NEN 7510:2024

Verklaring van Toepasselijkheid

Gepubliceerd op | 05-01-2026
Versie | 5.0
Gepubliceerd door | Frank Schonewille

Meer weten? Ga naar vcareconnect.nl

Scope

Informatiebeveiliging gerelateerd aan het leveren van het Vcare cloud telefonieplatform voor de zorgsector in overeenstemming met de Verklaring van Toepasselijkheid versie 5.0 17 februari 2025.

Legenda

S : Binnen Scope, Geselecteerd

R: Geselecteerd op basis van Risico

C: Geselecteerd op basis van Contractuele voorwaarde

W: Geselecteerd op basis van Wettelijke Verplichting

U: Uitbestede processen

#	Titel	Beheersmaatregel	S	R	W	C	U	Status	Toelichting
A.5.1	Beleidsregels voor informatiebeveiliging	Het informatiebeveiligingsbeleid moet de aanpak voor het beheer van informatiebeveiliging beschrijven en te zijn goedgekeurd door het topmanagement, vervolgens ten minste eenmaal per jaar en daarna telkens als er zich een ernstige beveiligingsgebeurtenis voordoet te worden beoordeeld. *Zorgspecifiek doel (aanvullend):* Waarborgen van de betrokkenheid van het topmanagement bij informatiebeveiliging, die altijd actueel wordt gehouden.	√	√				Gerealiseerd	
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Er behoort ten minste één persoon verantwoordelijk te zijn voor informatiebeveiliging. *Zorgspecifiek doel (aanvullend):* Waarborgen dat er sprake is van duidelijke richting en sturing, zichtbare ondersteuning vanuit het management voor activiteiten die gepaard gaan met het beveiligen van gezondheidsinformatie en toereikende technische expertise.	√	√				Gerealiseerd	
A.5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	√	√				Gerealiseerd	

A.5.4	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.	√	√				Gerealiseerd	
A.5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	√	√	√			Gerealiseerd	
A.5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	√	√				Gerealiseerd	
A.5.7	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	√	√				Gerealiseerd	
A.5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	√	√		√		Gerealiseerd	

A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Alle informatiestromen (zowel binnen als tussen organisaties) en de interfaces daarvan (waaronder integratieplatforms) behoren te worden opgenomen in de inventarisatie. *Zorgspecifiek doel (aanvullend):* De stromen van informatie en de interfaces van die stromen identificeren om de informatiebeveiliging ervan te behouden en er passende eigenaren aan toe te wijzen.	√	√		√		Gerealiseerd	
A.5.10	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.	√	√		√		Gerealiseerd	
A.5.11	Retourneren van bedrijfsmiddelen	Er behoort beleid te zijn dat vereist dat persone schriftelijk bevestigen dat alle bedrijfsmiddelen in hun bezit in alle formaten op veilige wijze zijn geretourneerd of verwijderd, indien van toepassing. *Zorgspecifiek doel (aanvullend):* Persoonlijke gezondheidsinformatie als onderdeel van de procedure voor het wijzigen of beëindigen van een dienstverband, contract of overeenkomst beschermen.	√	√		√		Gerealiseerd	

A.5.12	Classificeren van informatie	Persoonlijke gezondheidsinformatie behoort uniform als vertrouwelijk te worden geclassificeerd. *Zorgspecifiek doel (aanvullend):* De juiste classificatie van persoonlijke gezondheidsinformatie onder alle omstandigheden waarborgen.	√	√				Gerealiseerd	
A.5.13	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.	√	√				Gerealiseerd	
A.5.14	Overdragen van informatie	Vóórdat enige overdracht plaatsvindt, behoren er regels, procedures en overeenkomsten te zijn ingesteld. *Zorgspecifiek doel (aanvullend):* De beveiliging van informatieoverdracht gedurende de volledige levensduur ervan waarborgen.	√	√				Gerealiseerd	
A.5.15	Toegangsbeveiliging	Er behoort beleid voor op rollen gebaseerde toegangsbeveiliging te gelden voor de toegang tot persoonlijke gezondheidsinformatie.	√	√				Gerealiseerd	Deels niet van toepassing: Vcare heeft geen zorgrelatie met de client. Vcare heeft geen client gerelateerde eisen

