Model Verwerkersovereenkomst

VERWERKERSOVEREENKOMST

DE ONDERGETEKENDEN:

1. Het Leids Universitair Medisch Centrum (LUMC) gevestigd aan de Albinusdreef 2, 2333 ZA te Leiden en ingeschreven in het register van de Kamer van Koophandel onder nummer 27366422 , in deze rechtsgeldig vertegenwoordigd door dhr. drs. L.F. Been RC, Directeur Facilitair Bedrijf (hierna: "**Verwerkingsverantwoordelijke**"); en

2. [Naam Verwerker], gevestigd aan de [adres] te [plaats] en ingeschreven in het register van de Kamer van Koophandel onder nummer [KvK-nummer], in deze rechtsgeldig vertegenwoordigd door [titel, naam en functie] (hierna "**Verwerker**");

hierna gezamenlijk ook aan te duiden als: "Partijen" en afzonderlijk als "Partij".

OVERWEGENDE DAT:

(a) Verwerker diensten verricht ten behoeve van Verwerkingsverantwoordelijke, zoals beschreven in de Hoofdovereenkomst [titel/kenmerk/datum] waarbij deze Verwerkersovereenkomst Bijlage [X] is.
(b) De diensten meebrengen dat persoonsgegevens worden verwerkt.
(c) Verwerker de betreffende gegevens louter in opdracht van Verwerkingsverantwoordelijke verwerkt en niet voor eigen doeleinden.
(d) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (hierna: "AVG") op deze verwerking van toepassing is.
(e) Partijen in deze Verwerkersovereenkomst de afspraken met betrekking tot de verwerking van persoonsgegevens in het kader van de diensten wensen vast te leggen.
(f) Deze Verwerkersovereenkomst, indien van toepassing, alle eerdere Hoofdovereenkomst(en) van gelijke strekking tussen Partijen vervangt.
(g) De Brancheorganisaties Zorg hebben met deze Verwerkersovereenkomst een standaard willen opstellen.

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1. Definities

1.1. Termen met een hoofdletter die in deze Verwerkersovereenkomst worden gebruikt en die hierin niet worden gedefinieerd, hebben de betekenis die is uiteengezet in de AVG (waaronder Persoonsgegeven, Betrokkene, Verwerkingsverantwoordelijke en Verwerker).

1.2. In deze Verwerkersovereenkomst wordt onder de volgende met een hoofdletter aangeduide begrippen het volgende verstaan:

a) Inbreuk

i een onderzoek naar of beslaglegging door overheidsfunctionarissen op de

		persoonsgegevens of een vermoeden dat dit gaat plaatsvinden; ii een inbreuk in verband met persoonsgegevens als bedoeld in artikel 4 onder 12 AVG;
b)	Medewerker	de door Partijen voor de uitvoering van deze Verwerkersovereenkomst betrokken natuurlijke persoon die werkzaam is bij of voor een van de Partijen.
c)	Hoofdovereenkomst	de Hoofdovereenkomst(en) betreffende de levering van producten en/of diensten. waarvan deze Verwerkersovereenkomst als Bijlage onderdeel van uitmaakt.
d)	Verzoeken van betrokkene	Een klacht over de verwerking dan wel verzoek tot uitoefening van de rechten van betrokkene zoals omschreven in Hoofdstuk 3 van de AVG.

1.3. Waar in deze Verwerkersovereenkomst naar bepaalde normen wordt verwezen (zoals NEN7510) wordt daarmee steeds gedoeld op de meest actuele geldige versie daarvan. Voor zover de betreffende norm niet meer wordt onderhouden, stemmen Partijen af welke norm geldt als opvolger van de betreffende norm.

Artikel 2. Onderwerp van deze Verwerkersovereenkomst en beschrijving Bijlagen

2.1. Deze Verwerkersovereenkomst betreft de verwerking van persoonsgegevens door Verwerker in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Hoofdovereenkomst.

2.2. Onderdeel van deze Verwerkersovereenkomst zijn de volgende Bijlagen:
   a) Bijlage 1: Omschrijving van de verwerking
   b) Bijlage 2: Beveiliging persoonsgegevens
   c) Bijlage 3: Contactinformatie mbt. verwerking/Inbreuken/Verzoeken van betrokkenen

2.3. Deze Verwerkersovereenkomst maakt onverbrekelijk deel uit van de Hoofdovereenkomst. Voor zover het bepaalde in de Verwerkersovereenkomst strijdig is met het bepaalde in de Hoofdovereenkomst, prevaleert het bepaalde in de Verwerkersovereenkomst.

