Verklaring van Toepasselijkheid Triaspect BV

Norm: NEN 7510-1:2017+A1:2020 nl

Versie 3.3

Datum: 5 mei 2023

nummer	onderwerp	beheersmaatregel	van toepassing	geïmplementeerd	rechtvaardiging	interface (klantdata)	uitbesteed
5	**Informatiebeveiligingsbeleid**						
5.1	Aansturing door de directie van de informatiebeveiliging	Doelstelling: Het verschaffen van directieaansturing en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.					
5.1.1	Beleidsregels voor informatiebeveiliging	**Beheersmaatregel** Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. **Zorgspecifieke beheersmaatregel** Organisaties moeten 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	Risicoanalyse	Nee	Nee
5.1.2	Beoordeling van het informatiebeveiligingsbeleid	**Beheersmaatregel** Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. **Zorgspecifieke beheersmaatregel** Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	Ja	Ja	Risicoanalyse	Nee	Nee
6	**Organiseren van informatiebeveiliging**						
6.1	Interne organisatie	Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.					
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	**Beheersmaatregel** Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen. **Zorgspecifieke beheersmaatregel** Organisaties moeten: a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen; b) over een informatiebeveiligingsmanagementforum (IBMF) 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 (NEN 7510-2). Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie. Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, 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	Ja	Ja	Risicoanalyse	Nee	Nee

		kunnen urgente zaken binnen een korte periode in een geschikte vergadering worden besproken.) Er moet een formele verklaring van het toepassingsgebied worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen.					
6.1.2	Scheiding van taken	**Beheersmaatregel** Conflicterende taken en verantwoordelijkheden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. **Zorgspecifieke beheersmaatregel** Organisaties moeten, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden scheiden om de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Nee	Nee
6.1.3	Contact met overheidsinstanties	**Beheersmaatregel** Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Ja	Ja	Risicoanalyse	Nee	Nee
6.1.4	Contact met speciale belangengroepen	**Beheersmaatregel** Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	Ja	Ja	Risicoanalyse	Nee	Nee
6.1.5	Informatiebeveiliging in projectbeheer	**Beheersmaatregel** Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project. **Zorgspecifieke beheersmaatregel** Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Nee	Nee
6.2	Mobiele apparatuur en telewerken	Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.					
6.2.1	Beleid voor mobiele apparatuur	**Beheersmaatregel** Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beheren.	Ja	Ja	Risicoanalyse	Nee	Nee
6.2.2	Telewerken	**Beheersmaatregel** Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Ja	Ja	Risicoanalyse	Nee	Nee
7	**Veilig personeel**						
7.1	Voorafgaand aan het dienstverband	Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.					
7.1.1	Screening	**Beheersmaatregel** Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de vastgestelde risico's.	Ja	Ja	Risicoanalyse	Nee	Nee
7.1.1 deel 1		**Zorgspecifieke beheersmaatregel** Organisaties moeten minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie verifiëren.	Ja	Ja	Risicoanalyse	Nee	Nee
7.1.1 deel 2 7.1.1 deel 3	Screening	**Zorgspecifieke beheersmaatregel** Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband moeten een verificatie omvatten van de toepasselijke kwalificaties voor ***zorgverleners***, indien	Nee, Triaspect heeft geen zorgpersoneel in dienst. Ook heeft Triaspect geen fysieke				

		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***, moet de organisatie zich ervan 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.	beveiligingsmedewerkers in dienst.				
7.1.2	Arbeidsvoorwaarden	**Beheersmaatregel** De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden. **Zorgspecifieke beheersmaatregel** Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, moeten die betrokkenheid in relevante functieomschrijvingen vastleggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, moeten ook in relevante functieomschrijvingen worden vastgelegd. Er moet speciale aandacht worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten, stagiairs enz.	Ja	Ja	Risicoanalyse	Nee	Nee
7.2	Tijdens het dienstverband	Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.					
7.2.1	Directieverantwoordelijkheden	**Beheersmaatregel** De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Ja	Ja	Risicoanalyse	Nee	Nee
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	**Beheersmaatregel** Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten 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 moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	Ja	Ja	Risicoanalyse	Nee	Nee
7.2.3	Disciplinaire procedure	**Beheersmaatregel** Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Ja	Ja	Risicoanalyse	Nee	Nee
7.3	Beëindiging en wijziging van dienstverband	Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.					

