10 november 2021

Jouw Omgeving B.V.

NEN 7510-1:2017 +A1:2020

Verklaring van Toepasselijkheid (Statement of Applicability) - V2.2

Beheersmaatregelen

In de onderstaande tabel zijn de zorgspecifieke beheersmaatregelen gekenmerkt met een Z. Zie het volgende overzicht van gebruikte codes en bijbehorende uitleg bij de reden van selectie:

W	Wetgevende eis
C	Contractuele eis
R	Geïdentificeerd risico op basis van de uitgevoerde risico analyse

Maatregel	Omschrijving		Van Toepassing	Geïmplementeerd	Uitbesteed	Reden selectie	Reden uitsluiting
A.5	**Informatiebeveiligingsbeleid**						
A.5.1	**Aansturing door de directie van de informatiebeveiliging**						
A.5.1.1	Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Ja	Ja	Nee	R	
A.5.1.1 (Z)	Beleidsregels voor informatiebeveiliging	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	Nee	R	
A.5.1.2	Beoordeling van het informatiebeveiligingsbeleid	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.	Ja	Ja	Nee	R	
A.5.1.2 (Z)	Beoordeling van het informatiebeveiligingsbeleid	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	Nee	R	
A.6	**Organiseren van informatiebeveiliging**						
A.6.1	**Interne organisatie**						
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Ja	Ja	Nee	R	
A.6.1.1 (Z)	Rollen en verantwoordelijkheden bij informatiebeveiliging	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	Ja	Ja	Nee	R	

		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 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.					
A.6.1.2	Scheiding van taken	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.	Ja	Ja	Nee	R	
A.6.1.2 (Z)	Scheiding van taken	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	Nee	R	
A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Ja	Ja	Nee	W	
A.6.1.4	Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	Ja	Ja	Nee	R	
A.6.1.5	IB in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	Ja	Ja	Nee	C+R	
A.6.1.5 (Z)	IB in projectbeheer	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	Nee	C+R	
A.6.2	**Mobiele apparatuur en telewerken**						
A.6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beheren.	Ja	Ja	Nee	C+R	
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Ja	Ja	Nee	C+R	
A.7	**Veilig personeel**						
A.7.1	**Voorafgaand aan het dienstverband**						
A.7.1.1	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen	Ja	Ja	Nee	C+W	

		en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de vastgestelde risico's.					
A.7.1.1 (Z) Deel 1	Screening	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	Nee	C+W	
A.7.1.1 (Z) Deel 2		Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband moeten een verificatie 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.).	Nee	Nee			Jouw Omgeving heeft geen zorgverleners in dienst.
A.7.1.1 (Z) Deel 3		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.	Nee	Nee			Jouw Omgeving heeft geen zorgverleners in dienst.
A.7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Ja	Ja	Nee	C+R	
A.7.1.2 (Z)	Arbeidsvoorwaarden	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	Nee	C+R	
A.7.2	**Tijdens het dienstverband**						
A.7.2.1	Directie verantwoordelijkheden	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	Nee	R	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	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.	Ja	Ja	Nee	R	
A.7.2.2 (Z)	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	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	Ja	Ja	Nee	R	

		informatiebeveiliging.					
A.7.2.3	Disciplinaire procedure	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	Nee	R	
A.7.3	**Beëindiging en wijziging van dienstverband**						
A.7.3.1	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, moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	Ja	Ja	Nee	R	
A.8	**Beheer van bedrijfsmiddelen**						
A.8.1	**Verantwoordelijkheid voor bedrijfsmiddelen**						
A.8.1.1	Inventariseren van bedrijfsmiddelen	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Ja	Ja	Nee	C+R	
A.8.1.1 (Z)	Inventariseren van bedrijfsmiddelen	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	Nee	C+R	
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, moeten een eigenaar hebben.	Ja	Ja	Nee	C+R	
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	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	Nee	R	
A.8.1.4	Teruggeven van bedrijfsmiddelen	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.	Ja	Ja	Nee	R	
A.8.1.4 (Z)	Teruggeven van bedrijfsmiddelen	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	Nee	R	
A.8.2	**Informatieclassificatie**						
A.8.2.1	Classificatie van informatie	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Ja	Ja	Nee	R	