Artikel 3. Uitvoering verwerking

3.1. Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend persoonsgegevens zal verwerken voor zover:
   a) dit noodzakelijk is voor de uitvoering van de Hoofdovereenkomst (binnen de gespecificeerde omschrijving in Bijlage 1); of
   b) Verwerkingsverantwoordelijke daartoe nadere schriftelijke instructies heeft gegeven;

3.2. Verwerker zal alle redelijke instructies van Verwerkingsverantwoordelijke in verband met de verwerking van de persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in

strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van persoonsgegevens.

3.3. Onverminderd het bepaalde in het eerste lid van dit artikel 3, is het Verwerker toegestaan om persoonsgegevens te verwerken indien een wettelijk voorschrift (waaronder begrepen daarop gebaseerde rechterlijke of bestuurlijke bevelen) hem tot een verwerking verplicht. In dat geval stelt de Verwerker voorafgaand aan de verwerking Verwerkingsverantwoordelijke in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker zal Verwerkingsverantwoordelijke, waar mogelijk, in staat stellen zich te verweren tegen deze verplichte verwerking en ook overigens de verplichte verwerking beperken tot het strikt noodzakelijke.

3.4. Verwerker zal de persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze verwerken en in overeenstemming met de op hem als Verwerker rustende verplichtingen op grond van de AVG en overige wet- en regelgeving.

3.5. Verwerker zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Verwerkingsverantwoordelijke, geen persoonsgegevens verwerken of laten verwerken door hemzelf of door derden in landen buiten de Europese Economische Ruimte (“EER”).

3.6. Verwerker waarborgt dat betrokken Medewerkers een geheimhoudingsovereenkomst hebben getekend dan wel garandeert dat Medewerkers geheimhouding zullen betrachten ten aanzien van de verwerking van de persoonsgegevens.

Artikel 4. Beveiliging persoonsgegevens en controle (versie gezondheidsgegevens) [Doorhalen indien niet van toepassing]

4.1. Verwerker zal aantoonbaar, passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de (in Bijlage 1 gespecificeerde) aard van de te verwerken persoonsgegevens, ter bescherming van de persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid en integriteit van de gegevens te garanderen. In deze beveiligings- maatregelen zijn de mogelijk in de Hoofdovereenkomst reeds bepaalde maatregelen begrepen.

4.2. Verwerker beschikt over een ISO27001 certificering, een vergelijkbare certificering of werkt aantoonbaar in overeenstemming met ISO27001 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van persoonsgegevens, waarin in ieder geval de in het eerste lid van dit artikel 4 genoemde maatregelen uiteengezet zijn.

4.3. Verwerker beschikt over een NEN7510-certificering of werkt aantoonbaar in overeenstemming met NEN7510 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van persoonsgegevens. Daarbij voldoet Verwerker aantoonbaar (indien van toepassing) aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN7512 en aan de eisen ten aanzien van logging zoals beschreven in NEN7513.

4.4. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke een (kopie van een) door een onafhankelijke en ter zake deskundige derde afgegeven geldig certificaat overleggen

alsmede de verklaring van toepasselijkheid, indien deze daarover beschikt, of een Third Party Memorandum (TPM), waaruit volgt dat Verwerker de verplichtingen uit dit artikel naleeft.

4.5. Verwerker laat zelf regelmatig interne en/of externe audits uitvoeren met betrekking tot de naleving van bovengenoemde normen.

4.6. Verwerkingsverantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor onder artikel 4.1 tot en met 4.3 genoemde maatregelen indien Verwerkingsverantwoordelijke daarom vraagt naar aanleiding van (vermoeden van) informatie- of privacy-inbreuken. Verwerker en Verwerkingsverantwoordelijke bepalen in gezamenlijk overleg het tijdstip waarop en de onafhankelijke derde partij die de controle uitvoert. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijk onderzoek in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.
Dergelijke audits zijn beperkt tot Persoonsgegevens en gegevensverwerkingssystemen die relevant zijn voor de levering van de diensten aan Verwerkingsverantwoordelijke. Alle auditrapporten en -materialen zullen door Partijen vertrouwelijk worden behandeld en niet aan derden (ook niet andere Verwerkingsverantwoordelijken) worden geopenbaard.

