Verklaring van Toepasselijkheid
ISO27001:2022 / NEN 7510

Zorgspecifieke maatregelen zijn uitgelicht

Organisatorische beheersmaatregelen													
ISO27001:2022	NEN7510	Titel/ beschrijving	Beheersmaatregel	Risicoklasse					Wetgeving	MedMij	i.s.m Uitbesteed	Status
				A	B	C	D	E				
A.5.1	A.05.1.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	x					x	x		*
			Zorgspecifiek: Organisaties behoren te beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	x					x			*
	A.05.1.2								x			*
			Zorgspecifiek: Het informatiebeveiligingsbeleid behoort aan voortdurende, gefaseerde beoordelingen te worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid behoort te worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	x					x			*
A.5.2	A.06.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.			x	x	x		x		*
			Zorgspecifiek: Organisaties behoren: - duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging te definiëren en toe te wijzen; - over een informatiebeveiligingsmanagementforum (IBMF) te beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie. Er behoort minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie. Het gezondheidsinformatiebeveiligingsforum behoort regelmatig, maandelijks of bijna maandelijks, te vergaderen. Er behoort een formele verklaring van het toepassingsgebied te worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen.			x	x	x		x		*
A.5.3	A.06.1.2	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.					x		x	x	*
			Zorgspecifiek: Organisaties behoren, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden te scheiden om de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.					x				*
A.5.4	A.07.2.1	Managementverantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	x		x	x	x				*
A.5.5	A.06.1.3	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	x								*

A.5.6	A.06.1.4	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	x		x		x				*
A.5.7	Nieuw	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	x	x	x	x	x		x		*
A.5.8	A.06.1.5	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement,	x			x	x		x		*
			Bij het management van projecten behoort de patiëntveiligheid als projectrisico in aanmerking te worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.				x	x				*
	A.14.1.1		De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	x	x							*
	A.14.1.1.1		Zeker stellen dat zorgontvangers op unieke wijze worden geidentificeerd				x					*
			Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren: *- zeker te stellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem;* *- in staat te zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval.*				x					-
	A.14.1.1.2		Borgen dat opgevraagde gezondsheids informatie overeenkomst met de client die wordt behandeld				x					*
			Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren te voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.				x					*
A.5.9	A.08.1.1	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	x				x			x	*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren: - verantwoording af te leggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bij te houden van dergelijke bedrijfsmiddelen); - een eigenaar te hebben aangewezen voor deze informatiebedrijfsmiddelen; - regels te hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.					x			x	*
	A.08.1.2		Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.					x				*
A.5.10	A.08.1.3	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.					x				*
	A.08.2.3		Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.					x				*
A.5.11	A.08.1.4	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.					x				*

			Alle werknemers en contractanten behoren, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, terug te geven en erop toe te zien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.					x				*
A.5.12	A.08.2.1	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.				x	x	x			*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren dergelijke gegevens op uniforme wijze als vertrouwelijk te classificeren.				x	x				*
A.5.13	A.08.2.2	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.				x	x				*
			Zorgspecifiek: Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren de gebruikers te wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen), en behoren papieren output als vertrouwelijk te labelen als die output persoonlijke gezondheidsinformatie bevat.				x	x				*
A.5.14	A.13.2.1	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.			x	x	x				*
	A.13.2.2		Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.			x	x	x				*
	A.13.2.3		Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	..		x	x	x				*
A.5.15	A.09.1.1	Toegangsbeveiliging	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.			x	x	x		x		*

			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de toegang tot dergelijke informatie te controleren. In het algemeen behoren de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie te beperken tot situaties: - 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); - waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben; - waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen. Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren een toegangscontrolebeleid te hebben waarmee de toegang tot deze gegevens wordt geregeld. Het beleid van de organisatie met betrekking tot toegangscontrole behoort te worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol. Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, behoort professionele, ethische, juridische en cliëntgerelateerde eisen te weerspiegelen en behoort de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking te nemen. De organisatie behoort alle partijen te identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen behoren contractuele afspraken over toegang en rechten te worden gemaakt, alvorens cliëntgegevens uit te wisselen.				x	x				*
	A.09.1.2		Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.				x	x				*
A.5.16	A.09.2.1	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.				x	x				*
			De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoort onderhevig te zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers behoren te garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens behoren regelmatig te worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.				x	x				*
A.5.17	A.09.2.4	Authenticatie-informatie	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie				x	x				*
	A.09.3.1		Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.				x	x				*
	A.09.4.3		Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.				x	x				*
A.5.18	A.09.2.2	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.		x	x	x	x				*
	A.09.2.5		Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.				x	x				*

