

Verklaring van toepasselijkheid NEN7510:2017 + A1 2020 v1.1 PAQT.com B.V. en NewDays Solutions B.V. 30-04-2024			Van toepassing?	Geïmplementeerd?	Risico analyse	Wet	Contract	Interface	Niet van toepassing want:	Uitbesteed?
A.5	Beveiligingsbeleid									
A.5.1	Managementaanwijzing voor informatiebeveiliging	Het verschaffen van directieaansturing van en -stun voor informatiebeveiliging in overeenstemming met bedrijfsdoelen en relevante wet- en regelgeving.								
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. Zorgspecifieke beheersmaatregel: Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	Ja	Ja	X			X		
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. Zorgspecifieke beheersmaatregel: Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	Ja	Ja	X			X		
A.6	Organisatie van informatiebeveiliging									
A.6.1	Interne organisatie	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.								
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Organisaties moeten: a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Organisaties moeten: b) over een informatiebeveiligingsmanagementforum (IBMF) beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in B3 en B4 van bijlage B (6.1.1) in NEN 7510-2.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen. (Het is meestal het effectiefs 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.)	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: 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.	Ja	Ja	X			x		
A.6.1.2	Scheiding van taken	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Zorgspecifieke beheersmaatregel: Organisaties moeten, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden scheiden teneinde de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.	Ja	Ja	X			x		
A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Ja	Ja	X					
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	X					
A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project. Zorgspecifieke beheersmaatregel: Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gaat om het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja	X			x		
A.6.2	Mobiele computers 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 beheersen.	Ja	Ja	X					
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerkkollocaties wordt bereikt, verwerkt of opgeslagen.	Ja	Ja	X					
A.7	Beveiliging personeel									
A.7.1	Vooraanmelding aan het dienstverband	Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.								
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 en moet in verhouding staan tot de bedrijfsrisico's, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's. Zorgspecifieke beheersmaatregel: Organisaties moeten minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie verifiëren.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: 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					PAQT.com heeft geen zorgverleners in dienst.	
		Zorgspecifieke beheersmaatregel: Als een persoon wordt ingehuurd voor een specifieke beveiligingsfunctie, moet de organisatie zich ervan vergewissen dat: a) de kandidaat over de nodige competentie beschikt om de beveiligingsfunctie te vervullen; b) de functie de kandidaat toevertrouwd kan worden, in het bijzonder als de functie cruciaal is voor de organisatie.	Nee	Nee					PAQT.com heeft geen beveiligingsfuncties zoals bedoeld in de norm.	
A.7.1.2	Arbeidvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, moeten die betrokkenheid in relevante functomschrijvingen vastleggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, moeten ook in relevante functomschrijvingen worden vastgelegd.	Ja	Ja	X					
		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.								
A.7.2	Tijdens het dienstverband	Envoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.								
A.7.2.1	Directieverantwoordelijkheden	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	X					
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. Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstreekt aan alle werknemers, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Werknemers van de organisatie en, waar relevant, derdecontractanten moeten worden gewist op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	Ja	Ja	X					
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	X					
A.7.3	Beëindiging en wijziging dienstverband	Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het 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	X					
A.8	Beheer Bedrijfsmiddelen									
A.8.1	Verantwoordelijkheden voor bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.								
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. Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten: a) verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen); b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2); c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	Ja	Ja	X					
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Ja	Ja	X					
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	X					
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. Zorgspecifieke beheersmaatregel: Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bigewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.	Ja	Ja	X					
A.8.2	Classificatie van informatie	Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.								

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	X			X		
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten degelijke gegevens op uniforme wijze als vertrouwelijk classificeren.								
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	X			X		
		Zorgspecifieke beheersmaatregel: Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de gebruikers wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is via het systeem (bijv. bij het opstarten of inloggen), en moeten papieren output als vertrouwelijk labelen als die output persoonlijke gezondheidsinformatie bevat.	Ja	Ja	X			X		
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	X					
A.8.3	Behandeling media	Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.	Ja	Ja						
A.8.3.1	Beheer van verwijderbare media	Voor het beheeren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Media die persoonlijke gezondheidsinformatie bevatten moeten fysiek worden beschermd of de gegevens ervan moeten versleuteld worden. De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, moeten gemonitord worden.	Ja	Ja	X			X		
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	X					
		Zorgspecifieke beheersmaatregel: Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anderszins moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	Ja	Ja	X			X		
A.8.3.3	Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	Ja	X					
A.9	Toegangscontrole									
A.9.1	Bedrijfsvereisten voor toegangscontrole	Toegang tot informatie en informatieverwerkende faciliteiten beperken.								