7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	**Beheersmaatregel** Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	Ja	Ja	Risicoanalyse	Nee	Nee
8	**Beheer van bedrijfsmiddelen**						
8.1	Verantwoordelijkheid voor bedrijfsmiddelen	Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.					
8.1.1	Inventariseren van bedrijfsmiddelen	**Beheersmaatregel** Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten: a) verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen); b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2); c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	Ja	Ja	Risicoanalyse	Nee	Nee
8.1.2	Eigendom van bedrijfsmiddelen	**Beheersmaatregel** Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, moeten een eigenaar hebben.	Ja	Ja	Risicoanalyse	Nee	Nee
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	**Beheersmaatregel** Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja	Ja	Risicoanalyse	Ja	Nee
8.1.4	Teruggeven van bedrijfsmiddelen	**Beheersmaatregel** Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben, bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven. **Zorgspecifieke beheersmaatregel** Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien 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	Risicoanalyse	Nee	Nee
8.2	Informatieclassificatie	Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.					
8.2.1	Classificatie van informatie	**Beheersmaatregel** Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	Ja	Ja	Risicoanalyse	Nee	Nee
8.2.2	Informatie labelen	**Beheersmaatregel** Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja	Risicoanalyse	Nee	Nee

		Zorgspecifieke beheersmaatregel Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de gebruikers wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen) en behoren papierenoutput als vertrouwelijk te labelen als die output persoonlijke gezondheidsinformatie bevat					
8.2.3	Behandelen van bedrijfsmiddelen	**Beheersmaatregel** Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja	Risicoanalyse	Nee	Nee
8.3	Behandelen van media	Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen, voorkomen.					
8.3.1	Beheer van verwijderbare media	**Beheersmaatregel** Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld. **Zorgspecifieke beheersmaatregel** Media die persoonlijke gezondheidsinformatie bevatten, moeten fysiek worden beschermd of de gegevens ervan moeten versleuteld worden. De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, moeten gemonitord worden.	Ja	Ja	Risicoanalyse	Nee	Nee
8.3.2	Verwijderen van media	**Beheersmaatregel** Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. **Zorgspecifieke beheersmaatregel** Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Risicoanalyse	Nee	Nee
8.3.3	Media fysiek overdragen	**Beheersmaatregel** Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	Ja	Risicoanalyse	Nee	Nee
9	**Toegangsbeveiliging**						
9.1	Bedrijfseisen voor toegangsbeveiliging	Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.					
9.1.1	Beleid voor toegangsbeveiliging	**Beheersmaatregel** Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Ja	Ja	Risicoanalyse	Nee	Nee
9.1.1 deel 1a 9.1.1 deel 1b 9.1.1 deel 1c	Beleid voor toegangsbeveiliging	**Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie 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.	Nee, a) er is geen zorgrelatie tussen Triaspectmedewerkers en degene op wie de gegevens betrekking hebben. b) Triaspect voert geen acties uit namens cliënten, dat wordt door de verwerkingsverantwoordelijke gedaan. c) volgt uit a en b hierboven.			Nee	
9.1.1 deel 2a	Beleid voor toegangsbeveiliging	**Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken,	Ja	Ja	Risicoanalyse	Nee	Nee

