Dataprotocol

MKIB - ClaudicatioNet

Versiebeheer

Versie	Status	Datum	Auteur(s)	Opmerkingen
1.0	Concept	26 juni 2015	P. Vlaandere	
1.1	Concept	22 juli 2015	SOLV	
1.2	Concept	26 aug. 2015	SOLV	
1.3	Review	5 nov. 2015	KNGF	Commentaren van MediQuest, KNGF en ClaudicatioNet zijn verwerkt
1.4	Review	5 dec. 2015	SOLV	Verwerken feedback KNGF/CN
1.5	Review	9 dec. 2015	KNGF	
1.6	Review	22 dec. 2015	SOLV	
1.7	Aanpassingen i.v.m. LDF	8 februari 2016	SOLV	
1.8	Definitief	31 maart 2016	KNGF	Commentaren van MediQuest, KNGF en ClaudicatioNet zijn verwerkt

Status: Definitief
Datum: 31 maart 2016
Versie: 1.8
Beheer: Koninklijk Nederlands Genootschap voor Fysiotherapie

Deelnemende partijen:
Stichting ClaudicatioNet
Koninklijk Nederlands Genootschap voor Fysiotherapie
MediQuest B.V.
Softmedia Interactive VOF

Inhoud

1. Inleiding

Achtergrond en beschrijving van het project
Het Koninklijk Nederlands Genootschap voor Fysiotherapie (hierna te noemen: “KNGF”) heeft in het kader van haar kwaliteitsprogramma “*Masterplan Kwaliteit in Beweging*” (hierna te noemen: “MKIB”) een landelijke database ontwikkeld, genaamd Landelijke Database Fysiotherapie (hierna te noemen: “LDF”). De LDF heeft tot doel ervoor te zorgen dat fysiotherapeuten beschikken over betrouwbare informatie ten behoeve van kwaliteitsborging en verantwoording van de zorg. Hierdoor kunnen de fysiotherapeuten voldoen aan de eisen die de Kwaliteitswet Zorginstellingen oplegt. Voor betrouwbare kwaliteitsinformatie is het noodzakelijk dat de zorg aan de patiënt op uniforme en wettenschappelijk verantwoorde wijze wordt geregistreerd. Hierdoor wordt analyse, toetsing en rapportage over de kwaliteit van de zorg mogelijk en kunnen de resultaten van een fysiotherapeut of een praktijk worden afgezet tegen de ‘spiegelinformatie’ ten behoeve van kwaliteitsverbetering. Voor dit doel worden gegevens van patiënten opgenomen in de LDF en kunnen gegevens uit de LDF worden verstrekt aan derden voor het verrichten van kwaliteitsonderzoek.

De gegevens die verkregen worden in de LDF in het kader van het MKIB zijn voorts van grote waarde voor wetenschappelijk onderzoek. Binnen de daaraan gestelde grenzen, in onder meer het Dataprotocol LDF, kunnen gegevens uit de LDF voor dit doel ter beschikking worden gesteld.

De Stichting ClaudicatioNet (hierna te noemen: “ClaudicatioNet”) is een geïntegreerd zorgnetwerk dat streeft naar transparantie en hoogwaardige zorg van patiënten met *claudicatio intermittens* (hierna te noemen: “Patiënten”). In dit kader doet ClaudicatioNet onderzoek naar de effectiviteit en doelmatigheid van het *stepped care model* en *subsitutie van zorg*, waarbij door een bij ClaudicatioNet aangesloten fysiotherapeut (hierna te noemen: “Fysiotherapeut”) eerst looptherapie wordt ingezet, alvorens – bij het uitblijven van een resultaat – wordt overgegaan tot een invasief traject, de endovasculaire revascularisatie (hierna te noemen: “Onderzoek”). ClaudicatioNet is van mening dat in veel gevallen een operatie voorkomen kan worden indien Patiënten dit traject doorlopen. ClaudicatioNet ambieert daarom een continu proces van onderzoek, verbetering en bewijsvoering voor de door haar ontwikkelde methode op basis van *het stepped care model* en *substitutie van zorg*.

Voor het kunnen verrichten van het Onderzoek naar de behandeling van Patiënten en het in kaart brengen van de resultaten voor de Fysiotherapeuten zullen ClaudicatioNet en het KNGF een exclusieve samenwerking ten aanzien van het Onderzoek naar *claudicatio intermittens* aangaan. De gerichte gegevens ten behoeve van dit Onderzoek van ClaudicatioNet zullen via de LDF worden verzameld en beheerd. De LDF wordt ten behoeve van het KNGF beheerd door een *Trusted Third Party* met specialisme in de medische sector, MediQuest B.V. te Utrecht (hierna te noemen: “MediQuest”).

De technische aspecten van het uitvoeren van het Onderzoek heeft ClaudicatioNet uitbesteed aan Softmedia Interactive VOF (hierna te noemen: “Softmedia”). Softmedia zal op basis van geselecteerde relevante data een presentatiemodel ontwikkelen, zodat individuele Fysiotherapeuten hun eigen handelen en prestaties kunnen vergelijken met de totale populatie aan Fysiotherapeuten, aangesloten bij ClaudicatioNet. Daarnaast zal Softmedia in opdracht van ClaudicatioNet op geaggregeerd niveau diverse rapportages en vergelijkingen ontwikkelen die voor onderzoeksdoeleinden, zoals hiervoor omschreven, worden gebruikt, alsmede desgewenst voor overige doeleinden in het kader van het Onderzoek naar *claudicatio intermittens*, waaronder bijvoorbeeld het aantonen van de doeltreffendheid van de behandelmethode bestaande uit het inzetten van beweeginterventies.

Doel Dataprotocol
In dit dataprotocol hebben ClaudicatioNet en het KNGF de wijze van verwerking van persoonsgegevens van Patiënten en Fysiotherapeuten (hierna tezamen: “Persoonsgegevens”) in het kader van het Onderzoek vastgelegd, alsmede de uitvoering die zij hebben gegeven aan de

wettelijke verplichtingen die voortvloeien uit onder andere de Wbp (hierna: “Dataprotocol”). Tevens dient dit Dataprotocol transparantie te bieden aan Patiënten en Fysiotherapeuten ten aanzien van de verwerking van hun Persoonsgegevens in de samenwerking tussen het KNGF en ClaudicatioNet.

Wettelijk kader

In het kader van het door ClaudicatioNet voorgenomen Onderzoek zullen persoonsgegevens van Patiënten en Fysiotherapeuten worden verwerkt. In Nederland zijn de voorwaarden waaronder persoonsgegevens van natuurlijke personen[1] mogen worden verwerkt geregeld in onder andere de Wet bescherming persoonsgegevens (hierna: de “Wbp”).

> ***Verwerken***[2]*: 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 enig andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Anonimiseren van persoonsgegevens wordt ook gezien als verwerken.*
>
> ***Persoonsgegeven***[3]*: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Indien iemand (met gebruikmaking van welke middelen dan ook) direct of indirect identificeerbaar is, wordt dergelijke informatie ook als persoonsgegevens beschouwd.*
>
> ***Bijzonder persoonsgegeven***[4]***:*** *elk gegeven dat (direct of indirect) informatie geeft over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij aan één van de uitzonderingen is voldaan of uitdrukkelijke toestemming is gegeven.*

De verantwoordelijke voor de gegevensverwerking dient er zorg voor te dragen dat de verwerking in overeenstemming met de Wbp plaatsvindt. Het KNGF is verantwoordelijke ten aanzien van het verstrekken van persoonsgegevens aan ClaudicatioNet. Claudicationet is verantwoordelijke in het kader van de verwerking van persoonsgegevens voor het Onderzoek.

> ***Verantwoordelijk***[5]***:*** *de natuurlijke persoon of de rechtspersoon of ieder ander die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De verantwoordelijke dient te voldoen aan alle bepalingen van de Wbp. Het KNGF bepaalt of zij gegevens verstrekt aan Claudicationet, dus het KNGF is daarvoor de verantwoordelijke. Claudicationet bepaalt de wijze waarop het Onderzoek wordt verricht, hetgeen meebrengt dat Claudicationet verantwoordelijk is voor deze gegevensverwerking.*

[1] De betrokkene: degene op wie een persoonsgegeven betrekking heeft (artikel 1 sub f Wbp).
[2] Artikel 1 sub b Wbp.
[3] Artikel 1 sub a Wbp.
[4] Artikel 16 Wbp.
[5] Artikel 1 sub d Wbp.

