		Toepassingsgebied					Versie: 21-06-2024
	Scope	**Informatiebeveiliging met betrekking tot het verkopen, ontwerpen, ontwikkelen, beheren van en adviseren over software voor keteninformatisering in de zorg, sociaal en justitieel domein**					
5. Verklaring van Toepasselijkheid NEN7510-1:2017+A1:2020							
Hoofdstuk	**Paragraaf Annex A**	**Beheersdoelstellingen**	**beheersmaatregel**	**Van Toepassing?**	**Uitbesteed**	**Rechtvaardiging**	**Implementatie**
	5.1	Informatiebeveiligingsbeleid					
	5.1.1	Beleidsregels voor informatiebeveiliging		JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
Informatiebeveiligings-beleid		NEN 7510	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	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
	5.1.2	Beoordeling van het informatiebeveiligingbeleid		JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
		NEN 7510	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	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc KF.02 Incidentenformulier.docx KF.11 Directiebeoordeling
	6.1	Interne organisatie					
	6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging		JA	N.v.t.	**Normen/richtlijnen CV**	Arbeidscontract, 180918 RVL Rollen Taken en bevoegdheden
		NEN 7510	organisaties moeten a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen	JA	N.v.t.	**Normen/richtlijnen BM**	180918 RVL Rollen Taken en bevoegdheden, 180919 RvL procedure toegangsbeveiliging.docx
			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	N.v.t.	**Normen/richtlijnen BM**	minimaal 1x per maand NEN-ISO / IBMF overleg directielid en security Officer
		NEN 7510	Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie. Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen. 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	N.v.t.	**Normen/richtlijnen BM**	minimaal 1x per maand NEN-ISO / IBMF overleg directielid en security Officer 220901 Functieprofiel security officer
Organiseren van informatie-beveiliging	6.1.2	Scheiding van taken		JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	180918 RVL Rollen Taken en bevoegdheden, 180919 RvL procedure toegangsbeveiliging.docx AVG Database
		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.		N.v.t.	**Normen/richtlijnen**	Onze applicaties hebben hier ondersteuning voor (zie PGAx, recordmanager rol).
	6.1.3	Contact met overheidsinstanties		JA	N.v.t.	**Wet- en regelgeving**	A.01.01 Context van de organisatie
	6.1.4	Contact met speciale belangengroepen		JA	N.v.t.	**Wet- en regelgeving**	KF.06 Overzichtslijst complianceverplichtingen
	6.1.5	Informatiebeveiling in projectbeheer		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	Procedure A04-02 Management of Change KF.07 IB in projectbeheer
		NEN 7510	Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.	JA	N.v.t.	**Normen/richtlijnen**	opgenomen in C.01.02 Ontwerp en Ontwikkeling.docx Vragenlijst in uQuedo stoppen zodat iedereen dat gezien heeft en snapt waarom het is
	6.2	Mobiele apparatuur en telewerken					

	6.2.1	Beleid voor mobiele apparatuur		JA	N.v.t.	**Normen/richtlijnen**	20160912 RVL Arbeids en bedrijfsregels versie 4 en D01.04 Regels aanvaardbaar gebruik
	6.2.2	Telewerken		JA	N.v.t.	**Normen/richtlijnen**	A.03.02 Toegangsbeleid, 180919 RvL procedure toegangsbeveiliging.docx
Veilig Personeel	7.1	Voorafgaand aan het dienstverband					
	7.1.1	Screening		JA	N.v.t.	**RB (Mensen)**	181001 RVL Veilig Personeel RIAAB: Mensen - (On)Opzettelijk foutief handelen (fraude, diefstal)
		NEN 7510	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.	NEE	N.v.t.	**Normen/richtlijnen RB (Mensen)**	Wij valideren op dit moment bij sollicitatie niet de werkkring en adresgegevens van de sollicitant. Bij het aannemen van een medewerker gebeurt dit aan het begin van de eerste werkdag middels het identiteitsbewijs. De werkkring wordt voor kritieke functies gevalideerd door referenties te controleren
		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;	JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	KF.12 Competentiematrix
			b) de functie de kandidaat toevertrouwd kan worden, in het bijzonder als de functie cruciaal is voor de organisatie.	JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	Wij vragen een VOG op voor nieuwe medewerkers als ze een kritieke functie hebben
	7.1.2	Arbeidsvoorwaarden		JA		**Normen/richtlijnen RB (Mensen)**	20160912 RVL Arbeids en bedrijfsregels versie 4 en D01.04 Regels aanvaardbaar gebruik
		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	N.v.t.	**Normen/richtlijnen RB (Mensen)**	Cloud\Ranshuijsen Directie\Management\Personeelszaken\F - Functieprofielen
		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	N.v.t.	**Beleid BM**	Er is beleid t.a.v. IB-beleid dat voor iedereen geldt.
