mett

Verklaring van Toepasselijkheid

NEN 7510-1; 2017

Versie 2.0, datum 15-09-2022

Review: 23-09-2024

Activatie Verklaring van Toepasselijkheid

Voor u ligt de definitieve Verklaring van Toepasselijkheid (VVT) van Mett B.V. waarin de borging is beschreven van het informatieveiligheidsbeleid conform NEN 7510-1; 2017. De VVT beschrijft het normenkader waar de organisatie zich aan committeert en beschrijft eventuele redenen van uitsluiting.

Scope

De VVT strekt zich uit over de volgende onderneming: Mett B.V. Deze VVT is bestemd voor alle werknemers van Mett en haar stakeholders. Het gehanteerde Information Security Management System (ISMS) is van toepassing op de bedrijfsprocessen.

Verantwoordelijkheden

De reikwijdte van de VVT is vastgesteld in samenspraak met het directieteam. Met het ondertekenen is het de verantwoordelijkheid van de directie om de maatregelen te treffen die noodzakelijkerwijs volgen uit het ISMS. Toetsing van het NEN 7510 vindt plaats door geaccrediteerde certificatie instelling. Om het ISMS doeltreffend en efficiënt te houden treft de organisatie jaarlijks de nodige maatregelen en acties met de benodigde resources.

Ondertekend namens het directieteam van Mett B.V.		
Naam	Jeroen Rispens	*Handtekening*
Functie	Directeur Mett	
Plaats	Utrecht	
Datum	18-09-2023	

MET DE ONDERTEKENING ACTIVEERT EN BORGT METT B.V. HET NORMENKADER ALS VOLGT:

Normeisen niet van toepassing.

De volgende normeisen zijn niet van toepassing voor de organisatie Mett B.V.

Control	Maatregel	Reden uitsluiting
14.1.1.1 Zorgontvangers op unieke wijze identificeren	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 noodgeval.	Mett B.V. is geen zorgverlener. De analyse van het Mett-platform toont aan dat haar zorgklanten het platform niet voor medische dossiervoering inzetten. De eisen voor persoonsidentificatie zijn dan ook niet van toepassing.
14.1.1.2 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.	Mett B.V. is geen zorgverlener. De analyse van het Mett-platform toont aan dat haar zorgklanten het platform niet voor medische dossiervoering inzetten. De eisen voor persoonsidentificatie zijn dan ook niet van toepassing.
14.1.3.1 Openbaar beschikbare gezondheidsinformatie.	Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie behoort te worden vermeld en de integriteit ervan behoort te worden beschermd.	Mett B.V. is geen zorgverlener. De analyse van het Mett-platform toont aan dat haar zorgklanten het platform niet voor medische dossiervoering inzetten. De eisen voor persoonsidentificatie zijn dan ook niet van toepassing.

Normeisen van toepassing

De organisatie en omgeving zijn in kaart gebracht middels een context,- stakeholder- en risicoanalyse. Op basis van deze analyses is vastgesteld dat de normeisen in onderstaande tabel van toepassing zijn voor Mett. De tabel beschrijft naast de maatregelen ook de context die op de eis van toepassing is binnen Mett:

- Wet & regelgeving (W&R)
- Klant
- Operationeel
- Risico
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Beleid
- Monitor
- Uitbesteed

Als het gaat om eisen voor gezondheidsinformatiesystemen beschrijft Mett in de 'toelichting' of het Mett-platform dit ondersteunt.

5 Informatiebeveiligingsbeleid

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
05.1 Aansturing door de directie van de informatiebeveiliging													
05.1.1 Beleidsregels voor informatiebeveiliging	X				X	X	X	X		JA	NEE	Organisatie beschikt over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen. Zorgspecifieke beheersmaatregel Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid	Mett is verwerker echter heeft zij geen controle op het toevoegen van (bijzondere)persoonlijke gegevens door gebruikers. Dit is de verantwoordelijkheid van de klant/gebruiker.

												dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	
05.1.2 Beoordelen van het informatiebeveiligings-beleid				X		X	X		X	JA	NEE	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. 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.	