4.7. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 periodiek evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel 4. Het voorgaande laat de instructiebevoegdheid van Verwerkingsverantwoordelijke om zo nodig aanvullende maatregelen te (doen) treffen onverlet.

Artikel 4. Beveiliging persoonsgegevens en controle (versie niet-gezondheidsgegevens) [Doorhalen indien niet van toepassing]

4.1. Verwerker zal aantoonbaar, passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de (in Bijlage 1 gespecificeerde) aard van de te verwerken persoonsgegevens, ter bescherming van de persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid en integriteit van de gegevens te garanderen. In deze beveiligings- maatregelen zijn de mogelijk in de Hoofdovereenkomst reeds bepaalde maatregelen begrepen.

4.2. Verwerker beschikt over een ISO27001 certificering, een vergelijkbare certificering of werkt aantoonbaar in overeenstemming met ISO27001 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van persoonsgegevens.

4.3. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke (een kopie van) een door een onafhankelijke en ter zake deskundige derde afgegeven geldig certificaat overleggen, indien deze daarover beschikt, of een Third Party Memorandum (TPM), waaruit volgt dat Verwerker de verplichtingen uit dit artikel naleeft.

4.4. Verwerker laat zelf regelmatig interne en/of externe audits uitvoeren met betrekking tot de naleving van bovengenoemde normen.

4.5. Verwerkingsverantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor onder artikel 4.1 tot en met 4.3 genoemde maatregelen indien Verwerkingsverantwoordelijke daarom vraagt naar aanleiding van (vermoeden van) informatie- of privacy-inbreuken. Verwerker en Verwerkingsverantwoordelijke bepalen in gezamenlijk overleg het tijdstip waarop en de onafhankelijke derde partij die de controle uitvoert. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijk onderzoek in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

4.6. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 periodiek evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel 4. Het voorgaande laat de instructiebevoegdheid van Verwerkingsverantwoordelijke om zo nodig aanvullende maatregelen te (doen) treffen onverlet.

Artikel 5. Monitoring, informatieplichten en incidentenmanagement

5.1. Verwerker zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 5 rapporteren aan Verwerkingsverantwoordelijke.

5.2. In het geval van een Inbreuk zoals gespecificeerd in artikel 1.a onder i), zal Verwerker zich inspannen om de overheidsinstantie ertoe te bewegen gegevens rechtstreeks bij Verwerkingsverantwoordelijke op te vragen. Indien Verwerker verplicht wordt Persoonsgegevens te openbaren aan een overheidsinstantie, zal Verwerker Verwerkingsverantwoordelijke op de hoogte brengen, tenzij verboden onder toepasselijk recht, en, indien het verboden is Verwerkingsverantwoordelijke in kennis te stellen, zal Verwerker alle redelijke, rechtmatige inspanningen gebruiken om het bevel tot openbaarmaking aan te vechten op grond van juridische tekortkomingen krachtens toepasselijke wetgeving. Verwerker zal de verplichte verwerking beperken tot het strikt noodzakelijke. Zodra Verwerker een Inbreuk ontdekt zoals gespecificeerd in artikel 1.a onder ii), is Verwerker verplicht de contactpersoon van Verwerkingsverantwoordelijke genoemd in Bijlage 3 daarvan zonder onredelijke vertraging, doch binnen 48 uur, in kennis te stellen en daarbij alle relevante informatie te verstrekken over:

1) de aard van de inbreuk
2) de (mogelijk) getroffen persoonsgegevens;
3) de geconstateerde en de vermoedelijke gevolgen van het Inbreuk; en
4) de maatregelen die getroffen zijn of zullen worden om de Inbreuk op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken.

5.3. Verwerker is, onverminderd de overige verplichtingen uit dit artikel, verplicht om maatregelen te treffen die redelijkerwijs van hem kunnen worden verwacht om de Inbreuk zo snel mogelijk te herstellen dan wel de verdere gevolgen zoveel mogelijk te beperken. Partijen treden zo snel als mogelijk, doch binnen 24 uur na de kennisgeving over de Inbreuk, in overleg teneinde hierover nadere afspraken te maken. Als de aard van de Inbreuk vereist dat Verwerker

onmiddellijk handelt, is Verwerker gerechtigd eerst maatregelen te treffen en vindt dit overleg zo spoedig mogelijk, doch achteraf plaats.

