Versie 2.0 A. IBCW

A. Informatiebeveiliging, continuïteit, wet-regelgeving
Scope: SLA IT dienstverlening. Beschikbaarheid, Integriteit, Vertrouwelijkheid & Logging.
Doel: Continuïteit praktijkvoering. Voldoen aan wet & regelgeving.

Status	Definitief

Leverancier	Pinkroccade Healthcare
Product	mijnCaress versie 4.9
Naam invuller	Gerben Roebersen
Auditor	Onbekend
Datum van afronden	06-11-2017
Status	Gepubliceerd, geen keurmerk

Uitslag basis eisen

Categorie	Aantal getest	Ja	Nee	Onbekend	Percentage
OVEREENKOMST EN ICT DIENSTVERLENING	27	24	3	0	88.9%
LOGGING	25	22	3	0	88%

Uitslag plus eisen

Categorie	Aantal getest	Ja	Nee	Onbekend	Percentage
OVEREENKOMST EN ICT DIENSTVERLENING	1	1	0	0	100%
LOGGING	3	1	2	0	33.3%

1. Overeenkomst en ict dienstverlening

De Kwaliteitswet Zorginstellingen is van toepassing op iedere praktijk of instelling. Een goed functionerende ICT omgeving is cruciaal om aan deze Wet -en aan de verwachtingen van de patiënt- te kunnen voldoen. Ook op het handelen van daar werkzame fysiotherapeuten is wet en regelgeving van toepassing (Wet op de Geneeskundige Behandelingsovereenkomst en de Wet Bescherming Persoonsgegevens). Risico's op incidenten dienen te worden beperkt door maatregelen, zoals geformuleerd in de NEN norm Informatiebeveiliging voor de Zorg (NEN7510). Kennisname van dossiergegevens door onbevoegden moet zijn uitgesloten. Heldere afspraken met een IT leverancier zijn essentieel om deze in staat te stellen aan de verwachtingen van de organisatie, fysiotherapeut en patiënt te voldoen. Klik hier voor aanvullende informatie.

1.1. Overeenkomst algemeen

543 De overeenkomst bevat verifieerbare prestatiecriteria[1] aangaande de ICT producten en diensten, de wijze waarop daarop controle plaatsvindt en de rapportage daarover.

574 De overeenkomst is opgesteld in een, voor de fysiotherapeut begrijpelijke tekst, waarin wordt uiteengezet wat de wederzijdse rechten en plichten zijn. Hieronder vallen prijzen en vergoedingen, onderhouds- en ondersteuningsverplichtingen van de leverancier, inclusief mail en telefonische support, ook buiten kantoortijden.

653 De overeenkomst bevat in ieder geval bepalingen omtrent acceptatie, garanties en aansprakelijkheid van de leverancier. Het (verkapt) uitsluiten van garanties en aansprakelijkheid is niet toegestaan.

654 De overeenkomst bevat bepalingen over (tussentijdse) opzegging en beëindiging van de overeenkomst, inclusief de gevolgen ervan. Indien van toepassing bevat de overeenkomst bepalingen over een transitie na beëindiging (zogenaamde exit) – met name over (gevoelige) data van de fysiotherapeut.

655 Is sprake van een ICT product, dan is in de overeenkomst geregeld dat dit product zonder extra kosten, geschikt is voor outsourcing, cloud en/of virtualisatie doeleinden.

577 De overeenkomst bevat voorwaarden voor schadecompensatie, heronderhandeling en/of ontbinding van de overeenkomst als de overeengekomen producten of diensten niet deugdelijk en/of niet tijdig worden geleverd.

576 De overeenkomst bevat bepalingen m.b.t. intellectuele eigendomsrechten van leverancier en fysiotherapeut alsmede met betrekking tot de gebruiksrechten van de fysiotherapeut op ICT producten van de leverancier.

656 De overeenkomst bevat vrijwaringsverplichtingen voor de leverancier, in ieder geval ten aanzien van inbreuk op intellectuele eigendomsrechten alsmede voor het door leverancier niet nakomen van contractuele verplichtingen en/of schenden van wet- of regelgeving.

657 Leverancier garandeert dat hij zich op een naar verkeersnormen passende en gebruikelijke wijze heeft verzekerd tegen wettelijke aansprakelijk en beroepsaansprakelijkheid en dat hij zich gedurende de looptijd van de Overeenkomst verzekerd zal houden.

658 Leverancier zal gedurende de looptijd van de Overeenkomst geen wijzigingen in zijn verzekering aanbrengen ten nadele van de fysiotherapeut.