6. Organiseren van informatiebeveiliging

Paragraaf	W&R	KLANT	OPER	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
06.1 Interne organisatie													
06.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	X		X	X		X	X			JA	NEE	Organisatie moet: a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen 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. Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van	

												gezondheidsinformatie binnen de organisatie. Het gezondheidsinformatie-beveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen. (Het is meestal het effectiefst als het forum vergadert opeen tijdstip halverwege tussen twee vergaderingen vanhet bestuursorgaan waaraan het forum rapporteert. Zo kunnen urgente zaken binnen een korte periode in een geschikte vergadering worden besproken.). 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. 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.	
06.1.2 Scheiding van taken	X		X	X	X	X	X	X		JA	NEE	Organisatie stelt, indien dit haalbaar is, plichten en verantwoordelijkheids-gebieden scheiden teneinde de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie. 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.	
06.1.3 Contact met overheidsinstanties		X			X					JA	NEE	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	
06.1.4 Contact met speciale belangengroepen	X	X				X	X			JA	NEE	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	

06.1.5 Informatiebeveiliging in projectbeheer		X	X		X					JA	NEE	Bij het managen van projecten behoort de patiëntveiligheid als projectrisico in aanmerking te worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie. 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.	
06.2 Mobiele apparaten en telewerken													
06.2.1 Beleid voor mobiele apparatuur	X	X	X	X		X	X	X		JA	NEE	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	
06.2.2 Telewerken		X	X			X	X	X		JA	NEE	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	

Verklaring van Toepasselijkheid

NEN 7510-1; 2017

Publiek

7. Veilig personeel

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
07.1 Voorafgaand aan het dienstverband													
07.1.1 Screening	X					X	X			JA	NEE	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. 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.) 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. 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.	
07.1.2 Arbeidsvoorwaarden	X					X	X			JA	NEE	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. 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. 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.	
07.2 Tijdens het dienstverband													

07.2.1 Directieverantwoordelijkheden				X		X	X			JA	NEE	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	
07.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	X		X	X		X	X	X		JA	NEE	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. Werknemers van de organisatie en, waar relevant, derde-contractanten behoren te worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	

											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.	
07.2.3 Disciplinaire procedure	X		X			X	X	X		JA	NEE	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	
07.3 Beëindiging en wijziging van dienstverband													
07.3.1 Beëindiging of wijziging van verantwoordelijheden van het dienstverband	X		X			X	X			JA	NEE	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.	

8. Beheer van bedrijfsmiddelen

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
08.1 Verantwoordelijkheid voor bedrijfsmiddelen													
08.1.1. Inventariseren van bedrijfsmiddelen			X	X	X	X	X		X	JA	NEE	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. 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.	
08.1.2 Eigendom van bedrijfsmiddelen			X	X	X					JA	NEE	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	
08.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen			X		X			X	X	JA	NEE	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd. 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.	
08.1.4 Teruggeven van bedrijfsmiddelen			X		X			X	X	JA	NEE	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. 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.	
08.2 Informatieclassificatie												
08.2.1 Classificatie van informatie	X	X	X	X		X	X	X		JA	NEE	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren. 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.	
08.2.2. Informatie labelen						X	X	X		JA	NEE	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. 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.	Mett is geen zorgverlener. Het Mett-platform faciliteert de NEN 7510 eisen.
08.2.3. Behandelen van bedrijfsmiddelen	X	X	X	X		X	X			JA	NEE	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	

08.3 Behandelen van media												
08.3.1. Beheer van verwijderbare media	X	X	X	X	X	X	X	X		JA	NEE	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. 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.	
08.3.2 Verwijderen van media	X	X	X	X		X	X	X		JA	NEE	Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden. 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.	
08.3.3. Media fysiek overdragen		X	X	X			X	X		JA	NEE	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	

9. Toegangsbeveiliging

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geimplenteerd	Uitbesteed	NEN 7510 maatregel	Toelichting
09.1 Bedrijfseisen voor toegangsbeveiliging													
09.1.1 Beleid voor toegangsbeveiliging	X	X	X	X	X		X	X		JA	NEE	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); 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.	

												Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. 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 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. 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. 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.	