A.9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingsrisico's.	Ja	Ja	X					
A.9.1.1	Beleid voor toegangsbeveiliging	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie beperken tot situaties: a) waarin er een relatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de client 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. Organisations die persoonlijke gezondheidsinformatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld.	Ja	Ja	X			X		
		Zorgspecifieke beheersmaatregel: 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. Het toegangscontrolebeleid, als onderdeel 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. 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	X			X		
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	X					
A.9.2	Beheer van toegangsrechten van gebruikers	Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.								
A.9.2.1	Registratie en uitschrijving van gebruikers	Een formele registratie- en uitschrijving-procedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers moeten garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	Ja	Ja	X			X		
A.9.2.2	Gebruikers toegang verlenen	Een formele gebruikers toegangs-verleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Ja	Ja	X					
A.9.2.3	Beheer van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Ja	Ja	X					
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	X					
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Ja	Ja	X					
A.9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijziging moeten ze worden aangepast.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Alle organisaties die persoonlijke gezondheidsinformatie verwerken moeten voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie beëindigen.	Ja	Ja	X			X		
A.9.3	Verantwoordelijkheden van gebruikers	Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.								
A.9.3.1	Geheime authenticatie-informatie 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	X					
A.9.4	Systeem en applicatie toegangscontrole	Onbevoegde toegang tot systemen en toepassingen voorkomen.								
A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Alle 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.	Ja	Ja	X			X		
		Zorgspecifieke beheersmaatregel: 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	X			X		
A.9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerd door een beveiligde inlogprocedure.	Ja	Ja	X					
A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Ja	Ja	X					
A.9.4.4	Speciale systeemhulpmiddelen 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	X					
A.9.4.5	Toegangsbeveiliging op programmaprocedure	Toegang tot de programmaprocedure moet worden beperkt.	Ja	Ja	X					
A.10	Cryptografie									
A.10.1	Cryptografische beheersmaatregelen	Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.								
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ten bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja	X					
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	X					
A.11	Fysieke en omgevingsbeveiliging									
A.11.1	Beveiligde gebieden	Onbeveiligde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.								
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	X					
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gebruikmaken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheids toepassingen 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	X			X		
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	X					
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	Ja	X					
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	Ja	X					
A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	Ja	X					
A.11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerd, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Ja	Ja	X					
A.11.2	Beveiliging van apparatuur	Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.								
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	X					
A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontbrekingen in nutsvoorzieningen.	Ja	Ja	X					
A.11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het verspreiden van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Ja	Ja	X					
A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	Ja	X					
A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	Ja	X					

		Zorgspecifieke beheersmaatregel: Organisaties die uitsluitend gegevens van software voor het ondersteunen van een zorgtoepassing met persoonlijke gezondheidsinformatie leveren of gebruiken, mogen niet toestaan dat de uitsluiting, gegevens van software van de locatie wordt of worden verwijderd of er binnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven.	Ja	Ja	X		X			
A.11.2.6	Beveiliging van apparatuur en bedragsmiddelen buiten het terrein	Bedragsmiddelen 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	X					
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d.w.z. waar het een kenmerk is van de rol van de werknemer, zoals het geval is bij ambulancemedici, therapeuten enz.)	Nee	Nee					PAQT.com heeft binnen haar toepassingsgebied geen medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren.	
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geveerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden.	Ja	Ja	X		X			
A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja	X					
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	X					
A.12	Beveiliging operatie									
A.12.1	Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.								
A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja	X					
A.12.1.2	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerd.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkende faciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigings-beheersproces beheersen om de gepaste beheersing van host-toepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen.	Ja	Ja	X					
A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitsvragen om de vereiste systeemcapaciteit te waarborgen.	Ja	Ja	X					
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 verminderen.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel) scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er moeten regels voor het migreren van software van de ontwikkel- naar een operationele status worden gedefinieerd en gedocumenteerd door de organisatie die de betroffen toepassing(en) host.	Ja	Ja	X		X			
A.12.2	Bescherming Malware	Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.								