2. Partijen en rolverdeling

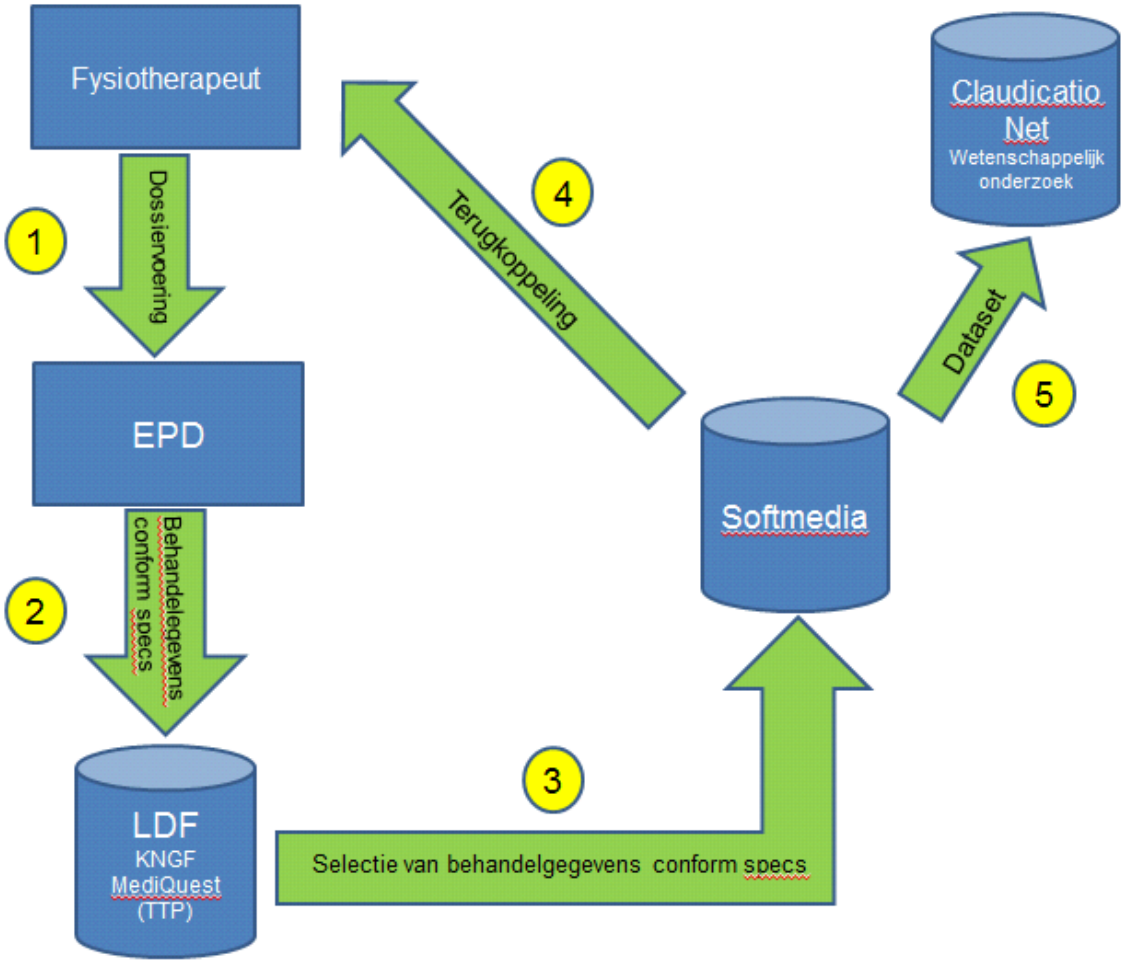
De bij dit Dataprotocol betrokken partijen zijn:

KNGF:	de vereniging met volledige rechtsbevoegdheid **Koninklijk Nederlands Genootschap voor Fysiotherapie**, gevestigd te (3817BA) Amersfoort aan de Stadsring 159 B, is verantwoordelijke voor de verwerking van Persoonsgegevens van Patiënten en Fysiotherapeuten in het kader van de LDF en in het kader van het Onderzoek naar (de behandelwijze voor) *claudicatio intermittens*.
ClaudicatioNet:	de **Stichting ClaudicatioNet**, gevestigd te (5623EJ) Eindhoven aan de Michelangelolaan 2, is verantwoordelijke voor de verwerking van Persoonsgegevens van Patiënten en Fysiotherapeuten in het kader van het Onderzoek naar (de behandelwijze voor) *claudicatio intermittens.*
MediQuest:	de besloten vennootschap **MediQuest B.V.**, gevestigd te (3581KP) Utrecht aan de Burgemeester Reigerstraat 89, is als dienstverlener en *Trusted Third Party* bewerker voor de verwerking van Persoonsgegevens van Patiënten en Fysiotherapeuten in het kader van de LDF en in het kader van het Onderzoek naar (de behandelwijze voor) *claudicatio intermittens*, in opdracht van het KNGF.
Softmedia:	de vennootschap onder firma **Softmedia Interactive VOF**, gevestigd te (5611VA) Eindhoven aan de Kanaaldijk-Zuid 15A, is als ICT dienstverlener bewerker voor de verwerking van Persoonsgegevens van Patiënten en Fysiotherapeuten in het kader van het Onderzoek naar (de behandelwijze voor) *claudicatio intermittens*, in opdracht van ClaudicatioNet.

Bovenstaande partijen worden in dit Dataprotocol tevens individueel “Partij” en tezamen “Partijen” genoemd.

3. Dataproces

Schematische weergave van het dataproces
Het dataproces ten aanzien van de verwerking van Persoonsgegevens in het kader van het Onderzoek, uitgevoerd door ClaudicatioNet in samenwerking met het KNGF, kan als volgt schematisch worden weergegeven:



1. Fysiotherapeut legt patiëntgegevens en behandelresultaten vast in het Elektronisch Patiënten Dossier ("EPD"):
   Conform de Nederlandse wet- en regelgeving is de fysiotherapeut tot het opstellen en bijhouden van een patiëntendossier, waarin de patiëntgegevens en behandelresultaten worden vastgelegd. De fysiotherapeut kan, indien hij geautomatiseerd werkt, de patiëntgegevens en behandelresultaten vastleggen in een EPD. Het opnemen en vastleggen van de patiëntgegevens en behandelresultaten door fysiotherapeuten geschiedt binnen de bedrijfstak fysiotherapie overwegend in een EPD.

   Het opnemen van patiëntgegevens en behandelresultaten in een EPD staat los van het Onderzoek door ClaudicatioNet. Het vastleggen van persoonsgegevens in een EPD valt derhalve buiten de scope van dit Dataprotocol.

2. Selectie van de patiëntgegevens en behandelresultaten wordt geëxporteerd naar de LDF:
   Een selectie van de patiëntgegevens en behandelresultaten in het EPD wordt vanuit het EPD geëxporteerd naar de LDF indien de patiënt daarvoor uitdrukkelijk toestemming heeft

gegeven (opt-in)[6].

Fysiotherapeuten die bij het KNGF bekend zijn als praktijkeigenaar, en derhalve een contract hebben met de EPD-leverancier, kunnen hun praktijk aanmelden voor aanlevering van patiëntgegevens en behandelresultaten aan de LDF. Dit geschiedt door middel van het instellen van de EPD-software en het aanmelden op de website van het KNGF: www.landelijkedatabasefysiotherapie.nl. Per in de praktijk werkzame fysiotherapeut wordt aangegeven of er patiëntgegevens en behandelresultaten door deze fysiotherapeut wordt aangeleverd aan de LDF.

De selectie van patiëntgegevens en behandelresultaten die vanuit het EPD wordt geëxporteerd naar de LDF wordt gespecificeerd in de meest recente specificatie zoals te vinden op de website www.landelijkedatabasefysiotherapie.nl, onder "*documenten/technische documentatie*".

3. Dataexport aan Softmedia.

4. ClaudicatioNet levert maandelijks een up-to-date lijst bij MediQuest aan ter identificatie van de Fysiotherapeuten. MediQuest levert in opdracht van het KNGF op basis van die lijst periodiek een dataexport van gegevens vanuit de LDF, waaronder Persoonsgegevens, aan Softmedia als bewerker van ClaudicatioNet, waarvan de verwerking noodzakelijk is in het kader van het Onderzoek. Een specificatie van de benodigde (Persoons)gegevens is opgenomen in bijlage 4 van de samenwerkingsovereenkomst tussen het KNGF en ClaudicatioNet. Een specificatie van deze afspraken tussen ClaudicatioNet en het KNGF is uitgewerkt in Bijlage 5 van dit Dataprotocol.

   In opdracht van Claudicationet verricht Softmedia de bewerkingen op en analyses van deze Persoonsgegevens, benodigd om rapportages en benchmarks te tonen aan Fysiotherapeuten en ClaudicatioNet.

5. Benchmark: terugkoppeling naar de individuele Fysiotherapeuten
   Softmedia bewerkt in opdracht van ClaudicatioNet de (Persoons)gegevens om aan Fysiotherapeuten rapportages en benchmarks ter beschikking te stellen op de website van ClaudicatioNet. Deze rapportages en benchmarks ontvangen de Fysiotherapeuten in een individuele en voor de buitenwereld afgeschermde omgeving.

6. Rapportages en data ten behoeve van ClaudicatioNet
   ClaudicatioNet verricht analyses op de Persoonsgegevens voor het Onderzoek. De analyses, rapportages en data die relevant zijn in het kader van het door ClaudicatioNet te verrichten Onderzoek worden door ClaudicatioNet opgeslagen in een hiertoe specifiek ingerichte en beveiligde locatie binnen de ICT omgeving van het Catharinaziekenhuis (zie ook bijlage 3).