5.4. Verwerker zal Verwerkingsverantwoordelijke te allen tijde zijn medewerking verlenen en zal de instructies van Verwerkingsverantwoordelijke opvolgen en verricht deugdelijk onderzoek naar de Inbreuk. Verwerker stelt daarover een rapportage op, inclusief een correcte respons en passende vervolgstappen. Deze rapportage deelt Verwerker zo spoedig mogelijk met Verwerkingsverantwoordelijke zodat deze tijdig de Autoriteit Persoonsgegevens (hierna: AP) en/of de Betrokkene kan informeren. Het melden aan de AP en/of betrokkenen kan alleen gedaan worden door de Verwerkingsverantwoordelijke.

5.5. Meldingen met betrekking tot Inbreuken en Verzoeken van betrokkenen worden gedaan aan de contactpersoon van Verwerkingsverantwoordelijke zoals beschreven in Bijlage 3.

5.6. Het is Verwerker niet toegestaan informatie te verstrekken over Inbreuken aan betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is of Partijen anderszins zijn overeengekomen.

5.7. Indien en voor zover Partijen zijn overeengekomen dat Verwerker in relatie tot een Inbreuk rechtstreeks contact onderhoudt met autoriteiten, anders dan de AP, of andere derde partijen, dan houdt de Verwerker de Verwerkingsverantwoordelijke daarvan voortdurend op te hoogte.

Artikel 6. Medewerkingsverplichtingen

6.1. De AVG en overige wetgeving kent aan de Betrokkene bepaalde rechten toe. Verwerker zal, rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, bijstand verlenen aan Verwerkingsverantwoordelijke bij de nakoming van de op Verwerkingsverantwoordelijke rustende verplichtingen voortvloeiend uit deze rechten.

6.2. Een door Verwerker ontvangen Verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zonder onredelijke vertraging nadat is vastgesteld dat het Verzoek gerelateerd is aan Verwerkingsverantwoordelijke doorgestuurd naar Verwerkingsverantwoordelijke.

6.3. Op het eerste daartoe strekkende verzoek van Verwerkingsverantwoordelijke zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de toepasselijke (privacy) wetgeving naleeft.

6.4. Verwerker zal voorts op verzoek van Verwerkingsverantwoordelijke, rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, alle noodzakelijke bijstand verlenen bij de nakoming van de op grond van de toepasselijke privacywetgeving op Verwerkingsverantwoordelijke rustende wettelijke verplichtingen, zoals het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA).

Artikel 7. Inschakeling subverwerkers

7.1. Verwerker zal zijn activiteiten die bestaan uit het verwerken van persoonsgegevens of vereisen dat persoonsgegevens verwerkt worden, niet uitbesteden aan een subverwerker zonder drie twee maanden van te voren dat mede te delen aan Verwerkingsverantwoordelijke, via de Contracteigenaar en de Functionaris Gegevensbescherming van Verwerkingsverantwoordelijke genoemd in Bijlage 3, en de Verwerkingsverantwoordelijke de gelegenheid te geven om

eventuele bezwaren aan de Verwerker kenbaar te maken. Indien Verwerkingsverantwoordelijke bezwaren heeft, zal Verwerker redelijke inspanningen leveren om het bezwaar van de Verwerkingsverantwoordelijke op te lossen of om de levering van de diensten zoals genoemd in de Hoofdovereenkomst - zonder daaraan afbreuk te doen - aan te passen om verwerking van persoonsgegevens door de voorgestelde (nieuwe) subverwerker te voorkomen.

7.2. Indien de Verwerker het bezwaar van de Verwerkingsverantwoordelijke niet kan oplossen of niet kan aanpassen om de verwerking van persoonsgegevens door de voorgestelde subverwerker te voorkomen, kan de Verwerkingsverantwoordelijke de Hoofdovereenkomst opschorten of geheel of gedeeltelijk beëindigen, met inachtneming van een opzegtermijn van zes maanden, gerekend vanaf de einddatum van het bezwaartermijn. Gedurende een schorsing van de Hoofdovereenkomst vanwege bezwaar tegen een (nieuwe) subverwerker en vanaf de einddatum van de Hoofdovereenkomst is de Verwerkingsverantwoordelijke niet verplicht om de Verwerker enige vergoeding op grond van de Hoofdovereenkomst of anderszins of enige schadevergoeding te betalen.