		Zorgspecifiek doel (aanvullend): Toegang op basis van op gedegen wijze vastgelegde rollen waarborgen.							die worden uitgevoerd door zorgverleners. Vcare wisselt geen clientgegevens uit
A.5.16	Identiteitsbeheer	Gebruikers die toegang willen hebben tot persoonlijke gezondheidsinformatie en andere vertrouwelijke informatie, behoren formeel te zijn geregistreerd. *Zorgspecifiek doel (aanvullend):* Waarborgen dat aan elk individu een correcte gebruikersidentiteit wordt toegewezen.	√	√		√		Gerealiseerd	
A.5.17	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	√	√				Gerealiseerd	
A.5.18	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.	√	√		√		Gerealiseerd	
A.5.19	Informatiebeveiliging in leveranciersrelaties	De risico's in verband met toegang door externe partijen tot systemen of de gegevens die zij bevatten behoren te worden beoordeeld en	√	√				Gerealiseerd	

		beheersmaatregelen passend bij het geïdentificeerde risico behoren te worden geïmplementeerd. *Zorgspecifiek doel (aanvullend):* De externe toegang van leveranciers tot systemen en gegevens beheren en beschermen.						
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	√	√		√	Gerealiseerd	
A.5.21	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.	√	√	√	√	Gerealiseerd	
A.5.22	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.	√	√		√	Gerealiseerd	

A.5.23	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.	√	√				Gerealiseerd	
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiliging sincidenten	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	√	√				Gerealiseerd	
A.5.25	Beoordelen van en besluiten over informatiebeveiliging sgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	√	√				Gerealiseerd	
A.5.26	Reageren op informatiebeveiliging sincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	√	√				Gerealiseerd	
A.5.27	Leren van informatiebeveiliging sincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	√	√				Gerealiseerd	

A.5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	√	√				Gerealiseerd	
A.5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	√	√		√		Gerealiseerd	
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	√	√				Gerealiseerd	
A.5.31	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.	√	√	√	√		Gerealiseerd	
A.5.32	Intellectuele-eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	√	√	√	√		Gerealiseerd	
A.5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	√	√	√	√		Gerealiseerd	

A.5.34	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.	√	√	√	√			Gerealiseerd	
A.5.35	Onafhankelijke review 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.	√	√					Gerealiseerd	
A.5.36	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.	√	√					Gerealiseerd	
A.5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	√	√					Gerealiseerd	
A.5.38	HLT – Analyse en specificatie van informatiebeveiligingseisen	De informatiebeveiligingsgerelateerde eisen behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen aan bestaande informatiesystemen.	√	√					Gerealiseerd	

		Doel: *Waarborgen dat risico's in verband met de ontwikkeling en/of aankoop van informatiesystemen gedurende de levenscyclus van het informatiesysteem doeltreffend worden aangepakt.*							
A.5.39	HLT – Zorgontvangers op unieke wijze identificeren	Beleid en processen behoren te waarborgen dat elke zorgontvanger op unieke wijze binnen het systeem kan worden geïdentificeerd en behoren in staat te zijn dubbele of meervoudige registraties samen te voegen als er dubbele of meervoudige registraties zijn voor een en dezelfde zorgontvanger. *Doel:* Voorkomen van onvolledige of niet-consistente informatie en dossiers over zorgontvangers.						Niet van toepassing	Vcare verwerkt geen gegevens van cliënten of persoonlijke gezondheidsinformatie met client /zorgontvanger identificatie.
A.5.40	HLT – Validatie van getoonde/geprinte gegevens	Als er gegevens worden getoond en/of geprint door gezondheidsinformatiesystemen behoren deze gegevens ook informatie te omvatten waarmee de zorgontvanger waarop de gegevens betrekking heeft wordt geïdentificeerd. *Doel:*						Niet van toepassing	Vcare verwerkt geen gegevens van cliënten of persoonlijke gezondheidsinformatie met client identificatie.