   ClaudicatioNet kan de rapportages en/of data verder verwerken. Hiertoe kan ClaudicatioNet gebruik maken van derden. ClaudicatioNet zal daarbij de privacyaspecten van de Persoonsgegevens van de Patiënten en Fysiotherapeuten in acht nemen. Eventuele samenwerkingen van ClaudicatioNet met derden binnen de kaders van het Onderzoek valt buiten de scope van dit Dataprotocol, tenzij deze derden zijn toegetreden tot het Dataprotocol door middel van ondertekening daarvan.

[6] Als (delen van) een patiëntendossier elektronisch beschikbaar worden gesteld voor anderen, dan moet de zorgverlener vooraf uitdrukkelijk toestemming vragen aan de patiënt. Die uitdrukkelijke toestemming wordt **opt-in** genoemd.

Uitvoering van de dataprocessen door bewerkers
MediQuest en Softmedia verbinden zich de Persoonsgegevens uitsluitend te verwerken ten behoeve van de doeleinden waarvoor zij door respectievelijk het KNGF en ClaudicatioNet zijn verzameld, waaronder in ieder geval begrepen de in dit Dataprotocol omschreven doeleinden, en louter volgens instructie van het KNGF en/of ClaudicatioNet.

MediQuest en Softmedia verbinden zich om geen gebruik te maken van de in het kader van de samenwerking tussen het KNGF en ClaudicatioNet verkregen Persoonsgegevens voor eigen doeleinden of doeleinden van derden zonder uitdrukkelijke en schriftelijke toestemming van het KNGF respectievelijk ClaudicatioNet en te voldoen aan overige (wettelijke) verplichtingen, waaronder het informeren en toestemming verkrijgen van de patiënt. Te dien aangaande hebben het KNGF en ClaudicatioNet een bewerkersovereenkomst gesloten met MediQuest respectievelijk Softmedia, welke bewerkersovereenkomsten zijn bijgevoegd in bijlage 1 van dit Dataprotocol.

Claudicationet verbindt zich voorts om geen gebruik te maken van de (Persoons)gegevens die zijn verkregen onder dit Dataprotocol voor een ander doel(einde) dan het Onderzoek, zonder voorafgaande schriftelijke toestemming van het KNGF.

4. Verkrijging en beheer van Persoonsgegevens

Verkrijging van Persoonsgegevens
De Persoonsgegevens die gebruikt worden ten behoeve van het Onderzoek door ClaudicatioNet worden verkregen via het EPD van de Fysiotherapeuten.

Voor het verwerken van de Persoonsgegevens in het kader van het MKIB door het KNGF is de toestemming van de Patiënt gevraagd door de Fysiotherapeut, en tevens heeft de Fysiotherapeut de Patiënt hieromtrent geïnformeerd ten tijde van het verlenen van voornoemde toestemming. Ook is bij het verkrijgen van de toestemming van de Patiënt er door de Fysiotherapeut op gewezen dat de Persoonsgegevens aan derden kunnen worden verstrekt voor wetenschappelijke onderzoek, waaronder het Onderzoek valt zoals door Claudicationet verricht wordt.

Verzoeken van Patiënt of Fysiotherapeut
Een Patiënt kan bij zijn Fysiotherapeut een verzoek doen om inzage in de van hem/haar verwerkte Persoonsgegevens en/of een verzoek doen tot verbetering, aanvulling, verwijdering of afscherming. Tevens kan een Fysiotherapeut bij het KNGF een verzoek tot inzage in de van hem/haar verwerkte Persoonsgegevens en/of een verzoek doen tot verbetering, aanvulling, verwijdering of afscherming doen.

Om ervoor te zorgen dat tijdig aan de verzoeken van een Patiënt of Fysiotherapeut kan worden voldaan, dienen Partijen in een voorkomend geval het Protocol Verzoeken Betrokkene nauwgezet te volgen. Het Protocol Verzoek Betrokkene is opgenomen in bijlage 2 bij dit Dataprotocol.

Op basis van de Wbp heeft de betrokkene het recht om inzage te vragen in de persoonsgegevens die een verantwoordelijke van hem verwerkt. Binnen vier weken moet de verantwoordelijke laten weten of er persoonsgegevens van die betrokkene worden verwerkt, en zo ja een overzicht verstrekken van de persoonsgegevens die worden verwerkt, onder vermelding van het doel, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.

De betrokkene kan vervolgens de verantwoordelijke verzoeken de hem betreffende persoonsgegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. De verantwoordelijke moet binnen vier weken aan het verzoek voldoen, danwel berichten waarom hij niet aan het verzoek zal voldoen.

Onder bijzondere omstandigheden heeft de betrokkene het recht verzet aan te tekenen tegen de verwerking van zijn of haar persoonsgegevens.

5. Beveiliging van Persoonsgegevens

Beveiliging
Alle Partijen die betrokken zijn bij de verwerking van de Persoonsgegevens in het kader van het Onderzoek van ClaudicatioNet en in dat kader dit Dataprotocol hebben ondertekend, zullen adequate technische en organisatorische maatregelen treffen om de Persoonsgegevens te beschermen tegen verlies en beschadiging.

Voorbeelden van organisatorische maatregelen die Partijen in dit verband kunnen treffen zijn:

- Fysieke beveiliging van de bedrijfsomgeving van Partijen en door hen ingeschakelde derden;
- Geautoriseerde toegang tot bedrijfsomgeving van Partijen en door hen ingeschakelde derden;
- Werknemersbeleid inzake mobiele opslag, zoals laptop en USB-sticks;
- Werknemersbeleid inzake documentatie;
- Beleid inzake vernietiging van hardware, software en data.

Voorbeelden van technische maatregelen die Partijen in dit verband kunnen treffen zijn:.

- Encryptie van de (persoons)gegevens en (internet)verbindingen;
- Autorisatieprotocol voor toegang tot de systemen van Partijen;
- Beveiliging van opslag (servers);
- Back-up op dubbele locatie;
- Mutatielog van (o.a.) inlogpogingen en muteren/verwijderen (persoons)gegevens (audit/trial);
- Anonimisering van persoonsgegevens.

Voor de verdere uitwerking van de door Partijen getroffen maatregelen, behaalde certificeringen en/of (interne) voorschriften die worden nageleefd ten aanzien van de beveiliging van (persoons)gegevens wordt verwezen naar bijlage 3 bij dit Dataprotocol.

De beveiliging van de EPD's en de ICT systemen bij de Fysiotherapeuten en/ of EPD leveranciers valt buiten de reikwijdte van dit Dataprotocol. Hiertoe dienen die (aanleverende) partijen zelf adequate maatregelen te treffen.

Beveiligingsbeheer
Voor het geval zich – ondanks de getroffen beveiligingsmaatregelen – bij een Partij of bij meerdere Partijen een beveiligingsincident voordoet, hebben Partijen een protocol beveiligingsbeheer geïmplementeerd. Dit protocol Beveiligingsbeheer is bijgevoegd als bijlage 4 bij dit Dataprotocol.

6. Controle en rapportage

Vaststellen van het Dataprotocol
Dit Dataprotocol zal door ClaudicatioNet, het KNGF, MediQuest en Softmedia worden ondertekend. Vanaf het moment van ondertekening door Partijen zal dit Dataprotocol voor onbepaalde tijd in werking treden.

Evalueren en wijzigen van het Dataprotocol
Partijen zullen de verwerking van Persoonsgegevens evalueren en van deze evaluatie schriftelijke documentatie bijhouden, een en ander volgens onderstaande tabel.

Rapport type	Periodiciteit	Wijze	Verantwoordelijke
• Beveiligingsincidenten. • Ongeautoriseerde mutaties aan sourcecode, data, databases, servers en netwerkcomponenten. • Fails van continuïteit, back-up en recovery. • (Indicatie van) Onbevoegde toegang. • Lekken van informatie en (patiënt)gegevens. • Overtreding van fysieke en logische beveiligings-maatregelen. • Verbetermaatregelen indien bovenstaande daar aanleiding toe geeft.	Wanneer zich één of meerdere van de situatie zich voordoet, alsmede maandelijks.	Schriftelijk	Betrokken partij(en) NB: Wanneer een partij ISO 27001 gecertificeerd is zijn de genoemde punten geborgd via signaal registratie, conform het kwaliteitsmanagement systeem.
• Review Dataprotocol. • Review beveiligingsbeleid van Partijen. • Review protocol beveiligingsbeheer.	Jaarlijks of na belangrijke wijzigingen in informatiesystemen/ernstige beveiligingsincidenten en/of relevante wetswijziging.	Schriftelijk	Betrokken partij(en)
• Review bewerkersovereenkomst. • Review privacy statement. • Review protocol verzoeken betrokkene.	Jaarlijks of na een relevante wetswijziging of wijziging in de verwerking ten aanzien van het Onderzoek	Schriftelijk	Betrokken partij(en)

Partijen zullen jaarlijks tezamen de uitkomsten van de individuele evaluaties bespreken. Voorstellen tot wijzigingen van dit Dataprotocol of één van de bijlagen worden op initiatief van één of meerdere Partijen ter inhoudelijke besluitvorming voorgelegd aan de overige Partijen bij dit Dataprotocol. Wijzigingen in het Dataprotocol treden pas in werking nadat alle Partijen hebben ingestemd met de wijziging. Partijen zullen instemming niet op onredelijke gronden onthouden.