	A.09.2.6		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.				x	x				*
			Zorgspecifiek: Alle organisaties die persoonlijke gezondheidsinformatie verwerken, behoren voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie te beëindigen.		x	x	x	x				*
A.5.19	A.15.1.1	Informatiebeveiliging in leveranciersrelaties	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.		x	x	x	x				*
			Zorgspecifiek: Organisaties die gezondheidsinformatie verwerken, behoren de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, te beoordelen en vervolgens beveiligingsbeheersmaatregelen te implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.		x	x	x	x				*
A.5.20	A.15.1.2	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.		x							*
A.5.21	A.15.1.3	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.		x							*
A.5.22	A.15.2.1	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.		x							*
	A.15.2.2		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.		x							*
A.5.23	Nieuw	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.			x	x	x				*
A.5.24	A.16.1.1	Plannen en voorbereiden van het beheer van informatiebeveiligings incidenten	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie beveiligingsincidenten te definiëren, vast te stellen en te communiceren.	x								*
A.5.25	A.16.1.4	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	x								*
A.5.26	A.16.1.5	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	x								*
A.5.27	A.16.1.6	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	x								*
A.5.28	A.16.1.7	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	x								*
A.5.29	A.17.1.1	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	x		x						*
	A.17.1.2		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.			x						*

	A.17.1.3		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.			x							*
A.5.30	Nieuw	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoel stellingen en ICT-continuïteitseisen.	x		x							*
A.5.31	A.18.1.1	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.	x					x				*
	A.18.1.5		Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.				x	x					*
A.5.32	A.18.1.2	Intellectuele-eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	x									*
A.5.33	A.18.1.3	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	x					x				*
A.5.34	A.18.1.4	Privacy en bescherming van persoonsgegevens	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	x					x				*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de geïnformeerde toestemming van cliënten te beheren. Waar mogelijk behoort geïnformeerde toestemming van cliënten te worden verkregen voordat persoonlijke gezondheidsinformatie per e-mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.					x	x				*
A.5.35	A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	x									*
A.5.36	A.18.2.2	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	x				x					*
	A.18.2.3		Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	x		x	x	x					*
A.5.37	A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.			x							*
6		**Mensgerichte maatregelen**											
A.6.1	A.07.1.1	Screening	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	x			x	x					*

			Zorgspecifiek: Organisaties behoren minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie te verifiëren. Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband behoren een verificatie te omvatten van de toepasselijke kwalificaties voor zorgverleners, indien er sprake is van accreditatie voor de beroepsgroep op basis van die kwalificaties (bijv. artsen, verplegend personeel enz.). Als een persoon wordt ingehuurd voor een specifieke beveiligingsrol, behoort de organisatie zich ervan te vergewissen dat: - de kandidaat over de nodige competentie beschikt om de beveiligingsrol te vervullen; - de kandidaat de rol kan worden toevertrouwd, in het bijzonder als de rol cruciaal is voor de organisatie.					x				*
A.6.2	A.07.1.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	x								*
			Zorgspecifiek: Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, behoren die betrokkenheid in relevante functieomschrijvingen vast te leggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, behoren ook in relevante functieomschrijvingen te worden vastgelegd.	x								*
A.6.3	A.07.2.2	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	x								*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken. Werknemers van de organisatie en, waar relevant, derde-contractanten behoren te worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.					x				*
A.6.4	A.07.2.3	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.					x				*
A.6.5	A.07.3.1	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.					x				*
A.6.6	A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden					x				*

			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst behoort van toepassing te zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.					x				*
A.6.7	A.06.2.2	Werken op afstand	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.				x	x				*
A.6.8	A.16.1.2	Melden van informatiebeveiligingsgebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings gebeurtenissen tijdig via passende kanalen kan melden.			x	x	x				*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vast te stellen: - om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; - 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; - om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden. Informatiebeveiligingsincidenten omvatten corruptie of onbedoelde openbaarmaking van persoonlijke gezondheidsinformatie of het niet langer beschikbaar zijn van gezondheidsinformatiesystemen waarbij dit niet beschikbaar zijn nadelige gevolgen heeft voor de zorg voor cliënten of bijdraagt aan nadelige klinische gebeurtenissen. Organisaties behoren de cliënt altijd te informeren als er per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt. Organisaties behoren de cliënt op de hoogte te stellen als het niet beschikbaar zijn van gezondheidsinformatiesystemen negatieve gehad kan hebben voor hun zorgverlening.			x	x	x				*
	A.16.1.3		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.			x	x	x				*
7		**Fysieke beheersmaatregelen**										
A.7.1	A.11.1.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.					x			x	*
A.7.2	A.11.1.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.					x			x	*
	A.11.1.6		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			x	x	x			x	*
A.7.3	A.11.1.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.					x			x	*
A.7.4	Nieuw	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.					x			x	*

