

Verklaring van Toepasselijkheid

IT&Care B.V.

NEN 7510:2017

Document index

Auteur	IT&Care B.V.
Documentnaam	Verklaring van Toepasselijkheid NEN 7510:2017
Documenttype	Verklaring van Toepasselijkheid (VvT)
Distributie	Medewerkers en klanten IT&Care

Inhoudsopgave

1. Inleiding	3
2. Directieverklaring	3
3. Scope.....	4
4. Verklaring van Toepasselijkheid NEN 7510:2017	5

1. Inleiding

De directie van IT&Care is verantwoordelijk voor het vaststellen van het informatiebeveiligingsbeleid. Bij de uitvoering en implementatie wordt de directie ondersteund door de afdeling Kwaliteit, Informatiebeveiliging en Privacy.

Binnen het ondernemingsbeleid is het informatiebeveiligingsbeleid gericht op het bereiken van een zo optimaal mogelijke beveiliging van de informatie die aansluit op de eisen van de klanten en voldoet aan wet- en regelgeving. Het informatiebeveiligingsbeleid voldoet onder andere aan de vereiste, meest recente normen zoals gesteld in ISO27001, NEN 7510 en de Algemene Verordening Gegevensbescherming.

Alle medewerkers worden actief betrokken bij de invulling, implementatie, uitvoering en verbetering van het informatiebeveiligingsbeleid en worden tijdig geïnformeerd over aanpassingen of veranderingen in dit beleid.

Dit document omvat de Verklaring van Toepasselijkheid (VvT) ten behoeve van de certificering voor de NEN 7510-standaard. De Verklaring van Toepasselijkheid bevat een omschrijving van de scope, toepassingsgebied en opsomming van de maatregelen waaraan voldaan moet worden en wordt, tenzij aangegeven dat maatregelen worden uitgesloten.

2. Directieverklaring

Deze Verklaring van toepasselijkheid, die door de directie van IT&Care B.V. is vastgesteld op 04 oktober 2024 en ondertekend door de algemeen directeur, is opgesteld in het kader van de NEN 7510:2017.

De directie verklaart hierbij de in deze VvT vermelde maatregelen bekrachtigd.

Vastgesteld d.d. 04 oktober 2024,
namens de directie IT&Care,

A handwritten signature in black ink, appearing to be 'F. Torcqué'.

F. Torcqué
Algemeen Directeur

3. Scope

Het toepassingsgebied voor informatiebeveiliging omvat de volgende primaire bedrijfsprocessen / dienstverlening binnen IT&Care:

Processen
Portfolio & Change
Platform Engineering
Operations & Infrastructuur
Business Operations
Strategie, Architectuur & Data
Information Security Management

4. Verklaring van Toepasselijkheid NEN 7510:2017

Norm: IT&Care_ NEN7510:2017

Omschrijving NEN 7510:2017

Uitgesloten controls: **A.14.1.1.1, A.14.1.3.1, A.14.2.7 en A18.1.4 (Met betrekking tot zorgspecifieke maatregelen)**

Annex ID	Beheersdoelstellingen en -maatregelen	Toelichting	Van toepassing?	Geïmplementeerd?	WR	CO	BL/RA	Reden van uitsluiting
A.5	Informatie-beveiligingsbeleid							
A.5.1	Aansturing door de directie van de informatie beveiliging							
A.5.1.1	Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	
A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	

A.6	Organiseren van informatiebeveiliging							
A.6.1	Interne organisatie							
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>Organisaties moeten: a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen</i>	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>Er moet minimaal één individu verantwoordelijk zijn voor beveiliging</i>	Ja	Ja			X	

		van gezondheidsinformatie binnen de organisatie.						
	Toevoeging NEN 7510	Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen. (Het is meestal het effectiefst als het forum vergadert op een tijdstip halverwege tussen twee vergaderingen van het bestuursorgaan waaraan het forum rapporteert. Zo kunnen urgente zaken binnen een korte periode in een geschikte vergadering worden besproken.)	Ja	Ja			X	
	Toevoeging NEN 7510	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	
A.6.1.2	Scheiding van taken	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Ja	Ja	X		X	
	Toevoeging NEN 7510	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.	Ja	Ja			X	
	Toevoeging NEN 7510	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.	Ja	Ja			X	
A.6.2	Mobiele apparatuur en telewerken							
A.6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Ja	Ja			X	
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	Ja	Ja			X	