1.2. ContinuÏteit en beveiliging

Dit hoofdstuk bevat onder meer een eis die een einde moet maken aan de situatie dat de fysiotherapeut zich belemmerd ziet in de keuze voor een ander ICT product of dienst in verband met te verwachten conversieproblemen. Bij leveranciers blijkt een drempel te bestaan om de eerste stappen te zetten om een einde te maken aan deze zogenaamde "vendor lock-in".

578 De overeenkomst bevat gedetailleerde en voor fysiotherapeut begrijpelijke informatie over aard en omvang van de te leveren diensten en de wijze waarop kan worden geverifieerd of daaraan wordt voldaan.

579 De overeenkomst geeft inzicht in dienst- en/of productbeveiliging, dienst- en/of productcontinuïteit (zoals escrow, back-up en dergelijke).

540 De overeenkomst bevat een gedetailleerde beschrijving van de genomen maatregelen om de beschikbaarheid, vertrouwelijkheid en integriteit te garanderen.

580 De overeenkomst bevat gedetailleerde en voor fysiotherapeut begrijpelijke informatie over draaiboeken bij calamiteiten.

581 Leverancier stelt de gebruiker zonder extra kosten in staat te allen tijde en op eerste verzoek te beschikken over alle geregistreerde data in een algemeen open format opdat eventuele conversie naar (hergebruik in combinatie met) een ander product mogelijk is.

582 Voor vragen is de helpdesk ook buiten kantooruren bereikbaar. Voor ernstige calamiteiten is een spoedlijn beschikbaar met een response tijd van maximaal 1 uur.

1.3. Vertrouwelijkheid en privacy

583 De leverancier garandeert dat onbevoegden geen toegang hebben tot vertrouwelijke gegevens, waaronder persoonsgegevens. In de overeenkomst verklaart de leverancier expliciet dat wordt voldaan aan artikel 13 en 14 van de Wet Bescherming Persoonsgegevens en de overeenkomst bevat dienovereenkomstige bepalingen.

554 De overeenkomst beschrijft de maatregelen die zijn genomen om de vertrouwelijkheid te garanderen. Meer in het bijzonder die met betrekking tot de toegang tot vertrouwelijke informatie en/of persoonsgegevens.

585 De overeenkomst beschrijft de beheermaatregelen om de teruggave of vernietiging van informatie en andere bedrijfsmiddelen te waarborgen. Zowel op een overeengekomen tijdstip tijdens de looptijd van de overeenkomst, als bij beëindiging daarvan.

584 De overeenkomst bevat afspraken over aard en omvang van rapportage, kennisgeving en onderzoek naar informatiebeveiligingsincidenten en lekken in de beveiliging.

659 De overeenkomst bevat bepalingen omtrent de verwerking van (bijzondere) persoonsgegevens.

660 Leverancier garandeert zich te allen tijde te houden aan de alsdan toepasselijke wet-en regelgeving op het gebied van de verwerking van (bijzondere) persoonsgegevens.

661 De overeenkomst bevat boeteclausules voor het door leverancier schenden van vertrouwelijkheid en/of privacybepalingen alsmede voor overtredingen van leverancier van relevante wet- en regeling, zoals de wet bescherming persoonsgegevens.

1.4. Keurmerk(en) / certificering(en)

586 De leverancier beschikt over een ISO 9001 certificering.

542 In de overeenkomst met de fysiotherapeut is vastgelegd dat de leverancier zich laat auditen op de vastgelegde verantwoordelijkheden (welke zijn opgenomen in de gesloten overeenkomst met de fysiotherapeut) en dat de fysiotherapeut in kennis wordt gesteld van het resultaat.

1.5. Opleiding(en)

587 De leverancier biedt productgebonden opleidingen en cursussen aan.

588 De leverancier biedt opleidingen en cursussen aan op meerdere plaatsen in het land en buiten kantooruren.

589 De door de leverancier aangeboden opleidingen en cursussen zijn geaccrediteerd door het Beleidsorgaan Centraal Kwaliteitsregister Fysiotherapie.

2. Logging

De Wet op de Geneeskundige Behandelingsovereenkomst verplicht de zorgverlener tot het aanleggen van een patiëntdossier. Essentieel is dat de integriteit van de gegevens in het dossier geborgd. Omdat het dossier vertrouwelijke en privacygevoelige gegevens bevat, verlangt de wetgever bovendien dat te allen tijde kan worden achterhaald wie toegang heeft gehad tot het dossier, volgens welke regels men die toegang heeft gekregen en welke acties men m.b.t. het dossier heeft uitgevoerd. Niet alleen moeten patiënten hieromtrent kunnen worden geïnformeerd, maar hebben bovendien recht op inzage in het dossier waarin de gegevens over hun behandeling zijn gedocumenteerd. ICT systemen moeten zorgverleners in staat stellen aan wet en regelgeving en de behoeften/rechten van de patiënt te voldoen. De, in 2010 gepubliceerde norm "Vastleggen van acties op elektronische patiëntendossiers" (NEN7513), beschrijft de stelselmatige geautomatiseerde registratie van gegevens rond de toegang tot het patiëntdossier. Een ICT omgeving die voldoet aan de eisen die worden beschreven in de NEN7513 stelt een zorgverlener in staat te voldoen aan de

verlangens patiënt en de eisen die de wetgever stelt. (Klik hier voor meer info)