Afstemmingscommissie.
In aanvulling op de jaarlijkse bespreking tussen Partijen, zullen het KNGF en ClaudicatioNet een afstemmingscommissie instellen. De afstemmingscommissie is verantwoordelijk voor de monitoring van de gegevensverwerking zoals bedoeld in dit Dataprotocol.

De afstemmingscommissie kan voorts zelfstandig beslissingen nemen over:

- Gezamenlijke externe communicatie van Partijen conform bijlage 5 ‘communicatieparagraaf’ van de samenwerkingsovereenkomst tussen het KNGF en ClaudicatioNet.;
- Communicatie waarin de andere Partij(en) direct of indirect worden genoemd;
- Methodologie (zoals bijvoorbeeld minimaal aantal waarnemingen voor presentatie van de data). Hierbij kunnen MediQuest en Softmedia gevraagd worden te adviseren;
- Delen van Persoonsgegevens of andere data met derden, danwel data openbaar maken, te allen tijde rekening houdende met de rechtmatigheid hiervan onder meer in het licht van de geldende privacy wet- en regelgeving;
- Toetreden van andere partijen tot dit Dataprotocol.

Ondertekening

ClaudicatioNet	KNGF	MediQuest	Softmedia
Dhr. Prof. Dr. J. Teijink	Dhr. Drs. M. Sturkenboom	Dhr. K. Verheijke	Dhr. E. van Vijfeijken
Voorzitter	Directeur	Projectleider	Eigenaar
Handtekening:	**Handtekening:**	**Handtekening:**	**Handtekening:**
Datum:	Datum:	Datum:	Datum:
Plaats:	Plaats:	Plaats:	Plaats:

BIJLAGEN

BIJLAGE 1 DATAPROTOCOL MKIB-CLAUDICATIONET - BEWERKERSOVEREENKOMST
BEWERKERSOVEREENKOMST

De ondergetekenden:

1. Koninklijk Nederlands Genootschap voor Fysiotherapie, kantoorhoudende en gevestigd te (3817BA) Amersfoort aan de Stadsring 159, vertegenwoordigd door dhr. Drs. M. Sturkenboom (hierna te noemen "***Verantwoordelijke***"),

   en,

2. MediQuest B.V. kantoorhoudende en gevestigd te (3581KP) Utrecht aan de Burgemeester Reigerstraat 89, vertegenwoordigd door dhr. J.R. Schaefer (hierna te noemen "***Bewerker***"),

Gezamenlijk hierna ook te noemen"***Partijen***",

Overwegende dat:

- Verantwoordelijke werkzaam is op het gebied van de verwerking van persoonsgegevens van patiënten en fysiotherapeuten ten behoeve van de Landelijke Database Fysiotherapie ("LDF") en, in dat kader persoonsgegevens vanuit Elektronische Patiënt Dossiers ("EPD") in de LDF worden opgenomen, verwerkt en eventueel verstrekt aan derden voor wetenschappelijk en/of kwaliteitsonderzoek overeenkomstig het Dataprotocol LDF en/of op de verstrekking van toepassing zijnde (aanvullende) dataprotocollen;
- Bewerker voor Verantwoordelijke als dienstverlener en *Trusted Third Party* voor de verwerking van persoonsgegevens van patiënten en fysiotherapeuten in het kader van de LDF, in opdracht van Verantwoordelijke (bijzondere) persoonsgegevens verwerkt;
- Verantwoordelijke ten aanzien van de verwerking van persoonsgegevens als verantwoordelijke in de zin van artikel 1 sub d van de Wet bescherming persoonsgegevens ("Wbp") is aan te merken;
- Bewerker ten aanzien van het voor Verantwoordelijke opslaan en verwerken, in de zin van artikel 1 sub b Wbp, van de persoonsgegevens als bewerker in de zin van artikel 1 sub e Wbp is aan te merken;
- Partijen - mede ter uitvoering van het bepaalde in artikel 14 lid 2 van de Wbp – in de onderhavige overeenkomst een aantal voorwaarden wensen vast te leggen die van toepassing zijn op hun relatie in verband met de genoemde activiteiten in opdracht van en ten behoeve van Verantwoordelijke.

Verklaren te zijn overeengekomen als volgt:

Artikel 1 Definities

1.1 In deze Bewerkersovereenkomst hebben de volgende begrippen, steeds met een hoofdletter geschreven, de volgende betekenis ongeacht of deze in meervoud of enkelvoud worden gebruikt:

a. *Annex*: aanhangsel bij de Bewerkersovereenkomst, dat onlosmakelijk deel uitmaakt van de Bewerkersovereenkomst;

b. *Bewerkersovereenkomst*: de onderhavige overeenkomst welke deel uitmaakt van de Overeenkomst;

c. *Incident*: elk incident dat betrekking heeft of kan hebben op de Verwerking van Persoonsgegevens, waaronder begrepen maar niet beperkt tot geconstateerde of vermoede ongeautoriseerde of onrechtmatige verwerking, verwijdering en verlies van persoonsgegevens, datalekken in de zin van artikel 34a Wbp, inbreuken op de beveiliging, geheimhouding of integriteit van systemen, infrastructuur en/of Persoonsgegevens;

d. *Overeenkomst*: de tussen Verantwoordelijke en Bewerker gesloten Mantelovereenkomst terzake de levering, implementatie en onderhoud van het systeem voor de landelijke database fysiotherapie, alsmede het addendum daarop van 31 december 2013 en het Dataprotocol LDF;

e. *Persoonsgegevens*: alle gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon als bedoeld in artikel 1 aanhef en onder a Wbp;

f. *Verwerken*: het verwerken van Persoonsgegevens als bedoeld in artikel 1 sub b Wbp.

Artikel 2 Verantwoordelijke voor en Bewerker van de gegevens

2.1 Bewerker verbindt zich in het kader van deze overeenkomst uitsluitend Persoonsgegevens te Verwerken in opdracht van Verantwoordelijke.

2.2 Verantwoordelijke is verantwoordelijk voor de Verwerking van de Persoonsgegevens in het kader van de Overeenkomst.

Artikel 3 Doel van de Verwerking

3.1 Verantwoordelijke en Bewerker hebben onderhavige Bewerkersovereenkomst gesloten met betrekking tot uitvoering van de Overeenkomst. Hiertoe zullen Persoonsgegevens door Bewerker worden Verwerkt.

3.2 Bewerker verbindt zich uitsluitend Persoonsgegevens te Verwerken ten behoeve van de in deze Bewerkersovereenkomst en/of de Overeenkomst genoemde activiteiten.

3.3 Bewerker verbindt zich om geen gebruik te maken van de in het kader van deze Bewerkersovereenkomst en/of de Overeenkomst te Verwerken en Verwerkte Persoonsgegevens voor eigen doeleinden of doeleinden van derden zonder uitdrukkelijke en schriftelijke toestemming van Verantwoordelijke.

Artikel 4 Algemene zorgplicht Bewerker

4.1 Bewerker draagt ten aanzien van de in artikel 2 bedoelde Verwerkingen zorg voor de naleving van deze Bewerkersovereenkomst en voor de naleving van privacywetgeving zoals de Wbp. Bewerker verbindt zich desgevraagd Verantwoordelijke te informeren over de door Bewerker genomen maatregelen aangaande deze zorgplicht.

Artikel 5 Technische en organisatorische voorzieningen

5.1 Bewerker zal passende technische en organisatorische maatregelen ten uitvoer leggen om Persoonsgegevens te beveiligen tegen (toevallig of opzettelijk) verlies, vernietiging of tegen enige vorm van onrechtmatige Verwerking, waaronder vervalsing en niet-toegelaten verspreiding of toegang, zoals nader gespecificeerd in Bijlage 4 bij het Dataprotocol LDF en/of in aanvullende dataprotocollen. Deze maatregelen zullen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen, gelet op de risico's die de Verwerking en de aard van de te beschermen gegevens met zich meebrengen.

5.2 Bewerker neemt passende technische en organisatorische maatregelen om de werkruimte te beveiligen en de toegang tot de werkruimte door derden te voorkomen. Indien Verantwoordelijke dat nodig acht, kan zij hieromtrent schriftelijke instructies (laten) geven, welke door Bewerker onverwijld zullen worden opgevolgd.

5.3 Verantwoordelijke is gerechtigd de maatregelen en de naleving van de op Bewerker rustende verplichtingen te controleren op de wijze als bepaald in artikel 9, hetgeen de verantwoordelijkheid van Bewerker voor desbetreffende verplichtingen onverlet laat.