A.7	Veilig Personeel							
A.7.1	Voorafgaand aan het dienstverband							
A.7.1.1	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Ja	X		X	

	Toevoeging NEN 7510	Organisaties moeten minimaal de identiteit, het huidige adres en de vorige werkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie verifiëren.	Ja	Ja	X		X
	Toevoeging NEN 7510	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.)	Ja	Ja	X		X
	Toevoeging NEN 7510	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.	Ja	Ja	X		X
A.7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Ja	Ja			X
	Toevoeging NEN 7510	Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, moeten die betrokkenheid in relevante functieomschrijvingen vastleggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, moeten ook in relevante functieomschrijvingen worden vastgelegd.	Ja	Ja			X
	Toevoeging NEN 7510	Er moet speciale aandacht worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten, stagiairs enz.	Ja	Ja			X
A.7.2	Tijdens het dienstverband						
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	Ja	Ja			X
	Toevoeging NEN 7510	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.	Ja	Ja			X
	Toevoeging NEN 7510	Werknemers van de organisatie en, waar relevant, derde-contractanten behoren te worden gewezen 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 van dienstverband								
A.7.3.1	Beëindiging en 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. (arbeidscontracten / geheimhouding)	Ja	Ja			X	
A.8 Beheer van bedrijfsmiddelen								
A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen								
A.8.1.1	Inventariseren van bedrijfsmiddelen	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>a) Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten: verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen);</i>	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2);</i>	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.</i>	Ja	Ja			X	
8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Ja	Ja			X	
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	
8.1.4	Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	
8,2 Informatie classificatie								
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	
	<i>Toevoeging NEN 7510</i>	<i>Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren dergelijke gegevens op</i>	Ja	Ja			X	

		<i>uniforme wijze als vertrouwelijk te classificeren.</i>						
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	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	
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	
8,3	Behandelen van media							
8.3.1	Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	
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	
	<i>Toevoeging NEN 7510</i>	<i>Alle persoonlijke gezondheidsinformatie behoort veilig te worden gewist of anders behoren de media te worden vernietigd als ze niet meer gebruikt hoeven te worden.</i>	Ja	Ja			X	
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	Toegangsbeveiliging							
9,1	Bedrijfseisen voor toegangsbeveiliging							
9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. (informatieclassificatieschema)	Ja	Ja	X		X	
	<i>Toevoeging NEN 7510</i>	<i>Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheids-informatiesystemen hun toegang tot persoonlijke gezondheids-informatie beperken tot situaties: a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt); b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben;</i>	Ja	Ja	X		X	

		c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen. Organisaties die persoonlijke gezondheids-informatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld.						
	Toevoeging NEN 7510	Het beleid van de organisatie met betrekking tot toegangscontrole moet worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol.	Ja	Ja	X		X	
	Toevoeging NEN 7510	Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, moet professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moet de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking nemen.	Ja	Ja	X		X	
	Toevoeging NEN 7510	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	
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		X	
9,2	Beheer van toegangsrechten van gebruikers							
9.2.1	Registratie en uitschrijving van gebruikers	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	Ja	X		X	
	Toevoeging NEN 7510	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.	Ja	Ja	X		X	
9.2.2	Gebruikers toegang verlenen	Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Ja	Ja	X		X	
9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten (bv Admin rollen / master keys, etc.) moeten worden beperkt en gecontroleerd.	Ja	Ja	X		X	
9.2.4	Beheer van geheime authenticatie informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie (inlog en wachtwoorden) moet worden beheerst via een formeel beheersproces.	Ja	Ja	X		X	