A.12.2.1	Beheersmaatregelen tegen malware	Tijd bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie-, detectie- en respons beheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software, en passende bewustzijns training voor gebruikers implementeren.	Ja	Ja	X			X		
A.12.3	Back-up	Beschermen tegen het verliezen van gegevens.								
A.12.3.1	Back-up van informatie	Regelmatig moeten back-up-opnamen van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving opslaan om te garanderen dat de informatie in de toekomst beschikbaar is.	Ja	Ja	X			X		
		Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie.								
A.12.4	Logging en bewaking	Gedocumenteerde vastleggen en bewaken van activiteiten.								
A.12.4.1	Gedocumenteerde registreren	Logbestanden van gebeurtenissen die gebruikactiviteiten, uitzonderingen en informatieveiligheidsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Ja	Ja	X					
A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen valsheid en onbevoegde toegang.	Ja	Ja	X					
		Zorgspecifieke beheersmaatregel: Auditverslagen moeten beveiligd zijn en 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	X			X		
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	X					
A.12.4.4	Klok synchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomin moeten worden gesynchroniseerd met één referentietijdbron.	Ja	Ja	X			X		
		Zorgspecifieke beheersmaatregel: Gezondheidsinformatiesystemen die tijdritmische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdsynchronisatie-diensten voorzien om het traceren en reconstrueren van de tijdpunten voor activiteiten waar vereist te ondersteunen.	Ja	Ja	X			X		
A.12.5	Beheersing van operationele programmatuur	De integriteit van operationele systemen waarborgen.								
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	X					
A.12.6	Beheer van technische kwetsbaarheden	Benutting van technische kwetsbaarheden voorkomen.								
A.12.6.1	Beheersing 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	X					
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	X					
A.12.7	Overwegingen bij audits van informatiesystemen	De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.								
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 op bedrijfsprocessen zo min mogelijk te verstoren.	Ja	Ja	X					
A.13	Beveiliging van verbindings									
A.13.1	Beheer van netwerkbeveiliging	De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.								
A.13.1.1	Beheersmaatregelen voor netwerken	Netwerk en moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	X					
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheersniveaus 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	X					
A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Ja	Ja	X					
A.13.2	Informatie uitwisseling	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.								
A.13.2.1	Beleid en procedures voor informatie transport	Tijd bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	Ja	Ja	X					
A.13.2.2	Overeenkomsten over informatie transport	Overeenkomsten met betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	Ja	X		X	X		
A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	Ja	Ja	X					
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	X		X			
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst moet van toepassing zijn op het personeel dat toegang heeft tot gezondheidsinformatie.	Ja	Ja	X		X	X		
A.14	Verwerving, ontwikkeling en onderhoud van informatiesystemen									
A.14.1	Beveiligingsbeelden voor informatiesystemen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hierbij behoren ook de eisen voor informatiesystemen die diensten verspreiden via openbare netwerken.								
A.14.1.1	Analyse en specificatie van informatie beveiligings-eisen	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Ja	Ja	X					
A.14.1.1.1	Zorgontvangers op unieke wijze identificeren	Zorgspecifieke beheersmaatregel: Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten: a) zekerstellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem; b) in staat zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodval.	Ja	Ja	X		X			
A.14.1.1.2	Validatie van outputgegevens	Zorgspecifieke beheersmaatregel: Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.	Ja	Ja	X		X			
A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoeringssystemen en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Ja	Ja	X					
A.14.1.3	Transacties van toepassingsdiensten beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd tegen voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vernietigen van afspelen.	Ja	Ja	X					
A.14.1.3.1	Openbaar beschikbare gezondheidsinformatie	Zorgspecifieke beheersmaatregel: Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden geclassificeerd. De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie moet worden vermeld en de integriteit ervan moet worden beschermd.	Nee	Nee					PAQT.com publiceert geen openbare gezondheidsinformatie.	
A.14.2	Beveiliging bij ontwikkelings- en onderhoudsfasen	Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingscyclus van informatiesystemen.								
