimisering centraal staan bij verwerkingen door het Albert Schweitzer ziekenhuis. Bij het inrichten van de beveiliging van persoonsgegevens spelen ook de volgende maatregelen een rol:

- versleuteling van persoonsgegevens (encryptie);
- de vertrouwelijkheid, integriteit, en beschikbaarheid van de systemen en diensten te garanderen;
- beschikbaarheid van de persoonsgegevens tijdig te herstellen bij incidenten;
- een procedure voor het testen, beoordelen en evalueren van de beveiligingsmaatregelen.

6.1.2 Organisatorische maatregelen

Het Albert Schweitzer ziekenhuis treft diverse organisatorische maatregelen om ervoor te zorgen dat persoonsgegevens zorgvuldig worden verwerkt. Daarbij worden de persoonsgegevens alleen verwerkt door artsen die een eed of belofte hebben afgelegd, medewerkers zoals BIG-geregistreerde verpleegkundigen die gehouden zijn aan de beroepscode, of overige medewerkers, waaronder inhuur, en externen die een geheimhoudingsplicht hebben. Ook is het van belang dat alleen geautoriseerde medewerkers werken met persoonsgegevens. Waarbij zij tevens weten wat hun verantwoordelijkheid is ten aanzien van de omgang met deze persoonsgegevens en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Het is dus belangrijk dat de medewerkers van het Albert Schweitzer ziekenhuis zich bewust zijn van de regels en gedragsnormen rondom privacy. Het vergroten van het privacy bewustzijn wordt onder meer bereikt door het ondersteunen van de medewerkers door privacy trainingen en kennissessies. De medewerkers moeten zich bewust zijn van het belang van privacy. Zo moeten zij persoonsgegevens verwerken zoals is bepaald in het privacyreglement en de bijbehorende documentatie.

6.1.3 Beveiliging (technische maatregelen)

Het Albert Schweitzer ziekenhuis beveiligt alle persoonsgegevens en documenten die persoonsgegevens bevatten. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Als uitgangspunt geldt dat naarmate de risico's van de verwerking hoger liggen er betere beveiligingsmaatregelen moeten worden getroffen. Het Albert Schweitzer ziekenhuis heeft hiervoor een specifiek beleid opgesteld in de vorm van het Informatiebeveiligingsbeleid. Het is aan het Albert Schweitzer ziekenhuis zelf om te bepalen hoe de persoonsgegevens organisatorisch en technisch moeten worden beveiligd.

De verwerking van persoonsgegevens wordt geregistreerd in een gebruiksregistratie (de log). De log wordt structureel gecontroleerd op het bestaan van een passende bevoegdheid de onderhavige persoonsgegevens te verwerken. Uit de controle voortkomende verdenkingen worden na beoordeling door de verantwoordelijk manager nader onderzocht en aan de verantwoordelijke voorgelegd voor het nemen van de daarvoor geëigende maatregelen.

6.1.4 Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan wettelijk is toegestaan en noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt. Hoe lang bepaalde gegevens worden bewaard is afhankelijk van de aard van de gegevens en de doeleinden waarvoor deze gegevens worden verwerkt. De bewaartermijn kan dus per doel verschillen.

De belangrijkste bewaartermijnen zijn:

Medisch dossier	20 jaar (WGBO)
Financiële/administratieve gegevens ten behoeve van de behandeling	7 jaar (wettelijk)
Klachten	3 jaar na afwikkeling van de klacht (klachtreglement ASz)

Persoonsgegevens dienen langer dan de vastgestelde bewaartermijnen bewaard te worden indien:

- De betrokkene hierom verzoekt;
- Dit voortvloeit uit de zorg van een goed hulpverlener;
- Bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, waaronder de verantwoordelijke.

6.2 Datalekken

Het Albert Schweitzer ziekenhuis maakt medewerkers en personen die werken voor of bij het Albert Schweitzer ziekenhuis bewust van het belang van de vertrouwelijke omgang met persoonsgegevens en de procedure 'meldplicht datalekken'

Uiterlijk 72 uur nadat een datalek heeft plaatsgevonden meldt het Albert Schweitzer ziekenhuis het datalek bij de Autoriteit Persoonsgegevens (AP), tenzij het onwaarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor betrokkenen. Afspraken met verwerkers over het doorgeven van bij hun opgetreden datalekken zijn vastgelegd in de verwerkersovereenkomst. Het uitgangspunt daarbij is dat beveiligingsincidenten waarbij persoonsgegevens van patiënten, bezoekers of leveranciers van het Albert Schweitzer ziekenhuis betrokken (kunnen) zijn, binnen 24 uur door de verwerker aan het Albert Schweitzer ziekenhuis worden gemeld.

Ingeval het datalek een hoog risico inhoudt voor de privacy van de betrokkene moet ook de betrokkene geïnformeerd worden. Het Albert Schweitzer ziekenhuis is dan ook verplicht in het geval van een datalek een dergelijke mededeling aan betrokkenen te verrichten.

Datalekken in het Albert Schweitzer ziekenhuis of in de gegevensverwerking van het Albert Schweitzer ziekenhuis worden gemeld aan de FG, aan de ISO en aan de verantwoordelijke door ieder die bij de verwerking betrokken is onder gezag van de verantwoordelijke, als verwerker, als betrokkene of als derde.

7 Functionaris voor de Gegevensbescherming

Het Albert Schweitzer ziekenhuis heeft een Functionaris voor de Gegevensbescherming (FG) aangesteld. De FG houdt toezicht op de naleving van de privacywetgeving en adviseert het ziekenhuis over de privacywetgeving.

De FG is onafhankelijk en geniet wettelijke ontslagbescherming. De FG rapporteert rechtstreeks aan de hoogste leidinggevende van het ziekenhuis. Tevens is de FG de contactpersoon voor alle vragen die over privacy en verwerking van uw persoonsgegevens gaan, zowel voor u als betrokkene als voor de toezichthouder de Autoriteit Persoonsgegevens.

De contactgegevens van de FG zijn:
e-mailadres: privacy@asz.nl
postadres:
Albert Schweitzer ziekenhuis
Postbus 444
3300 AK Dordrecht