9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Ja	Ja	X		X	
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 wijzigingen moeten ze worden aangepast.	Ja	Ja	X		X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja	X		X	
9.3	Gebruikersverantwoordelijkheden							
9.3.1	Geheime authenticatie 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		X	
9.4	Toegangsbeveiliging van systeem en toepassing							
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		X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja	X		X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja	X		X	
9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Ja	Ja	X		X	
9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen. (wachtwoordbeleid, evt password manager)	Ja	Ja	X		X	
9.4.4	Speciale systeemhulpmiddelen gebruiker	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd. (geen wachtwoorden in browser, wachtwoordbeleid, eventueel password manager)	Ja	Ja			X	
9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	Ja	Ja			X	
A.10	Cryptografie							
10.1	Cryptografische beheersmaatregelen							
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja	X		X	

10.1.2	Sleutelbeheer (cryptografisch)	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		X	
--------	--------------------------------	--	----	----	---	--	---	--

A.11 Fysieke beveiliging en beveiliging van de omgeving								
11.1 Beveiligde gebieden								
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	
	<i>Toevoeging NEN 7510</i>	<i>Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren gebruik te maken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden behoren te worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.</i>	Ja	Ja			X	
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	
11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	Ja			X	
11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	Ja			X	
11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	Ja			X	
11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Ja	Ja			X	
11.2 Apparatuur								
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	
11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja	Ja			X	
11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Ja	Ja			X	
11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	Ja			X	
11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	Ja			X	

	Toevoeging NEN 7510	Organisaties die uitrusting, gegevens of software voor het ondersteunen van een zorgtoepassing met persoonlijke gezondheidsinformatie leveren of gebruiken, mogen niet toestaan dat die uitrusting, gegevens of software van de locatie wordt of worden verwijderd of erbinnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven.	Ja	Ja			X	
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Ja	Ja			X	
	Toevoeging NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit behoort apparatuur te omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d.w.z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.).	Ja	Ja			X	
11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn overschreven	Ja	Ja			X	
	Toevoeging NEN 7510	Organisaties die gezondheidsinformatie verwerken, behoren alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig te wissen of te vernietigen als ze niet meer gebruikt hoeven te worden.	Ja	Ja			X	
11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja			X	
11.2.9	Clear Desk and 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 bedrijfsvoering						
12.1		Bedieningsprocedures en verantwoordelijkheden						
12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja			X	
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	
	Toevoeging NEN 7510	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	Ja	Ja			X	

		en de continuïteit van de cliëntenzorg te garanderen.						
12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Ja	Ja			X	
12.1.4	Scheiding van ontwikkel-, test- en productie omgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	
12,2	Bescherming tegen malware							
12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Ja	Ja	X		X	
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja	X		X	
12,3	Backup							
12.3.1	Back-up van informatie	Regelmatig moeten back-upkopieën van informatie, software en systeemaafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Ja	Ja	X		X	
	<i>Toevoeging NEN 7510</i>	<i>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. Om de vertrouwelijkheid ervan te beschermen behoren er versleutelde back-ups te worden gemaakt van persoonlijke gezondheidsinformatie.</i>	Ja	Ja	X		X	
12,4	Verslaglegging en monitoren							
12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Ja	Ja			X	
12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	Ja			X	

	Toevoeging NEN 7510	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.	Ja	Ja			X	
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	
12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron. (NTP)	Ja	Ja			X	
	Toevoeging NEN 7510	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.	Ja	Ja			X	
12,5	Beheersing van operationele software							
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	
12,6	Beheer van technische kwetsbaarheden							
12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	Ja	Ja	X		X	
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	
12,7	Overwegingen betreffende audits op informatiesystemen							
12.7.1	Beheersmaatregelen betreffende audits op informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Ja	Ja			X	

A.13	Communicatie beveiliging							
13,1	Beheer van netwerkbeveiliging							
13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	X		X	
13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Ja	Ja	X		X	
13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Ja	Ja			X	
13,2	Informatietransport							
13.2.1	Beleid en procedures voor informatie transport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele	Ja	Ja			X	

		beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.						
13.2.2	Overeenkomsten over informatie transport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	Ja			X	
13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn. (bv encryptie)	Ja	Ja			X	
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	
	<i>Toevoeging NEN 7510</i>	<i>Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te beschikken over een vertrouwelijkheids- of geheimhoudingsovereenkomst 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.</i>	Ja	Ja	X		X	