A.14.2.1	Beleid voor beveiliging ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Ja	Ja	X					
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerd door het gebruik van formele controleprocedures voor wijzigingsbeheer.	Ja	Ja	X					

A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Als bedieningsplatforms zijn veranderd, moeten bedrijfsspecifieke 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	X								
A.14.2.4	Wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontzaden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Ja	Ja	X								
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 veranderingen betreffende het implementeren van informatiesystemen.	Ja	Ja	X								
A.14.2.6	Beveiligde ontwikkelingsomgeving	Organisaties moeten beveiligde ontwikkelingsomgevingen vaststellen en passend beveiligen voor veranderingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Ja	Ja	X								
A.14.2.7	Uitbestede software- ontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Ja	Ja	X								
A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelcycli moeten de beveiligingsfunctionaliteit worden getest.	Ja	Ja	X								
A.14.2.9	Systemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	Ja	Ja	X								
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten acceptatiecriteria vaststellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie moeten ze geschikte testen van het systeem uitvoeren. A1>Klinische gebruikers moeten worden betrokken bij het testen van klinisch relevante systeemelementen. <A1	Ja	Ja	X								
A.14.3	Testgegevens	Bescherming van gegevens van gegevens die voor het testen zijn gebruikt.											
A.14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	Ja	X								
A.15	Relaties leveranciers												
A.15.1	Informatiebeveiliging in leveranciersrelaties	De bescherming van gegevens van bedrijfsinformatie van de organisatie die toegankelijk zijn voor leveranciers.											
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Met de leverancier moeten de informatiebeveiligingsvragen om risico's te verlagen in verband houden met de toegang van de leverancier tot de bedrijfsinformatie van de organisatie, worden overeengekomen en gedocumenteerd.	Ja	Ja	X								
		Zorgspecifieke beheersmaatregel: Organisaties die gezondheidsinformatie verwerken moeten de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, beoordelen en vervolgens beveiligingsbeheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	Ja	Ja	X								
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten	Alle relevante informatiebeveiligings-eisen 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 behandelt.	Ja	Ja	X			X		X			
A.15.1.3	Toeleveringsketen van informatie- en communicatie-technologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligings-risico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatie-technologie.	Ja	Ja	X								
A.15.2	Beheersing van leveranciersdiensten	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.											
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	Ja	X								
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Ja	Ja	X								
A.16	Beheer van informatiebeveiligingsincidenten												
A.16.1	Rapportage van informatiebeveiligings-gebeurtenissen en verbeteringen	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.											
A.16.1.1	Verantwoordelijkheden en procedures	Directe verantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en volledige respons op informatiebeveiligingsincidenten te bewerkstelligen.	Ja	Ja	X								
A.16.1.2	Rapportage van informatiebeveiligings-gebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Ja	Ja	X								
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen: a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; b) om te garanderen dat er een doeltreffend en geïntegreerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement; c) om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden.	Ja	Ja	X								
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Ja	Ja	X								
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligings-gebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja	Ja	X								
A.16.1.5	Respons op informatiebeveiligings-incidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	X								
A.16.1.6	Lering uit informatiebeveiligings-incidenten	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Ja	Ja	X								
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	X								
A.17	Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer												
A.17.1	Informatiebeveiliging in het proces van bedrijfscontinuïteitsbeheer	Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.											
A.17.1.1	Informatiebeveiligingscontinuïteit-plannen	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Ja	Ja	X								
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Ja	Ja	X								
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligings-continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Ja	Ja	X								
A.17.2	Redundancies	Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.											
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	X			X		X			
A.18	Naleving												
A.18.1	Naleving van wettelijke en contractuele verplichtingen	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingsgegevens.											
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	X		X	X		X			
A.18.1.2	Intellectuele eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigenomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Ja	Ja	X		X	X					
A.18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfsreken worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde wijziging.	Ja	Ja	X		X	X					
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	X		X	X					
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten	Ja	Ja	X		X						
		Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde toestemming van cliënten behoren. 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	X		X						
A.18.1.5	Voorschriften voor het gebruik van cyflografische beheersmaatregelen	Cyflografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja	Ja	X		X						
A.18.2	Herbeoordelingen van informatiebeveiliging	Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.											
A.18.2.1	Onafhankelijk beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	Ja	Ja	X								
A.18.2.2	Naleving van beveiligingsbeleid en -normen	A1>Leidinggevend moeten regelmatig de naleving van de informatieverwerking- en -procedures binnen hun <A1 verantwoordelijkheid beoordeelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	Ja	X		X	X		X			
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	X		X	X		X			