Verklaring van toepasselijkheid

Qics B.V.

ISO 27001:2017 en NEN 7510-1:2017+A1:2020

Datum	:	5 februari 2024
Auteur	:	Mark Velthuijsen
Versie	:	1.5
Doc.nr.	:	ISMS-312412935-1913

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Inhoudsopgave

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

1. Inleiding

Dit document omvat de Verklaring van Toepasselijkheid (VvT) van Qics ten behoeve van de certificering voor de ISO 27001 en NEN 7510 standaarden.

2. Scope

Informatiebeveiliging gerelateerd aan het ontwikkelen, implementeren, adviseren en leveren van onderhoud en support op de SaaS-software van Qics, te weten: QicsMilestones, Assist Planner en QicsDashboards.

De activiteiten vinden plaats vanuit onze Nederlandse vestiging, met uitzondering van het ontwikkelen van QicsMilestones, dat plaatsvindt vanuit onze dochteronderneming in Slowakije in opdracht van en onder toezicht van Qics Nederland.

Qics levert haar software en diensten primair aan accountants, ICT-bedrijven en andere zakelijke dienstverleners. Het product Assist Planner wordt geleverd aan zorgleveranciers die huishoudelijke hulp leveren vanuit de Wet Maatschappelijke Ondersteuning (WMO).

Qics heeft de opslag en hosting van haar SaaS-software uitbesteed bij een betrouwbare partij.

3. Directieverklaring

De directie van Qics B.V. verklaart hierbij de in deze Verklaring van Toepasselijkheid vermelde maatregelen bekrachtigd in relatie tot de uitgevoerde risicoanalyses en accepteert het restrisico van niet genomen maatregelen.

Katwijk, 5 februari 2024

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

4. Toelichting

In de tabel met beheersmaatregelen zijn de volgende kolommen opgenomen:

- Naam en nummer van de **maatregel** (een maatregel met de toevoeging ZS is een zorg specifieke beheersmaatregel)
- **Van toepassing** (Ja / Nee): geeft aan of de maatregel van toepassing is.
- **Geïmplementeerd** (Ja / Nee): geeft aan of we de maatregel geïmplementeerd hebben.
- **Uitbesteed (Deels / Volledig) :** geeft aan of de maatregel uitbesteed is.
  D = Gedeeltelijk V = Volledig, Blanco = niet uitbesteed
- **Reden** van toepassing
  (WE = Wet- en regelgeving, RA = Risico analyse, CE = Contractuele verplichting): geeft aan waarom we de maatregel toepassen.
- **Reden** niet van toepassing (Tekst): geeft aan waarom we de maatregel niet toepassen.