Artikel 6 Vertrouwelijkheid

6.1 Bewerker zal slechts na voorafgaande schriftelijke toestemming van Verantwoordelijke derden inschakelen bij de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Overeenkomst. Indien Bewerker met schriftelijke toestemming van Verantwoordelijke een derde inschakelt bij de Verwerking van Persoonsgegevens, staat Bewerker ervoor in dat aan die derde minimaal dezelfde verplichtingen worden opgelegd, zoals neergelegd in deze Bewerkersovereenkomst. Bewerker zal de overeenkomst met de derde, alsmede overig bewijs van het voldoen aan deze garantie aan Verantwoordelijke overleggen.

6.2 Bewerker zal op geen enkele wijze de informatie welke aan haar in het kader van de Overeenkomst bekend wordt aan derden bekend maken, tenzij zij daartoe verplicht is op grond van de wet, een rechterlijk bevel of als dit geschiedt op grond van voorafgaande schriftelijke toestemming en/of expliciete instructie van Verantwoordelijke.

6.3 Bewerker garandeert dat de van Verantwoordelijke verkregen Persoonsgegevens alsmede de uitwisseling van door haar vastgelegde en verwerkte Persoonsgegevens ten opzichte van haar werkzaamheden voor en de informatiestromen aan derden strikt gescheiden te houden van andere informatie en gegevens en deze informatie en gegevens logisch te scheiden.

Artikel 7 Aansprakelijkheid Bewerker

7.1 Bewerker vrijwaart Verantwoordelijke tegen claims en aanspraken van derden voor schade (beweerdelijk) veroorzaakt door wederrechtelijke Verwerking van Persoonsgegevens of door

enige daad die in strijd is met de Wbp, andere toepasselijke wettelijke bepalingen of met deze Bewerkersovereenkomst of de Overeenkomst, alsmede voor boetes opgelegd door bevoegde autoriteiten als gevolg van voornoemde daad. Het voorgaande geldt niet indien dergelijke claims het gevolg zijn van een toerekenbare tekortkoming van Verantwoordelijke.

7.2 Op Bewerker rust de bewijslast dat zij de nodige maatregelen zoals deze uit de Bewerkersovereenkomst en uit de Overeenkomst voortvloeien, heeft genomen.

7.3 Ten aanzien van het bepaalde in artikel 7.1, geldt ten aanzien van de aansprakelijkheid van Bewerker en Verantwoordelijke de in artikel 11 van de Overeenkomst opgenomen regeling inzake de beperking van aansprakelijkheid.

Artikel 8 Gegevensverwerking buiten Nederland

8.1 Het overbrengen van Persoonsgegevens door Bewerker buiten Nederland is alleen toegestaan met in achtneming van de daarvoor geldende wettelijke verplichtingen en na voorafgaande schriftelijke toestemming van Verantwoordelijke.

Artikel 9 Controle & toezicht

9.1 Bewerker is gehouden op verzoek van Verantwoordelijke dan wel door Verantwoordelijke aan te wijzen (externe) deskundigen, conform de beveiligingsnormen, steeds onvoorwaardelijke en ongelimiteerde inzage- en controlerecht te (doen) verschaffen in haar adequate, overzichtelijke en afzonderlijk bij te houden administratie, automatiseringssystemen, verwerkingsorganisatie en alle verdere relevante bescheiden in het kader van de uitvoering van de Bewerkersovereenkomst en de Overeenkomst, zodat Verantwoordelijke in staat is om de naleving van hetgeen Partijen zijn overeengekomen adequaat te kunnen toetsen. Tevens zal toegang worden verschaft aan de toezichthouders van Verantwoordelijke in het kader van de uitoefening van hun wettelijke taken.

9.2 Verantwoordelijke zal derden, die betrokken zijn bij inzage- en/of controlewerkzaamheden als bedoeld in het vorige lid, terzake een geheimhoudingsverklaring laten tekenen en zodanige maatregelen nemen, zoals beveiliging van gegevensdragers, teneinde te garanderen dat deze geheimhoudingsplicht wordt nagekomen.

9.3 De uitkomsten van het in het eerste lid genoemde controles zullen zowel aan Bewerker als aan Verantwoordelijke in schriftelijke vorm worden opgeleverd.

Artikel 10 Melding Incident

10.1 Bewerker zal Verantwoordelijke onverwijld, maar in ieder geval binnen 24 uur op de hoogte stellen van:

a. een Incident of een schending van één van de verplichtingen als opgenomen in deze Bewerkersovereenkomst, op de wijze zoals bedoeld in Bijlage 5 bij het Dataprotocol LDF en/of in aanvullende dataprotocollen;
b. een klacht of verzoek (tot bijvoorbeeld inzage, correctie, aanvulling, verwijdering of afscherming) van een individu waarvan Persoonsgegevens worden Verwerkt. Partijen kunnen nadere afspraken maken over de wijze waarop de Verantwoordelijke wordt geïnformeerd; en/of
c. een verzoek of bevel van, of onderzoek door, een toezichthouder of andere bevoegde autoriteit, voor zover dit is toegestaan ingevolge toepasselijke dwingende wet- en regelgeving Partijen kunnen nadere afspraken maken over de wijze waarop de Verantwoordelijke wordt geïnformeerd.

10.2 Bewerker zal voorts zo spoedig mogelijk aan de Verantwoordelijke alle relevante informatie verstrekken omtrent een Incident en de door Verantwoordelijke verzochte redelijke medewerking verlenen bij het uitvoeren van haar wettelijke verplichtingen ten aanzien van het Incident. Verder zal Bewerker Verantwoordelijke op de hoogte houden van eventuele nieuwe ontwikkelingen rond een Incident.

10.3 Bewerker zal na constatering van een Incident alle redelijke maatregelen nemen teneinde het Incident te verhelpen en de (mogelijke) gevolgen daarvan zo veel mogelijk te beperken. Bewerker zal tevens die maatregelen treffen die noodzakelijk zijn om een herhaling van het Incident te voorkomen.

10.4 Bewerker zal niet zelfstandig melding doen van Incidenten bij de betreffende toezichthouder en/of de Betrokkenen.

10.5 Bewerker zal haar redelijke medewerking verlenen aan Verantwoordelijke voor zover dat noodzakelijk is om uitvoering te kunnen geven aan:

a. een verzoek van een Betrokkene om mede te delen of over hem Persoonsgegevens worden verzameld als bedoeld in artikel 35 lid 1 Wbp; en/of
b. verzoek van Verantwoordelijke om de door Verantwoordelijke aangeduide Persoonsgegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen.

10.6 Bewerker heeft zodanige interne protocollen en regelingen geïmplementeerd dat zij aan haar verplichtingen uit dit artikel 10 van deze Bewerkersovereenkomst kan voldoen binnen de daartoe gestelde termijnen. Bewerker zal deze protocollen en regelingen op eerste verzoek aan Verantwoordelijke verstrekken.

Artikel 11 Beëindiging & varia

11.1 Ten aanzien van de beëindiging of ontbinding van deze Bewerkersovereenkomst, gelden de bepalingen daarover van de Overeenkomst.

11.2 De verplichtingen uit deze Bewerkersovereenkomst die naar hun aard bestemd zijn om beëindiging te overleven, blijven ook na beëindiging van deze Bewerkersovereenkomst van kracht.

11.3 De rechtskeuze en bevoegde rechter komen overeen met het bepaalde te dien aanzien in de Overeenkomst.

Ondertekening

Plaats en datum

Verantwoordelijke Bewerker

BIJLAGE 2 DATAPROTOCOL MKIB - CLAUDICATIONET PROTOCOL VERZOEK BETROKKENE

Dit protocol Verzoek Betrokkene heeft tot doel overeenstemming te bereiken tussen de bij het Dataprotocol betrokken partijen over de handelswijze en onderlinge communicatie, indien een verzoek van een betrokkene door één van partijen wordt ontvangen, voor zover dat verzoek zich (mede) richt tot of betrekking heeft op één of meer van de andere partijen.

Een verzoek van een betrokkene kan zien op het verstrekken, verbeteren, aanvullen, verwijderen of afschermen van persoonsgegevens die één of meerdere van de partijen onder zich houdt. Alle partijen dragen er zorg voor dat de uitvoering van de handelingen zoals bedoeld in dit protocol tijdig geschieden, zodat het verzoek binnen de daarvoor geldende wettelijke termijn kan worden afgerond.

Alle partijen dragen er zorg voor dat hun werknemers op de hoogte zijn van en handelen in lijn met dit protocol.

Verzoeken

Verzoeken dienen door de betrokkene gericht te worden aan ClaudicatioNet, voor zover het verzoek betrekking heeft op persoonsgegevens die verwerkt worden in het kader van het Onderzoek en aan KNGF voor zover het verzoek betrekking heeft op persoonsgegevens die in het kader van het LDF verwerkt worden – waaronder het verstrekken van de persoonsgegevens aan ClaudicatioNet.