9.1.1 deel 2c		moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. a) Het beleid van de organisatie met betrekking tot toegangscontrole moet worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol. c) De organisatie moet alle partijen identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen moeten contractuele afspraken over toegang en rechten worden gemaakt, alvorens cliëntgegevens uit te wisselen.					
9.1.1 deel 2b	Beleid voor toegangsbeveiliging	**Zorgspecifieke beheersmaatregel** Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, moet professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moet de taken die worden uitgevoerd door ***zorgverleners***, en de workflow van de taak in aanmerking nemen.	Nee, Triaspect heeft geen zorgverleners in dienst				
9.1.1 deel 3	Beleid voor toegangsbeveiliging	**Zorgspecifieke beheersmaatregel** De organisatie moet alle partijen identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen moeten contractuele afspraken over toegang en rechten worden gemaakt, alvorens cliëntgegevens uit te wisselen.	Ja	Ja	Risicoanalyse	Nee	Nee
9.1.2	Toegang tot netwerken en netwerkdiensten	**Beheersmaatregel** Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Ja	Ja	Risicoanalyse	Nee	Nee
9.2	Beheer van toegangsrechten van gebruikers	Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.					
9.2.1	Registratie en afmelden van gebruikers	**Beheersmaatregel** Een formele registratie- en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. **Zorgspecifieke beheersmaatregel** De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers moeten 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 moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	Ja	Ja	Risicoanalyse	Ja	Nee
9.2.2	Gebruikers toegang verlenen	**Beheersmaatregel** Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Ja	Ja	Risicoanalyse	Ja	Nee
9.2.3	Beheren van speciale toegangsrechten	**Beheersmaatregel** Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerst.	Ja	Ja	Risicoanalyse	Ja	Nee
9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	**Beheersmaatregel** Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	Ja	Ja	Risicoanalyse	Nee	Nee
9.2.5	Beoordeling van toegangsrechten van gebruikers	**Beheersmaatregel** Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Ja	Ja	Risicoanalyse	Ja	Nee
9.2.6	Toegangsrechten intrekken of aanpassen	**Beheersmaatregel** De toegangsrechten van alle medewerkers en externe gebruikers voor	Ja	Ja	Risicoanalyse	Ja	Nee

		informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast. **Zorgspecifieke beheersmaatregel** Alle organisaties die persoonlijke gezondheidsinformatie verwerken, moeten 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 beëindigen.					
9.3	Verantwoordelijkheden van gebruikers	Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.					
9.3.1	Geheime authenticatie-informatie gebruiken	**Beheersmaatregel** Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Ja	Ja	Risicoanalyse	Nee	Nee
9.4	Toegangsbeveiliging van systeem en toepassing	Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.					
9.4.1	Beperking toegang tot informatie	**Beheersmaatregel** Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. **Zorgspecifieke beheersmaatregel** Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet 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 moet geïsoleerd (en gescheiden) worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Ja	Nee
9.4.2	Beveiligde inlogprocedures	**Beheersmaatregel** Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Ja	Ja	Risicoanalyse	Nee	Nee
9.4.3	Systeem voor wachtwoordbeheer	**Beheersmaatregel** Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Ja	Ja	Risicoanalyse	Nee	Nee
9.4.4	Speciale systeemhulpmiddelen gebruiken	**Beheersmaatregel** Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Ja	Risicoanalyse	Ja	Nee
9.4.5	Toegangsbeveiliging op programmabroncode	**Beheersmaatregel** Toegang tot de programmabroncode moet worden beperkt.	Ja	Ja	Risicoanalyse	Nee	Nee
10	**Cryptografie**						
10.1	Cryptografische beheersmaatregelen	Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.					
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	**Beheersmaatregel** Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja	Risicoanalyse	Nee	Nee
10.1.2	Sleutelbeheer	**Beheersmaatregel** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	Ja	Ja	Risicoanalyse	Nee	Nee
11	**Fysieke beveiliging en beveiliging van de omgeving**						