A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen								
14.1 Beveiligingseisen voor informatiesystemen								
14.1.1	Analyse en specificatie van informatiebeveiligingseisen	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	
14.1.1.1	<i>Toevoeging NEN 7510</i>	<i>Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren:</i> <i>a) zeker te stellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem;</i> <i>b) 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.</i>	Nee	Nee				IT&Care is geen zorgverlener en onderkent geen zorgontvangers.
14.1.1.2	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Ja	Ja			X	
14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Ja	Ja			X	
14.1.3	Transacties van toepassingsdiensten beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Ja	Ja			X	
14.1.3.1	<i>Toevoeging NEN 7510</i>	<i>Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) behoort te worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie behoort te worden beschermd om</i>	Nee	Nee				IT&Care maakt geen gebruik van openbaar beschikbare gezondheidsinformatie.

		onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie behoort te worden vermeld en de integriteit ervan behoort te worden beschermd.						
14,2	Beveiliging in ontwikkelings- en ondersteunende processen							
14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Ja	Ja			X	
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	
14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	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.	Ja	Ja			X	
14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Ja	Ja			X	
14.2.5	Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Ja	Ja			X	
14.2.6	Beveiligde ontwikkelomgeving	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Ja	Ja			X	
14.2.7	Uitbestede software ontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Nee	Nee			X	Er wordt geen systeemontwikkeling uitbesteed.
14.2.8	Testen van systeem beveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Ja	Ja			X	
14.2.9	Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	Ja	Ja			X	
	<i>Toevoeging NEN 7510</i>	<i>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 systeemelementen.</i>	Ja	Ja			X	
14,3	Testgegevens							
14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	Ja			X	
A.15	Leveranciersrelaties							
15,1	Informatiebeveiliging in leveranciersrelaties							
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de	Ja	Ja			X	

		leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.						
	Toevoeging NEN 7510	<i>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.</i>	Ja	Ja			X	
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Ja	Ja			X	
15.1.3	Toevoeging van informatie- en communicatietechnologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Ja	Ja			X	
15,2	Beheer van dienstverlening van leveranciers							
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	Ja			X	
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 informatie beveiligingsincidenten							
16,1	Beheer van informatiebeveiligingsincidenten en -verbeteringen							
16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Ja	Ja			X	
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Ja	Ja			X	

	Toevoeging NEN 7510	<p>Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vast te stellen:</p> <p>a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen;</p> <p>b) om te garanderen dat er een doeltreffend en geprioriteerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement;</p> <p>c) om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden.</p> <p>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.</p>	Ja	Ja			X	
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	
16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja	Ja			X	
16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja			X	
16.1.6	Lering uit informatiebeveiligingsincidenten	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	
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 bedrijfscontinuïteit								
17.1 Informatiebeveiligingscontinuïteit								
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	
17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om	Ja	Ja			X	

		het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.							
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Ja	Ja				X	
17,2	Redundante componenten								
17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	X			X	

A.18	Naleving								
18,1	Naleving van wettelijke en contractuele eisen								
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	
18.1.2	Intellectuele eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Ja	Ja				X	
18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfsseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Ja	Ja				X	
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	
	<i>Toevoeging NEN 7510</i>	<i>Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de geïnformeerde toestemming van cliënten te beheren.</i>	Nee	Nee					Geïnformeerde toestemming van cliënten wordt niet beheerd vanuit de rol als verwerker.
	<i>Toevoeging NEN 7510</i>	<i>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.</i>	Nee	Nee					Geïnformeerde toestemming van cliënten wordt niet beheerd vanuit de rol als verwerker.
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja	Ja				X	
18,2	Informatiebeveiligingsbeoordelingen								
18.2.1	Onafhankelijke 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	

18.2.2	Naleving van beveiligingsbeleid en -normen	Leidinggevend en moeten regelmatig de naleving van de informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	Ja			X	
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	

WR: Wet en regelgeving, **CO:** Contractuele Overeenkomst, **BL/RA:** Baseline / Risico analyse