Contactgegevens

In het kader van de uitvoering van de handelingen zoals beschreven in dit protocol zullen partijen gebruik maken van de onderstaande contactgegevens:

Koninklijk Nederlands Genootschap voor Fysiotherapie: Gerrit Verrips
Afdeling/functie: Intern bedrijfsbureau
E-mail: verrips@kngf.nl
Adres: Stadsring 159B, 3817 BA Amersfoort

Stichting ClaudicatioNet: Yvonne Spierings-Peeters
Afdeling/functie: Landelijk coördinator ClaudicatioNet
E-mail: yvonne.peeters@catharinaziekenhuis.nl
Adres: Michelangelolaan 2, 5623 EJ Eindhoven

MediQuest: Kees Verheijke
Afdeling/functie: Projectleider
E-mail: Kverheijke@mediquest.nl
Adres: Burgemeester Reigerstraat 89, Utrecht

Softmedia: Emile van Vijfeijken
Afdeling/functie: Eigenaar Softmedia
E-mail: emile@softmedia.nl
Adres: Kanaaldijk-zuid 15A 5611 VA Eindhoven

Indien een verzoek van een betrokkene op een andere wijze dan via bovengenoemde contactgegevens bij één van partijen binnen komt, zal de medewerker van de betreffende partij die dit verzoek ontvangt, dit verzoek zo spoedig mogelijk doorzenden aan de hierboven vermelde afdeling van zijn bedrijf.

Afhandeling
Wanneer het verzoek is ontvangen op de juiste afdeling van één partij (hierna te noemen: “Ontvanger”), zal die partij de ontvangst van het verzoek aan de betrokkene bevestigen op het (e-mail)adres waarvan het verzoek afkomstig is. Tevens zal de Ontvanger het verzoek zo spoedig mogelijk toesturen aan de correcte afdelingen van de andere partijen zoals hierboven vermeld, voor zover die partij verantwoordelijk is voor de verwerking waarop het verzoek ziet, danwel indien de ondersteuning van die partij noodzakelijk is om aan het verzoek te voldoen.

De betreffende partijen zullen vervolgens de inhoud van het verzoek bestuderen. Indien een partij het verzoek onvolledig en/of onduidelijk acht, zal die partij om aanvullende informatie vragen bij de Ontvanger. De Ontvanger zal de betrokkene verzoeken om aanvullende informatie te verstrekken. Indien het verzoek wel duidelijk is of duidelijk is geworden na ontvangst van de aanvullende informatie, zullen partijen het verzoek onverwijld in behandeling nemen.

Indien het verzoek bestaat uit het verstrekken van persoonsgegevens aan de betrokkene, zullen partijen een overzicht van de gegevens die zij ten aanzien van die betrokkene verwerken in een algemeen gebruikt format aan de Ontvanger verstrekken, inclusief de informatie zoals bedoeld in artikel 35 lid 2 en 4 Wet bescherming persoonsgegevens (“Wbp”). Partijen kunnen nadere afspraken maken over het format dat wordt gehanteerd. Indien een partij geen gegevens van de betrokkene verwerkt, doet die partij daarvan tevens schriftelijk mededeling aan de Ontvanger.

Wanneer de Ontvanger van alle relevante partijen het overzicht van de verwerkte gegevens of de melding dat geen gegevens worden verwerkt heeft ontvangen, zal zij aan de betrokkene een volledig overzicht van de door partijen verwerkte persoonsgegevens verstrekken.

Indien het verzoek bestaat uit het verwijderen, verbeteren, aanvullen of afschermen van persoonsgegevens zullen partijen de Ontvanger er schriftelijk van op de hoogte brengen wanneer hier aan is voldaan. Indien een partij niet aan het verzoek tot verwijderen, verbeteren, aanvullen of afschermen kan of zal voldoen, informeert die de Ontvanger schriftelijk over het niet voldoen aan het verzoek en de redenen waarom.

Partijen zullen het overzicht en/of de mededelingen zoals hierboven beschreven onverwijld uitvoeren, ten minste op zodanige wijze dat Ontvanger binnen een termijn van vier (4) weken na ontvangst van een verzoek van betrokkene op het verzoek van betrokkene kan reageren.

BIJLAGE 3 DATAPROTOCOL MKIB-CLAUDICATIONET - BEVEILIGINGSMAATREGELEN PARTIJEN

Deze bijlage bevat de verdere uitwerking van de door Partijen getroffen maatregelen, behaalde certificeringen en/of (interne) voorschriften die worden nageleefd ten aanzien van de beveiliging van (persoons)gegevens.
De beveiliging van de EPD's en de ICT systemen bij de Fysiotherapeuten en/of EPD leveranciers valt buiten de reikwijdte van dit Dataprotocol. Hiertoe dienen die (aanleverende) Partijen zelf adequate maatregelen te treffen. In het Dataprotocol LDF van KNGF staat beschreven welke beveiligingsmaatregelen KNGF heeft getroffen.

De betreffende Partijen zijn:
- MediQuest
- Softmedia
- ClaudicatioNet

MEDIQUEST:

Certificering:
MediQuest heeft certificaten ISO 27001 en NEN 7510 behaald en voldoet hiermee aan de bijbehorende eisen. MediQuest garandeert dat zij gedurende de looptijd van het Dataprotocol MKIB-ClaudicatioNet en/of zolang zij Persoonsgegevens verwerkt in het kader van het Onderzoek zal blijven voldoen aan de ISO 27001 en NEN 7510 normen, alsmede haar certificering voor die duur zal behouden. De normen worden jaarlijks getoetst door een extern bevoegde audit organisatie.

Voorbeelden van door MediQuest ingevoerde maatregelen om te voldoen aan de NEN- en ISO-normen zijn:
1. Laten tekenen van geheimhoudingsverklaring door betrokken partijen;
2. Autorisatie op basis van toegewezen rechten;
3. Wachtwoordbeleid;
4. Backup-restore-procedure;
5. Anti-virus-software;
6. Gebruik van encryptie om de webservice te benaderen;
7. Secure Socket Layer verbinding (https).

NEN-ISO/IEC 27001 specificeert eisen voor het implementeren, onderhouden en verbeteren van beveiligingsmaatregelen die zijn aangepast aan de behoeften van afzonderlijke organisaties. De norm bevat ook de voorschriften voor de beoordeling en behandeling van veiligheidsrisico's. De voorschriften zijn generiek en gelden voor elk type organisatie.

NEN 7510; informatie beveiliging in de zorgsector: Deze norm geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg moet treffen ter beveiliging van de informatievoorziening. De organisaties waarop de norm zich richt, variëren van individuele zorgverleners tot grote zorginstellingen en andere organisaties die bij de informatievoorziening in de gezondheidszorg zijn betrokken, zoals netwerkorganisaties en zorgverzekeraars. Het toepassingsgebied omvat de beveiliging van alle typen informatie in en tussen de genoemde organisaties en alle mogelijke vormen waarin de informatie wordt weergegeven, vastgelegd en overgedragen. Om de vereiste waarborging van vertrouwelijkheid integriteit en beschikbaarheid van de informatie te bepalen is een risicobeoordeling nodig. Risicobeoordeling is onderdeel van de eerste fase in de cyclus voor het beheersen van de informatiebeveiliging. Door implementatie van de beheersmaatregelen bij elk van de beheersdoelstellingen in deze norm kan een organisatie voldoen aan de eisen die in een risicobeoordeling zijn vastgesteld. Deze norm geeft daarmee aanwijzingen voor het organisatorisch en technisch inrichten van de informatiebeveiliging en beid zo een basis voor vertrouwen in de zorgvuldige informatievoorziening bij en tussen de

verschillende organisaties in de gezondheidszorg.

SOFTMEDIA:

1. Toegang
De volgende systemen kunnen direct of indirect leiden tot de opgeslagen Persoonsgegevens betreffende patiënten die door Fysiotherapeuten worden behandeld. Voor elk systeem is beschreven wie hier toegang tot heeft en hoe met inloggegevens omgegaan wordt. Voor alle systemen geldt dat er geen beleid is om wachtwoorden periodiek te veranderen.

1.1. Kantooromgeving/automatisering
De digitale kantooromgeving van Softmedia is een gesloten systeem, waar lokaal - of extern via een VPN verbinding - toegang tot verkregen wordt. Medewerkers van Softmedia maken hier als enige gebruik van. Wachtwoorden kunnen door de systeembeheerder aangepast, maar niet ingezien worden. Op locatie is een server (hierna “kantoorserver” genoemd) in een afgesloten ruimte aanwezig, welke voor administratieve doeleinden en back-ups wordt gebuikt.

1.2. Server
Voor ClaudicatioNet wordt een virtuele server bij TransIP afgenomen. Een virtuele server is een server die niet direct herleidbaar is naar technische hardware. Deze server is opgebouwd uit software die op één of meerdere hardware-platformen zijn geïnstalleerd. De inloggegevens voor deze server zijn voor alle medewerkers van Softmedia - via de kantoorserver - in te zien.