5. Beheersmaatregelen

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
A5 Informatiebeveiligingsbeleid				
05.1.1 Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Ja	Ja		RA
05.1.1 ZS Beleidsregels voor informatiebeveiliging Organisaties behoren te beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	Ja	Ja		RA
05.1.2 Beoordeling van het informatiebeveiligingsbeleid Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Ja	Ja		RA
05.1.2 ZS Beoordeling van het informatiebeveiligingsbeleid Het informatiebeveiligingsbeleid behoort aan voortdurende, gefaseerde beoordelingen te worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid behoort te worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	Ja	Ja		RA
A6 Organiseren van informatiebeveiliging				
06.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
06.1.1 ZS Rollen en verantwoordelijkheden bij informatiebeveiliging Organisaties behoren: a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging te definiëren en toe te wijzen b) over een informatiebeveiligingsmanagementforum (IBMF) te beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in B.3 en B.4 van bijlage B. Er behoort minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie. Het gezondheidsinformatiebeveiligingsforum behoort regelmatig, maandelijks of bijna maandelijks, te vergaderen. (Het is meestal het effectiefst als het forum vergadert op een tijdstip halverwege tussen twee vergaderingen van het bestuursorgaan waaraan het forum rapporteert. Zo kunnen urgente zaken binnen een korte periode in een geschikte vergadering worden besproken.) Er behoort een formele verklaring van het toepassingsgebied te worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen.	Ja	Ja		RA, CE
06.1.2 Scheiding van taken Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Ja	Ja		RA
06.1.2 ZS Scheiding van taken Organisaties behoren, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden te scheiden om de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.	Ja	Ja		RA
06.1.3 Contact met overheidsinstanties Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	Ja	Ja		WE, RA, CE
06.1.4 Contact met speciale belangengroepen Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden.	Ja	Ja		RA
06.1.5 Informatiebeveiliging in projectbeheer Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
06.1.5 ZS Informatiebeveiliging in projectbeheer Bij het management van projecten behoort de patiëntveiligheid als projectrisico in aanmerking te worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja		RA
06.2.1 Beleid voor mobiele apparatuur Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beheren.	Ja	Ja		RA
06.2.2 Telewerken Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Ja	Ja	D	RA
A7 Veilig personeel				
07.1.1 Screening Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Ja		RA
07.1.1 ZS Screening Organisaties behoren minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie te verifiëren. Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband behoren een verificatie te omvatten van de toepasselijke kwalificaties voor zorgverleners, indien er sprake is van accreditatie voor de beroepsgroep op basis van die kwalificaties (bijv. artsen, verplegend personeel enz.). Als een persoon wordt ingehuurd voor een specifieke beveiligingsrol, behoort de organisatie zich ervan te vergewissen dat: a) de kandidaat over de nodige competentie beschikt om de beveiligingsrol te vervullen; b) de kandidaat de rol kan worden toevertrouwd, in het bijzonder als de rol cruciaal is voor de organisatie.	Ja	Ja		RA
07.1.2 Arbeidsvoorwaarden De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Ja	Ja		RA, WE

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
07.1.2 ZS Arbeidsvoorwaarden Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, behoren die betrokkenheid in relevante functieomschrijvingen vast te leggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, behoren ook in relevante functieomschrijvingen te worden vastgelegd. Er behoort speciale aandacht te worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten, stagiairs enz.	Ja	Ja		RA, WE
07.2.1 Directieverantwoordelijkheden De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Ja	Ja		RA
07.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Ja	Ja	D	RA
07.2.2 ZS Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken. Werknemers van de organisatie en, waar relevant, derde-contractanten behoren te worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	Ja	Ja	D	RA
07.2.3 Disciplinaire procedure Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Ja	Ja		RA, WE
07.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	Ja	Ja		RA, WE
A8 Beheer van bedrijfsmiddelen				