09.1.2 Toegang tot netwerken en netwerkdiensten		X	X	X		X		X			NEE	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	
09.2 Beheer van toegangsrechten van gebruikers													
09.2.1 Registratie en uitschrijving van gebruikers	X	X	X	X	X	X				JA	NEE	De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratie proces. 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 gebruikersregistratie-gegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is. 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.	
09.2.2 Gebruikers toegang verlenen	X	X	X	X	X	X		X		JA	NEE	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.	
09.2.3 Beheren van speciale toegangsrechten				X		X		X		JA	NEE	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	
09.2.4 Beheer van geheime authenticatie-informatie van gebruikers		X		X		X	X	X		JA	NEE	Beheer van geheime authenticatie- informatie van gebruikers	
09.2.5 Beoordeling van toegangsrechten van gebruikers		X	X	X		X		X		JA	NEE	Beoordeling van toegangsrechten van gebruikers	
09.2.6 Toegangsrechten intrekken of aanpassen		X	X	X		X				JA	NEE	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.	

09.3 Gebruikersverant-woordelijkheden													
09.3.1 Geheime authenticatie-informatie gebruiken	X	X	X	X		X		X		JA	NEE	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	
09.4 Toegangsbeveiliging van systeem en toepassing													
09.4.1 Beperking toegang tot informatie		X	X	X		X		X		JA	NEE	Gezondheidsinformatiesystemen die persoonlijkegezondheids-informatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie moet geïsoleerd (en gescheiden) worden van de toegang tot informatieverwerkings-infrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie. Zorgspecifieke beheersmaatregel Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt	Mett is geen zorgverlener. Het Mett-platform faciliteert de NEN 7510 eisen.

												gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	
09.4.2 Beveiligde inlogprocedures		X	X			X	X	X		JA	NEE	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	
09.4.3. Systeem voor wachtwoordbeheer		X	X	X		X		X		JA	NEE	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	
09.4.4 Speciale systeemhulpmiddelen gebruiken			X	X	X	X	X	X		JA	NEE	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	
09.4.5. Toegangsbeveiliging op programmabroncode				X		X	X	X		JA	NEE	Toegang tot de programmabroncode moet worden beperkt.	

10. Cryptografie

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
10.1 Cryptografische beheersmaatregelen													
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen						X	X	X		JA	NEE	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	
10.1.2 Sleutelbeheer						X	X	X		JA	NEE	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	

11. Fysieke beveiliging en beveiliging van de omgeving

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
11.1 Beveiligde gebieden													
11.1.1 Fysieke beveiligingszone			X	X	X		X	X		JA	JA	Organisaties die persoonlijke gezondheidsinformatieverwerken, 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. 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.	
11.1.2 Fysieke toegangsbeveiliging		X	X		X		X	X		JA	JA	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	
11.1.3 Kantoren, ruimten en faciliteiten beveiligen		X	X	X	X		X	X		JA	NEE	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	
11.1.4 Beschermen tegen bedreigingen van buitenaf			X		X		X	X		JA	JA	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	
11.1.5 Werken in beveiligde gebieden			X		X		X	X		JA	JA	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	
11.1.6 Laad- en loslocatie			X	X	X			X		JA	NEE	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.	
11.2 Apparatuur													
11.2.1 Plaatsing en bescherming van apparatuur	X	X	X	X	X			X		JA	JA	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en	

											gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	
11.2.2 Nutsvoorzieningen			X		X		X			JA	JA	Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	
11.2.3 Beveiliging van bekabeling			X	X	X		X			JA	JA	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	
11.2.4 Onderhoud van apparatuur			X		X				X	JA	JA	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	
11.2.5 Verwijdering van bedrijfsmiddelen		X	X		X	X		X		JA	JA	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. 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.	
11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein		X	X	X	X		X	X		JA	NEE	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.). 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.	
11.2.7 Veilig verwijderen of			X				X	X		JA	JA	Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor	

hergebruiken van apparatuur											gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden. 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.	
11.2.8 Onbeheerde gebruikersapparatuur		X	X	X		X	X	X		JA	NEE	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	
11.2.9 'Clear desk'- en 'clear screen'-beleid		X	X	X		X	X	X		JA	NEE	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	