		De bevestiging mogelijk maken dat informatie voor de juiste zorgontvanger is en voorkomen dat informatie wordt gebruikt die op iemand anders betrekking heeft.							
A.5.41	HLT – Openbaar beschikbare gezondheidsinformatie	Openbaar beschikbare gezondheidsinformatie behoort te worden beschermd, bewaard en beheerd gedurende de volledige levenscyclus. *Doel:* Waarborgen dat openbaar beschikbare gezondheidsinformatie beschikbaar is wanneer nodig, de integriteit wordt gehandhaafd, de herkomst wordt vastgelegd, er een audittraject wordt bijgehouden en historische informatie kan worden achterhaald. Informatie, inclusief bijwerkingen, over voorgeschreven medicijnen en andere medicijnen is vaak ook openbaar beschikbaar, samen met uitleg over de diagnose en behandeling van veel aandoeningen. Belangrijke beslissingen kunnen worden genomen door zorgvragers, hun begeleiders of plaatsvervangers op basis van openbaar beschikbare gezondheidsinformatie. Gezondheidszorgprofessionals kunnen ook vertrouwen op dergelijke informatie. Het is daarom essentieel dat openbaar beschikbare gezondheidsinformatie						Niet van toepassing	Vcare heeft geen openbaar beschikbare gezondheidsinformatie.

		betrouwbaar, nauwkeurig en up-to-date is. Om dit te garanderen: 1. moeten de integriteit en beschikbaarheid van de informatie worden beschermd; 2. moet de oorsprong van de informatie worden vermeld en moet de herkomst ervan worden gecontroleerd voordat deze beschikbaar wordt gesteld; 3. moet er een volledig audittraject zijn, zodat duidelijk is welk personeel de informatie heeft gemaakt, gewijzigd, verwijderd of andere acties heeft uitgevoerd; 4. moet er een uitgebreid archief van de informatie worden bijgehouden en moet er een faciliteit zijn om toegang te krijgen tot de historische informatie om vast te stellen welke inhoud op een bepaald moment beschikbaar was.							
A.5.42	HLT – Communicatie in noodsituaties	Noodcommunicatiekanalen binnen een zorgorganisatie die in werking treden wanneer er een storing is in de continuïteit van de ICT van de organisatie behoren te worden gepland, geïmplementeerd, onderhouden en beproefd. *Doel:* Waarborgen dat essentiële communicatie mogelijk is bij uitval van ICT.	√	√				Gerealiseerd	

A.5.43	HLT – Incidenten extern melden	Informatiebeveiligingsincidenten behoren volgens juridische of contractuele verplichtingen of verplichtingen uit hoofde van wet- en regelgeving te worden gemeld. *Doel:* Waarborgen dat wordt voldaan aan juridische of contractuele verplichtingen of verplichtingen uit hoofde van wet- en regelgeving met betrekking tot informatiebeveiligingsincidenten.	√	√				Gerealiseerd	
A.6.1	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.	√	√				Gerealiseerd	
A.6.2	Arbeidsovereenkomst	In functiebeschrijvingen behoren de beveiligingsrollen en verantwoordelijkheden te worden vermeld die van toepassing zijn op het verwerken van persoonlijke gezondheidsinformatie. *Zorgspecifiek doel (aanvullend):*	√	√				Gerealiseerd	

		Waarborgen dat de privacy van zorgontvangers wordt benadrukt en begrepen.							
A.6.3	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.	√	√				Gerealiseerd	
A.6.4	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.	√	√		√		Gerealiseerd	
A.6.5	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.	√	√		√		Gerealiseerd	
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Alle personeel dat bevoegd is tot toegang tot persoonlijke gezondheidsinformatie behoort er formeel toe te worden verplicht die informatie vertrouwelijk te behandelen.	√	√		√		Gerealiseerd	