Ontwikkelaars maken voor hun projecten gebruik van een op hun desktop of laptop geïnstalleerde ontwikkelomgeving. Tevens wordt een bij TransIP afgenomen virtuele testserver gebruikt.

De projecten op de testserver zijn publiekelijk toegankelijk - vanwege gebruik door klanten -en de toegang hiervoor is op dezelfde manier ingericht als die voor de ClaudicatioNet server. Dat betekent dat ontwikkelde software samen met software van andere klanten op één server zijn opgeslagen.

De instanties, ofwel de database-opdeling naar klanten, van de ClaudicatioNet website die op deze omgevingen draaien maken gebruik van fictieve patiëntgegevens.

1.3. Database
Aan de ClaudicatioNet website is een database gekoppeld. De inloggegevens hiervoor zijn inzichtelijk voor medewerkers van Softmedia, maar worden niet aan derden verstrekt. Medewerkers van ClaudicatioNet hebben ook geen directe toegang tot deze database. Dit betekent dat login (toegang) tot de database aan Softmedia is voorbehouden. Want een database op zichzelf heeft beveiliging in de vorm van logingegevens.

1.4. Content Management System
Het Content Management System (“CMS”) omvat het algemene beheer van de website van ClaudicatioNet, bereikbaar op https://www.claudicationet.nl.
Het CMS is een door Softmedia ontwikkeld platform en de broncode is niet publiekelijk beschikbaar. Wel is de code aan klanten uitgeleverd die de hosting van hun website zelf verzorgen. Dit omvat een risico, omdat de broncode geanalyseerd kan worden door kwaadwillenden. Dit risico wordt niet groot geacht.

Middels één account is toegang hiertoe mogelijk; de zogenaamde admin account. De inloggegevens van deze admin zijn alleen door medewerkers van Softmedia in te zien en aan te passen. Softmedia

heeft hiermee ook toegang tot het CMS. De inloggegevens worden alleen verstrekt aan personen waarvan geverifieerd kan worden dat ze werkzaam zijn voor ClaudicatioNet.
Via het CMS kan de admin inloggegevens van gebruikers van het inloggedeelte (hierna “middle-end” genoemd) van de website aanpassen, maar niet inzien. Ook heeft de admin de mogelijkheid om gebruikers beheerrechten tot het middle-end te geven of te ontzeggen. Meer hierover in het volgende onderdeel.
Het CMS biedt geen toegang tot of inzicht in de patiëntgegevens. Dit CMS is een brug naar de Middle-end website, beschreven in de volgende paragraaf.

1.5. Middle-end website
De ClaudicatioNet website bevat een middle-end, waar Fysiotherapeuten toegang toe kunnen krijgen. Meerdere beheeraccounts zijn aanwezig, welke los staan van de admin account van het CMS. Alleen medewerkers die beheeractiviteiten uitvoeren, zullen toegang hebben tot deze beheeraccounts.
Deze beheerders hebben onder andere toegang tot gegevens van de Fysiotherapeut en kunnen de dashboards met patiëntgegevens samenstellen.
De beheerders hebben de mogelijkheid om wachtwoorden van Fysiotherapeuten aan te passen, maar kunnen deze niet inzien.
De beheerders kunnen met het dashboardbeheer selecties in de patiëntgegevens maken. Het resultaat van deze selecties worden in grafieken en andere weergaven gevisualiseerd.

Dashboards kunnen met andere gebruikers van het middle-end gedeeld worden. De beheerders hebben de mogelijkheid om een Excel bestand van de patiëntgegevens te genereren, voor het verwerken in het kader van het Onderzoek. Dit bestand bevat alle gegevens die – op basis van de selectie door MediQuest in opdracht van KNGF - vanuit het LDF worden geïmporteerd.

De enige gebruikers die de dashboards te zien krijgen zijn Fysiotherapeuten. De registratie van een Fysiotherapeut wordt handmatig goedgekeurd door de beheerders voordat deze toegang tot het middle-end krijgen. De Fysiotherapeuten hebben alleen inzicht in de rapporten die de beheerders samenstellen op basis van de Persoonsgegevens.

Voor alle gebruikers van het middle-end geldt dat bij het loginformulier de mogelijkheid aanwezig is om het wachtwoord van hun account te resetten. Dit gebeurt middels een link die men op het e-mailadres van de account ontvangt. De wachtwoorden worden “gesalt” versleuteld in de database opgeslagen.

2. Back-ups
Back-ups van de ClaudicatioNet website worden enkel digitaal bewaard. Elke nacht wordt een dump van de database gemaakt en naar de kantoorserver gekopieerd. Deze back-up wordt elke nacht overschreven. Elke zondag van de week wordt een back-up apart gezet. Deze wekelijkse back-ups worden een jaar bewaard.

CLAUDICATIONET:
De normering die in het Catharina Ziekenhuis te Eindhoven gehanteerd wordt qua data beveiliging ligt vastgelegd in de NEN-7510 normering (zie uitgebreide beschrijving hierboven onder ‘MediQuest’).
Voorbeelden van door ClaudicatioNet ingevoerde maatregelen om te voldoen aan de NEN-norm zijn:

1. Laten tekenen van geheimhoudingsverklaring door betrokken partijen;
2. Autorisatie op basis van toegewezen rechten;
3. Wachtwoordbeleid;
4. Backup-restore-procedure;
5. Anti-virus-software;
6. Gebruik van encryptie om de webservice te benaderen;
7. Secure Socket Layer verbinding (https).

Authenticatie
Om gebruik te kunnen maken van de IT systemen binnen het Catharina Ziekenhuis en toegang te krijgen tot data moet de gebruiker zich identificeren middels een domein account. Dit betreft een inlogaccount binnen een bepaald domein. Hierbij heeft een cluster van computers onderlinge authenticatie geregeld.
Dit kan middels het aanmelden met een persoonlijke domein account (gebruiker naam en bijbehorend wachtwoord), of d.m.v. authentiseren met een persoonlijke pas aan een systeem met pas lezer, waarbij de pas is gekoppeld aan je persoonlijke domein account. De pas wordt alleen verstrekt aan medewerkers van het Catharina Ziekenhuis. De medewerkers van ClaudicatioNet zijn tevens medewerkers van het Catharina Ziekenhuis. Autorisatie tot bepaalde domeinen is gekoppeld aan werkzaamheden. Hierbij wordt vanuit het domein afgedwongen dat het wachtwoord van een gebruiker aan bepaalde eisen moet voldoen.

Dit is het standaard beleid dat voor iedere user (gebruikers in een domein), medewerkers van het Catharina Ziekenhuis, in de omgeving van het Catharina Ziekenhuis wordt afgedwongen (Default Domain Policy). Hierbij moet het wachtwoord o.a. aan complexiteit eisen voldoen (“Enabled”). Deze complexiteit eisen worden vanuit Microsoft afgedwongen. Wat deze complexiteit eisen inhouden is te vinden op: https://technet.microsoft.com/en-us/library/hh994562.aspx

Data opslag en autorisatie
Alle toegangen tot applicaties en data worden geregeld via unieke domein groepen in het Microsoft Windows Active Directory domein (AD). Dit betreft dus ook de toegan tot Persoonsgegevens die verwerkt worden in het kader van het Onderzoek. Om toegang te hebben tot bepaalde data (of gebruik te kunnen maken van een bepaalde applicatie) moet de account dus lid zijn van de betreffende groepen in AD.
De data opslag van ClaudicatioNet gebeurt op de M: schijf en staat in een aparte folder (ook wel Share genoemd) waarvoor dus een unieke groep in AD bestaat. Enkel accounts welke lid zijn van deze groep hebben derhalve toegang tot deze folder/data (Share). Deze accounts zijn voorbehouden aan medewerkers van het Catharina Ziekenhuis die tevens medewerker van ClaudicatioNet zijn.

BIJLAGE 4 DATAPROTOCOL MKIB-CLAUDICATIONET - PROTOCOL BEVEILIGINGSBEHEER

Dit protocol Beveiligingsbeheer heeft betrekking op de maatregelen die zijn en worden genomen in het kader van verlies of beschadiging van of ongeautoriseerde toegang tot persoonsgegevens, danwel overige incidenten ten aanzien van persoonsgegevens (een “incident”), en de stappen die ondernomen worden indien een incident zich voordoet.

Alle werknemers van Partijen worden geacht op de hoogte te zijn van en te handelen in lijn met dit protocol.