	7.2	Tijdens het dienstverband					
	7.2.1	Directieverantwoordelijkheden		JA	N.v.t.	**Normen/richtlijnen**	180918 RVL Rollen Taken en bevoegdheden
	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging		JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	opgenomen in: 20160912 RVL Arbeids en bedrijfsregels versie 4, D01.04 Regels aanvaardbaar gebruik en https://uquendo-rvl.renvl.nl/
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken.	JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	20160912 RVL Arbeids en bedrijfsregels versie 5, D01.04 Regels aanvaardbaar gebruik en https://uquendo-rvl.renvl.nl/
		NEN 7510	Werknemers van de organisatie en, waar relevant, derde-contractanten moeten worden gewezen op **disciplinaire** processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	20160912 RVL Arbeids en bedrijfsregels versie 4, D01.04 Regels aanvaardbaar gebruik en https://uquendo-rvl.renvl.nl/
	7.2.3	Disciplinaire procedure		JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	181001 RVL Veilig Personeel 20160912 RVL Arbeids en bedrijfsregels versie 4
	7.3.	Beëindiging en wijziging van dienstverband					
	7.3.1	Beëindiging of wijzigingen van verantwoordelijkheden bij wijziging van dienstverband		JA	N.v.t.	**Normen/richtlijnen RB (Mensen)**	Geheimhoudingsverklaring arbeidsovereenkomst en 180910 RvL Checklist Uit dienst medewerker.docx
	8.1	Beheer van bedrijfsmiddelen					

	8.1.1	Inventariseren van bedrijfsmiddelen		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten:				
			a) verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen);	JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc Asset register CRM
			b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2);	JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc Asset register CRM
			c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	Ja	N.v.t.	**Normen/richtlijnen**	D01.04 Regels aanvaardbaar gebruik
	8.1.2	Eigendom van bedrijfsmiddelen		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc
	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen		JA	N.v.t.	**Normen/richtlijnen**	D.01.04 Regels voor aanvaardbaar gebruik.doc
	8.1.4	Teruggeven van bedrijfsmiddelen		JA	N.v.t.	**Normen/richtlijnen**	Arbeidsovereenkomst en D.02.02 Facilitair management.doc en 180910 RvL Checklist Uit dienst medewerker.docx
		NEN 7510	Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.	JA	N.v.t.	**Normen/richtlijnen**	Arbeidsovereenkomst en D.02.02 Facilitair management.doc en 180910 RvL Checklist Uit dienst medewerker.docx
	8.2	Informatieclassificatie					
	8.2.1	Classificatie van informatie		JA	N.v.t.	**Normen/richtlijnen** **RB (Mensen)**	opgenomen in: 180919 RvL Classificatie en beveiligd delen van informatie.docx en AVG Database"
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	JA	N.v.t.	**Normen/richtlijnen** **RB (Mensen)**	180919 RvL Classificatie en beveiligd delen van informatie.docx en AVG Database
Beheer van bedrijfsmiddelen	8.2.2	Informatie labelen		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL Classificatie en beveiligd delen van informatie.docx en AVG Database
		NEN 7510	Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de gebruikers wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen), en moeten papieren output als vertrouwelijk labelen als die output persoonlijke gezondheidsinformatie bevat.	JA	N.v.t.	**Normen/richtlijnen**	180919 RvL Classificatie en beveiligd delen van informatie.docx en AVG Database
	8.2.3	Behandelen van bedrijfsmiddelen		JA	N.v.t.	**Normen/richtlijnen**	D.01.04 Regels voor aanvaardbaar gebruik.doc 20160912 RVL Arbeids en bedrijfsregels versie 4 181017 RvL Beheer van bedrijfsmiddelen.docx
	8.3						
	8.3.1	Beheer van verwijderbare media		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en D.01.04 Regels voor aanvaardbaar gebruik.doc
		NEN 7510	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	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en D.01.04 Regels voor aanvaardbaar gebruik.doc
	8.3.2	Verwijderen van media		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en D.01.04 Regels voor aanvaardbaar gebruik.doc
		NEN 7510	Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc
	8.3.3	Media fysiek overdragen		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en D.01.04 Regels voor aanvaardbaar gebruik.doc
	9.1	Bedrijfseisen voor toegangsbeveiliging					

	9.1.1	Beleid voor toegangsbeveiliging		JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
		NEN 7510	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 zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt);	JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