7.3. Artikel 7.1 is niet van toepassing op de in Bijlage 1 vermelde subverwerkers.

7.4. Verwerker zal met elke subverwerker een schriftelijke overeenkomst sluiten die gegevensbeschermingsverplichtingen bevat die niet minder beschermend zijn dan die in deze Verwerkersovereenkomst en de toepasselijke wetgeving. Voorts zal Verwerker toezien op de naleving hiervan door de subverwerker. Verwerker zal Verwerkingsverantwoordelijke op verzoek inzage geven in de met de subverwerker gesloten Verwerkersovereenkomst(en), tenzij Verwerker contractueel gehouden is aan geheimhoudingsclausules en geen toestemming krijgt van subverwerker inzage te geven. In ieder geval zal Verwerker inzicht geven in de aard van afspraken met de subverwerker. Verwerker mag bedrijfsgevoelige informatie verwijderen of onleesbaar maken.

7.5. Voor het inschakelen van een subverwerker blijft Verwerker volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een subverwerker. Voor de inzet van subverwerkers buiten de EER laat onverlet dat toestemming vereist is in overeenstemming met artikel 3.5 van deze Verwerkersovereenkomst.

Artikel 8. Aansprakelijkheid

8.1. Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen.

8.2. Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt als gevolg van enige tekortkoming in de nakoming van deze Verwerkersovereenkomst en/of overtreding van de AVG en of andere toepasselijke wet- en regelgeving in verband met de verwerking van persoonsgegevens. Deze aansprakelijkheid is beperkt tot een bedrag van maximaal 1,25 miljoen Euro per gebeurtenis en 2,5 miljoen Euro per kalenderjaar. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

8.3. De beperking van de aansprakelijkheid als hiervoor bedoeld, of enige andere (impliciete of expliciete) beperking of uitsluiting van de aansprakelijkheid, komt te vervallen indien er sprake is van:

a) verlies en/of verminking van Persoonsgegevens;

b) boetes die door de Autoriteit Persoonsgegevens of een andere toezichthouder worden opgelegd die rechtstreeks verband houden met een toerekenbare tekortkoming van Verwerker, of een aan Verwerker toerekenbaar gedraging of nalaten;
c) opzet of grove schuld aan de zijde van de schadeveroorzakende Partij; of
d) de schadeaansprakelijkheid op basis van wet- en regelgeving niet uitgesloten kan worden.

8.4 Voor zover in de Hoofdovereenkomst geen beperking van aansprakelijkheid voor Verwerkingsverantwoordelijke is opgenomen, geldt de in lid 2 opgenomen beperking voor Verwerker eveneens voor de Verwerkingsverantwoordelijke.

Artikel 9. Kosten

9.1. De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Verwerkersovereenkomst en de uitoefening van rechten van betrokkenen, worden geacht besloten te liggen in de op grond van de Hoofdovereenkomst reeds verschuldigde vergoedingen.

Artikel 10. Duur en beëindiging

10.1. Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de Hoofdovereenkomst inclusief eventuele verlengingen daarvan.

10.2. De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onverbrekelijk deel uit van de Hoofdovereenkomst. Beëindiging van de Hoofdovereenkomst, op welke grond dan ook (opzegging/ontbinding), heeft tot gevolg dat de Verwerkersovereenkomst eveneens op dezelfde grond beëindigd wordt, tenzij Partijen in voorkomend geval anders overeenkomen.

10.3. Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van deze Verwerkersovereenkomst gelden. Tot deze bepalingen behoren bijvoorbeeld die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid, geschillenbeslechting en toepasselijk recht.

10.4. Ieder der Partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Hoofdovereenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Hoofdovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te beëindigen indien:
a) de andere Partij wordt ontbonden of anderszins ophoudt te bestaan;
b) de andere Partij aantoonbaar [ernstig] tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;
c) een Partij in staat van faillissement wordt verklaard of surséance van betaling aanvraagt.