A.7.5	A.11.1.4	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.			x						x	*
A.7.6	A.11.1.5	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.										N
A.7.7	A.11.2.9	'Clear desk' en 'clear screen'	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen					x					*
A.7.8	A.11.2.1	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.			x						x	*
A.7.9	A.11.2.6	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.					x					*
A.7.10	A.08.3.1	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.					x				x	*
			Zorgspecifiek: Media die persoonlijke gezondheidsinformatie bevatten, behoren fysiek te worden beschermd of de gegevens ervan behoren versleuteld te worden. De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, behoren gemonitord te worden.					x				x	*
	A.08.3.2		Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures					x					*
			Zorgspecifiek: Alle persoonlijke gezondheidsinformatie behoort veilig te worden gewist of anders behoren de media te worden vernietigd als ze niet meer gebruikt hoeven te worden.					x				x	*
	A.08.3.3		Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.					x					*
	A.11.2.5		Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.					x					*
			Zorgspecifiek: 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.					x				x	*
A.7.11	A.11.2.2	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.		x							x	*
A.7.12	A.11.2.3	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.			x		x				x	*
A.7.13	A.11.2.4	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.			x	x	x				x	*
A.7.14	A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.					x				x	*
8		**Technologische beheersmaatregelen**											
A.8.1	A.06.2.1	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.				x	x					*
	A.11.2.8												*
A.8.2	A.09.2.3	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.				x	x					*

A.8.3	A.09.4.1	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.				x	x				*
			Zorgspecifiek: Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren de identiteit van gebruikers vast te stellen en dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie behoort geïsoleerd (en gescheiden) te worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.				x	x				*
A.8.4	A.09.4.5	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.			x	x	x				*
A.8.5	A.09.4.2	Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.				x	x				*
A.8.6	A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.			x						*
A.8.7	A.12.2.1	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.			x	x	x				*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren gepaste preventie-, detectie- en responsbeheersmaatregelen te implementeren om bescherming te bieden tegen kwaadaardige software en behoren passende bewustzijnstraining voor gebruikers te implementeren.			x	x	x			x	*
A.8.8	A.12.6.1	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.			x	x	x			x	*
	A.18.2.3		Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	x								*
A.8.9	Nieuw	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.		x							*
A.8.10	Nieuw	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.					x	x			*
A.8.11	Nieuw	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.					x				*
A.8.12	Nieuw	Voorkomen van gegevenslekken (data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.					x			x	*
A.8.13	A.12.3.1	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.			x	x					*
			Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren back-ups te maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving op te slaan om te garanderen dat de informatie in de toekomst beschikbaar is.			x	x				x	*

A.8.14	A.17.2.1	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.			x							x
A.8.15	A.12.4.1	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.			x							*
	A.12.4.2		Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.				x	x					*
			Zorgspecifiek: Auditverslagen behoren beveiligd te zijn en niet gemanipuleerd te kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten behoort te worden beveiligd om misbruik of compromittering te voorkomen.				x	x					*
	A.12.4.3		Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.			x	x						*
A.8.16	Nieuw	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.			x	x	x					*
A.8.17	A.12.4.4	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.			x							*
			Zorgspecifiek: Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen, behoren in tijdssynchronisatiediensten te voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.			x							*
A.8.18	A.09.4.4	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.				x	x					*
A.8.19	A.12.5.1	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.			x	x	x					*
	A.12.6.2		Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.		x	x	x	x					*
A.8.20	A.13.1.1	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.				x	x				x	*
A.8.21	A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.				x	x				x	*
A.8.22	A.13.1.3	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.				x	x					*
A.8.23	Nieuw	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.			x	x	x					*
A.8.24	A.10.1.1	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.				x	x				x	*
	A.10.1.2		Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.				x	x				x	*
A.8.25	A.14.2.1	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.			x	x	x					*
A.8.26	A.14.1.2	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.			x	x	x					*

	A.14.1.3	Transacties van toepassingsdiensten beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen				x	x				*
	A.14.1.3.1		Voorkomen van onbevoegde wijzigingen in openbaar beschikbare gezondheidsinformatie				x					*
			Zorgspecifiek: Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) behoort te worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie behoort te worden beschermd om onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie behoort te worden vermeld en de integriteit ervan behoort te worden beschermd.				x					*
A.8.27	A.14.2.5	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.			x	x	x				*
A.8.28	Nieuw	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.		x	x	x					*
A.8.29	A.14.2.8	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.			x	x	x				*
	A.14.2.9		Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.									*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren acceptatiecriteria vast te stellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie behoren ze geschikte tests van het systeem uit te voeren. Klinische gebruikers behoren te worden betrokken bij het testen van klinisch relevante			x	x	x				*
A.8.30	A.14.2.7	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.									N
A.8.31	A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.			x	x	x				*
			Zorgspecifiek: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel), te scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er behoren regels voor het migreren van software van de ontwikkel- naar een operationele status te worden gedefinieerd en gedocumenteerd door de organisatie die de betreffende toepassing(en) host.			x	x	x				*
	A.14.2.6		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.			x	x	x				*
A.8.32	A.12.1.2	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.			x						*
			Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigingsbeheersproces te beheersen om de gepaste beheersing van hosttoepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen.			x						*
	A.14.2.2		Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.			x	x	x				*

	A.14.2.3		Als bedieningsplatforms 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.			x	x	x				*
	A.14.2.4		Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.			x	x	x				*
A.8.33	A.14.3.1	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.				x	x				*
A.8.34	A.12.7.1	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management			x	x	x			x	*