			b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben;	JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
			c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen.	JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld.	JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
		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	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
		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	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
		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	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
	9.1.2	Toegang tot netwerken en netwerkdiensten		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx
	9.2	Beheer van toegangsrechten van gebruikers					
	9.2.1	Registratie en uitschrijving van gebruikers		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en 180910 Checklist Nieuwe medewerker.docx AVG Database
		NEN 7510	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.	JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en 180910 Checklist Nieuwe medewerker.docx AVG Database
Toegangs-beveiliging		NEN 7510	De gebruikersregistratiegegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx
	9.2.2	Gebruikers toegang verlenen		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en 180910 Checklist Nieuwe medewerker.docx AVG Database
	9.2.3	Beheren van speciale toegangsrechten		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en AVG Database
	9.2.4	Beheer van geheime authenticatieinformatie van gebruikers		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx
	9.2.5	Beoordeling van toegangsrechten van gebruikers		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en AVG Database

	9.2.6	Toegangsrechten intrekken of aanpassen		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en 180910 Checklist Uit dienst medewerker.docx AVG Database
		NEN 7510	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	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en 180910 Checklist Uit dienst medewerker.docx AVG Database
	9.3	Gebruikersverantwoordelijheden					
	9.3.1	Geheime authenticatie-informatie		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en D01.04 Regels voor aanvaardbaar gebruik en 20160912 RVL Arbeids en bedrijfsregels versie 4.docx
	9.4	Toegangsbeveiliging van systeem en toepassingen					
	9.4.1	Beperking toegang tot informatie		JA	N.v.t.	**Normen/richtlijnen RB (Mensen) RB (Software)**	180919 RvL procedure toegangsbeveiliging.docx en AVG Database
		NEN 7510	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	N.v.t.	**Normen/richtlijnen RB (Mensen) RB (Software)**	180919 RvL Classificatie en beveiligd delen van informatie.docx 180806 Wachtwoord beleid RVL.docx
		NEN 7510	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	N.v.t.	**Normen/richtlijnen Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc
	9.4.2	Beveiligde inlogprocedures		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180919 RvL procedure toegangsbeveiliging.docx en 180806 Wachtwoord beleid RVL.docx 180925 RVL Beveiliging bedrijfsvoering.docx
	9.4.3	Systeem voor wachtwoordbeheer		JA	N.v.t.	**Beleid BM**	180806 Wachtwoord beleid RVL.docx
	9.4.4	Speciale systeemhulpmiddelen gebruiken		NEE			
	9.4.5	Toegangsbeveiliging op programmabroncode		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180919 RvL procedure toegangsbeveiliging.docx
	10.1	Cryptografie					
Cryptografie	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen		JA	N.v.t.	**Beleid BM**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx
	10.1.2	Sleutelbeheer		JA	N.v.t.	**Normen/richtlijnen**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx
	11.1	Beveiligde gebieden					
	11.1.1	Fysieke beveiligingszone		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gebruikmaken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden moeten worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx
	11.1.2	Fysieke toegangsbeveiliging		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx
	11.1.3	Kantoren, ruimten en faciliteiten		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx
	11.1.4	Beschermen tegen bedreigingen van buitenaf		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx

	11.1.5	Werken in beveiligde gebieden		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	A.03.02 Informatie Beveiliging Beleid.doc en 180919 RvL procedure toegangsbeveiliging.docx
	11.1.6	Laad- en loslocatie		NEE		**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx
	11.2	Apparatuur					
	11.2.1	Plaatsing en bescherming van apparatuur		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	180919 RvL procedure toegangsbeveiliging.docx en D.01.04 Regels voor aanvaardbaar gebruik.doc