A.8.2.1 (Z)	Classificatie van informatie	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	Ja	Ja	Nee	R	
A.8.2.2	Informatie labelen	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	Nee	R	
A.8.2.2 (Z)	Informatie labelen	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 moeten papieren output als vertrouwelijk labelen als die output persoonlijke gezondheidsinformatie bevat.	Ja	Ja	Nee	R	
A.8.2.3	Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja	Nee	R	
A.8.3	**Behandelen van media**						
A.8.3.1	Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	Ja	Ja	R	
A.8.3.1 (Z)	Beheer van verwijderbare media	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	Ja	R	
A.8.3.2	Verwijderen van media	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Ja	Ja	Ja	R	
A.8.3.2 (Z)	Verwijderen van media	Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Ja	R	
A.8.3.3	Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	Ja	Ja	R	
A.9	**Toegangsbeveiliging**						
A.9.1	**Bedrijfseisen voor toegangsbeveiliging**						
A.9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Ja	Ja	Nee	R	
A.9.1.1 (Z) deel 1	Beleid voor toegangsbeveiliging	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren.	Ja	Ja	Nee	R	
A.9.1.1 (Z) deel 2		In het algemeen moeten de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie beperken tot situaties:	Nee	Nee			Jouw Omgeving heeft geen

		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.					zorgverleners in dienst.
A.9.1.1 (Z) deel 3		Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. 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.	Ja	Ja	Nee	R	
A.9.1.1 (Z) deel 4		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	Nee			Jouw Omgeving heeft geen zorgverleners in dienst.
A.9.1.1 (Z) deel 5		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	Nee	R	
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Ja	Ja	Nee	R	
A.9.2	**Beheer van toegangsrechten van gebruikers**						
A.9.2.1	Registratie en afmelden van gebruikers	Een formele registratie- en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	Ja	Nee	C+R	
A.9.2.1 (Z)	Registratie en afmelden van gebruikers	De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikers- registratieproces. 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	Nee	C+R	
A.9.2.2	Gebruikers toegang verlenen	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	Nee	R	
A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerst.	Ja	Ja	Nee	R	
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	Ja	Ja	Nee	R	

A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Ja	Ja	Nee	R	
A.9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie- verwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	Ja	Ja	Nee	R	
A.9.2.6 (Z)	Toegangsrechten intrekken of aanpassen	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 werkzaam- heden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie beëindigen.	Ja	Ja	Nee	R	
A.9.3	**Verantwoordelijkheden van gebruikers**						
A.9.3.1	Geheime authenticatie-inform atie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Ja	Ja	Nee	R	
A.9.4	**Toegangsbeveiliging van systeem en toepassing**						
A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Ja	Ja	Nee	R	
A.9.4.1 (Z)	Beperking toegang tot informatie	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	Nee	R	
A.9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Ja	Ja	Nee	R	
A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Ja	Ja	Nee	R	
A.9.4.4	Speciale systeemhulpmiddele n gebruiken	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	Nee	R	
A.9.4.5	Toegangsbeveiliging op programma broncode	Toegang tot de programmabroncode moet worden beperkt.	Ja	Ja	Nee	R	
A.10	**Cryptografie**						
A.10.1	**Cryptografische beheersmaatregelen**						

A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja	Nee	R	
A.10.1.2	Sleutelbeheer	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	Nee	R	
A.11	**Fysieke beveiliging en beveiliging van de omgeving**						
A.11.1	**Beveiligde gebieden**						
A.11.1.1	Fysieke beveiligingszone	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Ja	Ja	Ja	C+R	
A.11.1.1 (Z)	Fysieke beveiligingszone	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	Ja	C+R	
A.11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	Ja	Ja	C+R	
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	Ja	Ja	R	
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	Ja	Ja	C+R	
A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	Ja	Ja	R	
A.11.1.6	Laad- en los locatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatie- verwerkende faciliteiten om onbevoegde toegang te vermijden.	Nee	Nee			Er is geen sprake van laad- en loslocaties.
A.11.2	**Apparatuur**						
A.11.2.1	Plaatsing en bescherming van apparatuur	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	Ja	R	
A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja	Ja	Ja	R	
A.11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Ja	Ja	Ja	C+R	

A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	Ja	Ja	R	
A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	Ja	Ja	R	
A.11.2.5 (Z)	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	Ja	R	
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	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	Nee	R	
A.11.2.6 (Z)	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	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	Nee			Jouw Omgeving heeft geen medische apparaten.
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	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.	Ja	Ja	Ja	R	
A.11.2.7 (Z)	Veilig verwijderen of hergebruiken van apparatuur	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	Ja	R	
A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja	Ja	R	
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Ja	Ja	Nee	R	
A.12	**Beveiliging bedrijfsvoering**						
A.12.1	**Bedieningsprocedures en verantwoordelijkheden**						
A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja	Ja	R	
A.12.1.2	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, moeten worden beheerst.	Ja	Ja	Nee	R	