11.1	Beveiligde gebieden	Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.					
11.1.1	Fysieke beveiligingszone	**Beheersmaatregel** Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gebruikmaken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden moeten worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	Ja	Risicoanalyse	Ja	Nee
11.1.2	Fysieke toegangsbeveiliging	**Beheersmaatregel** Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	Ja	Risicoanalyse	Ja	Nee
11.1.3	Kantoren, ruimten en faciliteiten beveiligen	**Beheersmaatregel** Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	Ja	Risicoanalyse	Nee	Nee
11.1.4	Beschermen tegen bedreigingen van buitenaf	**Beheersmaatregel** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	Ja	Risicoanalyse	Nee	Nee
11.1.5	Werken in beveiligde gebieden	**Beheersmaatregel** Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	Ja	Risicoanalyse	Nee	Nee
11.1.6	Laad- en loslocatie	**Beheersmaatregel** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Ja	Ja	Best practice	Nee	Nee
11.2	Apparatuur	Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.					
11.2.1	Plaatsing en bescherming van apparatuur	**Beheersmaatregel** Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Ja	Ja	Risicoanalyse	Nee	Nee
11.2.2	Nutsvoorzieningen	**Beheersmaatregel** Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregeling in nutsvoorzieningen	Ja	Ja	Risicoanalyse	Nee	Nee
11.2.3	Beveiliging van bekabeling	**Beheersmaatregel** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Ja	Ja	Risicoanalyse	Ja	Nee
11.2.4	Onderhoud van apparatuur	**Beheersmaatregel** Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	Ja	Risicoanalyse	Nee	Nee
11.2.5	Verwijdering van bedrijfsmiddelen	**Beheersmaatregel** Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring. **Zorgspecifieke beheersmaatregel** Organisaties die uitrusting, gegevens of software voor het ondersteunen van een zorgtoepassing met persoonlijke	Ja	Ja	Best practice	Nee	Nee

		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.					
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	**Beheersmaatregel** Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Ja	Ja	Risicoanalyse	Nee	Nee
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	**Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van ***medische apparaten*** die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur 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, Triaspect maakt geen gebruik van medische apparaten				
11.2.7	Veilig verwijderen of hergebruiken van apparatuur	**Beheersmaatregel** Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten 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. **Zorgspecifieke beheersmaatregel** Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Risicoanalyse	Nee	Nee
11.2.8	Onbeheerde gebruikersapparatuur	**Beheersmaatregel** Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja	Risicoanalyse	Nee	Nee
11.2.9	'Clear desk'- en 'clear screen'-beleid	**Beheersmaatregel** Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Ja	Ja	Risicoanalyse	Ja	Nee
12	**Beveiliging bedrijfsvoering**						
12.1	Bedieningsprocedures en verantwoordelijkheden	Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.					
12.1.1	Gedocumenteerde bedieningsprocedures	**Beheersmaatregel** Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja	Risicoanalyse	Nee	Nee
12.1.2	Wijzigingsbeheer	**Beheersmaatregel** Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, moeten worden beheerst. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigingsbeheersproces beheersen om de gepaste beheersing van hosttoepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen.	Ja	Ja	Risicoanalyse	Nee	Nee
12.1.3	Capaciteitsbeheer	**Beheersmaatregel** Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten	Ja	Ja	Risicoanalyse	Nee	Nee

		verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.					
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	**Beheersmaatregel** Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel), scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er moeten regels voor het migreren van software van de ontwikkelaar een operationele status worden gedefinieerd en gedocumenteerd door de organisatie die de betreffende toepassing(en) host.	Ja	Ja	Risicoanalyse	Ja	Nee
12.2	Bescherming tegen malware	Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.					
12.2.1	Beheersmaatregelen tegen malware	**Beheersmaatregel** Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie-, detectie- en responsbeheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software en moeten passende bewustzijnstraining voor gebruikers implementeren.	Ja	Ja	Risicoanalyse	Nee	Nee
12.3	Back-up	Doelstelling: Beschermen tegen het verlies van gegevens.					
12.3.1	Back-up van informatie	**Beheersmaatregel** Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving opslaan om te garanderen dat de informatie in de toekomst beschikbaar is. Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Ja	Nee
12.4	Verslaglegging en monitoren	Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.					
12.4.1	Gebeurtenissen registreren	**Beheersmaatregel** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Ja	Ja	Risicoanalyse	Nee	Nee
12.4.2	Beschermen van informatie in logbestanden	**Beheersmaatregel** Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang. **Zorgspecifieke beheersmaatregel** Auditverslagen moeten beveiligd zijn en mogen niet gemanipuleerd kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten moet worden beveiligd om misbruik of compromittering te voorkomen.	Ja	Ja	Risicoanalyse	Nee	Nee
12.4.3	Logbestanden van beheerders en operators	**Beheersmaatregel** Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden	Ja	Ja	Risicoanalyse	Nee	Nee

		beschermd en regelmatig worden beoordeeld.					
12.4.4	Kloksynchronisatie	**Beheersmaatregel** De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	Ja	Ja	Risicoanalyse	Nee	Nee
12.4.4	Kloksynchronisatie	**Zorgspecifieke beheersmaatregel** Gezondheidsinformatiesystemen die tijdkritische activiteiten voor ***gedeelde zorg*** ondersteunen, moeten in tijdssynchronisatiediensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.	Nee, Triaspect gebruikt geen gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen				
12.5	Beheersing van operationele software	Doelstelling: De integriteit van operationele systemen waarborgen.					
12.5.1	Software installeren op operationele systemen	**Beheersmaatregel** Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	Ja	Ja	Risicoanalyse	Nee	Nee
12.6	Beheer van technische kwetsbaarheden	Doelstelling: Benutting van technische kwetsbaarheden voorkomen.					
12.6.1	Beheer van technische kwetsbaarheden	**Beheersmaatregel** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt, moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt, aan te pakken.	Ja	Ja	Risicoanalyse	Nee	Nee
12.6.2	Beperkingen voor het installeren van software	**Beheersmaatregel** Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	Ja	Ja	Risicoanalyse	Nee	Nee
12.7	Overwegingen betreffende audits van informatiesystemen	Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.					
12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	**Beheersmaatregel** Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Ja	Ja	Risicoanalyse	Nee	Nee
13	**Communicatiebeveiliging**						
13.1	Beheer van netwerkbeveiliging	Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.					
13.1.1	Beheersmaatregelen voor netwerken	**Beheersmaatregel** Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	Risicoanalyse	Ja	Nee
13.1.2	Beveiliging van netwerkdiensten	**Beheersmaatregel** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Ja	Ja	Risicoanalyse	Ja	Nee
13.1.3	Scheiding in netwerken	**Beheersmaatregel** Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Ja	Ja	Risicoanalyse	Ja	Nee
13.2	Informatietransport	Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.					
13.2.1	Beleid en procedures voor informatietransport	**Beheersmaatregel** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	Ja	Ja	Risicoanalyse	Ja	Nee
13.2.2	Overeenkomsten over informatietransport	**Beheersmaatregel** Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	Ja	Risicoanalyse	Nee	Ja