10.5. Gelet op de grote afhankelijkheid van Verwerkingsverantwoordelijke van Verwerker alsmede het continuïteitsrisico bij incidenten en calamiteiten (zoals faillissement), verklaart Verwerker zich reeds nu voor alsdan bereid op eerste verzoek van Verwerkingsverantwoordelijke aanvullende afspraken met Verwerkingsverantwoordelijke te maken teneinde voornoemde risico's te verkleinen.

10.6. Als Verwerker aan Verwerkingsverantwoordelijke schriftelijk te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of op basis van aan rechtspraak ontleende op Verwerker toepasselijke doctrines aan de verwerking van persoonsgegevens worden gesteld, treden Partijen direct in overleg om te bepalen of en hoe de Hoofd- en Verwerkersovereenkomst aanpassing behoeven, e.e.a. met inachtneming van de dan vigerende wet - en regelgeving, dan wel dat de gegevensverwerking/dienstverlening onmogelijk wordt, waarna de Verwerkersovereenkomst volledig en de Hoofdovereenkomst voor zover deze niet kunnen worden nagekomen zonder gegevensverwerking zo spoedig mogelijk moeten worden beëindigd.

10.7. ~~Verwerker dient Verwerkingsverantwoordelijke zo spoedig mogelijk te informeren over een voorgenomen overname of eigendomsoverdracht. Verwerkingsverantwoordelijke heeft het recht bij zwaarwegende bezwaren tegen de verandering van eigenaar de Hoofdovereenkomst te beëindigen zonder schadeplichtig te zijn.~~ Deze bepaling is geregeld in de Koopovereenkomst.

10.8. Het is Verwerker niet toegestaan om zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke deze Verwerkersovereenkomst en de rechten en plichten die samenhangen met deze Verwerkersovereenkomst over te dragen aan een derde partij.

10.9. De verplichtingen uit deze Verwerkersovereenkomst duren voort zolang de Verwerker persoonsgegevens van Verwerkingsverantwoordelijke verwerkt, ook nadat de Verwerker is opgehouden de in de Hoofdovereenkomst opgedragen zorg, diensten en/of faciliteiten ten behoeve van Verwerkingsverantwoordelijke te verlenen.

Artikel 11. Bewaartermijnen, teruggave en vernietiging van persoonsgegevens

11.1. Verwerker bewaart de Persoonsgegevens niet langer dan de tussen Partijen gemaakte afspraak over bewaartermijnen zoals vastgelegd in Bijlage 1. In geen geval bewaart Verwerker de Persoonsgegevens langer dan tot het einde van deze Verwerkersovereenkomst, tenzij anders is overeengekomen. Verwerkingsverantwoordelijke bepaalt of en zo ja hoelang gegevens bewaard moeten blijven.

11.2. Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker, tegen redelijke kosten, naar keuze van Verwerkingsverantwoordelijke, de persoonsgegevens onherroepelijk (doen) vernietigen of teruggeven aan Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens onherroepelijk zijn vernietigd of verwijderd. Eventuele teruggave van de gegevens zal in een algemeen gangbaar, gestructureerd en gedocumenteerd gegevensformaat langs elektronische weg plaatsvinden. Indien teruggave, onherroepelijke vernietiging of verwijdering niet mogelijk is, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

Artikel 12. Slotbepalingen

12.1. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

12.2. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

12.3. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de daartoe in de Overeenkomst aangewezen rechtbank of arbiter(s).

ALDUS OVEREENGEKOMEN EN DIGITAAL ONDERTEKEND MIDDELS VALIDSIGN:

Het Leids Universitair Medisch Centrum (LUMC)	<naam Verwerker>
{{esl:signer1:Signature:size(150,40)}}	{{esl:signer2:Signature:size(150,40)}}
Dhr. drs. L.F. Been RC	< Naam vertegenwoordiger Verwerker >
Directeur Facilitair Bedrijf	<Functie>

Bijlage 1: Omschrijving van de verwerking

Omschrijving van activiteiten en/of diensten, omvang en algemeen doel van de verwerking (benoem het aantal persoonsgegevens/betrokkenen):

Noem Hoofdovereenkomst: titel / kenmerk / ingangsdatum / partijen: Geef een omschrijving van activiteiten en/of diensten: Wat is het algemeen doel van de verwerking: Over hoeveel persoonsgegevens/betrokkenen gaat het:

Verwerking	Soort persoonsgegevens	Categorieën van betrokkenen	Doeleinden van de verwerking	Grondslag van de verwerking	Doorgifte buiten de EER	Afspraken bewaartermijnen	Afspraken verwijderprocedure
Noem de verwerking (bijvoorbeeld hosting, transfer, onderhoud, of naam van de applicatie)	Benoem de persoonsgegevens[2] (b.v. NAW, BSN, gegevens over gezondheid, etc.)	Benoem betrokkenen (patiënten, medewerkers, studenten, etc.)	Benoem het doel van de verwerking.	Benoem de grondslag waarop de verwerking plaatsvindt.[2]	Indien ja, benoem opslag/ verwerking buiten de EER en vermeld land, instrument waaronder doorgifte kan plaatsvinden (hoofdstuk 5 AVG) en aanvullende maatregelen.	Benoem afspraken bewaartermijnen.	Benoem de verwijderprocedure.

Subverwerkers

Subverwerker	Beschrijving dienst en persoonsgegevens	Gegevens buiten de EER	Verwerkers-overeenkomst
Naam en adres (incl. land)	Omschrijven	Ja/Nee (indien ja, vermeld land, instrument waaronder doorgifte kan plaatsvinden (hoofdstuk 5 AVG) en aanvullende maatregelen)	Ja/Nee

Toelichting:

Persoonsgegevens gaan over iemand (of zijn tot iemand te herleiden). Elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon is een persoonsgegeven. De identificatie kan bijvoorbeeld gebeuren aan de hand van een identificatiemiddel, zoals een naam, een identificatienummer, locatiegegevens, een online identificerende variabele of andere elementen die kenmerkend zijn. Hierbij kunt u denken aan fysieke, fysiologische, genetische, psychische, economische, culturele of sociale elementen.

Elke **verwerking** moet één of meerdere welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde **doeleinden** hebben. Het gaat hierbij om het doel of de doelen waarvoor de persoonsgegevens zijn verkregen/verzameld. Maak het **verwerkingsdoel/**de **verwerkingsdoelen** zo concreet mogelijk.

Grondslagen voor verwerking persoonsgegevens: Toestemming betrokkene / Noodzakelijk voor uitvoering van een overeenkomst / Wettelijke verplichting / Beschermen van vitale belangen van de betrokkene / Taak van algemeen belang of uitoefening van het openbaar gezag / Gerechtvaardigde belangen van de verwerkingsverantwoordelijke of`` van een derde.

Bijlage 2: Omschrijving nadere beveiligingsmaatregelen

Deze bijlage moet ingevuld worden per overeenkomst/contract en als Word bestand geretourneerd worden.

Certificering

- Beschikt de leverancier over certificeringen op het gebied van informatiebeveiliging?
  ( ) Ja, ISO27001 en/of NEN7510 (doorhalen wat niet van toepassing is). Graag het certificaat/ de certificaten en de Verklaring van Toepasselijkheid aanleveren.
  ( ) Nee.

Beschrijving systeem en verwerking

- Geef hieronder een samenvatting van het systeem (betreft het b.v. een SaaS-oplossing, mobiele app, website, e-learning, medische toepassing), de beoogde verwerking en datastromen.

- Indien het een webapplicatie betreft, zijn er maatregelen getroffen op de risico's uit de OWASP top 10?
  ( ) Ja
  ( ) Deels. Licht hieronder toe.
  ( ) Nee. Licht hieronder toe.

- Indien het een webapplicatie betreft, worden er periodiek penetratietests uitgevoerd op de web-omgeving?
  ( ) Ja. Geef hier onder aan hoe vaak deze tests plaatsvinden en wanneer de laatste is uitgevoerd.
  ( ) Nee. Licht hieronder toe.

Logische toegangsbeveiliging

- Accounts
  Systemen en applicaties behoren gebruik te maken van centrale Identity & Access Management systemen van het LUMC (Zoals bijvoorbeeld: Microsoft EntraID, LDAPS, SurfConext). Beschrijf de (voorgenomen) inrichting.

- Accountbeheer
  Beschrijf de verschillende typen accounts/rollen binnen het systeem. Denk hierbij aan systeemaccounts, beheerders- en gebruikersaccounts. Hoe is het beheer van de accounts en periodieke controle van rechten geregeld?