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
08.1.1 Inventariseren van bedrijfsmiddelen Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	Ja	Ja	D	RA, CE
08.1.1 ZS Inventariseren van bedrijfsmiddelen Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren: a) verantwoording af te leggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bij te houden van dergelijke bedrijfsmiddelen); b) een eigenaar te hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2); c) regels te hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	Ja	Ja		RA, CE
08.1.2 Eigendom van bedrijfsmiddelen Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	Ja	Ja		RA, CE
08.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja	Ja		RA, CE
08.1.4 Teruggeven van bedrijfsmiddelen Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben, bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	Ja	Ja		RA, CE
08.1.4 ZS Teruggeven van bedrijfsmiddelen Alle werknemers en contractanten behoren, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, terug te geven en erop toe te zien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.	Ja	Ja		RA, CE
08.2.1 Classificatie van informatie Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Ja	Ja		RA
08.2.1 ZS Classificatie van informatie Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren dergelijke gegevens op uniforme wijze als vertrouwelijk te classificeren.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
08.2.2 Informatie labelen Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja	D	RA
08.2.2 ZS Informatie labelen Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren de gebruikers te wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen), en behoren papieren output als vertrouwelijk te labelen als die output persoonlijke gezondheidsinformatie bevat.	Ja	Ja		RA
08.2.3 Behandelen van bedrijfsmiddelen Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja		RA
08.3.1 Beheer van verwijderbare media Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	Ja		RA
08.3.1 ZS Beheer van verwijderbare media Media die persoonlijke gezondheidsinformatie bevatten, behoren fysiek te worden beschermd of de gegevens ervan behoren versleuteld te worden. De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, behoren gemonitord te worden.	Nee	Nee		Er is geen persoonlijke gezondsheidsinformatie opgeslagen op media.
08.3.2 Verwijderen van media Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Ja	Ja	D	RA
08.3.2 ZS Verwijderen van media Alle persoonlijke gezondheidsinformatie behoort veilig te worden gewist of anders behoren de media te worden vernietigd als ze niet meer gebruikt hoeven te worden.	Nee	Nee		Er is geen persoonlijke gezondsheidsinformatie opgeslagen op media.
08.3.3 Media fysiek overdragen Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Nee	Nee		Het fysiek overdragen van media komt niet voor
A9 Toegangsbeveiliging				
09.1.1 Beleid voor toegangsbeveiliging Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
09.1.1 ZS Beleid voor toegangsbeveiliging Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de toegang tot dergelijke informatie te controleren. In het algemeen behoren de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie te beperken tot situaties: a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt); b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben; c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen. Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren een toegangscontrolebeleid te hebben waarmee de toegang tot deze gegevens wordt geregeld. Het beleid van de organisatie met betrekking tot toegangscontrole behoort te worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol. Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, behoort professionele, ethische, juridische en cliëntgerelateerde eisen te weerspiegelen en behoort de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking te nemen. De organisatie behoort alle partijen te identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen behoren contractuele afspraken over toegang en rechten te worden gemaakt, alvorens cliëntgegevens uit te wisselen.	Ja	Ja		RA
09.1.2 Toegang tot netwerken en netwerkdiensten Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Ja	Ja	D	RA
09.2.1 Registratie en afmelden van gebruikers Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	Ja		RA
09.2.1 ZS Registratie en afmelden van gebruikers De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoort onderhevig te zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers behoren te garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens behoren regelmatig te worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
09.2.2 Gebruikers toegang verlenen Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Ja	Ja		RA
09.2.3 Beheren van speciale toegangsrechten Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Ja	Ja		RA
09.2.4 Beheer van geheime authenticatie-informatie van gebruikers Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Ja	Ja	D	RA
09.2.5 Beoordeling van toegangsrechten van gebruikers Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Ja	Ja		RA
09.2.6 Toegangsrechten intrekken of aanpassen De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Ja	Ja		RA
09.2.6 ZS Toegangsrechten intrekken of aanpassen Alle organisaties die persoonlijke gezondheidsinformatie verwerken, behoren voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie te beëindigen.	Ja	Ja		RA
09.3.1 Geheime authenticatie-informatie gebruiken Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie- informatie houden aan de praktijk van de organisatie.	Ja	Ja		RA
09.4.1 Beperking toegang tot informatie Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Ja	Ja		RA
09.4.1 ZS Beperking toegang tot informatie Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren de identiteit van gebruikers vast te stellen en dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie behoort geïsoleerd (en gescheiden) te worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
09.4.2 Beveiligde inlogprocedures Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Ja	Ja	D	RA
09.4.3 Systeem voor wachtwoordbeheer Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Ja	Ja	D	RA
09.4.4 Speciale systeemhulpmiddelen gebruiken Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	Ja	Ja		RA
09.4.5 Toegangsbeveiliging op programmabroncode Toegang tot de programmabroncode behoort te worden beperkt.	Ja	Ja	D	RA
A10 Cryptografie				
10.1.1 Beleid over het gebruik van cryptografische beheersmaatregelen Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Ja	Ja		RA
10.1.2 Sleutelbeheer Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	Ja	Ja	D	RA
A11 Fysieke beveiliging en beveiliging van de omgeving				
11.1.1 Fysieke beveiligingszone Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Ja	Ja	D	RA, CE
11.1.1 ZS Fysieke beveiligingszone Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren gebruik te maken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden behoren te worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Nee	Nee		Er wordt geen persoonlijke gezondheidsinformatie opgeslagen of verwerkt binnen ons pand.
11.1.2 Fysieke toegangsbeveiliging Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	Ja	D	RA
11.1.3 Kantoren, ruimten en faciliteiten beveiligen Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Ja	Ja	D	RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
11.1.4 Beschermen tegen bedreigingen van buitenaf Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Ja	Ja	D	RA
11.1.5 Werken in beveiligde gebieden Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Ja	Ja		RA
11.1.6 Laad- en loslocatie Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Nee	Nee		QICS maakt geen gebruik van een laad-en losruimte
11.2.1 Plaatsing en bescherming van apparatuur Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang, worden verkleind.	Ja	Ja	D	WE, RA
11.2.2 Nutsvoorzieningen Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja	Ja	D	RA
11.2.3 Beveiliging van bekabeling Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Ja	Ja	D	WE, RA
11.2.4 Onderhoud van apparatuur Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	Ja	D	RA
11.2.5 Verwijdering van bedrijfsmiddelen Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	Ja	Ja		RA
11.2.5 ZS Verwijdering van bedrijfsmiddelen Organisaties die uitrusting, gegevens of software voor het ondersteunen van een zorgtoepassing met persoonlijke gezondheidsinformatie leveren of gebruiken, mogen niet toestaan dat die uitrusting, gegevens of software van de locatie wordt of worden verwijderd of erbinnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven.	Ja	Ja		RA
11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
11.2.6 ZS Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit behoort apparatuur te omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d.w.z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.).	Nee	Nee		Geen medische apparatuur die gezondheidsgegevens registreren
11.2.7 Veilig verwijderen of hergebruiken van apparatuur Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Ja	Ja		RA
11.2.7 ZS Veilig verwijderen of hergebruiken van apparatuur Organisaties die gezondheidsinformatie verwerken, behoren alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig te wissen of te vernietigen als ze niet meer gebruikt hoeven te worden.	Nee	Nee		Wij beheren geen media met gezondheidsinformatie.
11.2.8 Onbeheerde gebruikersapparatuur Gebruikers behoren ervoor te zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja		RA
11.2.9 'Clear desk'- en 'clear screen'-beleid Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	Ja	Ja		RA
A12 Beveiliging bedrijfsvoering				
12.1.1 Gedocumenteerde bedieningsprocedures Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja		RA
12.1.2 Wijzigingsbeheer Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, behoren te worden beheerst.	Ja	Ja		RA, CE
12.1.2 ZS Wijzigingsbeheer Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigingsbeheersproces te beheersen om de gepaste beheersing van hosttoepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen.	Ja	Ja		RA, CE