A.12.1.2 (Z)	Wijzigingsbeheer	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	Nee	R	
A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Ja	Ja	Nee	R	
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Ja	Ja	Nee	R	
A.12.1.4 (Z)	Scheiding van ontwikkel-, test- en productieomgevingen	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel), scheiden van operationele omgevingen waar die gezondheids- informatiesystemen gehost worden. Er moeten regels voor het migreren van software van de ontwikkel- naar een operationele status worden gedefinieerd en gedocumenteerd door de organisatie die de betreffende toepassing(en) host.	Ja	Ja	Nee	R	
A.12.2	**Bescherming tegen malware**						
A.12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Ja	Ja	Ja	R	
A.12.2.1 (Z)	Beheersmaatregelen tegen malware	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	Ja	R	
A.12.3	**Back-up**						
A.12.3.1	Back-up van informatie	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Ja	Ja	Ja	R	
A.12.3.1 (Z)	Back-up van informatie	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	Ja	R	
A.12.4	**Verslaglegging en monitoren**						
A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikers- activiteiten, uitzonderingen en informatie- beveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Ja	Ja	Nee	R	

A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	Ja	Nee	R	
A.12.4.2 (Z)	Beschermen van informatie in logbestanden	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	Nee	R	
A.12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	Ja	Ja	Nee	R	
A.12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligings- domein moeten worden gesynchroniseerd met één referentietijdbron.	Ja	Ja	Nee	R	
A.12.4.4 (Z)	Kloksynchronisatie	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.	Ja	Ja	Nee	R	
A.12.5	**Beheersing van operationele software**						
A.12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	Ja	Ja	Ja	R	
A.12.6	**Beheer van technische kwetsbaarheden**						
A.12.6.1	Beheer van technische kwetsbaarheden	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	Ja	C+R	
A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	Ja	Ja	Ja	R	
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	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	Ja	R	
A.13	**Communicatiebeveiliging**						
A.13.1	**Beheer van netwerkbeveiliging**						
A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	Ja	R	
A.13.1.2	Beveiliging van netwerkdiensten	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	Ja	W+C +R	
A.13.1.3	Scheiding in	Groepen van informatiediensten, -gebruikers en -systemen	Ja	Ja	Ja	R	

	netwerken	moeten in netwerken worden gescheiden.					
A.13.2	**Informatietransport**						
A.13.2.1	Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	Ja	Ja	Nee	C+R	
A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	Ja	Ja	C+R	
A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten, moet passend beschermd zijn.	Ja	Ja	Nee	C+R	
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	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.	Ja	Ja	Nee	C+R	
A.13.2.4 (Z)	Vertrouwelijkheids- of geheimhoudingsovereenkomst	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	Nee	C+R	
A.14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**						
A.14.1	**Beveiligingseisen voor informatiesystemen**						
A.14.1.1	Analyse en specificatie van IB-eisen	De eisen die verband houden met informatie- beveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Ja	Ja	Nee	C+R	
A.14.1.1.1 (Z)	Zorgontvangers op unieke wijze identificeren	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	Nee	C+R	
A.14.1.1.2 (Z)	Validatie van outputgegevens	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.	Ja	Ja	Nee	C+R	
A.14.1.2	Toepassings-diensten op openbare netwerken beveiligen	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	Nee	C+R	
A.14.1.3	Transacties van toepassings-diensten	Informatie die deel uitmaakt van transacties van toepassingen, moet worden beschermd ter voorkoming van onvolledige	Ja	Ja	Nee	R	

	beschermen	overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.					
A.14.1.3.1 (Z)	Openbaar beschikbare gezondheidsinformatie	Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd. De integriteit van openbaar beschikbare gezondheids-informatie 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	Nee			Er is geen sprake van openbaar beschikbare gezondheidsinformatie
A.14.2	**Beveiliging in ontwikkelings- en ondersteunende processen**						
A.14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkel- activiteiten binnen de organisatie worden toegepast.	Ja	Ja	Nee	R	
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	Ja	Ja	Ja	R	
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	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	Ja	R	
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Ja	Ja	Ja	R	
A.14.2.5	Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Ja	Ja	Ja	R	
A.14.2.6	Beveiligde ontwikkelomgeving	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	Nee	R	
A.14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Nee	Nee			Er is geen sprake van uitbestede software-ontwikkeling
A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligings-functionaliteit worden getest.	Ja	Ja	Nee	R	
A.14.2.9	Systeem acceptatie-tests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	Ja	Ja	Nee	C+R	
A.14.2.9 (Z)	Systeem acceptatie-tests	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten acceptatiecriteria vaststellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe	Ja	Ja	Nee	C+R	