- Heeft de leverancier (na implementatie) toegang nodig tot het systeem?
  ( ) Ja. Licht hieronder toe waarvoor de toegang nodig is en welke afspraken hierover zijn gemaakt
  ( ) Nee

- Voldoet het systeem aan het LUMC-wachtwoordbeleid?
  - Minimaal 14 karakters;
  - Tenminste 3 van de volgende 4 groepen:
    - Hoofdletters
    - Kleine letters
    - Cijfers
    - Bijzondere tekens (! @ # $, etc.)
  - Onbeperkte geldigheid

  ( ) Ja
  ( ) Nee. Licht hieronder toe.

- Wordt voor *alle* accounts multifactor authenticatie technisch afgedwongen?
  ( ) Ja. Licht hieronder toe hoe hierin wordt voorzien.
  ( ) Nee. Licht hieronder toe.

- Sessiemanagement
  Wordt het systeem na een periode van inactiviteit automatisch gelocked en na hoelang?
  ( ) Ja, na … minuten.
  ( ) Nee.

Opslag en encryptie

- Waar wordt de data opgeslagen?
  ( ) Binnen LUMC-omgeving.
  ( ) Buiten LUMC-omgeving. Geef hieronder aan waar de data wordt opgeslagen, incl. land van opslag.

- Is data ‘at rest’ voorzien van encryptie?
  ( ) Ja. Licht hieronder toe met welke techniek hierin wordt voorzien.
  ( ) Nee. Licht hieronder toe waarom er geen encryptie wordt toegepast.

- Is data ‘in transit’ voorzien van encryptie?
  ( ) Ja. Licht hieronder toe met welke techniek hierin wordt voorzien.
  ( ) Nee. Licht hieronder toe waarom er geen encryptie wordt toegepast.

- Back-up/recovery
  Licht hieronder de wijze van back-up nader toe. Welke back-up methodiek wordt gebruikt? Hoe vaak vindt back-up plaats? Hoe lang worden de back-ups bewaard? Wordt het terugzetten van back-ups regelmatig getest?

- Logging
  Vindt er logging plaats conform ISO27001 en op welke wijze? Is de toegang tot de logging beperkt?
  Indien er (gepseudonimiseerde) gezondheidsgegevens worden verwerkt, voldoet de logging dan aan NEN7513?

Technisch- en functioneel beheer

- Waar is het technisch beheer van de applicatie belegd?
  ( ) Binnen LUMC
  ( ) Bij leverancier
  ( ) Anders. Licht hieronder toe door wie en op welke wijze het technisch beheer plaatsvindt.

- Waar is het functioneel beheer van de applicatie belegd?
  ( ) Binnen LUMC
  ( ) Bij leverancier
  ( ) Anders. Licht hieronder toe doe wie en op welke wijze het functioneel beheer plaatsvindt.

Rechten van de betrokkene

- Is het mogelijk om te voldoen aan het recht van betrokkene om de persoonsgegevens in de applicatie of het systeem te rectificeren of wissen?
  ( ) Ja. Licht hieronder toe op welke manier dit uitgevoerd wordt.
  ( ) Nee. Licht hieronder toe.

- Is het mogelijk om te voldoen aan het recht van betrokkene om een kopie te krijgen van de persoonsgegevens die verwerkt worden en het recht van gegevensoverdraagbaarheid?
  ( ) Ja. Licht hieronder toe op welke manier dit uitgevoerd wordt.
  ( ) Nee. Licht hieronder toe.

Bijlage 3: Contactinformatie mbt. Inbreuken/Verzoeken van betrokkenen

Contactinformatie voor Verwerkingsverantwoordelijke:

Naam: <<Naam>>
Functie: <<Functie>>
Telefoonnummer: <<Telefoonnummer>>
E-mailadres: <<E-mailadres>>

Contactinformatie voor Verwerker:

Gegevens contactpersoon datalekken LUMC
Functie: Functionaris voor Gegevensbescherming LUMC
Telefoonnummer: +31 (0)71 526 2779
E-mailadres: privacy@lumc.nl

Inbound emergency contact (24/7 te bereiken op):
Cyber Emergency Response Team LUMC: cert@lumc.nl
Telefoonnummer: CERT: +31 (0)6-21338599

Contactgegevens Contracteigenaar LUMC (in te vullen door LUMC)
Naam: <<Naam>>
Functie: <<Functie>>
Telefoonnummer: <<Telefoonnummer>>
E-mailadres: <<E-mailadres>>