12. Beveiliging bedrijfsvoering

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
12.1 Bedieningsprocedures en verantwoordelijkheden													
12.1.1 Gedocumenteerde bedieningsprocedures		X	X		X					JA	JA	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	
12.1.2 wijzigingsbeheer			X		X					JA	JA	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. 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.	
12.1.3 Capaciteitsbeheer			X	X	X				X	JA	JA	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	
12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen			X	X	X		X	X		JA	JA	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren ontwikkel- en testomgevingen voor gezondheidsinformatie-systemen 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. 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.	
12.2 Bescherming tegen malware													
12.2.1 Beheersmaatregelen tegen malware			X			X	X	X		JA	JA	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. 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.	
12.3 Backup													
12.3.1 Back-up van informatie		X	X		X			X		JA	JA	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. Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie. 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.	
12.4 Verslaglegging en monitoren													
12.4.1 Gebeurtenissen registreren		X	X						X	JA	NEE	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	
12.4.2 Beschermen van informatie in logbestanden		X	X						X	JA	NEE	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.	

												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.	
12.4.3 Logbestanden van beheerders en operators		X	X						X	JA	NEE	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	
12.4.4 Kloksynchronisatie								X		JA	NEE	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. 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.	

12.5 Beheersing van operationele software													
12.5.1 Software installeren op operationele systemen			X		X	X	X			JA	NEE	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	
12.6 Beheer van technische kwetsbaarheden													
12.6.1 Beheer van technische kwetsbaarheden			X	X	X	X	X			JA	NEE	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.	
12.6.2 Beperkingen voor het installeren van software			X			X	X	X		JA	NEE	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	

12.7 Overwegingen betreffende audits van informatiesystemen													
12.7.1 Beheersmaatregelen betreffende audits		X	X		X					JA	NEE	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	

van informatiesystemen												

13. Communicatiebeveiliging

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
13.1 Beheer van netwerkbeveiliging													
13.1.1 Beheersmaatregelen voor netwerken		X	X	X	X	X	X			JA	NEE	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	
13.1.2 Beveiliging van netwerkdiensten		X	X	X	X	X	X			JA	NEE	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.	
13.1.3 Scheiding in netwerken		X	X	X	X	X	X	X		JA	NEE	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	
13.2 Informatietransport													

13.2.1 Beleid en procedures voor informatietransport		X	X			X	X	X		JA	NEE	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	
13.2.2 Overeenkomsten over informatietransport		X	X			X	X			JA	NEE	Overeenkomsten over informatietransport	
13.2.3 Elektronische berichten		X	X	X		X	X	X		JA	NEE	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	
13.2.4 Vertrouwelijkheids- of geheimhoudings overeenkomst	X	X	X	X	X	X	X	X		JA	NEE	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. 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.	

Verklaring van Toepasselijkheid

NEN 7510-1; 2017

Publiek

14. Acquisitie, ontwikkeling en onderhoud van informatiesytemen

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geimplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
14.1 Beveiligingseisen voor informatiesystemen													
14.1.1 Analyse en specificatie van informatiebeveiligingseisen		X	X			X	X	X		JA	NEE	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. 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.	

14.1.2 Toepassingsdiensten op openbare netwerken beveiligen			X	X		X	X	X		JA	NEE	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.	
14.1.3 Transacties van toepassingsdiensten beschermen			X	X		X	X	X		JA	NEE	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	
14.2 Beveiliging in ontwikkelings- en ondersteunende processen													
14.2.1 Beleid voor beveiligd ontwikkelen	X	X	X	X	X	X	X	X		JA	NEE	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	
14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen		X	X	X	X	X	X			JA	NEE	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	

14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform			X	X		X	X			JA	NEE	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.	
14.2.4 Beperkingen op wijzigingen aan softwarepakketten			X	X		X	X	X		JA	NEE	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	
14.2.5 Principes voor engineering van beveiligde systemen			X	X		X	X	X		JA	NEE	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	
14.2.6 Beveiligde ontwikkelomgeving			X			X	X	X		JA	NEE	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.	
14.2.7 Uitbestede softwareontwikkeling			X	X		X	X	X	X	JA	NEE	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	

14.2.8 Testen van systeembeveiliging			X	X	X		X	X		JA	NEE	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	
14.2.9 Systeemacceptatietests			X	X	X		X	X		JA	NEE	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 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.	
14.3 Testdata													
14.3.1 Bescherming van testgegevens	X	X		X		X				JA		Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	