		versies. Voorafgaand aan acceptatie moeten ze geschikte tests van het systeem uitvoeren. [A1>Klinische gebruikers moeten worden betrokken bij het testen van klinisch relevante systeemelementen.<A1]					
A.14.3	**Testgegevens**						
A.14.3.1	Bescherming van test gegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	Ja	Nee	R	
A.15	**Leveranciersrelaties**						
A.15.1	**Informatiebeveiliging in leveranciersrelaties**						
A.15.1.1	IB-beleid voor leveranciersrelaties	Met de leverancier moeten de informatie- beveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	Ja	Ja	Ja	C+R	
A.15.1.1 (Z)	IB-beleid voor leveranciersrelaties	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 beveiligings- beheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	Ja	Ja	Ja	C+R	
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuur- elementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Ja	Ja	Ja	C+R	
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatie- beveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatie-technologie.	Ja	Ja	Ja	C+R	
A.15.2	**Beheer van dienstverlening van leveranciers**						
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	Ja	Ja	C+R	
A.15.2.2	Beheer van veranderingen in de dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheers- maatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritika- liteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Ja		Ja	C+R	
A.16	**Beheer van informatiebeveiligingsincidenten**						
A.16.1	**Beheer van informatiebeveiligingsincidenten en -verbeteringen**						
A.16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatie- beveiligingsincidenten te bewerkstelligen.	Ja	Ja	Nee	R	
A.16.1.2	Rapportage van	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk	Ja	Ja	Nee	R	

	IB-gebeurtenissen	via de juiste leidinggevende niveaus worden gerapporteerd.					
A.16.1.2 (Z)	Rapportage van IB-gebeurtenissen	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 crisis- management 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 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 gezondheidsinformatie- systemen negatieve gevolgen gehad kan hebben voor hun zorgverlening.	Ja	Ja	Nee	R	
A.16.1.3	Rapportage van zwakke plekken in de IB	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 informatie- beveiliging registreren en rapporteren.	Ja	Ja	Nee	R	
A.16.1.4	Beoordeling van en besluitvorming over IB-gebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja	Ja	Nee	R	
A.16.1.5	Respons op IB-incidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	Nee	R	
A.16.1.6	Lering uit IB-incidenten	Kennis die is verkregen door informatiebeveiligings- incidenten te analyseren en op te lossen, moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Ja	Ja	Nee	R	
A.16.1.7	Verzamelen van bewijsmateriaal	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Ja	Ja	Nee	R	
A.17	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**						
A.17.1	**Informatiebeveiligingscontinuïteit**						
A.17.1.1	IB-continuïteit plannen	De organisatie moet haar eisen voor informatie- beveiliging en voor de continuïteit van het informatie- beveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Ja	Ja	Nee	C+R	
A.17.1.2	IB-continuïteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van	Ja	Ja	Nee	C+R	

		continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.					
A.17.1.3	IB-continuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatie-beveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Ja	Ja	Nee	C+R	
A.17.2	**Redundante componenten**						
A.17.2.1	Beschikbaarheid van informatieverwerken de faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	Ja	C+R	
A.18	**Naleving**						
A.18.1	**Naleving van wettelijke en contractuele eisen**						
A.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 moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Ja	Ja	Nee	W+C +R	
A.18.1.2	Intellectuele eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele- eigendomsrechten en het gebruik van eigendoms- softwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Ja	Ja	Nee	W+C +R	
A.18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Ja	Ja	Nee	W+C +R	
A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Ja	Ja	Nee	W+C +R	
A.18.1.4 (Z)	Privacy en bescherming van persoonsgegevens	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.	Ja	Ja	Nee	W+C +R	
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja	Ja	Nee	W+C +R	
A.18.2	**Informatiebeveiligingsbeoordelingen**						
A.18.2.1	Onafhankelijke beoordeling van IB	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	Nee	R	

A.18.2.2	Naleving van beveiligingsbeleid en normen	Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	Ja	Nee	R	
A.18.2.3	Beoordeling van technische naleving	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Ja	Ja	Nee	R	