	11.2.2	Nutsvoorziening		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	180919 RvL procedure toegangsbeveiliging.docx
	11.2.3	Beveiling van bekabeling		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	180919 RvL procedure toegangsbeveiliging.docx
	11.2.4	Onderhoud van apparatuur		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	180925 RVL Beveiliging bedrijfsvoering.docx
	11.2.5	Verwijdering van bedrijfsmiddelen		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx
Fysieke beveiliging en beveiliging van de omgeving		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 er binnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven.	JA	N.v.t.	**Normen/richtlijnen**	D.01.04 Regels voor aanvaardbaar gebruik.doc
	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	180919 RvL procedure toegangsbeveiliging.docx en D.01.04 Regels voor aanvaardbaar gebruik.doc
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d.w.z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.)	NVT			
	11.2.7	Veilig verwijderen of hergebruiken van apparatuur		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx
		NEN 7510	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	N.v.t.	**Normen/richtlijnen**	A.03.02 Informatie Beveiliging Beleid.doc
	11.2.8	Onbeheerde gebruikersapparatuur		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx D.01.04 Regels voor aanvaardbaar gebruik en 180919 RvL Clear screen policy.docx
	11.2.9	Clear desk'- en 'clear screen' beleid		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	D.01.04 Regels voor aanvaardbaar gebruik en 180919 RvL Clear screen policy.docx 180919 RvL Clean desk policy.docx
	12.1	Bedieningsprocedures en verantwoordelijkheden					
	12.1.1	Gedocumenteerde bedieningsprocedures		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx en F.01.01 Verbeter- en incidentenmanagement.doc en IB.07 Lijst leveranciers
	12.1.2	Wijzigingsbeheer		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigingsbeheersproces beheersen om de gepaste beheersing van host-toepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen.	JA	N.v.t.	**Beleid BM**	C.01.02 Ontwerp en ontwikkeling 7510 KF.07 IB in projectbeheer
	12.1.3	Capaciteitsbeheer		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx

	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	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	N.v.t.	**Beleid BM RB (Software)**	C.01.02 Ontwerp en ontwikkeling 7510 180925 RVL Beveiliging bedrijfsvoering KF.07 IB in projectbeheer
	12.2	Bescherming tegen malware					
	12.2.1	Beheersmaatregelen tegen malware		JA	N.v.t.	**Normen/richtlijnen RB (Hardware, Netwerk- en Communicatie-voorzieningen)**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie-, detectie- en responsbeheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software, en passende bewustzijnstraining voor gebruikers implementeren.	JA	N.v.t.	**Normen/richtlijnen RB (Hardware, Netwerk- en Communicatie-voorzieningen)**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx uQuendo IBB training + Zorgapplicaties ontwikkelen module
	12.3	Back-up					
Beveiliging bedrijfsvoering	12.3.1	Back-up van informatie		JA	N.v.t.	**Normen/richtlijnen RB (Hardware, Netwerk- en Communicatie-voorzieningen) RB (Omgeving)**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	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	N.v.t.	**Normen/richtlijnen RB (Hardware, Netwerk- en Communicatie-voorzieningen) RB (Omgeving)**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie.	JA	N.v.t.	**Normen/richtlijnen RB (Hardware, Netwerk- en Communicatie-voorzieningen) RB (Omgeving)**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
	12.4	Verslaglegging en monitoring					
	12.4.1	Gebeurtenissen registreren		JA	N.v.t.	**Normen/richtlijnen RB (Software) SIEM nog te implenteren**	180925 RVL Beveiliging bedrijfsvoering.docx
	12.4.2	Beschermen van informatie in logbestanden		JA	N.v.t.	**Normen/richtlijnen RB (Software) SIEM nog te implenteren**	180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	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	N.v.t.	**Normen/richtlijnen RB (Software) SIEM nog te implenteren**	A.12.4.2 Beschermen van informatie in logbestanden
	12.4.3	Logbestanden van beheerders en operators		JA	N.v.t.	**Normen/richtlijnen RB (Software) SIEM nog te implenteren**	180925 RVL Beveiliging bedrijfsvoering.docx
	12.4.4.	Kloksynchronisatie		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdssynchronisatiediensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.	JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	12.5	Beheersing van operationele software					