13.2.3	Elektronische berichten	**Beheersmaatregel** Informatie die is opgenomen in elektronische berichten, moet passend beschermd zijn.	Ja	Ja	Risicoanalyse	Ja	Ja
13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	**Beheersmaatregel** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst moet van toepassing zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Nee	Nee
14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**						
14.1	Beveiligingseisen voor informatiesystemen	Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.					
14.1.1	Analyse en specificatie van informatiebeveiligingseisen	**Beheersmaatregel** De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Ja	Ja	Risicoanalyse	Nee	Nee
14.1.1.1	Zorgontvangers op unieke wijze identificeren	**Zorgspecifieke beheersmaatregel** Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten: a) zekerstellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem; b) in staat 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	Risicoanalyse	Ja	Nee
14.1.1.2	Validatie van outputgegevens	**Zorgspecifieke beheersmaatregel** Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.	Nee, Triaspect levert geen elektronische gezondheidsregistratie	nee		Nee	Nee
14.1.2	Toepassingen op openbare netwerken beveiligen	**Beheersmaatregel** Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Ja	Ja	Risicoanalyse	Ja	Nee
14.1.3	Transacties van toepassingen beschermen	**Beheersmaatregel** Informatie die deel uitmaakt van transacties van toepassingen, moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Ja	Ja	Risicoanalyse	Ja	Nee
14.1.3.1	Openbaar beschikbare gezondheidsinformatie	**Zorgspecifieke beheersmaatregel** ***Openbaar*** beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie moet worden vermeld en de integriteit ervan moet worden beschermd.	Nee, Triaspect levert geen openbare gezondheidsinformatie.				

14.2	Beveiliging in ontwikkelings- en ondersteunende processen	Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.					
14.2.1	Beleid voor beveiligd ontwikkelen	**Beheersmaatregel** Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Ja	Ja	Risicoanalyse	Nee	Nee
14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	**Beheersmaatregel** Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	Ja	Ja	Risicoanalyse	Nee	Nee
14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	**Beheersmaatregel** Als besturingsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Ja	Ja	Risicoanalyse	Nee	Nee
14.2.4	Beperkingen op wijzigingen aan softwarepakketten	**Beheersmaatregel** Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Ja	Ja	Risicoanalyse	Nee	Nee
14.2.5	Principes voor engineering van beveiligde systemen	**Beheersmaatregel** Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Ja	Ja	Risicoanalyse	Nee	Nee
14.2.6	Beveiligde ontwikkelomgeving	**Beheersmaatregel** Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Ja	Ja	Risicoanalyse	Nee	Nee
14.2.7	Uitbestede softwareontwikkeling	**Beheersmaatregel** ***Uitbestede*** systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Nee, Triaspect besteedt geen softwareontwikkeling uit.				
14.2.8	Testen van systeembeveiliging	**Beheersmaatregel** Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Ja	Ja	Risicoanalyse	Nee	Nee
14.2.9	Systeemacceptatietests	**Beheersmaatregel** Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten acceptatiecriteria vaststellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie moeten ze geschikte tests van het systeem uitvoeren.	Ja	Ja	Risicoanalyse	Ja	Nee
14.2.9	Systeemacceptatietests	**Zorgspecifieke beheersmaatregel** Klinische gebruikers moeten worden betrokken bij het testen van klinisch relevante systeemelementen.	Nee	Nee			
14.3	Testgegevens	Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.					
14.3.1	Bescherming van testgegevens	**Beheersmaatregel** Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	Ja	Risicoanalyse	Ja	Nee
15	**Leveranciersrelaties**						
15.1	Informatiebeveiliging in leveranciersrelaties	Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.					
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	**Beheersmaatregel** Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie,	Ja	Ja	Risicoanalyse	Ja	Nee

		worden overeengekomen en gedocumenteerd.					
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	**Zorgspecifieke beheersmaatregel** Organisaties die gezondheidsinformatie verwerken, moeten de risico's in verband met toegang door ***externe partijen*** tot deze systemen of gegevens die zij bevatten, beoordelen en vervolgens beveiligingsbeheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	Ja	Ja	Risicoanalyse	Ja	Nee
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	**Beheersmaatregel** Alle relevante informatiebeveiligingseisen moeten 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	Risicoanalyse	Ja	Nee
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	**Beheersmaatregel** Overeenkomsten met leveranciers moeten eisen 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	Risicoanalyse	Ja	Nee
15.2	Beheer van dienstverlening van leveranciers	Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.					
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	**Beheersmaatregel** Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	Ja	Risicoanalyse	Nee	Nee
15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	**Beheersmaatregel** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Ja	Ja	Risicoanalyse	Nee	Nee
16	**Beheer van informatiebeveiligingsincidenten**						
16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.					
16.1.1	Verantwoordelijkheden en procedures	**Beheersmaatregel** Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Ja	Ja	Risicoanalyse	Nee	Nee
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	**Beheersmaatregel** Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd. **Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen: 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.	Ja	Ja	Risicoanalyse	Ja	Nee

