

Verklaring van toepasselijkheid NEN7510:2017+A1:2020 v4.0

Techni Team 6 oktober 2023



			Van toepassing?	Geïmplementeerd?	Uitbesteed?	Wet	Contract	Risico analyse	Niet van toepassing want:
A.5.1.1	Zorgspecifieke beheersmaatregel:	Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan <u>alle werknemers en relevante externe partijen</u>	Ja	Ja			x		
A.5.1.2	Zorgspecifieke beheersmaatregel:	Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan	Ja	Ja			X		
A.6.1.1	Zorgspecifieke beheersmaatregel:	Organisaties moeten: a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen	Ja	Ja			x		
A.6.1.1	Zorgspecifieke beheersmaatregel:	Organisaties moeten: b) over een informatiebeveiligingsmanagementforum (IBMF) beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in B3 en B4 van bijlage B (6.1.1) in NEN 7510-2.	Ja	Ja			x		
A.6.1.1	Zorgspecifieke beheersmaatregel:	Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie.	Ja	Ja			x		
A.6.1.1	Zorgspecifieke beheersmaatregel:	Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen. (Het is meestal het effectiefst als het forum vergadert op een tijdstip halverwege tussen twee vergaderingen van het bestuursorgaan waaraan het forum rapporteert. Zo kunnen urgente zaken binnen een korte periode in een geschikte vergadering worden besproken.)	Ja	Ja			x		
A.6.1.1	Zorgspecifieke beheersmaatregel:	Er moet een formele verklaring van het toepassingsgebied worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen.	Ja	Ja			x		
A.6.1.2	Zorgspecifieke beheersmaatregel:	Organisaties moeten, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden scheiden teneinde de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke <u>gezondheidsinformatie</u> .	Ja	Ja		x	x		
A.6.1.5	Zorgspecifieke beheersmaatregel:	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 <u>gezondheidsinformatie</u> .	Ja	Ja		X	X		
A.7.1.1	Zorgspecifieke beheersmaatregel:	Organisaties moeten minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie verifiëren.	Ja	Ja		x			
A.7.1.1	Zorgspecifieke beheersmaatregel:	Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband moeten een verificatie omvatten van de toepasselijke kwalificaties voor zorgverleners, indien er sprake is van accreditatie voor de beroepsgroep op basis van die kwalificaties (bijv. artsen, verplegend personeel enz.)	Nee	Nee					Techni Team heeft geen zorgverleners in dienst.
A.7.1.1	Zorgspecifieke beheersmaatregel:	Als een persoon wordt ingehuurd voor een specifieke beveiligingsfunctie, moet de organisatie zich ervan vergewissen dat: a) de kandidaat over de nodige competentie beschikt om de beveiligingsfunctie te vervullen; b) de functie de kandidaat toevertrouwd kan worden, in het bijzonder als de functie cruciaal is voor de organisatie.	Nee	Nee					Techni Team heeft geen personeel met een specifiek beveiligingsfunctie in dienst, dan wel huurt niet dergelijke personen in

Verklaring van toepasselijkheid NEN7510:2017+A1:2020 v4.0

Techni Team 6 oktober 2023



			Van toepassing?	Geïmplementeerd?	Uitbesteed?	Wet	Contract	Risico analyse	Niet van toepassing want:
A.7.1.2	Zorgspecifieke beheersmaatregel:	Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, moeten die betrokkenheid in relevante functieomschrijvingen vastleggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, moeten ook in relevante functieomschrijvingen worden vastgelegd.	Ja	Ja			x		
A.7.1.2	Zorgspecifieke beheersmaatregel:	Er moet speciale aandacht worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten, stagiairs enz.	Ja	Ja			x		
A.7.2.2	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken.	Ja	Ja		x	X		
A.7.2.2	Zorgspecifieke beheersmaatregel:	Werknemers van de organisatie en, waar relevant, derdecontractanten moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	Ja	Ja		x	x		
A.8.1.1	Zorgspecifieke beheersmaatregel:	a) Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten:verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke <u>bedrijfsmiddelen</u>);	Ja	Ja			x		
A.8.1.1	Zorgspecifieke beheersmaatregel:	b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2);	Ja	Ja			X		
A.8.1.1	Zorgspecifieke beheersmaatregel:	c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	Ja	Ja			X		
A.8.1.4	Zorgspecifieke beheersmaatregel:	Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.	Ja	Ja			X		
A.8.2.1	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	Ja	Ja			x		
A.8.2.2	Zorgspecifieke beheersmaatregel:	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	Ja			X		
A.8.3.1	Zorgspecifieke beheersmaatregel:	Media die persoonlijke gezondheidsinformatie bevatten moeten fysiek worden beschermd of de gegevens ervan moeten versleuteld worden. De status en locatie van media die niet-versleutelde <u>persoonlijke gezondheidsinformatie bevatten, moeten gemonitord worden.</u>	Ja	Ja			x		
A.8.3.2	Zorgspecifieke beheersmaatregel:	Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anderszins moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Ja	x	x		