Aanspreekpunt
Iedere Partij heeft een medewerker aangesteld die als contactpersoon fungeert in het kader van het beveiligingsbeleid. Deze medewerker wordt als Security Officer aangeduid. De Security Officer is verantwoordelijk voor het aansturen en coördineren van de (uitvoering van) dit Protocol beveiligingsbeheer. In dat kader heeft de Security Officer onder meerde volgende taken:

- Fungeren als meldpunt voor incidenten;
- Het (doen) instellen van een onderzoek naar het incident, waaronder ten minste begrepen de omvang van het incident, de betrokken persoonsgegevens en de wijze van ontstaan van het incident;
- Het (doen) initiëren van een actieplan en/of disaster recovery plan, zoals onderdeel uitmaakt van de beveiligingsmaatregelen, gespecificeerd in Bijlage 3.
- Het beoordelen – tezamen met de daarbij relevante personen binnen zijn/haar Partij, zoals bijvoorbeeld de juridische afdeling – of zijn/haar Partij als verantwoordelijke of als bewerker kwalificeert ten aanzien van de (verwerking van) persoonsgegevens die betrokken zijn bij het incident;
- Indien zijn/haar Partij kwalificeert als bewerker: het doorgeven van het incident aan de verantwoordelijke voor de gegevensverwerking;
- Indien zijn/haar Partij kwalificeert als verantwoordelijke: het beoordelen of het incident kwalificeert als een datalek in de zin van artikel 34a Wet bescherming persoonsgegevens en het melden van een incident bij de Autoriteit Persoonsgegevens;
- Het beoordelen – tezamen met de daarbij relevante personen binnen zijn/haar Partij, zoals bijvoorbeeld de juridische afdeling – of het datalek ook gemeld moet worden aan de betrokkene en zo ja, het (doen) verrichten van de melding aan de betrokkene;
- Het – in samenspraak met de daarbij relevante personen binnen zijn/haar Partij, zoals bijvoorbeeld de technische en/of juridische afdeling – (doen) treffen van maatregelen ter voorkoming en/of beperking van (de gevolgen van) het incident;
- Het tijdig aanleveren van de in dit Protocol beveiligingsbeheer vermelde rapportages;
- Beantwoorden van vragen van medewerkers over informatiebeveiliging en toepassing van het Protocol beveiligingsbeheer.

Incidenten
Indien een werknemer constateert of het redelijk vermoeden heeft dat er een incident heeft plaatsgevonden, zal hij/zij dit, vergezeld van zo veel mogelijk informatie omtrent het (vermoedelijke) incident, zo spoedig mogelijk melden aan zijn Security Officer. De Security Officer zal de melding van de werknemer beoordelen en de vereiste maatregelen treffen.

Indien de Partij de rol van bewerker in de zin van artikel 1 sub e Wbp vervult, zal de Security Officer de Partij onder wiens verantwoordelijkheid hij opereert zo spoedig mogelijk – doch uiterlijk binnen 24 uur – op de hoogte stellen van het incident via de door de Partijen opgegeven contactgegevens.

De melding aan de verantwoordelijke Partij bevat, voor zover mogelijk, de volgende gegevens:

- een beschrijving van het incident, waaronder de aard, de datum/periode en de omvang van het incident, alsmede het type persoonsgegevens en het aantal betrokkenen waarvan de persoonsgegevens betrokken zijn bij het incident;
- de (mogelijke) gevolgen van het incident;
- de genomen of aanbevolen maatregelen om de gevolgen van het incident zo veel mogelijk te beperken;
- de verwachtte tijd die gemoeid is met het oplossen van (de gevolgen van) het incident.

Voorts zal de Partij bij wie het incident zich heeft voorgedaan de verantwoordelijke Partij op de hoogte houden van de ontwikkelingen aangaande het incident en verantwoordelijke Partij voorzien van regelmatige rapportages dienaangaande.

Partijen zullen in het kader van het incident aan alle redelijke verzoeken van de andere Partijen voldoen en indien vereist haar medewerking verlenen. Waar mogelijk en/of vereist omvatten de maatregelen die Partijen treft in het kader van een incident work-arounds om onderliggende bedrijfsprocessen draaiende te houden tot de systemen volledig hersteld zijn.

Maatregelen en Standaarden
De door Partijen doorgevoerde beveiligingsmaatregelen zijn gespecificeerd in Bijlage 3 bij het Dataprotocol MKIB-ClaudicatioNet.

Audit
Partijen zullen eenmaal per jaar een audit uitvoeren. Onderdeel van een dergelijke audit is ten minste het onderzoeken of de beveiligingsmaatregelen zoals bedoeld in Bijlage 3 daadwerkelijk zijn geïmplemteerd, of de beveiligingsmaatregelen en/of het beleid inzake deze beveiligingsmaatregelen zwakke plekken bevat en/of nog steeds passend is gezien de te verwerken gegevens en/of de stand van de techniek, alsmede om te toetsen of het informatiebeveiligingsbeleid binnen het bedrijf of de instantie voldoende wordt nageleefd. De resultaten van de audit zullen aan het management van die Partij, alsmede aan de andere Partijen bij het Dataprotocol MKIB-ClaudicatioNet worden gerapporteerd.

Derde partijen
Indien één van Partijen in het kader van de informatiebeveiliging gebruik maakt van derde partijen zal zij ervoor zorgdragen dat de bepalingen uit het Dataprotocol MKIB-ClaudicatioNet, waaronder mede begrepen de Bijlagen, ook door deze derde partijen worden onderschreven en nageleefd, alsmede dat adequate beveiligingsmaatregelen door de derde partij worden geïmplementeerd en gehandhaafd.

BIJLAGE 5 DATAPROTOCOL MKIB-CLAUDICATIONET - AFSPRAKEN CLAUDICATIONET

Voor het Onderzoek van ClaudicatioNet levert MediQuest maandelijks alle gegevens van de deelnemende Fysiotherapeuten die beschikbaar zijn in het LDF aan Softmedia om daarmee de rapportages te bouwen ten behoeve van het Onderzoek van ClaudicatioNet. Dit document specificeert het proces van verstrekking door MediQuest aan Softmedia.
De volgende algemene afspraken zijn gemaakt:

- ClaudicatioNet levert maandelijks een lijst met BIG nummers aan van de deelnemende Fysiotherapeuten in Microsoft Office Excel format.
- MediQuest levert op basis van het door ClaudicatioNet verstrekte overzicht van BIG nummers maandelijks de Persoonsgegevens van deze Fysiotherapeuten in de LDF zoals gespecificeerd in bijlage 4 bij de samenwerkingsovereenkomst tussen KNGF en Claudicationet uitsluitend per e-mail in een beveiligd ZIP bestand of via een beveiligde versleutelde (SSL) verbinding van de server aan Softmedia.
- MediQuest heeft voor het begin van levering van de Persoonsgegevens op voornoemde wijze ten behoeve van het Onderzoek een XSD naar Softmedia gestuurd, waarin het formaat van de XML wordt beschreven, het datatype en indien relevant de veldlengte.

2. Specificaties van de maandelijkse aanlevering aan ClaudicatioNet

2.1 Specificaties in het kort

De aanlevering van de ruwe data (Persoonsgegevens) uit de LDF aan Softmedia neemt de vorm aan van een XML-bestand, waarvan de structuur door MediQuest bepaald wordt.

In deze aanlevering worden opgenomen, zoals nader gespecificeerd in het bij KNGF, ClaudicatioNet, MediQuest en Softmedia bekende document “Documentatie maandelijkse levering van MediQuest aan ClaudicatioNet (SoftMedia)” (in beheer en opvraagbaar bij MediQuest):

- De geselecteerde en voor ClaudicatioNet van toepassing zijnde meetinstrumenten en verrichtingen met een BIG nummer dat voorkomt in de door ClaudicatioNet aangeleverde lijst.
- Alle overige proceskenmerken van de behandelepisodes waar deze meetinstrumenten en/of verrichtingen onder vallen, die benodigd zijn voor de dataverwerking voor ClaudicatioNet
    - *In ieder geval met uitzondering van verrichtingen en meetinstrumenten met BIG nummers van niet deelnemende behandelaars*.
- Er wordt alleen data doorgeleverd vanuit de LDF aan Softmedia uit aanleveringen door de Fysiotherapeuten via het EPD vanaf 1 januari 2016 en vanuit webservice specificatie 3.1 (en verder)[7], voor de duur van de samenwerkingsovereenkomst tussen KNGF en ClaudicatioNet. Eventuele eerdere aanleveringen van deelnemende Fysiotherapeuten via het EPD aan de LDF worden niet mee geleverd.

2.2 Wat wordt precies meegestuurd in de maandelijkse aanlevering van de Fysiotherapeut uit het EPD naar de LDF

De Fysiotherapeut zal elke maand een aanlevering doen vanuit het EPD aan de LDF met daarin de hiervoor onder 2.1 gespecificeerde behandelepisodes (inclusief verrichtingen en meetinstrumenten). Het aanleveren gebeurt onder verantwoordelijkheid van de Fysiotherapeut zelf.

De aan te leveren (delen van de) behandelepisodes is een vaste instelling in het EPD, zodat de continuïteit van de inhoud van de aanlevering kan worden gewaarborgd.

[7] De actuele specificaties van de webservice zijn te vinden via http://www.landelijkedatabasefysiotherapie.nl/documenten/technische_documentatie/

Indien een Fysiotherapeut meer dan één keer per maand een aanlevering doet aan de LDF, worden de data uit *alle* aanleveringen van de door te leveren maand doorgestuurd naar Softmedia. Er vindt daarbij geen ontdubbeling plaats vanuit de kant van MediQuest.