		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.					
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	**Zorgspecifieke beheersmaatregel** Organisaties moeten de cliënt altijd informeren als er per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt. Organisaties moeten de ***cliënt op de hoogte stellen*** als het niet beschikbaar zijn van gezondheidsinformatiesystemen negatieve gevolgen gehad kan hebben voor hun zorgverlening.	Nee, Triaspect communiceert niet met cliënten van haar klanten.				
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	**Beheersmaatregel** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie, moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Ja	Ja	Risicoanalyse	Nee	Nee
16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	**Beheersmaatregel** Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja	Ja	Risicoanalyse	Nee	Nee
16.1.5	Respons op informatiebeveiligingsincidenten	**Beheersmaatregel** Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	Risicoanalyse	Nee	Nee
16.1.6	Lering uit informatiebeveiligingsincidenten	**Beheersmaatregel** Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Ja	Ja	Risicoanalyse	Nee	Nee
16.1.7	Verzamelen van bewijsmateriaal	**Beheersmaatregel** De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Ja	Ja	Risicoanalyse	Nee	Nee
17	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**						
17.1	Informatiebeveiligingscontinuïteit	Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.					
17.1.1	Informatiebeveiligingscontinuïteit plannen	**Beheersmaatregel** De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Ja	Ja	Risicoanalyse	Nee	Nee
17.1.2	Informatiebeveiligingscontinuïteit implementeren	**Beheersmaatregel** De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Ja	Ja	Risicoanalyse	Nee	Nee
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	**Beheersmaatregel** De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Ja	Ja	Risicoanalyse	Nee	Nee
17.2	Redundante componenten	Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.					
17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	**Beheersmaatregel** Informatieverwerkende faciliteiten moeten met voldoende redundantie	Ja	Ja	Risicoanalyse	Ja	Ja

		worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.					
18	**Naleving**						
18.1	Naleving van wettelijke en contractuele eisen	Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.					
18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	**Beheersmaatregel** Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Ja	Ja	Risicoanalyse	Nee	Nee
18.1.2	Intellectuele eigendomsrechten	**Beheersmaatregel** Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Ja	Ja	wet- en regelgeving	Nee	Nee
18.1.3	Beschermen van registraties	**Beheersmaatregel** Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Ja	Ja	wet- en regelgeving	Ja	Nee
18.1.4	Privacy en bescherming van persoonsgegevens	**Beheersmaatregel** Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante weten regelgeving.	Ja	Ja	wet- en regelgeving	Ja	Nee
18.1.4 deel 1 18.1.4 deel 2	Privacy en bescherming van persoonsgegevens	**Zorgspecifieke beheersmaatregel** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde ***toestemming van cliënten*** beheren. Waar mogelijk moet geïnformeerde ***toestemming van cliënten*** worden verkregen voordat persoonlijke gezondheidsinformatie per e-mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.	Nee, Triaspect communiceert niet met de cliënten van onze klanten. Deze verantwoordelijkheid ligt bij de verwerkingsverantwoordelijke.				
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	**Beheersmaatregel** Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja	Ja	wet- en regelgeving	Nee	Nee
18.2	Informatiebeveiligingsbeoordelingen	Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.					
18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	**Beheersmaatregel** 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) moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	Ja	Risicoanalyse	Nee	Ja
18.2.2	Naleving van beveiligingsbeleid en -normen	**Beheersmaatregel** Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	Ja	Risicoanalyse	Nee	Nee
18.2.3	Beoordeling van technische naleving	**Beheersmaatregel** Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Ja	Ja	Risicoanalyse	Nee	Nee