2.1. Functionele eisen m.b.t. logging

In de norm NEN7513 wordt er van uitgegaan dat ieder product of systeem, dat voorziet in de mogelijkheid tot vastlegging, opslag en verstrekking van patiëntgegevens, aan een aantal functionele eisen voldoet.

601 Het systeem voorziet in de mogelijkheid om de identiteit van een gebruiker eenduidig vast te stellen (identificatie) en te verifiëren (authenticatie).

602 Het systeem voorziet in de mogelijkheid om bij een gebruiker één of meer rollen vast te leggen en te verwijderen (roltoekenning)

603 Het systeem voorziet in de mogelijkheid om regels vast te leggen waarin de toegang tot bepaalde gegevens wordt gebonden aan bepaalde rollen (autorisatieprotocollen).

604 Het systeem voorziet in de mogelijkheid om door de patiënt zelf aan te geven toegangsaanwijzingen (toestemmingsprofielen) vast te leggen en te wijzigen.

605 Het systeem voorziet in de mogelijkheid om de toegang tot gegevens te beperken tot hetgeen overeenkomstig de regels en de beperkingen is geoorloofd (toegangscontrole).

606 Het systeem voorziet in de mogelijkheid om gegevens over verleende toegang te registreren (loggen) waarmee de rechtmatigheid van de toegang achteraf kan worden gevalideerd.

2.2. Informatiebehoeften

2.2.1. Algemeen

De logging moet het mogelijk maken achteraf onweerlegbaar vast te stellen welke acties hebben plaatsgevonden op een patiëntdossier. Daartoe moeten de ICT omgeving minimaal inzicht verschaffen in de actie, het tijdstip en de identiteit van betrokkenen.

607 De loggegevens van het systeem bieden inzicht in welke actie heeft plaatsgevonden.

608 De loggegevens van het systeem bieden inzicht in het tijdstip van de actie.

609 De loggegevens van het systeem bieden inzicht in de identiteit van de patiënt.

610 De loggegevens van het systeem bieden inzicht in de identiteit van de actor.

611 De loggegevens van het systeem bieden inzicht in de identiteit van de *verantwoordelijke* voor de actie.
(toelichting: eventueel onder wiens verantwoordelijkheid de handeling plaatsvond).

2.2.2. PatiËnt

Patiënten hebben recht op informatie over hun behandeling en recht op inzage in hun patiëntdossier. In het verlengde daarvan hebben patiënten recht te weten wie toegang tot hun dossier hebben gehad. De logging van de toegang moet hiertoe ondersteuning bieden. Personen die zijn gemachtigd om namens een patiënt op te treden of wettelijke vertegenwoordigers van patiënten worden hier als belanghebbenden gelijk gesteld aan patiënten. In de logging worden deze vertegenwoordigers wel in die rol onderscheiden. De logging die een patiënt te zien krijgt mag alleen betrekking hebben op het eigen dossier. In bepaalde gevallen willen patiënten kunnen nagaan wie welke gegevens in het dossier heeft genoteerd of gelezen. In het bijzonder kan dat het geval zijn wanneer de patiënt daarvoor aanwijzingen heeft gegeven of beperkingen heeft kenbaar gemaakt. Die kunnen afwijken van generieke autorisatieprofielen, waarin de geldende regels voor toegang tot de gegevens zijn vastgelegd. Wettelijke kaders beschrijven de minimumsituatie van de gevallen waarin deze wensen van de patiënt gehonoreerd moeten kunnen worden. De logging moet kunnen worden getoetst aan het autorisatieprofiel en het toestemmingsprofiel[2] zoals die ten tijde van de actie van kracht waren.