	12.5.1	Software installeren op operationele systemen		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	12.6	Beheer van technische kwetsbaarheden					
	12.6.1	Beheer van technische kwetsbaarheden		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
	12.6.2	Beperking voor het installeren van software		JA	N.v.t.	**Normen/richtlijnen**	D.02.03 ICT-management.doc en 180925 RVL Beveiliging bedrijfsvoering.docx
	12.7	Beheersmaatregelen betreffende audits van informatiesystemen					
	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	13.1.	Beheer van netwerkbeveiliging					

Communicatie-beveiliging	13.1.1	Beheersmaatregelen voor netwerken		JA	N.v.t.	**Normen/richtlijnen RB (Hardware, Netwerk- en Communicatie-voorzieningen)**	180925 RVL Beveiliging bedrijfsvoering.docx
	13.1.2	Beveiliging van netwerkdiensten		JA	N.v.t.	**Normen/richtlijnen RB (Hardware, Netwerk- en Communicatie-voorzieningen)**	180925 RVL Beveiliging bedrijfsvoering.docx
	13.1.3	Scheiding in netwerken		JA	N.v.t.	**Normen/richtlijnen**	180919 RvL procedure toegangsbeveiliging.docx en 180925 RVL Beveiliging bedrijfsvoering.docx
	13.2.	Informatietransport					
	13.2.1	Beleid en procedures voor informatietransport		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	13.2.2	Overeenkomsten over informatietransport		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	13.2.3	Elektronische berichten		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx en 180919 RvL Classificatie en beveiligd delen van informatie.docx
	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst moet van toepassing zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.	JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx Arbeidsovereenkomst met medewerker, artikel 9.1
Acquisitie, ontwikkeling en onderhoud van informatie-systemen	14.1	Beveiligingseisen voor informatiesystemen					
	14.1.1	Analyse en specificatie van beveiligingseisen		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	A14.1.1.1	NEN 7510: Zorgontvangers op unieke wijze identificeren	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten:				Deze punten worden altijd in het programma van eisen door Opdrachtgever benoemd. Per applicatie geven we hier invulling aan. Soms dmv een BSN en soms ook obv geb datum en achternaam. Onze systemen hebben waar nodig inderdaad een samenvoeg functie voor personen.
			a) zekerstellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem;	JA			
			b) in staat zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval.	JA			
	A14.1.1.2	NEN 7510: Validatie van outputgegevens	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.	JA			
	14.1.2	Toepassingsdiensten op openbare netwerken beveiligen		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.1.3	Transacties van toepassingsdiensten beschermen		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	A.14.1.3.1	NEN 7510: Openbaar beschikbare gezondheidsinformatie	Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd.	NVT			wij hebben deze informatie niet publiek staan
			De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om onbevoegde wijzigingen te voorkomen.	NVT			wij hebben deze informatie niet publiek staan
			De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie moet worden vermeld en de integriteit ervan moet worden beschermd.	NVT			wij hebben deze informatie niet publiek staan
	14.2	Beveiling in ontwikkelings- en ondersteunende processen					
	14.2.1	Beleid voor beveiligd ontwikkelen		JA	N.v.t.	**Normen/richtlijnen**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.2.4	Beperking op wijzigingen aan softwarepakketten		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.2.5	Principes voor engineering van beveiligde systemen		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.2.6	Beveiligde omtwikkelomgeving		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx

	14.2.7	Uitbestede softwareontwikkeling		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.2.8	Testen van systeembeveiliging		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
	14.2.9	Systeemacceptatietests		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
		NEN 7510	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.	JA	N.v.t.	**Normen/richtlijnen RB (Software)**	C.01.02 Ontwerp en ontwikkeling 7510 180925 RVL Beveiliging bedrijfsvoering.docx
	14.3	Overwegingen bij audits van informatiesystemen					
	14.3.1	Bescherming van testgegevens		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	180925 RVL Beveiliging bedrijfsvoering.docx
Leveranciersrelaties	15.1	Informatiebeveiliging in leveranciersrelaties					