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
12.1.3 Capaciteitsbeheer Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Ja	Ja	D	RA
12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Ja	Ja	D	RA
12.1.4 ZS Scheiding van ontwikkel-, test- en productieomgevingen Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel), te scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er behoren regels voor het migreren van software van de ontwikkel- naar een operationele status te worden gedefinieerd en gedocumenteerd door de organisatie die de betreffende toepassing(en) host.	Ja	Ja	D	RA
12.2.1 Beheersmaatregelen tegen malware Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Ja	Ja	D	RA
12.2.1 ZS Beheersmaatregelen tegen malware Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren gepaste preventie-, detectie- en responsbeheersmaatregelen te implementeren om bescherming te bieden tegen kwaadaardige software en behoren passende bewustzijnstraining voor gebruikers te implementeren.	Ja	Ja	D	RA
12.3.1 Back-up van informatie Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Ja	Ja	D	RA
12.3.1 ZS Back-up van informatie Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren back-ups te maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving op te slaan om te garanderen dat de informatie in de toekomst beschikbaar is. Om de vertrouwelijkheid ervan te beschermen behoren er versleutelde back-ups te worden gemaakt van persoonlijke gezondheidsinformatie.	Ja	Ja	D	RA
12.4.1 Gebeurtenissen registreren Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Ja	Ja	D	RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
12.4.2 Beschermen van informatie in logbestanden Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	Ja	D	RA
12.4.2 ZS Beschermen van informatie in logbestanden Auditverslagen behoren beveiligd te zijn en niet gemanipuleerd te kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten behoort te worden beveiligd om misbruik of compromittering te voorkomen.	Ja	Ja	D	RA
12.4.3 Logbestanden van beheerders en operators Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Ja	Ja	D	RA
12.4.4 Kloksynchronisatie De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Ja	Ja	D	RA
12.4.4 ZS Kloksynchronisatie Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen, behoren in tijdssynchronisatiediensten te voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.	Nee	Nee		Geen informatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen.
12.5.1 Software installeren op operationele systemen Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	Ja	Ja		RA
12.6.1 Beheer van technische kwetsbaarheden Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt, behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt, aan te pakken.	Ja	Ja	D	RA
12.6.2 Beperkingen voor het installeren van software Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Ja	Ja		RA
12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Ja	Ja		RA
A13 Communicatiebeveiliging				
13.1.1 Beheersmaatregelen voor netwerken Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	D	RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
13.1.2 Beveiliging van netwerkdiensten Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Ja	Ja	D	RA
13.1.3 Scheiding in netwerken Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	Ja	Ja		RA
13.2.1 Beleid en procedures voor informatietransport Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Ja	Ja		RA
13.2.2 Overeenkomsten over informatietransport Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	Ja		RA
13.2.3 Elektronische berichten Informatie die is opgenomen in elektronische berichten, behoort passend te zijn beschermd.	Ja	Ja		RA
13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	Ja	Ja		RA, CE
13.2.4 ZS Vertrouwelijkheids- of geheimhoudingsovereenkomst Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst behoort van toepassing te zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.	Ja	Ja		RA, CE
A14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen				
14.1.1 Analyse en specificatie van informatiebeveiligingseisen De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Ja	Ja		CE, RA
14.1.1.1 ZS Zorgontvangers op unieke wijze identificeren Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren: a) zeker te stellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem; b) in staat te zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval.	Ja	Ja		WE