15. Leveranciersrelaties

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geimplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
15.1 Informatiebeveiliging in leveranciersrelaties													
15.1.1 Informatiebeveiligings-beleid voor leveranciersrelaties	X		X	X		X	X	X		JA	NEE	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. 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.	
15.1.2 Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten			X	X		X	X			JA	NEE	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.	
15.1.3 Toeleveringsketen van informatie- en communicatietechnologie			X	X		X	X	X		JA	NEE	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	
15.2 Beheer van dienstverlening van leveranciers													
15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers			X		X		X		X	JA	NEE	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	
15.2.2 Beheer van veranderingen in dienstverlening van leveranciers			X		X		X		X	JA	NEE	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.	

16. Beheer van informatiebeveiligingsincidenten

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen													
16.1.1 Verantwoordelijkheden en procedures			X			X				JA	NEE	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 geprioriteerd 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.	

16.1.2 Rapportage van informatiebeveiligings gebeurtenissen			X			X				JA	NEE	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vast te stellen: a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; 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; c) om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden. Informatiebeveiligingsincidenten omvatten corruptie of onbedoelde openbaarmaking van persoonlijke	

												gezondheidsinformatie of het niet langer beschikbaar zijn van gezondheidsinformatiesystemen waarbij dit niet beschikbaar zijn nadelige gevolgen heeft voor de zorg voor cliënten of bijdraagt aan nadelige klinische gebeurtenissen. Organisaties behoren de cliënt altijd te informeren als er per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt. Organisaties behoren de cliënt op de hoogte te stellen als het niet beschikbaar zijn van gezondheidsinformatiesystemen negatieve gehad kan hebben voor hun zorgverlening. 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.	
16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging			X			X	X	X	X	JA	NEE	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.	
16.1.4 Beoordeling van en besluitvorming over informatiebeveiligings gebeurtenissen			X			X	X			JA	NEE	Informatiebeveiliging-gebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligings incidenten.	
16.1.5 Respons op informatiebeveiligings incidenten		X	X	X	X	X				JA	NEE	Op informatiebeveiligings-incidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	
16.1.6 Lering uit informatiebeveiligings incidenten			X	X	X	X	X		X	JA	NEE	Kennis die is verkregen door informatiebeveiliging-incidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	
16.1.7 Verzamelen van bewijsmateriaal		X	X							JA	NEE	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	

17. Informatiebeveiligingsaspecten van bedrijfs continuïteitsbeheer

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
17.1 Informatiebeveiligingscontinuïteit													
17.1.1 Informatiebeveiligings continuïteit plannen			X	X	X					JA	NEE	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	
17.1.2 Informatiebeveiliging-continuïteit implementeren		X	X	X	X	X	X			JA	NEE	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.	
17.1.3 Informatiebeveiliging-continuïteit verifiëren,			X		X				X	JA	NEE	De organisatie moet de ten behoeve van informatiebeveiligings continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren	

beoordelen en evalueren												om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	
17.2 Redundante componenten													
17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten			X		X					JA	JA	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	

18. Naleving

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	Geïmplementeerd	Uitbesteed	NEN 7510 maatregel	Toelichting
18.1 Compliance met juridische standaarden													
18.1.1 Identificatie van toepasbare wet- en regelgeving	X	X	X	X		X	X			JA	NEE	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.	

18.1.2 Intellectueel eigendom rechten	X	X	X	X		X				JA	NEE	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.	
18.1.3 Bescherming van records	X	X		X		X	X			JA	NEE	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	
18.1.4 Privacy en bescherming van persoonlijke data	X	X		X		X	X			JA	NEE	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde toestemming van cliënten beheren. 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. 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.	

18.1.5 Beheersmaatregel van cryptografische controls		X	X			X	X	X		JA	NEE	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	
18.2 Informatie veiligheid reviews													
18.2.1 onafhankelijke review van inform veiligheid						X	X	X		JA	NEE	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.	
18.2.2 Compliance met beleid en standaarden						X	X	X		JA	NEE	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	
18.2.3 Technische compliance review						X	X		X	JA	NEE	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en	

												normen van de organisatie voor informatiebeveiliging.	