		Zorgspecifiek doel (aanvullend): Formeel de vertrouwelijkheid van informatie waartoe personeel of derden toegang hebben in stand houden.							
A.6.7	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.	√	√		√		Gerealiseerd	
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	√	√				Gerealiseerd	
A.6.9	HLT – Managementtraining	Het management van de organisatie behoort passende training te krijgen, naarmate relevant is voor hun rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en hoe het wordt beheerd. *Doel:* Waarborgen dat het management zijn rollen kan vervullen en zijn verantwoordelijkheden kan nemen met betrekking tot het managementsysteem voor informatiebeveiliging.	√	√				Gerealiseerd	
A.7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden	√	√		√		Gerealiseerd	

		beschermd door beveiligingszones te definiëren en te gebruiken.							
A.7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	√	√		√		Gerealiseerd	
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	√	√				Gerealiseerd	
A.7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	√	√				Gerealiseerd	
A.7.5	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.	√	√		√		Gerealiseerd	
A.7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	√	√				Gerealiseerd	
A.7.7	'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.	√	√				Gerealiseerd	

A.7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	√	√				Gerealiseerd	
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	√	√				Gerealiseerd	
A.7.10	Opslagmedia	Alle persoonlijke gezondheidsinformatie die op verwijderbare media wordt opgeslagen, behoort te worden versleuteld. *Zorgspecifiek doel (aanvullend):* Voorkomen van misbruik van persoonlijke gezondheidsinformatie, waaronder ongeautoriseerde toegang, onthulling of wijziging.	√	√				Gerealiseerd	
A.7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	√	√				Gerealiseerd	
A.7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	√	√	√			Gerealiseerd	
A.7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	√	√			√	Gerealiseerd	

A.7.14	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.	√	√				Gerealiseerd	
A.8.1	Gebruikersapparatuur	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	√	√		√		Gerealiseerd	
A.8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	√	√				Gerealiseerd	
A.8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	√	√				Gerealiseerd	
A.8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	√	√				Gerealiseerd	
A.8.5	Beveiligde authenticatie	Er behoort ten minste tweefactorauthenticatie te worden gebruikt voor systemen die persoonlijke gezondheidsinformatie verwerken.	√	√				Openstaand	

		Zorgspecifiek doel (aanvullend): Betere beveiliging waarborgen voor toegang tot persoonlijke gezondheidsinformatie.						Gerealiseerd	
A.8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	√	√				Gerealiseerd	
A.8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.	√	√				Gerealiseerd	
A.8.8	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.	√	√		√		Gerealiseerd	
A.8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	√	√				Gerealiseerd	

A.8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	√	√				Gerealiseerd	
A.8.11	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.	√	√				Gerealiseerd	
A.8.12	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.	√	√				Gerealiseerd	
A.8.13	Back-up van informatie	Back-ups van persoonlijke gezondheidsinformatie behoren te worden versleuteld. *Zorgspecifiek doel (aanvullend):* De vertrouwelijkheid van persoonlijke gezondsheidsinformatie beschermen.	√	√				Gerealiseerd	
A.8.14	Redundantie van informatieverwerken de faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	√	√		√		Gerealiseerd	

A.8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	√	√				Gerealiseerd		
A.8.16	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.	√	√				Gerealiseerd		
A.8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	√	√				Gerealiseerd		
A.8.18	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.	√	√				Gerealiseerd		
A.8.19	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.	√	√				Gerealiseerd		
A.8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	√	√				Gerealiseerd		

A.8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	√	√	√	√		Gerealiseerd	
A.8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	√	√				Gerealiseerd	
A.8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	√	√				Gerealiseerd	
A.8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	√	√				Gerealiseerd	
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	√	√				Gerealiseerd	
A.8.26	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en	√	√		√		Gerealiseerd	

		goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.							
A.8.27	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.	√	√				Gerealiseerd	
A.8.28	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	√	√				Gerealiseerd	
A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	√	√		√		Gerealiseerd	
A.8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	√	√				Gerealiseerd	
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	√	√				Gerealiseerd	
A.8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	√	√				Gerealiseerd	

A.8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	√	√				Gerealiseerd	
A.8.34	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.	√	√				Gerealiseerd	
A.8.35	HLT – Zero trust-beginselen	Aan een netwerksegment toegewezen groepen informatiediensten, gebruikers en informatiesystemen behoren zo klein mogelijk te worden gehouden en behoren slechts toegang tot een ander netwerksegment te hebben nadat beide betrokken segmenten elkaar hebben geauthentiseerd. Doel: Waarborgen dat met een netwerk verbonden entiteiten niet standaard worden vertrouwd.	√	√				Gerealiseerd	