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
14.1.1.2 ZS Validatie van outputgegevens Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren te voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.	Ja	Ja		WE
14.1.2 Toepassingen op openbare netwerken beveiligen Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Ja	Ja		RA
14.1.3 Transacties van toepassingen beschermen Informatie die deel uitmaakt van transacties van toepassingen, behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Ja	Ja		RA
14.1.3.1 ZS Openbaar beschikbare gezondheidsinformatie Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) behoort te worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie behoort te worden beschermd om onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie behoort te worden vermeld en de integriteit ervan behoort te worden beschermd.	Nee	Nee		Er is geen sprake van openbare gezondheidsinformatie
14.2.1 Beleid voor beveiligd ontwikkelen Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	Ja	Ja		RA
14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	Ja	Ja		RA
14.2.3 Technische beoordeling van toepassingen na wijzigingen besturingsplatform Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Ja	Ja	D	RA
14.2.4 Beperkingen op wijzigingen aan softwarepakketten Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.	Ja	Ja		RA
14.2.5 Principes voor engineering van beveiligde systemen Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
14.2.6 Beveiligde ontwikkelomgeving Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Ja	Ja	D	RA
14.2.7 Uitbestede softwareontwikkeling Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Ja	Ja		RA
14.2.8 Testen van systeembeveiliging Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Ja	Ja	D	RA
14.2.9 Systeemacceptatietests Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Ja	Ja	D	RA
14.2.9 ZS Systeemacceptatietests Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren acceptatiecriteria vast te stellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie behoren ze geschikte tests van het systeem uit te voeren. Klinische gebruikers behoren te worden betrokken bij het testen van klinisch relevante systeemelementen.	Ja	Ja	D	RA
14.3.1 Bescherming van testgegevens Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	Ja	Ja	D	RA
A15 Leveranciersrelaties				
15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	Ja	Ja		RA
15.1.1 ZS Informatiebeveiligingsbeleid voor leveranciersrelaties Organisaties die gezondheidsinformatie verwerken, behoren de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, te beoordelen en vervolgens beveiligingsbeheersmaatregelen te implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	Ja	Ja		RA
15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
15.1.3 Toeleveringsketen van informatie- en communicatietechnologie Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Ja	Ja		RA
15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	Ja	Ja	D	RA
15.2.2 Beheer van veranderingen in dienstverlening van leveranciers Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Ja	Ja		RA
A16 Beheer van informatiebeveiligingsincidenten				
16.1.1 Verantwoordelijkheden en procedures Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Ja	Ja		RA
16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Ja	Ja		RA
16.1.2 ZS Rapportage van informatiebeveiligingsgebeurtenissen Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vast te stellen: a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; b) om te garanderen dat er een doeltreffend en geprioriteerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement; c) om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden. Informatiebeveiligingsincidenten omvatten corruptie of onbedoelde openbaarmaking van persoonlijke gezondheidsinformatie of het niet langer beschikbaar zijn van gezondheidsinformatiesystemen waarbij dit niet beschikbaar zijn nadelige gevolgen heeft voor de zorg voor cliënten of bijdraagt aan nadelige klinische gebeurtenissen. Organisaties behoren de cliënt altijd te informeren als er per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt. Organisaties behoren de cliënt op de hoogte te stellen als het niet beschikbaar zijn van gezondheidsinformatiesystemen negatieve gehad kan hebben voor hun zorgverlening.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie, behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Ja	Ja	D	RA
16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja	Ja		RA
16.1.5 Respons op informatiebeveiligingsincidenten Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja		RA
16.1.6 Lering uit informatiebeveiligingsincidenten Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Ja	Ja		RA
16.1.7 Verzamelen van bewijsmateriaal De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Ja	Ja		RA
A17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer				
17.1.1 Informatiebeveiligingscontinuïteit plannen De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.	Ja	Ja		RA
17.1.2 Informatiebeveiligingscontinuïteit implementeren De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Ja	Ja		RA
17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Ja	Ja		RA
17.2.1 Beschikbaarheid van informatie verwerkende faciliteiten Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja		RA
A18 Naleving				