	15.1.1	Informatiebeveiliging in leveranciersrelaties		JA	N.v.t.	**Normen/richtlijnen RB (Leveranciers)**	180925 RVL Beveiliging bedrijfsvoering.docx en E.01.03 Leveranciersbeoordeling
		NEN 7510	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	N.v.t.	**Normen/richtlijnen RB (Leveranciers)**	180925 RVL Beveiliging bedrijfsvoering.docx en E.01.03 Leveranciersbeoordeling Leveranciers uit de RIABB benoemd
	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten		JA	N.v.t.	**Normen/richtlijnen RB (Leveranciers)**	180925 RVL Beveiliging bedrijfsvoering.docx en E.01.03 Leveranciersbeoordeling
	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie		JA	N.v.t.	**Normen/richtlijnen RB (Leveranciers)**	180925 RVL Beveiliging bedrijfsvoering.docx en E.01.03 Leveranciersbeoordeling
	15.2	Beheer van dienstverlening van leveranciers					
	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers		JA	N.v.t.	**Normen/richtlijnen RB (Leveranciers)**	180925 RVL Beveiliging bedrijfsvoering.docx en E.01.03 Leveranciersbeoordeling
	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers		JA	N.v.t.	**Normen/richtlijnen RB (Leveranciers)**	180925 RVL Beveiliging bedrijfsvoering.docx en E.01.03 Leveranciersbeoordeling
Beheer van informatie-beveilingsincidenten	16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen					
	16.1.1	Verantwoordelijkheden en procedures		JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen		JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen:	JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
			a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen;	JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
			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;	JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
			c) om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden.	JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging		JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx en D.01.04 Regels voor aanvaardbaar gebruik
	16.1.4	Beoordeling en besluitvorming over informatiebeveiligingsgebeurtenissen		JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx

	16.1.5	Respons op informatiebeveiligingsgebeurtenissen		JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
	16.1.6	Lering uit informatiebeveiligingsincidenten		JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
	16.1.7	Verzamelen van bewijsmateriaal		JA	N.v.t.	**Normen/richtlijnen**	F.01.01 Verbeter- en incidentenmanagement en 180927 RvL Beheer van informatie-beveiligingsincidenten.docx
Informatiebeveiligingsaspecten van bedrijfscontinuïteits-beheer	17.1	Informatiebeveiligingscontinuïteit					
	17.1.1	Informatiebeveiligingscontinuïteit plannen		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	F.01.2 continuïteitsmanagement en IB.08 continuïteitsplan
	17.1.2	Informatiebeveiligingscontinuïteit implementeren		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	F.01.2 continuïteitsmanagement en IB.08 continuïteitsplan
	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren		JA	N.v.t.	**Normen/richtlijnen RB (Omgeving)**	F.01.2 continuïteitsmanagement en IB.08 continuïteitsplan
	17.2	Redundante componenten					
	17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten		JA	N.v.t.	**Normen/richtlijnen RB (Software)**	IB.08 continuïteitsplan
Naleving	18.1	Naleving van wettelijke en contractuele eisen					
	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen		JA	N.v.t.	**Wet- en regelgeving WG/ RB (Mensen)**	KF.06 Overzichtslijst complianceverplichtingen
	18.1.2	Intellectuele eigendomsrechten		JA	N.v.t.	**Wet- en regelgeving**	KF.06 Overzichtslijst complianceverplichtingen
	18.1.3	Bescherming van registraties		JA	N.v.t.	**Normen/richtlijnen**	D.04.02 Beheer van Registraties
	18.1.4	Privacy en bescherming van persoonsgegevens		JA	N.v.t.	**Normen/richtlijnen / Wet- en regelgeving WG/ RB (Mensen)**	KF.06 Overzicht Complianceverplichtingen en AVG Database
		NEN 7510	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde toestemming van cliënten beheren.	NVT			Wij faciliteren dit in de software voor de klant indien nodig
			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.	NVT			Wij faciliteren dit in de software voor de klant indien nodig
	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen		JA	N.v.t.	**Normen/richtlijnen**	KF.06 Overzichtslijst complianceverplichtingen
	18.2	Informatiebeveiligingsbeoordelingen					
	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging		JA	N.v.t.	**Normen/richtlijnen**	E.02.01 Interne audits.doc
	18.2.2	Naleving van beveiligingsbeleid en -normen		JA	N.v.t.	**Normen/richtlijnen**	E.02.01 Interne audits.doc
	18.2.3	Beoordeling van technische naleving		JA	N.v.t.	**Normen/richtlijnen**	E.02.01 Interne audits.doc