612 De logging biedt de patiënt inzicht in welke gegevens de actie betrof.

613 De logging biedt de patiënt inzicht in welk autorisatieprotocol[3] is toegepast.

614 De logging biedt de patiënt inzicht in welk toestemmingsprofiel[2] gold.

2.2.3. Instelling - fysiotherapeut

De behandelend fysiotherapeut moet een dossier bijhouden op grond van de Wet op de geneeskundige behandelingsovereenkomst. Verstrekking van informatie daaruit aan derden is volgens de WGBO in beginsel alleen geoorloofd in het kader van een behandelingsovereenkomst. De fysiotherapeut moeten tevens patiënten inzage kunnen geven in wie toegang heeft gehad tot het dossier dat over die patiënt is bijgehouden. Voor gebruik van gegevens uit het dossier voor bijvoorbeeld wetenschappelijk onderzoek is ook toestemming vereist, maar laat de wet een mogelijkheid open de toestemming achterwege te laten in gevallen waarin het vragen van toestemming niet uitvoerbaar is. In dat geval wordt van dit gebruik wel logging verlangd. Uit de logging moet blijken of aan de regels is voldaan.

615 De logging biedt de instelling of fysiotherapeut inzicht in het toegepaste autorisatieprotocol[3].

616 De logging biedt de instelling of fysiotherapeut inzicht in de rol die de actor vervulde.

2.3. Te loggen gebeurtenissen

2.3.1. Dossieracties

Alle acties moeten worden gelogd waarbij gegevens die betrekking hebben op een patiënt worden ingezien, gewijzigd of anderszins verwerkt.

626 De actie: aanmaken van een dossier wordt gelogd

628 De actie: invoer van gegevens wordt gelogd

629 De actie: toevoegen van gegevens wordt gelogd

630 De actie: lezen van gegevens wordt gelogd

631 De actie: samenvoegen of splitsen van dossiers wordt gelogd

632 De actie: overdragen van gegevens vanuit of naar een ander systeem, met inbegrip van afdrukken en kopiëren op draagbare media wordt gelogd

633 De actie: verwijderen van eerder vastgelegde gegevens wordt gelogd

634 Zoekacties worden gelogd

2.4. Zekerheidseisen

2.4.1. Verantwoordelijkheid

In het verlengde van de dossierplicht die op een zorgaanbieder rust op grond van de WGBO is deze zorgaanbieder verantwoordelijk voor het loggen van de acties op het deel van het elektronisch patiëntdossier dat onder diens dossierplicht valt. De zorgaanbieder is ook verantwoordelijk voor het beheer van de logging die daaruit voortkomt. Een zorgaanbieder of een daartoe wettelijk aangestelde organisatie die als intermediair optreedt bij het opvragen of doorgeleiden van gegevens die tot het elektronisch patiëntdossier behoren, is verantwoordelijk voor het loggen van de verkeersgegevens en voor het beheer van de logging die daaruit voortkomt. Het technische of totale beheer van de logging kan worden uitbesteed. De verantwoordelijkheid voor het beheer verandert daardoor niet.

649 In de overeenkomst met de fysiotherapeut of instelling vermeldt de IT leverancier expliciet aan welke eisen uit het hoofdstuk logging wordt voldaan.

650 Tot het moment waarop aan alle eisen uit het hoofdstuk logging wordt voldaan, stelt de leverancier de contractant op de hoogte van zijn inspanningen en resultaten om aan de norm NEN7513 te voldoen.

2.4.2. Integriteit en onweerlegbaarheid logging

De beheerder van de logging moet zorgen voor voldoende beveiliging om de integriteit en onweerlegbaarheid van de loggegevens te bewaken. Op de beveiliging van de logging is NEN 7510 van toepassing.

651 De IT leverancier garandeert de integritet en onweerlegbaarheid van de loggegevens

2.4.3. Beschikbaarheid en toegankelijkheid logging

Ten aanzien van beschikbaarheid en toegankelijkheid dient te zijn vastgelegd dat deze is gegarandeerd en dat aan de informatiebehoeften van instelling/fysiotherapeut, patiënt (eventueel toezichthouder) kan worden voldaan.

652 De IT leverancier garandeert de beschikbaarheid en toegankelijkheid van de loggegevens

Voetnoten

[1] Prestatiecriteria: Waardering ICT product en/of ICT dienstverlening uitgedrukt in transparante, meetbare indicatoren. Voorbeelden: werking en/of bereikbaarheid – response en oplostijd,maximaal aantal verstoringen en/of incidenten per periode et cetera. Ook wel service level specificaties genoemd.

[2] Toestemmingsprofiel: vastlegging, landelijk, regionaal of lokaal, door de patiënt zelf bepaald, van wie in welke omstandigheden al of niet toegang mag krijgen tot bepaalde eigen gegevens. Patiënt heeft mogelijkheid afwijkingen te kiezen van een algemeen geldend toestemmingsprofiel

[3] Autorisatieprotocol: door zorgaanbieders gedefinieerde autorisatietabel, landelijk, regionaal of lokaal, die bepaalt welke categorieën patiëntgegevens voor welke categorieën zorgaanbieders toegankelijk zijn onder welke voorwaarden