Verklaring van toepasselijkheid NEN7510:2017+A1:2020 v4.0

Techni Team 6 oktober 2023



			Van toepassing?	Geïmplementeerd?	Uitbesteed?	Wet	Contract	Risico analyse	Niet van toepassing want:
A.9.1.1	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheids-informatiesystemen hun toegang tot persoonlijke gezondheids-informatie beperken tot situaties: a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt); b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben; c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen. Organisaties die persoonlijke gezondheids-informatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld.	Nee	Nee				X	Techni Team heeft geen directe relatie tot patienten.
A.9.1.1	Zorgspecifieke beheersmaatregel:	Het beleid van de organisatie met betrekking tot toegangscontrole moet worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol.	Ja	Ja				x	
A.9.1.1	Zorgspecifieke beheersmaatregel:	Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, moet professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moet de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking nemen.	Ja	Ja				x	
A.9.1.1	Zorgspecifieke beheersmaatregel:	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.	Nee	Nee					Techni Team wisselt geen cliëntgegevens uit.
A.9.2.1	Zorgspecifieke beheersmaatregel:	De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers moeten garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	Ja	Ja				x	
A.9.2.6	Zorgspecifieke beheersmaatregel:	Alle organisaties die persoonlijke gezondheidsinformatie verwerken moeten voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie beëindigen.	Ja	Ja			x		
A.9.4.1	Zorgspecifieke beheersmaatregel:	Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden.	Ja	Ja				X	
A.9.4.1	Zorgspecifieke beheersmaatregel:	De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie moet geïsoleerd (en gescheiden) worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja				X	

Verklaring van toepasselijkheid NEN7510:2017+A1:2020 v4.0

Techni Team 6 oktober 2023



			Van toepassing?	Geïmplementeerd?	Uitbesteed?	Wet	Contract	Risico analyse	Niet van toepassing want:
A.11.1.1	Zorgspecifieke beheersmaatregel:	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	Ja			x	x	
A.11.2.5	Zorgspecifieke beheersmaatregel:	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	Ja				X	
A.11.2.6	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d.w.z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.)	Nee	Nee					Techni Team gebruikt geen medische apparatuur in haar werkzaamheden als verwerker.
A.11.2.7	Zorgspecifieke beheersmaatregel:	Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden.	Ja	Ja			x	x	
A.12.1.2	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigings-beheersproces beheersen om de gepaste beheersing van host-toepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen	Ja	Ja				X	
A.12.1.4	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel) scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er moeten regels voor het migreren van software van de ontwikkel- naar een operationele status worden gedefinieerd en gedocumenteerd door de organisatie die de betroffen toepassing(en) host.	Nee	Nee					Techni Team ontwikkelt zelf geen software
A.12.2.1	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie-, detectie- en respons-beheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software, en passende bewustzijnsstraining voor gebruikers implementeren.	Ja	Ja			x	x	
A.12.3.1	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving opslaan om te garanderen dat de informatie in de toekomst beschikbaar is. Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie.	Ja	Ja				X	
A.12.4.2	Zorgspecifieke beheersmaatregel:	Auditverslagen moeten beveiligd zijn en niet gemanipuleerd kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten moet worden beveiligd om misbruik of compromittering te voorkomen.	Ja	Ja			x	x	

Verklaring van toepasselijkheid NEN7510:2017+A1:2020 v4.0

Techni Team 6 oktober 2023



Van toepassing?
Geïmplementeerd?
Uitbesteed?
Wet
Contract
Risico analyse
Niet van toepassing want:

A.12.4.4	Zorgspecifieke beheersmaatregel:	Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdssynchronisatie-diensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.	Ja	Ja					
A.13.2.4	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst moet van toepassing zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.	Ja	Ja				X	
A.14.1.1.1	Zorgontvangers op unieke wijze identificeren, Zorgspecifieke beheersmaatregel:	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten: a) zekerstellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem; b) in staat zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval.	nee	nee					Techni Team is niet verantwoordelijk voor de inhoudelijke werking van de zorgspecifieke software (m.b.t. identificatie van de cliënt).
A.14.1.1.2	Validatie van outputgegevens, Zorgspecifieke beheersmaatregel:	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.	nee	nee					Techni Team is niet verantwoordelijk voor de inhoudelijke werking van de zorgspecifieke software (m.b.t. identificatie van de cliënt)
A.14.1.3.1	Openbaar beschikbare gezondheidsinformatie, Zorgspecifieke beheersmaatregel:	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 moet worden vermeld en de integriteit ervan moet worden beschermd.	Nee	Nee					Techni Team verwerkt geen openbare gezondheidsinformatie onder eigen verantwoordelijkheid
A.14.2.9	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten acceptatiecriteria vaststellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie moeten ze geschikte testen van het systeem uitvoeren. Klinische gebruikers moeten worden betrokken bij het testen van klinisch relevante systeemelementen.	ja	ja				X	
A.15.1.1	Zorgspecifieke beheersmaatregel:	Organisaties die gezondheidsinformatie verwerken moeten de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, beoordelen en vervolgens beveiligingsbeheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	Ja	Ja			x	x	
A.16.1.2	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen: a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; b) om te garanderen dat er een doeltreffend en 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.	Ja	Ja				X	

Verklaring van toepasselijkheid NEN7510:2017+A1:2020 v4.0

Techni Team 6 oktober 2023



Van toepassing?
Geïmplementeerd?
Uitbesteed?
Wet
Contract
Risico analyse
Niet van toepassing want:

A.18.1.4	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde toestemming van cliënten beheren.	Nee	Nee					Techni Team beheert de geïnformeerde toestemming van cliënten niet.
A.18.1.4	Zorgspecifieke beheersmaatregel:	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.	Nee	Nee					Techni Team beheert de geïnformeerde toestemming van cliënten niet.