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geïmplementeerd	Uitbesteed	Reden wel/niet van toepassing
18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Ja	Ja	D	WE, RA
18.1.2 Intellectuele-eigendomsrechten Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele- eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.	Ja	Ja		WE, RA
18.1.3 Beschermen van registraties Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Ja	Ja	D	WE, RA
18.1.4 Privacy en bescherming van persoonsgegevens Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Ja	Ja		WE, CE, RA
18.1.4 ZS Privacy en bescherming van persoonsgegevens Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de geïnformeerde toestemming van cliënten te beheren. Waar mogelijk behoort geïnformeerde toestemming van cliënten te worden verkregen voordat persoonlijke gezondheidsinformatie per e-mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.	Ja	Ja		WE, RA
18.1.5 Voorschriften voor het gebruik van crypto grafische beheersmaatregelen Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja	Ja		RA
18.2.1 Onafhankelijke beoordeling van informatiebeveiliging De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	Ja	Ja	D	RA
18.2.2 Naleving van beveiligingsbeleid en -normen De directie behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	Ja		RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368

Maatregel	Van toepassing	Geimplementeerd	Uitbesteed	Reden wel/niet van toepassing
18.2.3 Beoordeling van technische naleving Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Ja	Ja	D	RA

VALKENBURGSEWEG 89 | 2223 KC KATWIJK | T 071 750 15 30 | WWW.QICS.NL
BTWNUMMER NL8084.34.494.B.01 | NL30 ABNA 0432 0024 21 | KVK RIJNLAND 28084368